VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

DETEKCE VOLUMETRICKÝCH ÚTOKŮ DOS A DDOS V REÁLNÍM ČASE NA L3 SÍŤOVÉ VRSTVĚ

DETECTION OF VOLUMETRIC DOS AND DDOS ATTACKS IN REAL TIME ON THE L3 NETWORK LAYER

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **ANTON ŠKÁPIK**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. MARTIN HOLKOVIČ**
SUPERVISOR

BRNO 2018

Abstrakt

Táto bakalárska práca skúma a implementuje možnosti detekcie DoS a DDoS útokov v reálnom čase. S využitím nástroja na prúdové spracovanie NetFlow záznamov, poskytuje výsledný produkt možnosti detegovať útoky a vytvoriť pravidlá pre zmiernenie útoku v časovom rozmedzí pár sekúnd. Pravidla sú prevedené z formy NetFlow záznamu na formát flowspec, ktorý je distribuovaný pomocou BGP protokolu medzi smerovačmi v monitorovanej sieti. Program bol implementovaný a testovaný vo virtuálnom laboratóriu. Práca je písaná v spolupráci s firmou Flowmon Networks a.s. s využitím proprietárnych aplikácii na spracovanie NetFlow záznamov.

Abstract

This bachelor thesis explores and implements capabilities of real-time DoS and DDoS detection. Leveraging NetFlow stream processing tool, the resulting product provides the ability to detect attacks within a few seconds and create rules to mitigate the attack. The rules are converted from an form of records into a flowspec filter that is distributed by BGP between the routers in the monitored network. The program was implemented and tested. The work is written in collaboration with Flowmon Networks a.s., using their proprietary applications for NetFlow record processing.

Kľúčové slová

DoS, DDoS, počítačová sieť, BGP, ExaBGP, Flowspec, NetFlow, IPFIX, Flowmon, RRDtool, Flow, xfcapd

Keywords

DoS, DDoS, computer network, BGP, ExaBGP, Flowspec, NetFlow, IPFIX, Flowmon, RRDtool, Flow, xfcapd

Citácia

ŠKÁPIK, Anton. *Detekce volumetrických útoků DoS a DDoS v reálním čase na L3 síťové vrstvě*. Brno, 2018. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Holkovič Martin.

Detekce volumetrických útoků DoS a DDoS v reálním čase na L3 síťové vrstvě

Prehlásenie

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením Ing. Martina Holkoviča a Mgr. Martina Elicha RNDr. Ďalšie informácie mi poskytli vo firme Flowmon Networks. Uviedol som všetky literárne pramene, z ktorých som čerpal.

.....
Anton Škápik
17. mája 2018

Poďakovanie

Týmto chcem poďakovať firme Flowmon Networks, ktorá mi poskytla možnosti a materiály, bez ktorých by nebolo možné túto prácu vypracovať. Špeciálne poďakovanie potom patrí Ing. Martinovi Holkovičovi a Mgr. Martinovi Elichovi RNDr. za odbornú pomoc, trpezlivosť a dôveru.

Obsah

Kapitola 1

Úvod

Útoky typu DoS a DDoS sú v dnešnom svete, ktorý je výrazne závislý na Internetových službách, veľmi špecifickou a obzvlášť nebezpečnou hrozbou. Pre mnohé firmy môže znamenať i pár minútový výpadok služby problém, ktorý sa môže vyšplhať na kompenzáciách zákazníkom do výšky týždenných príjmov. Keďže takýto útok sa dá kúpiť za zlomok straty obeti, nie je prekvapujúce, že rastie počet a sila týchto útokov. Útoky so silou stovky gigabitov za sekundu dokáže do pár sekúnd vyradiť nie len koncovú obeť, ale dokonca aj poskytovateľa pripojenia, preto je rýchlosť, akou sa dokáže reagovať na hrozbu kľúčová.

1.1 Ciele práce

Cieľom práce je navrhnúť a implementovať ochranu proti DoS a DDoS útokom na tretej a štvrtej sieťovej vrstve modelu v reálnom čase, pretože DDoS zatopenie obrovských rozmerov môže vyradiť sieťovú aplikáciu do pár sekúnd. Tejto ochrany sa dosiahne pomocou špecializovaného filtra pre aplikáciu xfcapd[1] s následným spracovaním dát a výpočtu signatúry útoku. Na distribúciu pravidiel pre odstránenie alebo zmiernenie útoku budeme využívať protokol BGP s podporou flowspec. K tomu využijeme nástroj s otvoreným zdrojovým kódom *ExaBGP*.

1.2 Postup práce

Je dôležité sa zoznámiť s architektúrou sietí, dátovými tokmi, implementáciou IPFIX, NetFlow a protokolom BGP spolu s rozšírením flowspec u majoritných spoločností *Cisco* a *Juniper*. Rozhodnúť sa, ako bude možné realizovať tento projekt. Následne bude popísané stávajúce riešenie firmy Flowmon Networks a.s. a to hlavne spôsob exportu dát z Flowmon sond, Flowmon kolektor, ako prebieha filtrovanie dát a aké všetky informácie sú z NetFlow dostupné. Zoznámiť sa so stávajúcim riešením zásuvného modulu pre detekciu a mitigáciu útokov *DDoS Defender*.

Po zhodnotení všetkých informácii bude navrhnuté, aké sú možnosti pre zrýchlenú detekciu, ako bude možné filtrovať dáta, kam sa budú ukladať a ako z nich dokážeme zistiť sieťové anomálie. Taktiež treba navrhnúť spôsob výpočtu signatúry útoku pre nasledovné vytvorenie flowspec pravidiel pre zmiernenie útoku. Keďže súčasťou tohoto projektu nie je implementácia vlastného distribuovania BGP správ, je nutné urobiť prieskum a porovnanie stávajúcich riešení (Bird, ExaBGP, QUAGGA) pre distribúciu BGP správ a podľa

[1] aplikácia firmy Flowmon na prúdové spracovanie NetFlow tokov

toho sa rozhodnúť pre vhodný nástroj. Po dôkladnej analýze a návrhu architektúry nášho riešenia, vytvoríme program spĺňajúci požiadavky vyplívajúce zo zadania. Po implementácii rozšírenia pre DDoS Defender je nutné v laboratórnych podmienkach aplikáciu testovať, pomocou tradične používaných aplikácií na vytváranie zlomyseľnej prevádzky ako sú t50, hping3 či balík thc6. Vytváraný program tieto hrozby deteguje a zaznamená. Okrem toho vytvorí pravidlá podľa ktorých sa pomocou vhodného nástroja nastavia pravidlá na smerovače.

Kapitola 2

Sieťová komunikácia a NetFlow

V nasledujúcej časti budú popísané nezbytné teoretické základy počítačových sietí s dôrazom na protokol BGP a NetFlow protokol. NetFlow sa využíva na monitorovanie počítačových sietí na úrovni smerovačov, čiže ešte pred koncovými zariadeniami, pričom vidí do všetkých vrstiev sieťovej prevádzky. BGP protokol je využívaný na komunikáciu medzi smerovačmi a presmerovanie prevádzky na najlepšie vyhovujúcu cestu ku koncovým zariadeniam.

2.1 Charakteristika sietí

Počítačovou sieťou sa označuje súbor nástrojov, ktoré umožňujú spojenie a výmenu informácií medzi zariadeniami na diaľku. Najväčšou takou sieťou je Internet. Na celú sieť sa dá pozerať z viacerých strán (smerovanie, technológie prenosu, protokoly, zabezpečenie atď.). Je dôležité zoznámiť sa s referenčným ISO/OSI (*Open System Interconnection*) modelom, ktorý popisuje jednotlivé vrstvy komunikácie[6]. Tento model sa skladá zo siedmich vrstiev, z čoho každá vykonáva jasne danú funkciu. Vrstvy na rôznych úrovniach spolu komunikujú pomocou rozhraní.

V dnešných počítačových sietiach sa využíva rodina protokolov TCP/IP (*Transmission Control Protocol/Internet Protocol*), ktorá vychádza z modelu OSI. TCP/IP je štvorvrstvový konceptuálny model známy ako model DARPA[12], ktorý využíva Internet. Jeho vrstvy modelu sú: aplikačná, transportná, sieťová a vrstva sieťového rozhrania (prístupová vrstva). Každá vrstva v modeli TCP/IP zodpovedá jednej alebo viacerým vrstvám modelu OSI, ako zobrazuje tabuľka 2.1. Ak používateľ alebo aplikačný program zadá požiadavku na prenos správy, správa prechádza postupne jednotlivými vrstvami od aplikačnej až po vrstvu sieťového rozhrania a je príslušnými vrstvami spracovaná. Vrstva môže komunikovať iba s priľahlou vrstvou, vyššia vrstva odovzdá správu na spracovanie nižšej vrstve. Po prenose spojovacím vedením na stanicu adresáta je správa opäť spracovaná jednotlivými vrstvami v opačnom poradí.

2.2 NetFlow

NetFlow je sieťový protokol vyvinutý firmou Cisco, pre účely monitorovania prevádzky na sieti pomocou IP tokov. Zo začiatku bol navrhnutý len ako proprietárny (pre interné použitie spoločnosti Cisco), no následne sa z neho stal otvorený štandard (od verzie 5), ktorý bol implementovaný pre rôzne platformy. Pomocou NetFlow dát môžu správcovia sietí

TCP/IP	ISO/OSI
Aplikačná vrstva	Aplikačná vrstva
	Prezenčná vrstva
	Relačná vrstva
Transportná vrstva	Transportná vrstva
Sieťová (IP) vrstva	Sieťová vrstva
Vrstva sieťového rozhrania	Linková vrstva
	Fyzická vrstva

Tabuľka 2.1: Premietnutie protokolov TCP/IP na model OSI

v reálnom čase zobrazovať prehľad o prevádzke, z ktorého sa dajú vyhodnotiť podmienky pre rozširovanie siete alebo napríklad ako pomôcka pre ISP na účtovanie konektivity. Pre účely monitorovania je veľmi vhodné používať toky, pretože nie je potrebná dátová časť paketu, ale práve zoskupené informácie koľko podobných paketov sa spracovalo za časové obdobie a s akou priemernou veľkosťou paketu.

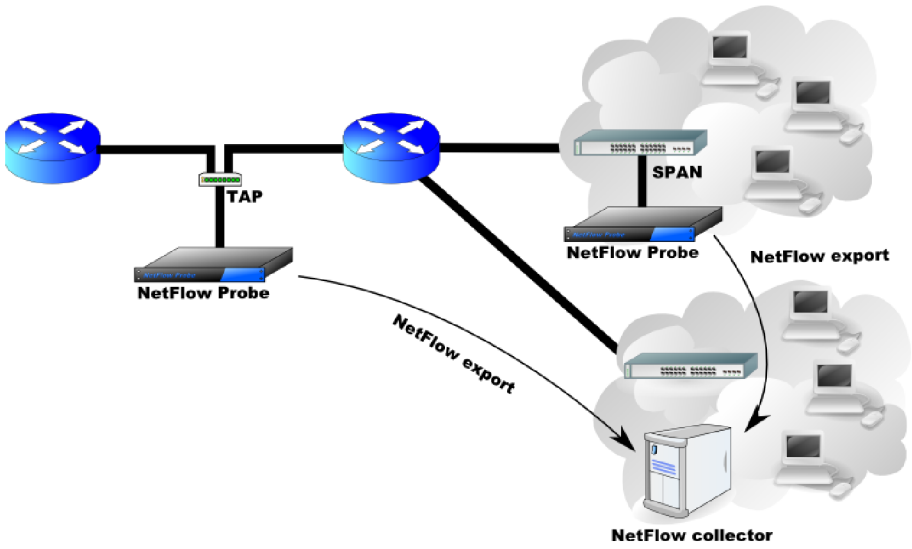
2.2.1 Architektúra NetFlow

NetFlow architektúra sa skladá z niekoľkých exportérov a minimálne jedného kolektoru určeného na zber dát. Na vytváranie záznamov sa používajú sondy alebo priamo smerovače s podporou exportovania NetFlow dát. Avšak používanie len smerovačov na export záznamov sa ukázal ako nevhodný pre dnešné siete, pretože smerovače ktoré majú dostatočný výkon na spracovanie všetkých NetFlow dát sú drahé. V dnešných architektúrach siete preberajú funkciu exportovania záznamov pasívne NetFlow sondy, určené výhradne pre tento účel. Sondy pracujú ako samostatné prvky v sieti, ktoré majú nastavenú sieťovú kartu v promiskuitnom móde[1] ktorá je pripojená buď na *SPAN port* v smerovači/rozbočovači alebo pomocou TAPu[2] ako je možné vidieť na obrázku 2.1. Netflow je súhrnný názov pre zber, monitorovanie a vyhodnocovanie dát. Hlavnými súčasťami NetFlow sú:

- **exportér** - smerovač či sonda pripojená na monitorovací port alebo pomocou TAPu k serveru (napr. Cisco smerovač CSR1000v alebo Flowmon Sonda);
- **kolektor** - zariadenie s dátovým úložiskom pre ukladanie záznamov (napr. Flowmon kolektor alebo server využívajúci aplikáciu Nfdump);
- **komunikačný protokol NetFlow** - NetFlow v5, NetFlow v9, IPFIX, sFlow, bFlow;
- **nástroje na zobrazovanie dát** - NfSen, RRDtool, Flowmon Monitoring Centrum.

Zhromažďovanie NetFlow dát obmedzuje výkon celého zariadenia, preto veľa zariadení používa pri zbere záznamov vzorkovanie (anglicky *sampling*). Znamená to, že sa pre výpočet použije iba každý N-tý paket monitorovanej prevádzky. V tomto prípade hovoríme o *Sampled NetFlow*. Nevýhoda tohto prístupu nastáva, ak monitorovaná prevádzka obsahuje periodicky sa opakujúce udalosti. Vzorkovaním sa môžu zanedbať časti prevádzky a vzniknúť skreslenia, kde je jedného typu komunikácie (napr. VoIP) buď ohromné množstvo alebo naopak sa tam nezobrazí. Preto nie je vhodné vyberať presne každý N-tý paket v sérii, ale

[1] prijímajú všetky pakety, aj tie, ktoré nie sú priamo určené pre nich
[2] zariadenie na kopírovanie prevádzky idúcej cez metalickú alebo optickú kabeláž



Obr. 2.1: Architektúra NetFlow s použitím sond [3]

radšej využiť určitý štýl heuristiky a vyberať náhodný paket z rozsahu určeného vzorkovaním. Prípadne sa pre vzorkovanie môže využiť zložitejšia heuristika na získanie presnejších informácii o štatistikách siete.

2.2.2 Sieťový tok

Sieťový tok je séria paketov, ktorá má spoločnú vlastnosť a prechádzajúca bodom pozorovania za určitý časový interval. Sieťový tok je definovaný normou RFC [1] a v rámci NetFlow sa používa pre zoskupovanie informácii a meranie výkonu siete. Táto komunikácia je jednoznačne definovaná päticou:

- zdrojová IP adresa;
- cieľová IP adresa;
- zdrojový port pre UDP alebo TCP, pre ostatné protokoly 0;
- cieľový port pre UDP alebo TCP, typ a kód pre ICMP alebo 0 pre ostatné protokoly;
- IP protokol.

