

Preporuke za analizu mrežnog saobraćaja pomoću NetFlow protokola

**Dokument najbolje prakse
(smernice i preporuke)**

Izrađen u okviru AMRES tematske grupe za oblast NMS
(AMRES BPD 104)

Autor: Ivan Ivanović

Novembar, 2011.

© TERENA 2010. All rights reserved. (Sva prava zadržana.)

Dokument broj: GN3-NA3-T4-AMRES-BPD-104
Verzija / datum: Novembar, 2011.
Izvorni jezik : Srpski
Originalni naslov: "Preporuka za analizu mrežnog saobraćaja pomoću NetFlow protokola"
Originalna verzija / datum: Revizija 1 (dokumenta iz septembra 2010.)/ 11. novembar 2011.
Kontakt: ivan.ivanovic@rcub.bg.ac.rs

AMRES/RCUB snosi odgovornost za sadržaj ovog dokumenta. U izradi dokumenta učestvovala je tematska grupa za NMS organizovana u AMRESu radi sprovođenja zajedničkih aktivnosti na razvoju i širenju dokumenata sa tehničkim smernicama i preporukama za mrežne servise u višokoškolskim obrazovnim i istraživačkim ustanovama u Srbiji.

Delovi dokumenta mogu se slobodno kopirati, nepromenjeni, pod uslovom da je originalni izvor naveden i autorska prava sačuvana.

Dokument je nastao kao rezultat istraživanja koja su finansirana sredstvima Sedmog okvirnog programa Evropske zajednice (FP7/2007-2013) po ugovoru br. 238875, koji se odnosi na projekat „Multi-Gigabit European Research and Education Network and Associated Services (GN3)“.



Sadržaj

Rezime	4
Uvod	5
1 Analiza mrežnog saobraćaja	6
1.1 Pregled tehnologija za analizu mrežnog saobraćaja	6
1.1.1 Prednosti i mane analize eksportovane NetFlow statistike	7
1.2 Arhitektura sistema za analizu prikupljene NetFlow statistike	8
1.3 Lokacija NetFlow kolektora u mreži	9
2 Konfigurisanje NetFlow eksportera	10
2.1 I Grupa – Samo centralni uređaj podržava NetFlow tehnologiju	10
2.2 II Grupa – Uređaji na obodu mreže podržavaju NetFlow tehnologiju	12
2.3 III Grupa – Dupliranje saobraćaja	12
3 Eksportovanje NetFlow statistike sa L2 segmenta	14
4 Pravilno definisanje vremenskih intervala za eksport	17
5 Virtuelizacija i NetFlow protokol	19
6 Analiza NetFlow statistike pomoću ICmyNet.Flow aplikacije	21
6.1 Konfiguracija i rezultati analize	22
7 Primeri iz prakse	27
7.1 Analiza pomoću grafičkog prikaza	27
7.2 Direktna analiza raw fajlova	29
8 Reference	31
9 Rečnik	32

Rezime

Cilj ovog dokumenta je da predstavi postupke koji se koriste za analizu saobraćaja u mreži, čime se postiže jasan uvid u strukturu saobraćaja i efikasno otkrivanje eventualnih problema i anomalija.

Prvo su predstavljene tehnologije za analizu mrežnog saobraćaja, kao i njihove prednosti i mane. Zatim su detaljno obrađene preporuke za analizu mrežnog saobraćaja zasnovanu na statistici prikupljenoj preko NetFlow protokola. Preporuke obuhvataju primere ispravnog konfigurisanja NetFlow protokola na mrežnim uređajima kao i primere indirektnog korišćenja NetFlow protokola u situacijama kada ga mrežni uređaji ne podržavaju.

Dokument obuhvata i pregled korišćenja ICmyNet.Flow sistema za analizu NetFlow statistike, koji se koristi kao jedan od Network Management sistema ne samo u Akademskoj mreži Srbije već i u drugim NREN-ovima.

Uvod

Sve veća potreba za uvidom u ponašanje mrežnog saobraćaja dovela je do razvoja više tehnologija koje nam mogu pružiti takvu mogućnost. NetFlow tehnologija nam može omogućiti uvid u statistiku saobraćaja koji prolazi kroz našu mrežu. U okruženjima gde mrežni uređaji podržavaju NetFlow tehnologiju, preporučuje se njeno korišćenje.

NetFlow tehnologija je danas postala standard i većina proizvođača mrežne opreme je implementira u svoje uređaje. Na taj način se može iskoristiti postojeća mrežna infrastruktura i bez dodatnih ulaganja i dodavanja specifičnih uređaja obezbediti uvid u karakteristike saobraćaja. U ovom dokumentu su opisani osnovni principi i smernice kojima administratori treba da se vode prilikom pokretanja NetFlow protokola.

Pored toga što je ova tehnologija često dostupna na običnim ruterskim platformama postoje i besplatna softverska rešenja koja nam mogu omogućiti korišćenje NetFlow tehnologije i u situacijama gde je mrežna oprema ne podržava. U daljem tekstu će biti opisana neka od tih rešenja.