Okrem spomínanej pätice, záznam NetFlow obsahuje aj rozhranie (interface), IP typ služby (Type of Service), dátum, čas zaznamenania a množstvo prenesených dát. NetFlow záznam je menší než prenesené dáta v rámci daného toku. Veľkosť záznamu je na veľkosti prenesených dát takmer nezávislá (pre krátke aj dlhé toky s veľkým množstvom prenesených dát je veľkosť záznamu takmer identická). Veľkosť prenesených dát pomocou NetFlow záznamu v pomere k monitorovaným dátam je v rozmedzí 1:50 až 1:300 s ohľadom na sieťovú prevádzku. Je to spôsobené tým, že podstatné informácie z paketov sa len agregujú do už existujúceho záznamu na exportéri, v zázname sa zvyšuje počet paketov v toku, veľkosť prenesených dát v rámci toku atď. Podobné je to aj s TCP príznakmi paketu. Tie sa zjednocujú s už existujúcimi príznakmi tak, že záznam vypovedá o tom, aké príznaky sa objavili v priebehu celého toku, čo umožňuje uchovávať záznamy o veľkom počte tokov na kolektore (pár mesiacov až rokov).

Počet informácii o toku v NetFlow zázname sa mení s verziou NetFlow, pričom v novších verziách štandardu sa nachádza viacej informácii. Pakety monitorovanej siete sú pomocou exportéra zaznamenané a spracované, určí sa ich identifikátor (v angličtine zvané *IP packet identity*, alebo tiež *fingerprint*) podľa ktorého sa následne agregujú do záznamov a tie sa následne uložia do NetFlow databázy, známej tiež ako *flowcache* na sonde. Ak spracovaný paket nepatrí do žiadneho toku v databáze, vytvorí sa nový tok. Inak sa len upraví záznam o čase prijatia posledného paketu v toku, zvýši sa počítadlo paketov a bajtov.

NetFlow záznamy sú obvykle exportované na kolektor pomocou protokolov Stream Control Transmission Protocol (SCTP) alebo User Datagram Protocol (UDP). V prípade UDP protokolu neexistuje možnosť ako znovu odoslať NetFlow záznam, ak sa paket nepodarí doručiť. Je to z dôvodu, že exportér okamžite po exportovaní NetFlow záznamu tento záznam z flowcache zahodí (výrazné zvýšenie efektivity). Exportované pakety sú zvyčajne odosielané na porty 2055, 3000-3010, 9555 alebo 9995.

2.2.3 Verzie NetFlow

Prvou výrazne rozšírenou verziou bola až verzia NetFlow v5, ktorá poskytovala základné informácie nad IPv4. V súčasnosti sa však prechádza skôr na využívanie verzie NetFlow v9 a IPFIX. Existujúce verzie NetFlow sú:

- **Verzia 1** - prvá udávaná verzia;
- **Verzia 2** až **Verzia 4** neboli nikdy publikované;
- **Verzia 5** poskytovala základné informácie nad IPv4.
- **Verzia 9** je rozšírením verzie 5 o šablóny, ktoré popisujú štruktúru záznamov. Táto zmena pridáva možnosť variability a informácie z L2 vrstvy (VLAN, BGP, IPv6 atp.);
- **IPFIX** - *IP Flow Information Export* [4, 5] rozširuje NetFlow v9 o možnosť posielať informácie o akýchkoľvek dátach na aplikačnej vrstve paketu, má podporu pre bFlow (*bidirectional flow*), pomocou ktorých je možné vypočítať NPM (*Network performance management*) štatistiky ako RTT(*round-trip time*), SRT(*Server response time*) a jitter. Položky, ktoré môžu byť s použitím IPFIX exportované, sú IPv4, IPv6, MPLS, VLAN, MAC, GRE, HTTP, NBAR2, VoIP (SIP) a metriky Jitter, SRT, RTT.

2.2.4 Exportér

Exportér je program na sonde, ktorý spracováva pakety a vytvára z nich NetFlow záznamy. Tieto záznamy sú exportované pomocou TCP alebo UDP spojenia na kolektor, ktorý naslúcha na určitom porte. V jednej sieti môže byť zapojených viacero kolektorov a viacero sond, ktoré medzi sebou komunikujú. Jedna sonda môže exportovať záznamy šifrovaným alebo nešifrovaným spojením na viacero kolektorov. Aby sa zabránilo preplneniu pamäti sondy, záznamy sa udržujú v pamäti iba obmedzený čas, pokiaľ tok nie je ukončený. Ukončenie toku môže nastať v jednom z nasledujúcich prípadov:

- **dlhotrvajúci tok** - tok je dôležité po určitom čase rozdeliť na viac menších tokov. Tento časový úsek sa nazýva *Aktívny timeout*;
- **neaktívny tok** - ak záznam o toku, nebol dlho aktualizovaný tak vyprší *Neaktívny timeout*;

- **kolízia pamäti** - vo flow cache došlo ku kolízii z dôvodu zaplnenia. Vtedy sa exportér prepne do výkonného režimu a vyprázdni celú pamäť;
- **manuálne ukončenie** - tok môže byť manuálne ukončený na základe údajov z prichádzajúceho paketu (RST alebo FIN príznak).

2.2.5 Kolektor

Kolektor slúži na ukladanie dát pre neskoršie použitie a pre vyhodnocovanie štatistík. Jednou z najbežnejších možností je, že na kolektore beží aplikácia NfSen s otvorenými zdrojovými kódmi, ktorý pochádza od rovnakého autora, ako program NFDUMP tools. Tieto nástroje sú dostupné pod licenciou BSD. NfSen nie je úplne samostatná aplikácia, ale poskytuje webový front-end. Jeho funkcie sú závislé na NFDUMP tools a *Round Robin Database* (RRD). Najdôležitejšími funkciami programu NfSen sú:

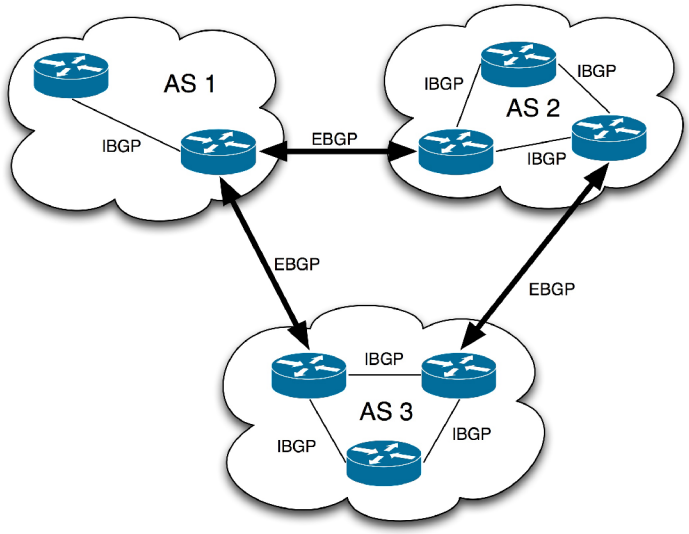
- grafické zobrazenie NetFlow dát pri použití RRD;
- jednoduchá navigácia medzi NetFlow dátami;
- spracovanie NetFlow dát vo vybranom časovom úseku;
- automatické spúšťanie alertov podľa definovaných pravidiel;
- rozšíriteľnosť funkcii pomocou zásuvných modulov.

Kolektor môže prijímať záznamy na viacerých portoch, z viacerých exportérov, z vnútornej i vonkajšej siete. Zvyčajne kolektor spracováva a ukladá záznamy s 5 minútovou granularitou.

2.3 Border Gateway Protokol

Border Gateway Protokol (BGP) je veľmi robustný a škálovateľný smerovací protokol, o čom svedčí skutočnosť, že je často používaný na Internete. V súčasnej dobe sa používa štvrtá verzia protokolu BGP (BGPv4) definovaná v norme RFC[10]. V tomto čase, smerovacie tabuľky BGP na Internete obsahujú viac ako 700 000 trás[11]. Protokol BGP je využívaný primárne k výmene smerovacích informácii medzi *autonómnymi systémami*. Podľa použitia môžeme rozdeliť použitie na *internal BGP* (iBGP) a *external BGP* (eBGP). Pre smerovanie vnútri jedného autonómneho systému sa používa iBGP a pri komunikácii medzi rôznymi autonómnymi systémami sa jedná o eBGP ako je možné vidieť na obrázku 2.2.

Protokol BGP je typu *Path vector* (oznamuje zoznam sietí a zoznam parametrov o ceste do nich) a garantuje bez-slučkovú výmenu smerovacích informácií. Bez-slučková výmena je zaručená nepovolením smerovaču akceptovať aktualizáciu, ktorá obsahuje jeho vlastné číslo AS. Okrem výmeny smerovacích informácií, sa BGP používa pre zmenšenie smerovacích tabuliek (sumarizácie adries) pomocou beztriedneho smerovania *classless interdomain routing (CIDR)*[2]. Taktiež ale poskytuje rozdelenie triednych adries do väčšieho počtu podsietí, čo naopak výrazne zvyšuje počet smerovacích informácii v tabuľkách[9].



Obr. 2.2: Ukážka BGP komunikácie medzi autonómnymi systémami

2.3.1 Autonómne systémy

Autonómny systém (AS) je skupina sietí a smerovačov, ktoré používajú spoločnú smerovaciu politiku (spôsob výberu ciest do rôznych cieľov, filtrovanie smerovacích informácií, oznamovanie smerovacích ciest) a patria pod spoločnú administratívnu doménu[4]. Jedná sa napríklad o ISP (*Internet service provider*), veľkú spoločnosť, univerzitu, divíziu firmy alebo spoločenstvo firiem. Tento systém reprezentuje prepojenú skupinu jedného alebo viacerých blokov IP adries (nazývaných tiež *IP prefixes*), ktoré boli pridelené tejto organizácii a poskytuje smerovaciu politiku systémom mimo tohto autonómneho systému. Väčšina organizácii nemá AS vo vlastnej réžii, ale pripája sa k ISP, ktorý je správcom AS, alebo je tento ISP súčasťou väčšieho AS[7]. Z vonkajšej siete je AS vnímaný ako jedna nerozdelená entita, čiže všetky členské siete v AS sú v ňom z pohľadu iných AS priamo dostupné. V prípade, že je AS pripojený na verejný Internet s použitím EGP (BGP), číslo AS musí byť pridelené organizáciou IANA. V súčasnosti sa používajú 2B čísla (0-65535) ako označenie AS, no štandard RFC[13] špecifikuje použitie aj 4B čísiel.

2.3.2 Komunikácia medzi dvomi smerovačmi

Smerovače a aplikácie využívajúce protokol BGP využívajú pre komunikáciu spoľahlivý protokol TCP, zvyčajne na cieľovom porte 179. Komunikácia prebieha ako výmena správ typu: OPEN, KEEPALIVE, UPDATE a NOTIFICATION. Smerovač komunikujúci protokolom BGP sa nazýva „BGP rečník“ (speaker). Po založení TCP spojenia medzi dvomi BGP rečníkmi za účelom výmeny smerovacích informácií, sa BGP rečníci stávajú „BGP susedia“ (*BGP neighbors*). Pre otvorenie TCP spojenia, sa použije správa typu OPEN pričom sa smerovač, ktorý otvára spojenie prepne do stavu OPENSENT. Ak druhá strana súhlasí so spojením, naviaže spojenie a prepne sa do stavu OPENCONFIRM. Ak je spojenie naviazané, v pravidelných intervaloch si susedia vymieňajú správy typu KEEPALIVE, ktoré slúžia ako prostriedok pre potvrdenie dohody o zriadení susedských vzťahov (pre-

[4]dosah administratívnej právomoci správcu

pína stav spojenia z OPENCONFIRM na ESTABLISHED). Táto správa tiež slúži aj na monitorovanie činností po dobu pripojenia. Ak druhá strana nesúhlasí, pošle správu typu NOTIFICATION s kódom, ktorý vysvetľuje dôvod pre zamietnutie, spojenie je prerušené a smerovač sa prepne do stavu IDLE.

Pre propagovanie alebo odvolanie cesty sa používajú správy UPDATE. Ihneď po naviazaní spojenia sa susedia synchronizujú. Pomocou UPDATE správy odošlú všetky najlepšie smery zo svojich BGP tabuliek susedovi. V tomto prípade hovoríme o plnej aktualizácii *full update*. BGP smerovače neposielajú aktualizácie pravidelne, ale iba ak sa niečo zmenilo. V prípade zmeny na smerovači sa namiesto všetkých trás odošlú iba tie trasy, ktoré sa zmenili (pridanie alebo odobranie). Jedná sa o *inkrementálne aktualizácie*, ktoré sú efektívnejšie na prenosy. Obzvlášť na chrbticových smerovačoch môže veľkosť smerovacích tabuliek dosahovať rádovo desiatky až stovky MB.

2.3.3 BGP Atribúty

K zaisteniu správneho a stabilného smerovania pri obrovskom počte možných destinácii a ciest využíva BGP viacero atribútov, na základe ktorých sa pri výbere správnej cesty rozhoduje (výber cesty je popísaný v sekcii 2.3.4). Zoznam atribútov je nasledujúci:

Váha - Weight

Predstavuje váhu, s akou sa má BGP cesta vkladať do smerovacej tabuľky. Je však len lokálna pre konkrétny smerovač, takže nie je propagovaná susedným smerovačom. Ak sa smerovač dozvie o viacerých cestách k rovnakému cieľu, použije sa tá, s najväčšou váhou. Jedná sa len Cisco proprietárny atribút.

Local preference

Atribút *local preference* označuje preferenciu výstupnej cesty z AS. Odovzdáva sa len cez iBGP, neprechádza cez eBGP. Implicitná hodnota je 100 a je propagovaná medzi všetkými BGP smerovačmi v rámci tohoto AS. Ak obdrží viacej smerovačov daného AS informáciu o ceste do rovnakej cieľovej destinácie, porovná hodnoty *local preference* a uprednostní cestu, ktorá vedie cez smerovač s vyššou hodnotou tohoto atribútu.

Origin-type

BGP Origin kódy obsahujú informáciu o pôvode cesty, odkiaľ bola prevzatá. Sú tri možné kódy používané v BGP:

1. **igp** - interná cesta do podsiete autonómneho systému;
2. **egp** - cesta distribuovaná z eBGP;
3. **incomplete** - cesta redistribuovaná do BGP.

AS path

Usporiadaný zoznam AS path obsahuje čísla autonómnych systémov, ktoré BGP postupne ukladá ako cestu kadiaľ prechádza. Ak sa v atribúte AS path už nachádza číslo AS, ktorým práve prechádza, smerovač zahodí túto aktualizáciu. Týmto predchádza vytváraniu smerovacích slučiek (*routing loops*).

Next-hop

Atribút next-hop obsahuje IP adresu smerovača, cez ktorý je dostupná cieľová sieť. V prípade iBGP sa dá pomocou atribútu next-hop dosiahnuť presmerovanie cez nie optimálnu cestu, za účelom úpravy prevádzky. U eBGP spojenia sa jedná o IP adresu smerovača, ktorý generuje informácie o tejto ceste. Smerovač musí poskytovať niektorý z IGP protokolov, ktorý zaistí dostupnosť next-hop adresy, inak je cesta neplatná.

Community string

Community string umožňuje združovať siete do skupín a aplikovať na ne pravidlá podľa lokálnej politiky smerovača. Tento atribút sa priamo pri výbere cesty nezúčastňuje, ale jedná sa o atribút, pomocou ktorého sa upravujú ostatné atribúty. Typické pomenované hodnoty, ktoré môže community string obsahovať, sú:

- **No-export** - cesta je propagovaná len v rámci AS, ktorý obdržal správu s touto aktualizáciou;
- **No-advertise** - atribút značí, že táto cesta nemá byť propagovaná nikomu inému, ani v rámci jeho AS;
- **Internet** - cesty s týmto príznakom sú distribuované bez obmedzenia v rámci všetkých AS (Internetu).

Mimo tieto pomenované hodnoty môže komunitný reťazec obsahovať aj užívateľom definované hodnoty, prípadne rozšírené *extended* pomenované hodnoty (napr. *redirect*, *vrf-export*, *origin*), ktoré sa ale môžu líšiť v závislosti na implementácii od výrobcu. Medzi rozšírené komunitné reťazce sa radí aj flowspec.

2.3.4 BGP Výber cesty

Keďže BGP môže prijať viac ciest z viacerých zdrojov, vyberie len najlepšiu cestu. Ak je zvolená cesta, nastaví cestu v smerovacej tabuľke a propaguje cesty k svojim susedom. BGP používa kritériá k výberu najlepšej cesty k cieľu v nasledujúcom poradí:

1. V prípade, že cesta ukazuje na ďalší krok, ktorý je neprístupný zo smerovača, aktualizácia sa zastaví.
2. Preferuje cestu, s najväčšou váhou (platné len pre smerovače Cisco).
3. Pokiaľ nie je zadané Origin, preferuje sa cesta s najnižším AS.
4. Ak je Origin zadané a všetky cesty majú rovnaký AS, preferuje sa Origin-type s nižšou hodnotou, pričom IGP je nižšie než EGP a EGP hodnota je nižšia než incomplete[2].
5. Preferuje sa najnižší MED atribút.
6. Preferuje sa externá cesta pred internými.
7. Preferuje sa najbližšia IGP cesta.
8. Preferuje sa cesta s najnižšou IP adresou, špecifikovaná atribútom BGP router ID.

2.3.5 Flowspec

BGP *Flow Specification* dovoľuje rýchlo nastavovať a distribuovať filtrovacie pravidlá a pravidlá určené na základe nastavenia, medzi veľkým množstvom BGP smerovačov. Každé flowspec pravidlo obsahuje časť s kritériami a časť s akciou ktorá má byť vykonaná. Ako kritéria pre porovnanie sa používajú položky definujúce sieťový tok. Ak IP tok zodpovedá všetkým uvedeným kritériám, tomuto toku sú pridelené viaceré atribúty, vzhľadom na nastavenú akciu pridruženú k flowspec pravidlu. Atribúty, pravidlá a akcie sa môžu líšiť, vzhľadom na hardwarové možnosti. Najčastejšie akcie, ktoré podporujú smerovače s flowspec sú: *accept*, *decline*, *rate-limit*, *mark* a *redirect*. Pričom *rate-limit* nastavuje maximálnu priepustnosť v bytoch za sekundu a *decline* je to isté ako *rate-limit* s hodnotou „0“. *Mark* označuje jednotlivé pakety užívateľom definou značkou pre neskoršie použitie a *redirect* nastavuje hodnotu nasledujúceho skoku ako je vidieť na obrázku 2.3. Toto je veľmi vhodné na použitie pre mitigáciu DDoS útokov.

```
Flow           :Dest:10.20.20.25/32,Source:10.31.4.2/32,Proto:=6,DPort:=35239
  Actions      :Nexthop: 10.100.0.190  (bgp.1)
Flow           :Dest:10.20.20.25/32,Source:10.31.6.2/32,Proto:=6,DPort:=35239
  Actions      :DSCP: 1  (bgp.1)
Flow           :Dest:10.20.20.25/32,Source:10.31.7.2/32,Proto:=6,DPort:=35239
  Actions      :Traffic-rate: 64000 bps  (bgp.1)
Flow           :Dest:10.20.20.25/32,Source:10.31.10.2/32,Proto:=6,DPort:=35239
  Actions      :Traffic-rate: 0 bps  (bgp.1)
```

Obr. 2.3: Ukážka aplikovaných flowspec pravidiel na smerovači Cisco CSR1000v

Tradične sa pre DDoS mitigáciu používa *remotely triggered blackhole* (RTBH). BGP cesta je odoslaná s IP adresou alebo podsieťou pod útokom so špeciálnym komunitným reťazcom. Tento komunitný reťazec nastaví na hraničných smerovačoch next-hop na špeciálny next-hop. Ak je pre túto komunitu na smerovači nastavené pravidlo, že má preposielať prevádzku na discard/null, zabráni to útočníkovi prístup do našej siete. I keď presmerovanie celej podsiete poskytuje dobrú ochranu, činí to server(mimo lokálnu sieť) kompletne neprístupný.

Na druhú stranu BGP flowspec poskytuje oveľa škálovatelnejší prístup ako efektívne vytvoriť pravidlá, pre presné zachytenie škodlivých tokov so zdrojom, cieľom, L4 parametrami a špecifikáciami paketov ako dĺžka, fragmentovanie atp. Flowspec umožňuje dynamické nasadenie pravidiel a akcií na okrajových smerovačoch, pre zahodenie sieťovej prevádzky, presmerovanie prevádzky do inej VRF (*Virtual Routing and Forwarding*) alebo nastaví politiku priepustnosti paketov podľa definovaných kritérií. Takže namiesto posielania BGP cesty so špeciálnym komunitným reťazcom, ku ktorému musí byť na smerovači nastavená smerovacia politika pre presmerovanie takejto prevádzky, BGP flowspec pošle špecifický formát na smerovače na vytvorenie prístupových zoznamov (*access list*) s mapami podľa politiky a triedy na vytvorenie pravidiel a akcii na distribúciu ciest[3].

Kapitola 3

Flowmon a DDoS Defender

Spoločnosť Flowmon je český start-up projekt, ktorý sa dostal na svetovú úroveň v monitorovaní a ochrane sietí. Flowmon pomáha firmám spravovať a zabezpečovať ich sieťovú infraštruktúru prostredníctvom najmodernejších dostupných technologických prostriedkov. Vďaka navrhnutému riešeniu získali po celom svete IT profesionálovia kontrolu nad sieťovými službami, zvyšujú výkonnosť aplikácií a chránia svoje systémy pred modernými kybernetickými hrozbami. Pracuje s najnovšími technológiami a podieľa sa na viacerých výskumoch v spolupráci s organizáciami *VUT-FIT*, *MUNI-FI* a *Cesnetom*. Jedným z úspešných projektov je bezpochyby aj plugin pre detekciu a mitigáciu[1] DoS a DDoS útokov *DDoS Defender*.

3.1 Flowmon Sonda

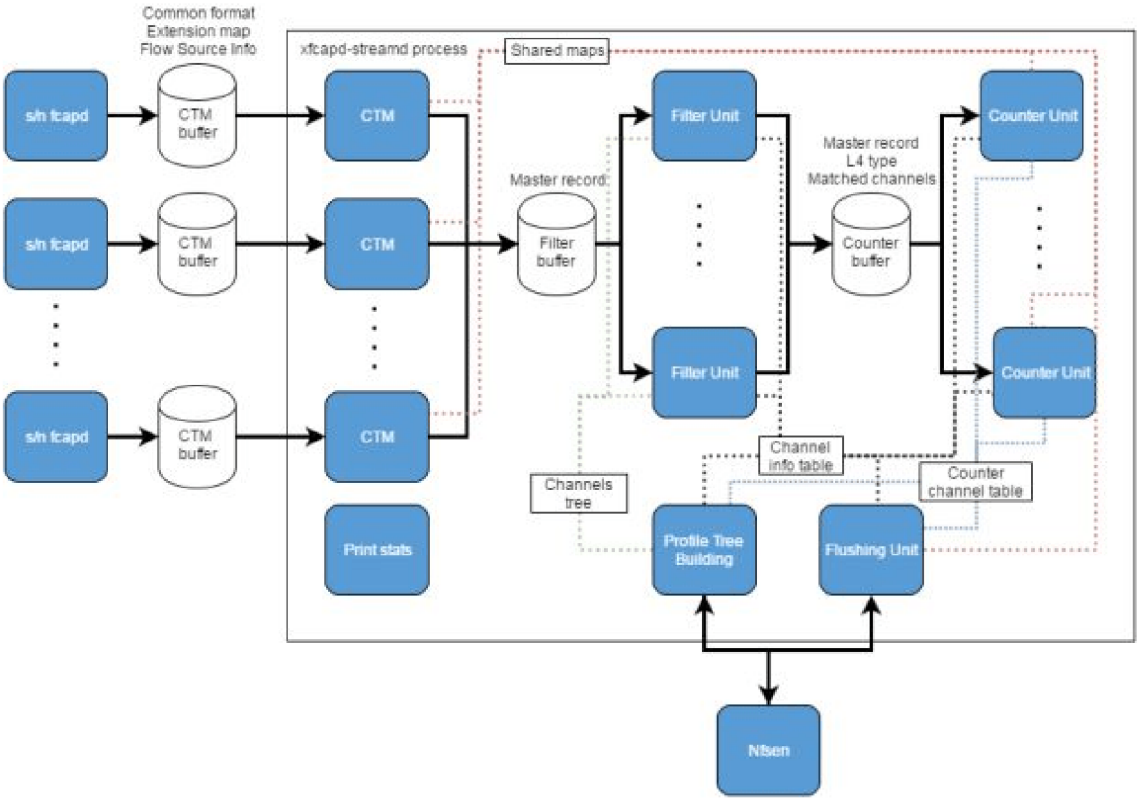
Vysoko-výkonná Flowmon sonda (anglicky probe) je zdrojom IP Flow records vo formáte NetFlow v5, v9 a IPFIX. Je neviditeľná na L2 a vyšších vrstvách monitorovanej siete. Sonda môže byť buď ako softvér inštalovaný na sieťovom zariadení či ako virtuálny model pre VMware, HyperV alebo KVM, pričom virtuálna sonda potrebuje mať vytvorený virtuálny switch, ktorý monitoruje sieťovú prevádzku a je v promiskuitnom móde. Ak je inštalovaná ako software na vlastnom zariadení, môže byť hardvérovo akcelerovaná sieťovými kartami od MIRICOM alebo Netcope. Sonda sa vzdialene konfiguruje pomocou webového rozhrania, ktoré umožňuje jednoducho nastaviť všetky potrebné parametre ako napríklad položky z L7 ktoré majú byť exportované, ako majú byť NetFlow záznamy vzorkované, na akom porte naslúcha kolektor a hodnoty aktívneho a neaktívneho timeoutu. Hardvérovo akcelerované sondy sú schopné exportovať až 100 Gbps na jeden port.

Každá sonda obsahuje aj vstavaný kolektor malej veľkosti, takže na nej zároveň môžu bežať zásuvné moduly ako napríklad DDoS Defender. Avšak exportovanie NetFlow záznamov je náročné na výkon, preto sa využívanie vstavaných kolektorov nedoporučuje pri väčšom počte spracovávaných tokov.

3.2 Flowmon Kolektor

Kolektor poskytuje dlhodobé úložisko štatistík z viacerých zdrojov NetFlow dát. Obsahuje aplikácie na zbieranie, analýzu, vizualizáciu a vytváranie dlhodobých reportov z NetFlow, IPFIX, sFlow štatistík pomocou Flowmon monitorovacieho centra. Väčšinou sa kolektor

[1] zmierňovanie útoku



Obr. 3.1: Streamova architektúra

dodáva s RAIDom, redundantným napájaním a diskovou kapacitou 1 až 24TB. Primárne slúži na monitorovanie celej siete, prípadne viacerých sietí z jedného miesta. Kolektory sú zvyčajne oveľa výkonnejšie než sondy, preto sú vhodnejšie na inštaláciu viacero zásuvných modulov. Bezpochyby ďalšou veľkou výhodou pre DDoS Defender umiestený na kolektore je, že môže strážiť viacero segmentov, vo viacerých sieťach, takže stačí jedna licencia pre pokrytie nadnárodnej spoločnosti.

3.2.1 nfcapd

Na kolektore beží nfcapd proces, ktorý sa stará o primárne filtrovanie záznamov z exportérov a následné filtrovanie do profilov pre jednotlivé zdroje tokov. Ako už bolo spomenuté v kapitole 2.2.5, nástroj nfcapd pracuje s 5 minútovou granularitou, preto je jeho použitie pre rýchlu detekciu sieťových anomálii alebo volumetrických útokov nedostatočné.

3.2.2 xfcapd

Nástroj xfcapd[14] je navrhnutý tak, aby v reálnom čase analyzoval dáta spracovávané pomocou aplikácie nfcapd a pritom nenarušil normálnu funkciu kolektoru. Zdrojom dát sú procesy nfcapd a sfcapd, ktoré normálnym spôsobom spracovávajú vstupné dáta. Tieto dáta následne predávajú tomuto systému pre spracovanie v reálnom čase. Systém ich spracúva prúdovým spôsobom. Ďalej tento systém bude volaný *Streamová architektúra* .

3.3 DDoS Defender

Flowmon DDoS Defender[8] je riešenie pre detekciu a mitigáciu volumetrických útokov - DoS (Denial of Service) alebo DDoS (Distributed Denial of Service). Bez zmeny konfigurácie, zmeny topológie siete alebo iných prídavných investícii do sieťových prvkov, je možné detekovať volumetrické útoky proti IT infraštruktúre, serverom, kritickým systémom alebo aplikáciam v pomerne krátkom časovom období. V spolupráci so scrubbing centrami alebo inými špecializovanými riešeniami pre eliminovanie DDoS útokov mimo napadnuté segmenty, Flowmon DDoS Defender mitiguje a blokuje útoky automaticky. Defender je súčasťou kolektoru a používa Flowmon Monitoring Centrum, takže nepotrebuje špeciálne konfigurovať separátny zdroj tokov. Defender môže byť inštalovaný v jednom z týchto troch scenárov:

- **Standalone** - Defender pasívne deteguje útoky a hlási výskyt útoku, no nijako nemitiguje tieto útoky;
- **Out-of-band elimination** - Defender pasívne deteguje útoky a hlási výskyt útoku a môže vzdialene vytvoriť BGP cestu pre zahadzovanie sieťovej prevádzky;
- **Scrubbing Center** - v tomto prípade, Defender môže vykonávať všetko čo už bolo spomenuté vyššie, no môže byt integrovaný spoločne so scrubbing centrom (SC), pre čistenie sieťovej prevádzky a návratu vyčistenej prevádzky späť do siete. SC je pripojené mimo siete a v prípade útoku, Defender môže zmeniť smerovanie na vybranom smerovači/smerovačoch, pre presmerovanie prevádzky cez SC na vyčistenie. Defender tiež nakonfiguruje SC pre čistenie a poskytne dôležité štatistiky sieťovej prevádzky, baseliny atď. potrebné pre správne zmierňovanie útoku.

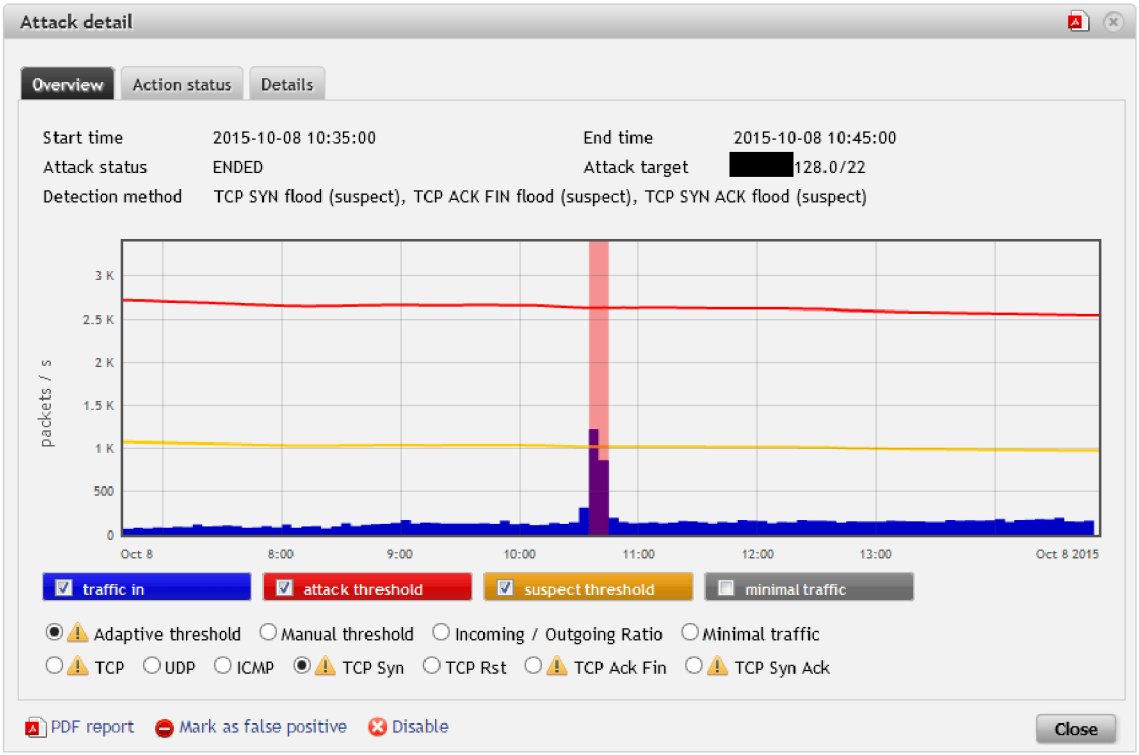
3.3.1 Integrácia so sieťovými prvkami

Integrácia DDoS Defender-u so sieťovými prvkami je podporovaná pomocou techniky PBR (Policy Based Routing), BGP 2.3 alebo je možné vytvoriť a použiť RTHB (Remotely Triggered Black Hole) mechanizmus, na jednoduché zmiernenie útoku. Na nastavovanie pravidiel pomocou PBR sa používajú ACL (access listy) na smerovačoch, ku ktorým sa pripája pomocou SSH spojenia a aplikujú sa pravidlá na presmerovanie subnetu, zvyčajne do scrubbing centra alebo na zahodenie. Na smerovanie pomocou BGP sa používa nástroj *ExaBGP*, ktorý je stále vyvíjaný a má širokú podporu rozšírení BGP protokolu, ako napríklad BGP flowspec, ktorý je veľmi vhodný pre zmierňovanie útokov.

3.3.2 Detekcia útokov

Detekcia útokov je vykonávaná pre každý *protected segment* definovaný v DDos Defenderi (ďalej len Defender). Protected segmenty sú definované pomocou sieťových subnetov. Pre každý segment sa vyberá, ktorá metóda na detekciu sa použije. V súčasnej dobe sa na výpočet signatúr útokov používajú dotazy pre program *nfdump*, ktorý dokáže na výstup vygenerovať zadaný počet podsietí s najväčšou prevádzkou. Avšak aplikovaním týchto dotazov nad veľkým množstvom dát je veľmi časovo a výkonnostne náročné, preto je potrebné nájsť efektívnejší spôsob. Pre každý protected segment sa pravidelne vykonávajú následné metódy:

1. **Baseline metóda** - tu sa radí metóda pre manuálny prah a metóda používajúca adaptívny prah.



Obr. 3.2: Podozrenie na útok detekovaný z počtu paketov za sekundu

2. **Statická metóda** - používa sa pre metódu pomeru prichádzajúcej sieťovej prevádzky k odchádzajúcej.

Viac sa téme detekcii útokov budeme venovať v kapitole 4.2.2.

3.3.3 Nastavenie smerovačov

Aby bolo možné presmerovávať prevádzku pomocou BGP injekcie pre napadnutý segment, musia byť splnené nasledujúce podmienky:

- Defeneder ASN (Autonomous system number) musí byť nastavený. Ak sa použije rovnaké ASN pre smerovač a Defender, je použitá metóda iBGP v prípade rozdielnych ASN sa použije metóda eBGP;
- aspoň jeden smerovač, podporujúci BGP cesty, musí byť pridelený pre protected segmen;
- smerovač musí byť nakonfigurovaný v Defendere s nasledujúcimi položkami:
  1. názov smerovača;
  2. IP adresa (IPv4 a v prípade mitigácie IPv6 podsietí aj IPv6 adresa smerovača);
  3. community string;
  4. ASN smerovača;
  5. nastavená položka „next-hop“ pre iBGP alebo „Defender ASN“ pre eBGP.

Kapitola 4

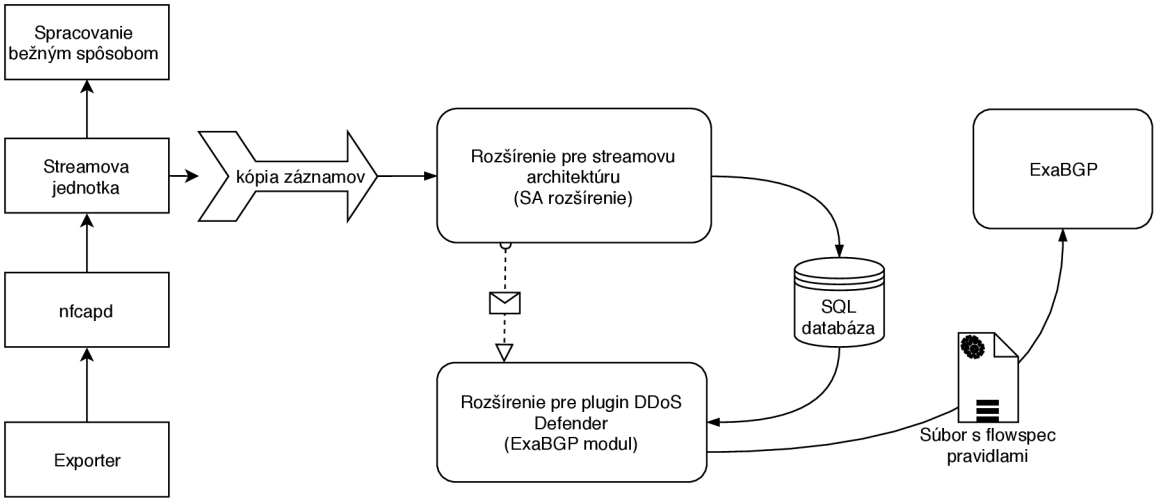
Návrh

V tejto kapitole bude popísaný návrh implementácie rozšírenia pre Flowmon kolektor. Program pre detekciu záplavových útokov DoS a DDoS je navrhovaný pre prúdové spracovávanie NetFlow tokov a pre výpočet štatistík potrebných pre detekciu v reálnom čase. Následne bude možné podľa detailov útoku vytvoriť signatúru útoku a tak zmierniť prebiehajúci útok pomocou BGP flowspec.

Navrhované riešenie sa skladá sa z dvoch hlavných častí:

- rozšírenie pre streamovu architektúru (*SA rozšírenie*)
- a rozšírenia pre Perlovú časť DDoS Defender (*ExaBGP modul*).

Na obrázku 4.1 je ukážka pripojenia rozšírenia do architektúry Flowmon kolektoru. Pred kompletným spracovaním záznamov NetFlow kolektorom, sa skopírujú práve spracovávané záznamy do *SA rozšírenia*. Tu sa vyberú iba pamäťové bloky, ktoré spĺňajú podmienky určené definíciou chráneného segmentu. Tieto sú spracované a následne uložené pre ďalšie použitie. Popri ukladaní štatistík do RRD a záznamov do databázy sú detekované sieťové anomálie pomocou porovnávania vytvorených štatistík s prahovými hodnotami uloženými v RRD.



Obr. 4.1: Návrh rozšírení pre streamovú architektúru a perlový démon s načítaním záznamov z xfcapd a odoslaním konfiguračného súboru pre ExaBGP.

Pri detekovaní anomálie je odoslaná správa do *Perl rozšírenia* s informáciou o napadnutom chránenom segmente. Po prijatí takejto správy o novom útoku sa z dát uložených v databáze začne výpočet signatúry útoku. Tieto vypočítané informácie sa agregujú do pravidiel podľa percentuálneho zastúpenia počtu paketov a prenesených dát v prevádzke. Z vypočítaných pravidiel sa spojením s akciou na zmiernenie útoku vytvoria flowspec pravidlá, ktoré sú zapísané vo formáte JSON do dočasného súboru. Tento dočasný súbor sa následne použije ako konfiguračný súbor pre aplikáciu ExaBGP. Podľa konfiguračného súbora sa distribuujú jednotlivé pravidlá na smerovače.

4.1 Vytváranie baseline

Baseline sa vytvárajú pre výpočet štatistík o sieťovej prevádzke v čase, keď nie je detekovaný útok. SA rozšírenie vytvorí kópiu *Master Record* (pamäťový blok obsahujúci nespracovaný sieťový tok) a vyberie len tie záznamy, ktoré spĺňajú kritérium chráneného segmentu. Chránený segment môže byť definovaný zoznamom IP adries, prefixom alebo číslami autonómneho systému. Tieto vybrané záznamy sú následne filtrované *filtračnou jednotkou* pre získanie všetkých hodnôt z pätice doplnené o príznaky TCP, ak je spracovávaný tok typu TCP.

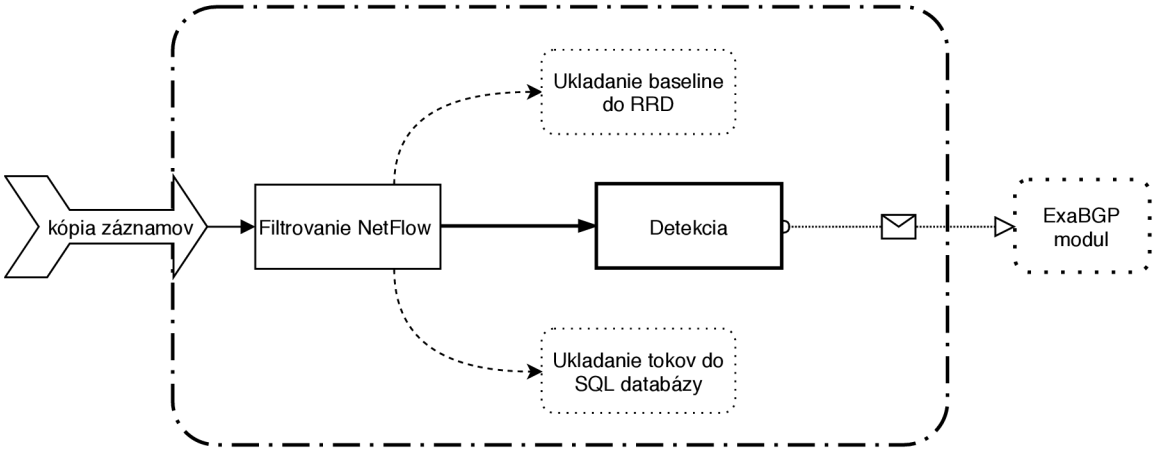
Zo záznamov spĺňajúcich podmienky sa vytvárajú štatistiky, ktoré sa po prijatí nových dát a spracovaní zapisujú do RRD súborov. Ku každému chránenému segmentu je vytvorených viacero RRD súborov, podla kritérií pre záplavové útoky. Tieto štatistiky sa neskôr použijú pre vizualizáciu prevádzky a na účely výpočtu prahových hodnôt. Okrem štatistík, sa vytriedené záznamy používajú i pre detekciu anomálii a zápisu pätice do databázy, pre neskorší výpočet signatúry útoku.

4.1.1 Filtrovanie NetFlow dát

Cieľom filtrovania je z NetFlow záznamov odstrániť nepotrebné dáta. Flowmon kolektor sa momentálne používa na filtrovanie všetkých položiek uložených v toku. Tento prístup je náročný na výkon a následne uložené výsledky sú pre využitie v Defenderi výrazne obsiahle. Preto je treba vytvoriť filtračnú jednotku, ktorá bude pracovať veľmi rýchle, efektívne a bude spracovávať len hodnoty, ktoré potrebujeme. Toho je možné dosiahnuť filtračnou jednotkou pracujúcou v odľahčenom režime. V tomto režime sa vytvorí „šablóna“ na zistenie len položiek zo základnej pätice a príznakov TCP. Po aplikovaní šablóny na NerFlow záznam sa získajú len relevantné položky, preto priamo úmerne klesne pamäťová náročnosť, ako i procesorový čas.

4.1.2 Ukladanie baseline do RRD

Filtrované dáta sa uložia do pripravených súborov Round-Robin databázy (ďalej aj RRD) sprostredkovanej pomocou nástroja *RRDtools*. Tento nástroj ponúka rozšírenú funkcionalitu pre vkladanie dát, výpočet priemernej a maximálnej hodnoty dát a expiráciu starých dát. RRD súbory obsahujú dlhodobé štatistiky podľa filtru pre chránené segmenty, z ktorých sa zároveň vytvorí baseline štandardnej prevádzky. Ukladá sa počet paketov za sekundu, počet tokov za sekundu a počet bytov za sekundu. *RRDtools* je vhodný nástroj aj kvôli otvoreným zdrojovým kódom a stabilite. Pre každú detekčnú metódu (TCP flood, SYN ACK, ICMP atp.) je vytvorená samostatná baseline. Po vytvorení chráneného segmentu začne učiace obdobie definované časovým úsekom, z ktorého sa vypočítavajú prahové hodnoty.



Obr. 4.2: Rozšírenie pre streamovú architektúru, pre detekciu útokov v reálnom čase.

4.1.3 Ukladanie tokov do SQL databázy

Okrem štatistík, sa ukladajú aj záznamy o sieťových tokoch (pätica). Pri výbere databázy bolo dôležité vziať do úvahy viacero faktorov ako:

- rýchlosť zapisovania a čítania;
- možnosť ukladania veľkého množstva dát;
- súbežný prístup viacero užívateľov;
- údržba z pohľadu dlhodobého používania;
- keďže je v pláne následné rozširovanie, bolo potrebné vziať v úvahu aj znalosti ľudí, ktorí s databázou budú pracovať.

Na základe týchto kritérií som sa rozhodol využiť mne dobre známu SQL databázu PostgreSQL, ktorá je stabilná, dáta ukladá na disk (s možnosťou využiť aj externé úložisko), pri zmenách dát sa dajú používať databázové spúšťače, cudzie kľúče a je možnosť písať skripty priamo v jazyku psql. Ďalší dôvod pre výber PostgreSQL je, že Flowmon kolektor využíva PostgreSQL a teda nie je nutné inštalovať ďalšiu databázu.

Na ukladanie dát do databázy sú použité tri tabuľky, ktoré sú vzájomne prepojené cudzími kľúčmi ako je zobrazené v prílohe. V prvej tabuľke sa nachádzajú informácie o chránených segmentoch spolu s číslom útoku. Okrem primárneho kľúča, slúžiaceho ako jednoznačný identifikátor pravidla, obsahuje aj postup ukladania záznamov do tretej tabuľky. Tiež je v tabuľke dátum poslednej zmeny a informácia o aplikovaní pravidla na smerovači (obrázok 4.3).

```
iad=> select * from flowspec_rules where attack_id = 45;
 id | segment_id | attack_id | progress |        date         |  state
----+------------+-----------+----------+---------------------+----------
 45 |          4 |        45 | 4/4      | 2018-05-02 11:55:00 | disabled
(1 row)
```

Obr. 4.3: Tabuľka flowspec_rules použitá pre flowspec pravidlá vypočítaná pre útok

Druhá tabuľka obsahuje kľúč pravidla, na ktorý sa odkazuje z prvej tabuľky. Pre jeden kľúč, môže byť v tabuľke viacero záznamov. Taktiež sa tu nachádzajú akcie s hodnotami,

ktoré sa majú aplikovať po splnení kritérií pomocou flowspec pravidla a informácia o aktuálnosti cesty (obrázok 4.4).

```
iad=> select * from flowspec_routes where rule_id = 45;
 id  | rule_id |   action   |    option    | share |   state
-----+---------+------------+--------------+-------+-----------
 135 |      45 | mark       | 1            |       | confirmed
 136 |      45 | redirect   | 10.10.10.190 |       | confirmed
 137 |      45 | rate-limit | 1000         |       | confirmed
 138 |      45 | accept     |              |       | confirmed
(4 rows)
```

Obr. 4.4: Tabuľka flowspec_routes použitá pre udržovanie flowspec akcií

V tretej tabuľke sú hodnoty pre jednotlivé cesty a hodnota *Share*, ktorá je vypočítaná ako pomer prevádzky na tejto ceste, k celkovej prevádzke pre chránený segment. Pravidlá sú zložené maximálne z piatich položiek, pričom vždy musí byť jednoznačne určená minimálne cieľová adresa. Status v tejto tabuľke označuje, či sa má daná hodnota započítať do tvorby flowspec pravidiel. Ukážka záznamu o toku v databázy je na obrázku 4.5.

```
iad=> select * from flowspec_matches where route_id in
iad-> ( select id from flowspec_routes where rule_id = 45 ) order by route_id;
 id  | route_id |       item       |      value      |  share   |   state
-----+----------+------------------+-----------------+----------+-----------
 438 |      135 | destination      | 10.20.20.25/32 | 0.451111 | confirmed
 440 |      135 | destination-port | =45023          | 0.451111 | disabled
 441 |      135 | protocol         | tcp             | 0.451111 | confirmed
 439 |      135 | source           | 10.31.5.2/32    | 0.451111 | confirmed
 443 |      136 | source           | 10.31.7.2/32    |     0.02 | disabled
 442 |      136 | destination      | 10.20.20.25/32 |     0.02 | disabled
 445 |      136 | protocol         | tcp             |     0.02 | confirmed
 444 |      136 | destination-port | =45023          |     0.02 | disabled
 449 |      137 | protocol         | tcp             |      0.4 | confirmed
 446 |      137 | destination      | 10.20.20.25/32 |      0.4 | disabled
 447 |      137 | source           | 10.31.10.2/32   |      0.4 | confirmed
 448 |      137 | destination-port | =45023          |      0.4 | confirmed
 452 |      138 | destination-port | =45023          |  0.11242 | disabled
 451 |      138 | source           | 10.31.4.2/32    |  0.11242 | disabled
 450 |      138 | destination      | 10.20.20.25/32 |  0.11242 | confirmed
 453 |      138 | protocol         | tcp             |  0.11242 | disabled
(16 rows)
```

Obr. 4.5: Tabuľka flowspec_matches použitá pre udržovanie kritérií pre flowspec

4.2 Výpočet prahov a detekcia útokov

Detekcia útokov bude prebiehať v tejto aplikácii formou porovnávania objemu sieťovej prevádzky s vypočítanou prahovou hodnotou. Štatistiky o sieťovej prevádzke sú uložené v RRD súboroch a tvorí sa baseline. Z týchto RRD súborov je možné vygenerovať, za pomoci nástroja *rrdtool fetch*, hodnoty priemernej sieťovej prevádzky za sekundu. Táto hodnota sa používa na výpočet prahov pre porovnanie. Priemerné hodnoty objemu prevádzky za sekundu sa násobia konštantami, manuálne zadanými podľa znalostí štandardnej sieťovej prevádzky. Ak aktuálne spracovávaná hodnota počtu paketov za sekundu alebo počtu bytov za sekundu presiahne vypočítaný prah, je detekovaná anomália.

4.2.1 Výpočet podielu zložiek

Priemerný počet paketov za sekundu (pps) a bytov za sekundu (bps) za dlhší časový úsek (zvyčajne týždeň) sa získava z baseline uložených v RRD. Tieto hodnoty sa násobia užívateľom definovanými konštantami a konštantami pre zložky prevádzky, ktoré sú v tabuľke 4.1. Užívateľ môže definovať, aké percentuálne zvýšenie prevádzky je prijateľné pre jeho sieť. Vypočítané prahové hodnoty sa ukladajú do ďalších RRD súborov, pre neskoršiu prípadnú vizualizáciu. V prípade pravidelne počítaných prahových hodnotách, je možné používať okrem prahu pre útok, aj hodnotu pre podozrenie z útoku. Prah útoku je vždy väčší než pre podozrenie o pomernú hodnotu k množstvu sieťovej prevádzky.

Typ detekcie	ICMP	UDP	TCP	TCP SYN	TCP SYN&ACK	TCP ACK&FIN	TCP RST
Veľkosť paketu	65	300	64	64	64	64	60
Podiel na prevádzke	10%	30%	60%	10%	1%	2%	1%

Tabuľka 4.1: Konštanty použité pre výpočet prahových hodnôt

4.2.2 Detekcia útoku z NetFlow

Útoky DoS sú anomálie v sieti, ktoré často majú jednoznačnú signatúru pomocou ktorej ich vieme rozlíšiť. Jednou z možností detekcie útoku je nastavenie prahu množstva a objemu sieťovej prevádzky, ktorú ešte považujeme za bežnú. Ak sa zvýši počet tokov alebo paketov nad túto hranicu, označíme to ako anomáliu (v tomto prípade DoS útok). Samostatne táto technika na spoľahlivú detekciu nestačí, pretože by to mohlo spôsobiť viaceré falošne pozitívne detekcie. Napríklad by túto hodnotu mohla prekročiť aj bežná prevádzka v rušných hodinách a taktiež by sa tento prah musel upravovať po pripojení nových služieb alebo užívateľov. Lepšie riešenie je použiť adaptívny prah, ktorý by sa učil a prispôsoboval prahové hodnoty, podľa aktivity na sieti za určitý časový úsek. Pre ukladanie a ľahké vymazávanie dát po určitom časovom období je vhodné použiť Round-Robin databázu, ktorá automaticky po vopred zadanom čase odstraňuje staré dáta.

Manuálny prah

Systém generuje jednu baseline pre maximálnu hodnotu (peak) prichádzajúcich paketov za sekundu (pps). Užívateľ si môže definovať prahovú hodnotu Treshold (Th) v percentách ako upravenie spúšťača útoku. Systém porovnáva množstvo prichádzajúcich paketov, baseline a definovanú prahovú hodnotu. Útok je detekovaný, ak počet prichádzajúcich paketov za sekundu je väčší ako hodnota baseline násobená Th.

Adaptívny prah

Prahové hodnoty sú počítané vzhľadom na charakteristiku prichádzajúcej sieťovej prevádzky. Tieto hodnoty sa postupom času menia v závislosti na maximálnom množstve prenesených dát a paketov za časový úsek stanovený užívateľom. Pre výpočet adaptívneho prahu sa používajú len dáta z časových úsekov, kedy nebol na chránenom segmente detegovaný útok. Pre každý typ útoku, sa vypočítajú dve prahové hodnoty. Jedna hodnota pre útok a druhá pre podozrenie z útoku. Systém porovnáva množstvo prichádzajúcich paketov, s týmito prahovými hodnotami a spúšťa akcie po detegovaní útoku, respektíve akcie pre podozrenie z útoku, ak prevádzka prekročí len prah pre podozrenie. Defender vkladá

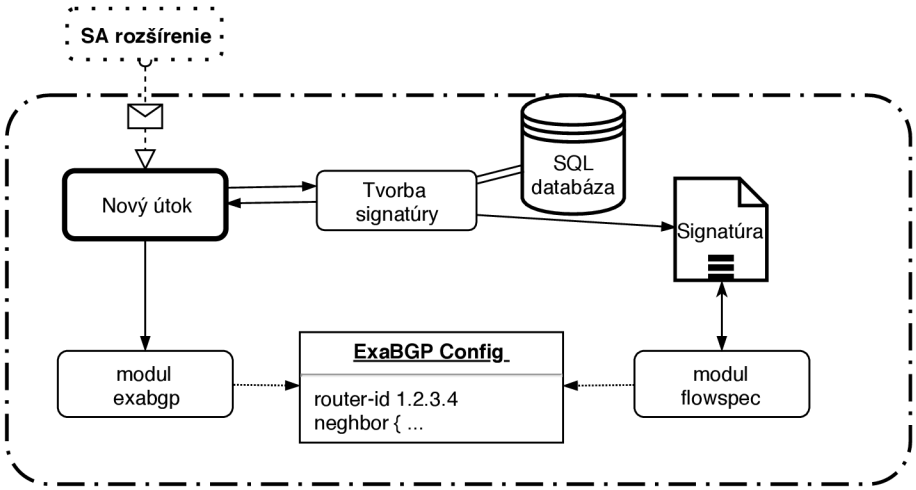
hodnoty do RRD podľa tradičných typov útokov: TCP flood, UDP flood, ICMP flood, TCP Syn pakety, TCP RST pakety, TCP ACK FIN packety a TCP SYN ACK pakety.

Statická metóda

Defender porovnáva množstvo prichádzajúcich paketov (Ip) a odchádzajúcich paketov (Op) a užívateľom definovaný Treshold (Th) v percentách. Útok je detekovaný, ak počet prichádzajúcich paketov je väčší ako počet odchádzajúcich paketov násobený Th.

4.3 Zmiernenie útoku

Zmierňovaním útoku sa rozumie technika používana pre odstránenie škodlivej prevádzky a obmedzenie vplyvu útoku na bežný chod siete. Pre zmiernenie útoku je potrebné zistiť čo najpresnejšie informácie o typu útoku a nájsť spoločné rysy dominujúce v útoku. Po zistení vlastností paketov tvoriacich útok, je možné ich identifikovať a zo sieťovej prevádzky presmerovať a odstrániť. Na odstránenie škodlivých paketov sa zvyčajne používajú špecializované zariadenie na hĺbkovú kontrolu dátovej časti paketu (scrubbing centrá). Tieto zariadenia sú veľmi nákladné a poskytovatelia ISP, ktorý sa starajú o sieťové linky s priepustnosťou rádovo desiatok Gb za sekundu, by potrebovali veľké množstvo týchto zariadení. Alternatívou je zahodenie identifikovaných paketov priamo na smerovači, ešte pred dosiahnutím cieľa útoku. Pre túto metódu je dôležité správne nastaviť smerovače, aby odstránili len škodlivé pakety. Keďže manuálne nastavovanie smerovačov je zdĺhavé a sú potrebné znalosti pre správu smerovačov, je ideálny postup tieto akcie automatizovať. Automatizácia sa dá dosiahnuť vytvorením rozšírenia pre DDoS Defender (Obrázok 4.6).



Obr. 4.6: Rozšírenie pre DDoS Defender, pre generovanie flowspec pravidiel a komunikácie so smerovačmi pomocou ExaBGP.

4.3.1 Výpočet signatúry

Po detekovaní útoku vieme na ktorý segment sa útočí, no táto vedomosť nám nestačí na ochranu siete pred útokom. Zahodenie všetkej podozrivej prevádzky by klientov na určitú dobu úplne odpojilo od Internetu a teda by bola aplikácia, poskytovaná služba či webovská

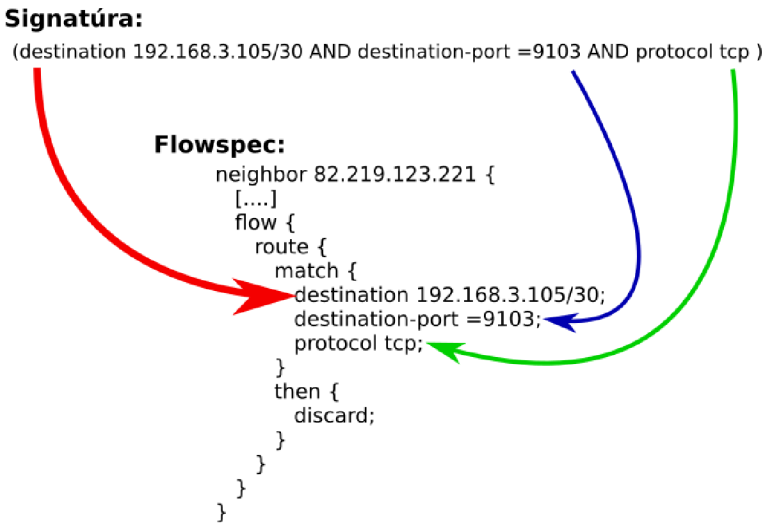
stránka prakticky nepoužiteľná. Preto je nutné zo získaných dát čo najpresnejšie určiť jasné informácie odkiaľ a kam je útok vedený. Na základe týchto získaných informácií by sme následne zabránili prístupu iba skutočne škodlivej prevádzke a ostatnú prevádzku aplikovaním pravidiel neovplyvnili.

Signatúra útoku sa tvorí konkatenáciou pätice hodnôt značiacich tok, pričom cieľová adresa je z chráneného rozsahu adries, alebo je súčasťou chráneného autonómneho systému. Nie vždy sa do signatúry vkladajú všetky položky z pätice uloženej v NetFlow zázname. V prípade DDoS útokov, pri ktorých útočníci útočia z viacerých sietí a každý na iný port, musela by signatúra zahrnúť veľa portov zároveň a filtrovanie by bolo časovo náročnejšie. Preto sa tieto položky zo signatúry vynechávajú a zostáva napríklad iba cieľová adresa a protokol.

4.3.2 Vytvorenie a aplikovanie flowspec pravidiel

Flowsspec pravidlo sa vytvára zo signatúry a akcie na zmiernenie útoku. Pre program ExaBGP sa vytvára súbor formátu JSON, do ktorého sa vkladajú flowspec pravidlá. Tvorba flowspec pravidiel je sprostredkovaná pomocou rozšírenia pre Defender v module *flowspec*. Modul *flowspec* spolupracuje s modulom *exabgp* na generovaní konfiguračného súboru pre presmerovanie. Tento postup je možné vidieť na obrázku 4.6. Po detekcii útoku sa načítajú pravidlá spĺňajúce podmienku pre útok a postupne sa prevádzajú na formát JSON.

Konfiguračný súbor pre ExaBGP obsahuje na začiatku, v rámci autonómneho systému označenú ako *router-id*, jednoznačnú identifikáciu smerovača. Tradične sa na označenie *router-id* používa IP adresa smerovača. IP adresa sa primárne vyberá podľa sieťového rozhrania, na ktorom naslúcha smerovač pre BGP komunikáciu alebo podľa loopback adresy na smerovači. Nasleduje identifikácia susedného smerovača, kam chceme flowspec pravidlá propagovať. Sused je identifikovaný pomocou *router-id*, *peer-as* a voliteľne, podľa adresy na sieťovom interface cez ktorú sa naväzuje spojenie *local-address*. Ak ide o eBGP spojenie, tak je nutné vyplniť lokálne číslo AS *local-as*. Po identifikácii suseda je možné pridávať flowspec pravidlá uzavreté v zložených zátvorkách, ako je možné vidieť na obrázku 4.7.



Obr. 4.7: Príklad vypočítanej signatúry a jej prepis signatúry do formátu, ktorý podporuje ExaBGP

Po vložení všetkých flowspec pravidiel, je nutné prekopírovať dočasný súbor namiesto konfiguračného súboru ExaBGP a poslať signál *SIGUSR2* na ExaBGP soket, pre znovu načítanie konfiguračného súboru. Ak je konfiguračný súbor vygenerovaný správne, stav spojenia so susedom zostane v stave *ESTABLISHED*. O následné čiastkové úpravy ciest na smerovačoch sa stará aplikácia ExaBGP. Všetky informácie o aplikovaných flowspec pravidlách sú uložené v databáze. Pre odstránenie pravidla stačí nastaviť príznak pravidla na *disabled* a znovu vygenerovať konfiguračný súbor pre ExaBGP.

Kapitola 5

Implementácia

V tejto kapitole je popísaná implementácia rozšírenia pre Flowmon kolektor o detekciu DoS a DDoS útokov v reálnom čase a tvorbu flowspec pravidiel. V prvom rade sa musí dbať na kompatibilitu so súčasnou architektúrou Flowmon kolektoru, ako aj stávajúceho rozšírenia *DDoS Defender*. I keď v požiadavkách na rozšírenie pre okamžitú detekciu útokov nie sú špecifikované technológie, ktoré majú byť použité, stále musí program spĺňať kritéria firmy. Preto program:

- musí byť spustiteľný na systéme CentOS 7;
- nesmie obsahovať úniky pamäte;
- štýl písania kódu je v súlade so zaužívaným štýlom;
- pri chybe nemôže ovplyvniť beh ostatných bežiacich procesov.

Aby pri neočakávanej chybe modul neobmedzil iné bežiace procesy som docielil tak, že som čo najviac oddelil prácu s NetFlow záznamami od stávajúceho spracovávania pomocou *streamovej architektúry*. Moje riešenie je založené na dvoch častiach, pričom prvá časť (*SA rozšírenie*) je samostatne spustiteľná aplikácia napísaná v C++17 a druhá časť ako modul pre Perl 5 (*ExaBGP modul*).

SA rozšírenie sa stará o načítavanie dát zo streamovej architektúry a detekciu útokov. Mimo to vytvára baseline sieťovej prevádzky a výpočet prahových hodnôt pre detekciu útoku. Po detekcii útoku odošle správu pre *ExaBGP modul* na zmiernenie útoku.

ExaBGP modul je súčasťou DDoS Defendera. Keď DDoS Defender dostane správu o novom útoku, vyhodnotí podľa nastavenia chráneného segmentu (uloženého v PostgreSQL databázy), ako sa má zmierniť útok. Ak je nastavené zmiernenie útoku pomocou flowspec, DDoS Defender zavolá vzdialenú funkciu z *ExaBGP modulu* na vytvorenie BGP presmerovania. *ExaBGP modul* sú dve rozšírenia písané ako balíky pre Perl.

Prvý balík *redirectionExaBGP* obsahuje súbor funkcií na vytvorenie konfiguračného súboru pre naviazanie komunikácie aplikácie *ExaBGP* s BGP smerovačmi (definovanými užívateľom), vo formáte vhodnom pre program *ExaBGP*. Po vytvorení súboru a zapísaní základných identifikátorov BGP smerovačov, zavolá balík *flowspec* pre doplnenie flowspec pravidiel. Tento balík vypočíta flowspec pravidlá zo signatúry a vloží ich do súboru na pripravené miesto.

5.1 Načítanie dát zo streamovej architektúry

Dáta zo streamovej architektúry sú predávané do *SA rozšírenia* pomocou vyrovnávacej pamäte (buffer). *Xfcapd* uloží práve spracovávané záznamy do vyrovnávacej pamäti, ktorá je realizovaná ako FIFO fronta. Tento buffer môže fungovať v dvoch režimoch: v *blokujúcom* - ak sa naplní vyrovnávacia pamäť určená pre kopírovanie záznamov, tak streamova architektúra čaká na uvoľnenie kapacity alebo v *neblokujúcom* - kde pokiaľ príde k zaplneniu bufferu, tak sa ďalšie položky zahadzujú. V našom prípade, keďže nemáme obmedziť normálny chod Flowmon kolektoru, som zvolil neblokujúci režim.

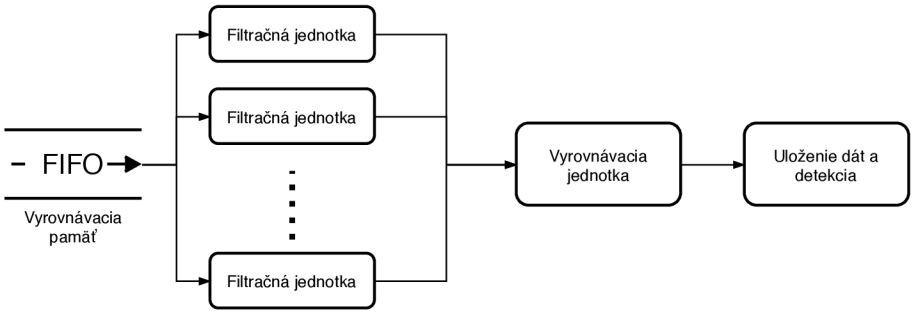
Do bufferu sa ukladajú celé NetFlow záznamy, prevedené do formátu *Master record*. Jedná sa o jednu veľkú štruktúru, obsahujúcu všetky položky, ktoré boli prijaté v NetFlow toku. Je popísaná štruktúrou „extension_map_t“, pričom jej veľkosť nie je jednoznačne známa. Veľkosť sa dynamicky mení podľa toho, ako sa časom pridávajú nové položky pre spracovanie streamovou architektúrou. Každý *Master record* získaný z vyrovnávacej pamäte, je pridelený jednej z filtračných jednotiek podľa času stráveného vo fronte.

5.2 Filtračná jednotka

Filtračná jednotka je implementovaná ako odľahčená verzia filtračnej jednotky v aplikácii xfcapd, prepísaná podľa nových štandardov C++17. Filter je načítaný zo súborov pre vstupný a výstupný filter, uložených v koreňovej zložke pre chránený segment. Filter je vytvorený rovnakým spôsobom ako filter pre aplikáciu *nfdump* podľa definície chráneného segmentu.

Filtrovanie záznamov je náročné na výkon, preto sa používa viacero filtračných jednotiek. Tieto jednotky načítajú *Master record* priamo zo zdielanej pamäte (vytiahnu prvý záznam v poradí). Pre každý filter vytvorený podľa chránených segmentov sa vykoná porovnanie v nasledujúcom poradí:

- aplikuje sa filter pre získanie pätice na *Master record*;
- ak sa našla zhoda medzi filtrom a *Master record*, vyplnia sa L3 a L4 položky do výstupnej štruktúry pre vyrovnávaciu jednotku;
- túto výstupnú štruktúru odošle do FIFO fronty pre vyrovnávaciu jednotku.



Obr. 5.1: Načítanie dát z vyrovnávacej pamäte filtračnými jednotkami a následné spracovanie vyrovnávacou jednotkou

5.3 Vyrovnávacia jednotka

Vyrovnávacia jednotka zbiera pred-spracované dáta z filtračných jednotiek a zaisťuje vytváranie zoznamu pätíc a sieťových štatistík (čítače). Čítač obsahuje počet prenesených paketov, tokov a bytov. Tento zoznam je tvorený za behu (on-the-fly) z dát prijímaných z filtračných jednotiek. Pre každý chránený segment sú vytvorené vlastné zoznamy a vlastné čítače, podľa kanálov pre typy útokov (napr. TCP, UDP, SYN ACK). Ak je v metadátach z filtračnej jednotky záznam ktorý nie je v zozname, tak sa vloží do zoznamu, inak len aktualizujú hodnoty čítačov.

Vyrovnávacia jednotka si udržuje záznamy 30 sekúnd, pričom každý záznam obsahuje časovú známku, kedy bol záznam naposledy aktualizovaný a koľko dát sa pridalo. Mimo to sa udržuje história aktualizácie hodnôt čítačov so sekundovou granularitou (história má maximálne 30 položiek). Podľa histórie aktualizácie čítačov, sa po každom pridaní novej hodnoty do záznamu o histórii (každú sekundu), dekrementujú čítače o hodnotu aktualizácie dát v čase t-30 získanú z histórie. Ak je hodnota čítača menšia ako 1, záznam sa vymaže zo zoznamu.

5.3.1 Ukladanie štatistík do RRD databázy

Vyrovnávacia jednotka má samostatné vlákno pre ukladanie štatistík do RRD súborov. Každých 30 sekúnd sa pre všetky kanály chránených segmentov vezmú hodnoty čítačov (pakety, toky a byty) a zapíšu sa do RRD súborov. RRD súbory sú nazvané podľa typu detegovaneho útoku (napr. TCP SYN -> *tcp_s-baseline.rrd*, ICMP flood -> *icmp-baseline.rrd*). Týmto zápisom vzniká baseline sieťovej prevádzky, ktorá sa neskôr využije pre výpočet prahových hodnôt. Do RRD súborov sa ukladajú hodnoty čítačov pomocou knižnice (*librrd*). Knižnica je importovaná pomocou „extern“ z jazyka C, pretože oficiálna alternatíva napísaná v jazyku C++ nie je.

5.3.2 Detekcia

Podľa priemeru množstva prenesených paketov za sekundu násobenú konštantou (threshold) sa vypočítavajú prahové hodnoty pre metódy detekcie útokov popísané v kapitole 4.2.2. Výpočet je realizovaný, pre počet paketov z každého čítača chránených segmentov. Pre získanie informácii o počtu prenesených paketov za určité časové obdobie, sa používa RRD databáza. Pre získanie priemerného počtu paketov prevádzky sa však nemôže použiť celý užívateľom definovaný interval, no len úseky kde nebol detegovaný útok. Toho sa dá dosiahnuť pomocou zreťazenia príkazov „rrdtool fetch“ s časovými úsekmi medzi útokmi.

Ku každému RRD súboru so štatistikami, existuje aj RRD súbor obsahujúci prahové hodnoty pre detekciu útokov (napr. TCP SYN&ACK -> *tcp_sa.rrd*). Výpočet prahových hodnôt prebieha vždy po úprave baseline, čiže každých 30 sekúnd. Po zápise štatistík sieťovej prevádzky do RRD sa vypočítajú prahové hodnoty pre metódy detekcie určené nastavením segmentu. Metódy výpočtu prahových hodnôt sú identické ako v sekcii 4.2.

Počas behu vyrovnávacej jednotky sa každú sekundu porovnávajú počty paketov v čítačoch chránených segmentov a porovnávajú sa s aktuálnymi prahovými hodnotami podľa typu detekcie priradenej ku chránenému segmentu. Ak počet paketov o ktorý bol za poslednú sekundu inkrementovaný čítač presiahne prahovú hodnotu, je detegovaný útok.

5.3.3 Vkladanie záznamov do SQL databázy

Po detekcii nového útoku sa vytvorí nový záznam v PostgreSQL databázy v tabuľke *attacks*, kde sa zapíšu informácie o detekcii a aktuálny čas, ako čas začiatku útoku. Ak v SQL databázy v tabuľke *attacks* nie je informácia o prebiehajúcom útoku, zapíšu sa záznamy do SQL databázy a do DDoS Defenderu sa odošle cez unixový socket informácia o novom útoku. V prípade že už prebieha útok na danom segmente, aktualizuje len status útoku na *Detected*.

Mimo zápisu do tabuľky *attacks*, sa vytvoria záznamy v tabuľkách *flowspec_rules*, *flowspec_routes* a *flowspec_matches*. Do tabuľky *flowspec_rules* sa vloží číslo útoku, číslo segmentu a progres sa nastaví na „1/4“ (nový záznam). Do tabuľky *flowspec_rules* sa vloží toľko riadkov, koľko je záznamov v zozname pre segment pätíc a do tabuľky *flowspec_matches* sa vložia pätice.

5.4 Tvorba signatúry

Signatúra je vytvorená pomocou konkatenácie informácii z SQL databázy, kde medzi uzátvorkovanými pravidlami je vložená spojka „OR“. Informácie z SQL databázy sa získajú spojeným dotazom na tabuľky *flowspec_routes* a *flowspec_matches*. Z tabuliek sa vyberú len potvrdené záznamy, ktoré majú hodnotu „share“ dostatočne vysokú, aby tvorili signifikantnú časť prevádzky. V mojom prípade som použil pre porovnanie hodnotu 10%. Táto hodnota však môže byť zmenená užívateľom, aby sa lepšie prispôsobila prevádzke na monitorovanej sieti. Zároveň sa vyberú len záznamy, ktoré majú v stĺpci „state“ hodnotu „confirmed“. Táto hodnota udáva v prípade kritéria pre filtrovanie podla pätice, či sa má kritérium použiť v tvorbe signatúr.

5.5 Úprava databázy pre generovanie flowspec

Pre účely generovania plnohodnotných flowspec pravidiel (kritéria + akcie) je nutné upraviť tabuľky z ktorých sa flowspec pravidlá generujú. Postup úpravy tabuliek je uvedený v tabuľke *flowspec_rules* v stĺpci „progress“:

- **1/4** - stav po vložení nových záznamov z vyrovnávacej jednotky do databázy;
- **2/4** - podľa BGP smerovača prideleného k segmentu, sa načíta štandardná flowspec akcia a uloží sa spolu s hodnotou do tabuľky *flowspec_routes*;
- **3/4** - podľa globálneho nastavenia sa potvrdia alebo nepotvrdia zdrojové IP adresy pre výpočet flowspec;
- **4/4** - flowspec pravidlá sú pripravené pre načítanie.

5.6 Prevod pravidiel do JSON formátu

Pre účely bezpečného zapisovania do súboru a aby sa predišlo k načítaniu neúplného a teda nevalidného konfiguračného súboru pre ExaBGP, som sa rozhodol zapisovať najskôr do dočasného súboru. Vytvorím nový súbor, nastavím správne práva, aby ho mohol ExaBGP čítať a získam deskriptor súboru, cez ktorý budem následne pristupovať ku koncu súboru na pripisovanie.

Ako prvé program zapíše označenie *router-id*, z ktorého chce vysielať nové BGP cesty na smerovače. Následne prechádza zoznam smerovačov a pre každý zapíše najskôr nutné informácie o susedovi (viď. kapitola 4.3.2). Po zapísaní všetkých dôležitých údajov pre naviazanie spojenia, sa zavolá procedúra z balíku pre flowspec, ktorá prevádza výstup z SQL dotazu na formát JSON.

SQL dotaz spojí záznamy z tabuliek *flowspec_routes* a *flowspec_matches* do novej tabuľky (obrázok 5.2), v ktorej sú len relevantné informácie pre vytvorenie flowspec pravidiel. Postupne prechádza riadky s rovnakou hodnotou „route_id“, z ktorých načíta kritéria z „item“ nasledované hodnotou „value“. Po pridaní všetkých kritérií jedného flowspec pravidla vloží riadok s akciou nasledovaný jeho hodnotou (ak nejaká je). Týmto spôsobom postupne spracuje všetky pravidlá pre všetky BGP smerovače definované pre DDoS Defender.

```
 route_id |       item       |     value      |   action   |    option
----------+------------------+----------------+------------+--------------
 135      | destination      | 10.20.20.25/32 | mark       | 1
 135      | protocol         | tcp            | mark       | 1
 135      | source           | 10.31.5.2/32   | mark       | 1
 136      | protocol         | tcp            | redirect   | 10.10.10.190
 137      | destination-port | =45023         | rate-limit | 1000
 137      | protocol         | tcp            | rate-limit | 1000
 137      | source           | 10.31.10.2/32  | rate-limit | 1000
 138      | destination      | 10.20.20.25/32 | accept     |
(8 rows)
```

Obr. 5.2: Tabuľka vytvorená na základe sql dotazu v prílohe [2]

Ak je pre BGP smerovač definovaný komunitný reťazec, tak sa vloží do každého flowspec pravidla za akciu. Komunitný reťazec môže byť buď vo formáte „community“ alebo „extended-community“. Tu som narazil na problém, že niektoré rozšírené komunitné reťazce majú viacej možností zápisu, pričom ExaBGP vždy posiela len jeden typ. Napríklad rozšírený reťazec *target*, môže použiť kombináciu IPV4:AS, ale aj AS:AS a AS32:AS. Preto som musel prevádzať všetky rozšírené komunitné reťazce do hexadecimálneho formátu, ktorý sa odosiela presne tak, ako je vložený do konfiguračného súboru.

Kapitola 6

Testovanie

Pred nasadením aplikácie do komerčného prostredia je nutné dôkladné testovanie. Aplikácia nesmie ohroziť plynulý beh ostatných súčastí Flowmon kolektora ako ani plynulý beh sieťovej prevádzky na nechránených segmentoch. Je potrebné dbať na správne generovanie flowspec pravidiel, pretože chybné pravidlo distribuované na okrajový smerovač v siete, môže zabrániť prístup do celej siete a spôsobiť tým obrovské škody.

6.1 Testovacie prostredie

Pre testovanie rozšírenia som navrhol testovacie laboratórium. Laboratórium beží na servere, na ktorom je inštalovaný *VMware ESXi hypervisor*. Hypervizor sa stará o distribúciu prostriedkov pre virtuálne prístroje, inštalované v ESXi.

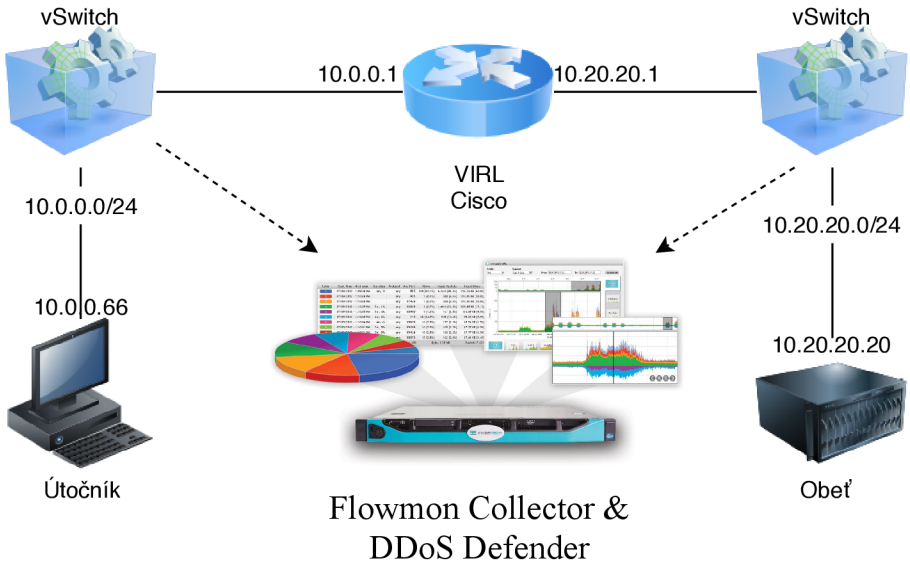
Laboratórium sa skladá z virtuálneho Flowmon kolektora, ktorý je doplnený o exportér s monitorovacími portami. Ďalej sú súčasťou laboratória dva virtuálne systémy linuxovej distribúcie *Kali linux*. Pre testovanie flowspec pravidiel, je laboratórium doplnené o virtualizačný nástroj *VIRL* vyvinutý firmou Cisco, ktorý poskytuje možnosť nasadiť virtuálne smerovače od firmy Cisco pre testovanie, bez nutnosti drahých investícii. Virtuálne prístroje sú prepojené pomocou *vSwitch*, ktoré pracujú v promiskuitnom móde, pre možnosť zberu všetkých dát ktoré cez ne prechádzajú. K týmto virtuálnym prepínačom sú pripojené monitorovacie porty Flowmon kolektoru. Celé zapojenie je ukázané na obrázku 6.1.

6.1.1 Obeť

Pre zníženie množstva spotrebovaných hardvérových prostriedkov na virtualizáciu viacerých cieľov útoku, som pridelil zariadeniu *Victim* viacero sieťových rozhraní. Okrem portu pre správu, obsahuje *Victim* ďalších 9 portov, ktoré sú všetky pripojené k virtuálnemu prepínaču. Každé toto pripojené rozhranie obsahuje dve IPv4 a jednu IPv6 adresu, z podsiete „10.20.20.0/27“ a IPv6 podsiete „FD20::/64“.

6.1.2 Útočník

Ako generátor štandardnej sieťovej prevádzky, som použil volne dostupný PCAP súbor z konferencie *Hackaton*. Nevyrovná sa síce reálnym dátam zo siete poskytovateľov ISP, no 5 minútový záznam paketov s dátovou časťou na chrbticovej sieti napr. *UPC* je ohromne veľký pre naše použitie. Pre správne smerovanie je potrebné zmeniť cieľovú adresu paketov, ktoré sú preposielané z tohoto PCAP súboru. K tomuto účelu som využíval nástroj



Obr. 6.1: Virtuálne laboratórium pre účely testovania monitorovania NetFlow, detekcie útokov a flowspec pravidiel.

tcpreplay-edit, ktorý dokáže odosielať pakety načítané z PCAP súboru a za behu meniť ich cieľové adresy na iný rozsah adries. Program *tcpreplay-edit* bol spustený počas celej doby testovania na pozadí s použitím *screen*. V mojom prípade som používal príkaz v tomto formáte :

```
# tcpreplay-edit -i eth3 -q -l 0 -x 2 –dstipmap='0.0.0.0/0:10.20.20.20/27' ./ctf_dc17.pcap075 &
```

Pre účely generovania útokov, som používal aplikácie, ktoré sú súčasťou distribúcie *Kali linux*. Primárne sa jednalo o nástroje: „hping3“, „t50“ a pre testovanie IPv6 „atk6-thcsyn6“ (z balíka *thc6*). Používané príkazy, ktoré som najčastejšie využíval sú:

```
50k pps ICMP: # hping3 –1 –w 64 –d 20 –p 80 ––faster 10.20.20.20
50k pps TCP syn–ack: # hping3 –AS –w 64 –d 20 –p 80 ––faster 10.20.20.20
50k pps TCP fin–ack: # hping3 –AF –w 64 –d 20 –p 80 ––faster 10.20.20.20
100k+ pps TCP : # hping3 –w 64 –d 20 –p 80 ––flood 10.20.20.20
max pps:      # t50 10.20.20.20 ––flood ––turbo ––protocol TCP –AS
on IPv6 :     # atk6–thcsyn6 –S –p 666 eth3 fd20::20 x
```

6.1.3 Virtuálne smerovače

Pre virtualizáciu smerovačov, som využíval nástroj *Virtual Internet Routing Lab* (VIRL). Jedná sa o virtualizačný nástroj na vytváranie topológii sietí, ktorý podľa návrhu topológie, nasadí sieťové prvky. Pred nasadením smerovačov a prepínačov vygeneruje základné nastavenie pre smerovanie. V rámci nastavení je možné vytvoriť na každom sieťovom prvku správcovský port, ktorý je dostupný cez SSH do vonkajšej siete. Návrh topológie a zmena nastavenia sa dajú upraviť pomocou nástroja *VM Maestro*. Následne je možné nechať celú topológiu nasadiť, pričom jednotlivé nasadené prvky sa správajú ako reálne fyzické stroje.

Pre moje účely som využíval zvyčajne smerovač *Cisco CSR1000v*, ktorý má podporu flowspec. Pred prvým použitím bolo nutné povoliť na tomto smerovači flowspec pre IPv4 a IPv6. Následne som musel nastaviť ako BGP suseda IP adresu portu pre správu z Flow-

mon kolektoru. Keďže sa jedná o virtuálnu sieť do ktorej pristupujem z vonkajšej siete cez port na správu (port na správu je súčasťou VRF[1] *Mgmt-intf*), je nutné nastaviť všetku komunikáciu s týmto smerovačom cez VRF. Následne je dôležité aj sledovať všetky aplikovania pravidiel, či sú súčasťou VRF. Ak však chceme presmerovať sieťovú prevádzku, ktorá nie je súčasťou VRF, je dôležité na smerovači ešte nastaviť exportovanie prijatých pravidieľ do globálnej smerovacej tabuľky a medzi globálne flowspec pravidlá.

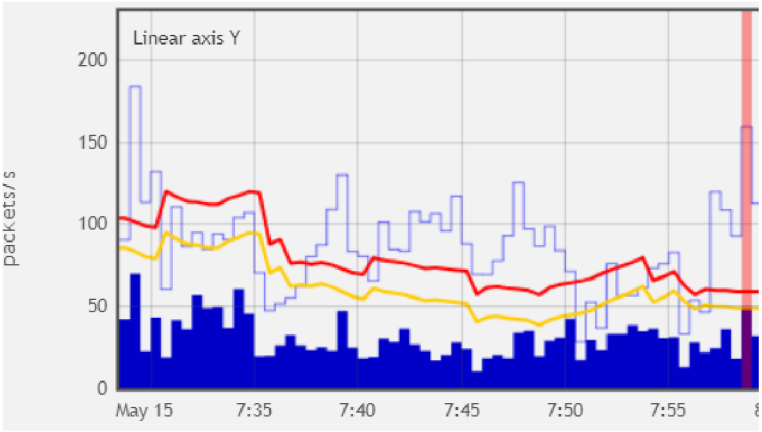
Výhoda nasadzovania smerovačov cez VIRL je, že sa dá extrahovať konfigurácia a preto nie je problém simuláciu dočasne zastaviť, upraviť (vymeniť sieťové prvky za iné) a spustiť znovu. Nanešťastie tieto nasadené zariadenia sa nasadzujú s obmedzenou licenciou, takže prepustia maximálne 1 Mbit za sekundu. Pre naše účely je to postačujúce, no pre výkonnostné testy bude nutné nasadiť plnú verziu smerovačov.

6.1.4 Virtuálny Flowmon kolektor

Virtuálny Flowmon kolektor je mierne upravený oproti hardwardovému. Podstatnou zmenou je, že okrem kolektoru, obsahuje aj 4 monitorovacie rozhrania pre exportovanie tokov. Preto nie je potrebný externá sonda, či nastavovanie exportu tokov zo smerovača. Po pripojení monitorovacích portov na virtuálne prepínače, možeme monitorovať sieťovú prevádzku pred vstupom a po výstupe zo smerovača. Týmto spôsobom je možné skontrolovať, či nasadené flowspec pravidlá pracujú tak, ako očakávame. Pre účely DDoS Defendera, je veľmi vhodné nastaviť pri exportovaní dát, aktívny a neaktívny timeout na čo najnižšie hodnoty.

6.2 Vypĺňanie baseline a prahových hodnôt

Na obrázku 6.2 je ukážka grafu, v ktorom sú spojené baseline prevádzky s prahovými hodnotami. Tmavo modrou vyplnenou farbou je zobrazená zložka prevádzky, ktorá reprezentuje množstvo TCP paketov, ktoré mali nastavený príznaky ACK a FIN. Modrou farbou no bez výplne je označená celková sieťová prevádzka, na chránenom segmente, ktorá mierne ovplyvňuje vytváranie prahových hodnôt. Žltou farbou je značený prah pre podozrenie na útok a červenou je útok. Prahové hodnoty sa zvyčajne nemenia tak náhle, no pre účely testovania, som nastavil učiace obdobie len na 5 minút. Zvyčajná hodnota učiaceho obdobia je 7 dní.



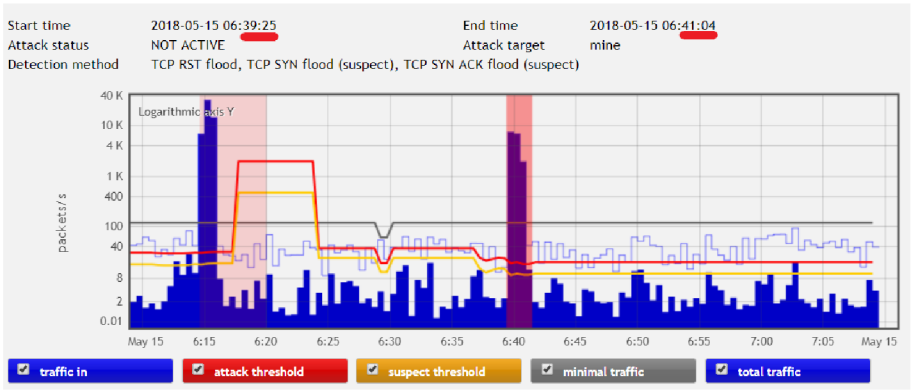
Obr. 6.2: Ukážka adaptívnej baseline s učiacim obdobím nastaveným na 5 minút

[1] virtual routing and forwarding

6.3 Detekcia a ochrana proti útokom

Pre testovanie detekcie útoku, som využil laboratórne podmienky. Sieť v mojom laboratóriu som úplne odtienil od vonkajšej siete, pretože ak by prišlo k chybnému presmerovaniu, mohol by som zahltiť celú firemnú sieť.

Pre jeden z testov (ktorého ukážka je na obr. 6.3) som použil útok typu *TCP RST*, tiež zvaný „forget TCP resets“. Ako je vidieť, počet generovaných paketov výrazne prekročil obe prahové hodnoty (suspect aj attack), takže sa detegoval útok. Útok sa detegoval za cca 2 sekundy od spustenia, čo keďže ide o RST pakety a teda sa exportujú takmer okamžite, pripisujem virtuálnemu prostrediu.



Obr. 6.3: Ukážka detekcie útoku typu TCP RST s využitím *SA rozšírenia*

6.4 Kontrola na smerovačoch

Po začatí mitigácie na segmente, kde je pripojený smerovač s podporou flowspec, sa v dialógu (*Action status*) vypíšu aplikované pravidlá. Tieto pravidlá musia byť zapísané aj v súbore pre aplikáciu *ExaBGP*, ktorý sa nachádza na Flowmon kolektore v adresáre „/opt/exabgp/config/“.

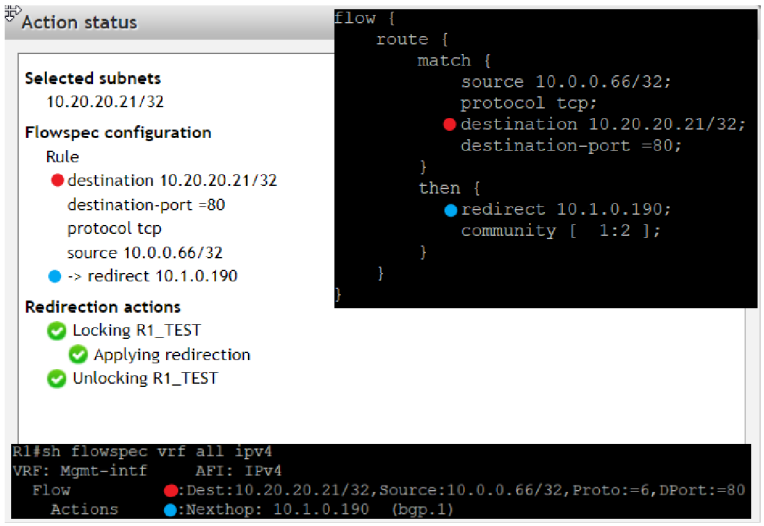
Po pripojení na smerovač, kam sa aplikovali pravidlá, si vypíšem flowspec pravidlá. Ak ku smerovaču nepristupuje nikto iný, tak by tam mali byť iba pravidlá, nastavené pomocou DDoS Defendera. V mojom prípade, keďže pracujem s Cisco smerovačom a využívam tabuľky VRF, sa vypíše zoznam aplikovaných flowspec pravidiel pomocou nasledujúceho príkazu:

```
# show flowspec vrf all ipv4
```

Ako je možné vidieť na obrázku 6.4, názov flowspec akcie sa môže líšiť podľa výrobcu. Napríklad na smerovačoch od *Juniper* sa akcia „discard“ zobrazí rovnakým názvom, no na smerovačoch od *Cisco* sa zobrazí ako „Traffic-rate: 0 bps“. Na to treba myslieť pri tvorení automatických testov.

6.5 Rýchlosť detegovania a mitigácie

Rýchlosť detegovania útoku je priemerne 3 a pol sekundy po spustení útoku. Toto je ovplyvnené viacerými faktormi: vyťaženie kolektora, vyťaženie exportéra a typ sieťovej prevádzky.



Obr. 6.4: Ukážka aplikovaných flowspec pravidiel v Defendery, na smerovači a v súbore pre ExaBGP

Typ útoku najviac ovplyvňoval čas detekcie, pretože ovplyvňoval čas odosielania NetFlow záznamov z exportéra. Po detekcii útoku trvalo vytvorenie flowspec pravidiel zvyčajne menej ako sekundu, v závislosti na počte spracovaných záznamov. Aj pri extrémnych situáciach, keď bola vypnutá podpora agregácie pravidiel a vzniklo teda 10 000 flowspec pravidiel, trvalo vloženie záznamov do databázy a prevedenie ich na flowspec pravidlá 3 sekundy. Išlo však o extrémnu situáciu, ktorá sa v reálnom prostredí neočakáva a čas je aj tak prijateľný. Celkový čas simulácie od spustenia útoku po objavenie flowspec pravidiel na smerovači sa pohyboval v priemere 6 a pol sekundy. Zdržanie bolo zapríčinené výhradne distribúciou pravidiel na smerovače ako možno vidieť v tabuľke 6.1. Časové údaje v tabuľke sú počítané od spustenia útoku.

Typ útoku	Čas do detekcie	Vytvorený súbor	Pravidlá na smerovači
ICMP	8s	8s	12s
UDP	9s	9s	13s
TCP	1s	1s	3s
SYN	2s	2s	5s
SYN&ACK	2s	2s	5s
ACK&FIN	1s	1s	3s
RST	1s	1s	4s
Priemer	3.43s	3.43s	6.43s

Tabuľka 6.1: Výsledky testovania detekcie útokov so zapnutým rozšírením pre okamžitú detekciu.

6.6 Vyhodnotenie výsledkov

Mojim cieľom bolo zrýchliť čas detekcie útoku z pôvodných 30-tich sekúnd, na čas blížiaci sa jednej sekunde. Toto sa mi podarilo, no len ak sú splnené isté kritéria. Pre správnu

funkčnosť musí byt export NetFlow dát z exportéru nastavený na najnižšie hodnoty (1 sekunda) a exportér musí mať rýchle spojenie s kolektorom.

Najlepšie dopadlo detegovanie útokov typu TCP RST a TCP FIN ACK. Tu sa každý paket posiela ako samostatný tok a preto je okamžite po spracovaní exportérom odoslaný na kolektor. V tomto prípade sa naozaj podarilo skrátiť dobu detekcie na 1 až 2 sekundy.

Najhoršie dopadlo testovanie útokov typu UDP a ICMP s nemenným cieľovým portom. V tomto prípade exportér odoslal dáta až po uplynutí aktívneho timeoutu, pretože sa útok javil ako jeden aktívny tok. No aj v tomto prípade nastala detekcia maximálne za 11 sekúnd, čo znamená že ide o výrazné zlepšenie.

Pri testovaní som narazil na problém s exportérmi. Problém vytvárajú exportéry, ktoré nemajú nastavený aktívny a neaktívny timeout na nižší ako 30 sekúnd alebo ak exportér nastavuje čas toku na čas kedy ho odoslali (Cisco smerovače). V tomto prípade kolektor dostane NetFlow dáta ako jednu veľkú hromadu. Dáta sa tak spracujú v jednom okamžiku a teda sa razantne zvýši počet paketov za sekundu, ktoré prijal a deteguje sa falošne pozitívny útok. Mimo to, keďže nejde v RRDtools zapisovať do minulosti, dáta sa zapíšu v jednom čase, čo sa prejaví ako veľká špička v množstve prenesených dát. Riešením by mohlo byť uchovávanie dát v inom formáte s prepočítaním prevádzky podľa dĺžky tokov.

Flowspec pravidlá sa vygenerovali vždy správne a komunikácia so smerovačmi od majoritných výrobcov prebieha stabilne.

Výkonnostné testy som nemohol spraviť, pretože som nemal prístup k hardvérovému kolektoru. Pri virtuálnom kolektore sa nedá spoľahnúť, že má vždy pridelené všetky prostriedky, ktoré by mal mať. Mimo to som využíval smerovače s obmedzenou licenciou na 1 MBit za sekundu a to na testovanie výkonu nestačí.

Kapitola 7

Záver

Cieľom tejto práce bolo porozumieť problematike *Denial of Service* a *Distributed Denial of Service* útokov ako aj ich detekcii a zmierneniu za pomoci nástroja DDoS Defender z NetFlow a následné vytvorenie zásuvného modulu pre zrýchlenie detekcie a tvorbu pravidiel pre zmierňovanie pomocou Flowspec presmerovaní na sieťových uzloch. V teoretickej časti ja rozobratá problematika počítačových sietí. Konkrétne bol kladený dôraz na správne porozumenie obsahu NetFlow záznamov, ako aj ich vytváranie, spracovávanie, analýzu a využitie pre možnosti detekcie volumetrických útokov.

Pre možnosť zmierňovania útokov na smerovačoch je použitý protokol BGP, pomocou voľne dostupného nástroja ExaBGP, ktorý dokáže využívať pokročilé špecifikácie protokolu ako Flowspec. Práve Flowspec je pre zmierňovanie útokov mimoriadne vhodný a aj účinný. Pre navrhnutie zásuvného modulu na okamžitú detekciu útokov, bolo nutné dôkladne sa zoznámiť s celkovou architektúrou pre zber a spracovanie NetFlow záznamov od firmy Flowmon Networks, ako aj s aplikáciou na detekovanie volumetrických útokov pomocou dávkového spracovania, DDoS Defender.

V praktickej časti je popísaný návrh zásuvného modulu pre zrýchlenie detekcie útokov a vytvorenie Flowspec pravidiel pre zmiernenie útoku. Navrhnutý modul dokáže efektívne agregovať signatúry útokov a prevádzať ich do formátu pravidiel tak, aby s nimi aplikácia ExaBGP dokázala efektívne pracovať. Riešenie bolo implementované ako dva moduly pre Flowmon kolektor, ktoré medzi sebou komunikujú a je možné ich nasadiť na kolektor bez výraznej zmeny v architektúre. Aplikácia bola testovaná vo virtuálnom laboratóriu na typické druhy útokov, ktoré vždy detegovala a úspešne mitigovala pomocou flowspec pravidiel. Keďže sa výrazne znížil čas detekcie útokov, považujem riešenie za úspešné.

V budúcnosti by bolo perspektívne rozšíriť modul o možnosť používania súčasne SQL a noSQL databázy pre zrýchlenie výpočtov pri zachovaní perzistencie dát. Ďalej by bolo efektívne pridať automatické konfigurovanie chránených segmentov pomocou analýzy *Routing Information Base*.

Literatúra

[1] Brownlee, N.; Mills, C.; Ruth, G.: Traffic Flow Measurement: Architecture. RFC 2722, October 1999.

[2] Cisco: *Border Gateway Protocol*. 2013, online, navštívené 29.1.2017.
URL http://docwiki.cisco.com/wiki/Border_Gateway_Protocol

[3] Cisco: *Implementing BGP Flowspec*. 2016, online, navštívené 29.1.2018.
URL https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-2/routing/configuration/guide/b_routing_cg52xasr9k/b_routing_cg52xasr9k_chapter_011.pdf

[4] Claise, B.; Trammell, B.: Information Model for IP Flow Information Export (IPFIX). RFC 7012, RFC Editor, September 2013.

[5] Claise, B.; Trammell, B.; Aitken, P.: Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information. STD 77, RFC Editor, September 2013.
URL http://www.rfc-editor.org/rfc/rfc7011.txt

[6] Groth, D.: *Network+ study guide*. Sybex; 4 edition, April 14, 2005, ISBN ISBN-10: 0782144063.

[7] Krzyzanowski, P.: Understanding Autonomous Systems. 03 2016, online, navštívené 01.05.2018.
URL https://www.cs.rutgers.edu/~pxk/352/notes/autonomous_systems.html

[8] Martin Elich, J. P. a. k. F. N.: Flowmon DDoS Defender - User Guide. 2017.

[9] Odom, W.: CCNP Route 642-902 Official Certification Guide / W. Odom ; pról. de Erik Ullanderson. 04 2018.

[10] Rekhter, Y.; Li, T.; Hares, S.: A Border Gateway Protocol 4 (BGP-4). RFC 4271, RFC Editor, January 2006.
URL http://www.rfc-editor.org/rfc/rfc4271.txt

[11] Reports, B.: *Border Gateway Protocol*. 2018, online, navštívené 30.04.2018.
URL http://bgp.potaroo.net

[12] Shipley, T.; Bowker, A.: Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace. 11 2013: s. 1–472.

[13] Vohra, Q.; Chen, E.: BGP Support for Four-octet AS Number Space. RFC 4893, RFC Editor, May 2007.

[14] Václav Pacholík, J. P. a. k. F. N.: Flowmon Streamova architektura - Specifikace aplikace. 2016.

Prílohy

```
iad=> select * from flowspec_rules where attack_id = 45;
 id | segment_id | attack_id | progress |        date         |  state
----+------------+-----------+----------+---------------------+----------
 45 |          4 |        45 | 4/4      | 2018-05-02 11:55:00 | disabled
(1 row)
iad=> select * from flowspec_routes where rule_id = 45;
 id  | rule_id |   action   |    option    | share |   state
-----+---------+------------+--------------+-------+-----------
 135 |      45 | mark       | 1            |       | confirmed
 136 |      45 | redirect   | 10.10.10.190 |       | confirmed
 137 |      45 | rate-limit | 1000         |       | confirmed
 138 |      45 | accept     |              |       | confirmed
(4 rows)

iad=> select * from flowspec_matches where route_id in
iad-> ( select id from flowspec_routes where rule_id = 45 ) order by route_id;
 id  | route_id |       item       |     value      |  share   |   state
-----+----------+------------------+----------------+----------+-----------
 438 |      135 | destination      | 10.20.20.25/32 | 0.451111 | confirmed
 440 |      135 | destination-port | =45023         | 0.451111 | disabled
 441 |      135 | protocol         | tcp            | 0.451111 | confirmed
 439 |      135 | source           | 10.31.5.2/32   | 0.451111 | confirmed
 443 |      136 | source           | 10.31.7.2/32   |     0.02 | disabled
 442 |      136 | destination      | 10.20.20.25/32 |     0.02 | disabled
 445 |      136 | protocol         | tcp            |     0.02 | confirmed
 444 |      136 | destination-port | =45023         |     0.02 | disabled
 449 |      137 | protocol         | tcp            |      0.4 | confirmed
 446 |      137 | destination      | 10.20.20.25/32 |      0.4 | disabled
 447 |      137 | source           | 10.31.10.2/32  |      0.4 | confirmed
 448 |      137 | destination-port | =45023         |      0.4 | confirmed
 452 |      138 | destination-port | =45023         |  0.11242 | disabled
 451 |      138 | source           | 10.31.4.2/32   |  0.11242 | disabled
 450 |      138 | destination      | 10.20.20.25/32 |  0.11242 | confirmed
 453 |      138 | protocol         | tcp            |  0.11242 | disabled
(16 rows)
```

Obr. 1: Tabuľky v databázy obsahujúce kritéria pre filtrovanie prevádzky a akcie pre flowspec

```
{("SELECT split_part(rule,'|',1) AS route_id,
    split_part(rule,'|',2) AS item,
    split_part(rule,'|',3) AS value, action, option FROM (
        SELECT unnest(rules) as rule, action, option FROM (
        SELECT DISTINCT ON (array_agg(item||','||value))
        array_agg(route_id||'|'||item||'|'||value)
        AS rules, max(action) AS action, max(option) AS option FROM
    (SELECT m.route_id, m.item, m.value, r.action
        AS action, r.option AS option FROM flowspec_routes r
     JOIN flowspec_matches m ON (r.id = m.route_id) WHERE r.rule_id=?
     AND r.state='confirmed' AND m.state='confirmed' AND m.value>?
     ORDER BY m.route_id, m.item, m.value)
     AS foo GROUP BY route_id
    ) AS MATCHES
    ) AS RULES ORDER BY route_id, item;");}
```

Obr. 2: SQL dotaz pre PostgreSQL databázu, pre získanie flowspec pravidiel