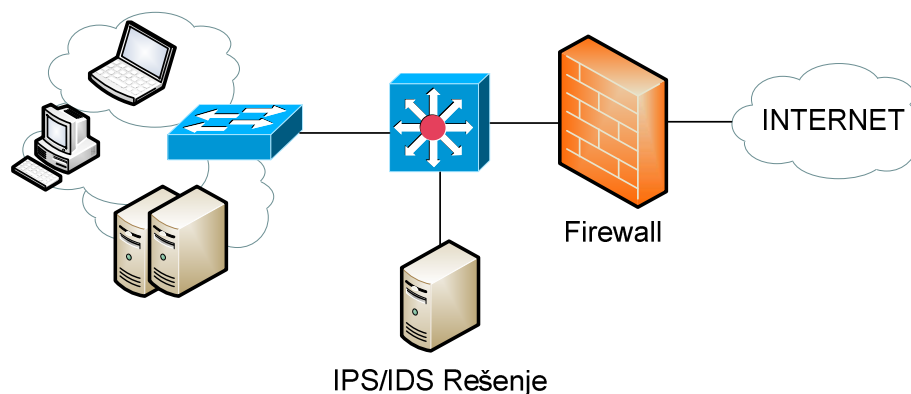
1 Analiza mrežnog saobraćaja

1.1 Pregled tehnologija za analizu mrežnog saobraćaja

U današnjim mrežama se preporučuje da se analiza saobraćaja vrši, ne samo do L2 nivoa (SNMP - broj prenetih bajtova ili broj prenetih paketa na nivou interfejsu uređaja) već i na L3 i L4 nivou.

Postoji dosta alata pomoću kojih se može vršiti analiza saobraćaja. Dele se na rešenja koja zahtevaju specijalizovan hardver, i na softverska rešenja koja ne zavise od hardvera.

Rešenja koja se oslanjaju na hardver su dosta skupa ali su i značajno brža, jer imaju podršku u hardveru. Najčešće se postavljaju u mrežu tako da su transparentna za ostatak mreže. Ovakva rešenja nude DPI (Deep Packet Inspection) mogućnosti kao i akcije u slučaju detekcije problema. Na slici 1.1 je dat primer postavljanja jednog ovakvog uređaja u mrežu. Neke varijante ovih uređaja se koriste ne samo kao uređaji za detekciju problema (IDS - Intrusion Detection System), već kao i uređaji za prevenciju problema (IPS - Intrusion Prevention System).



Slika 1.1 - Primer postavljanja uređaja za analizu saobraćaja

Da bi uvid u statistiku saobraćaja u mreži bio što obuhvatniji, IDS/IPS uređaj je potrebno postaviti što bliže krajnjim korisnicima. Zato se implementacija IDS/IPS rešenja preporučuje da bi se pokrilo samo jedan link (segment mreže). Da bi se pokrila cela mreža, obično je potrebno postaviti više IDS/IPS uređaja. Mana takve implementacije je ta što se prikupljeni podaci za pojedine segmente mreže nalaze na više lokacija (IDS/IDS uređaja). Da bi se stekao uvid u celokupan saobraćaj u mreži potrebno je na neki način centralizovati menadžment, tj. prikupiti sve te podatke na jednom mestu i koordinirati automatske procedure sa tog mesta.

Drugo rešenje se bazira na analizi statistike koju mrežni uređaji sakupljaju i eksportuju. Uređaji koji imaju mogućnost obrade podataka na L3 i L4 nivou (ruteri, L3-svičevi) mogu da vrše prikupljanje statistike saobraćaja

do L4 nivoa i da takvu statistiku eksportuju ka serveru gde se vrši dodatna obrada podataka. Rešenje koje nam pruža tu mogućnost je NetFlow protokol.

NetFlow se koristi kao termin koji označava tehnologiju, protokol, ali i format u kome se definiše i zapisuje statistika prikupljena na mrežnim uređajima. Naziv NetFlow, kao i tehnologija su vezani za Cisco kompaniju, koja je prva ponudila ovo rešenje. Ostali proizvođači su razvijali slične protokole pod različitim imenima (Juniper - jflow, Huawei - netstream...). Pošto su svi kompatibilni sa NetFlow tehnologijom, naziv NetFlow je najzastupljeniji.

Danas se najčešće sreću dve verzije NetFlow protokola, verzija 5 i verzija 9. U verziji 5, prikupljena statistika se zapisuje u fiksnom formatu. Verzija 9 podržava fleksibilan format, koji odgovara skupu odabranih parametara za koje se prikuplja statistika. Zato se verzija 9 naziva i fleksibilni NetFlow.

Usled potrebe za univerzalnim standardom, od strane IETF organizacije definisan je IPFIX protokol kao protokol za eksport prikupljene statistike saobraćaja. IPFIX protokol je ekvivalentan Cisco NetFlow V9 protokolu.

1.1.1 Prednosti i mane analize eksportovane NetFlow statistike

Prikupljena NetFlow statistika se eksportuje ka serveru na kome je pokrenuta aplikacija koja vrši obradu tih podataka prema zadatim kriterijumima, i kao rezultat analize se obično prikazuju grafici i tabele sa rezultatima. Iz grafika i rezultata se lako mogu uvideti problemi koji su se javili. Na osnovu analize prikupljene NetFlow statistike postoji mogućnost automatskog detektovanja problema ili napada u mreži.

Rezultati ovakve analize nam pružaju sledeće informacije:

- Informacije o ukupnom prenetom saobraćaju između pojedinih sabneta (bajti, paketi, konekcije).
- Informacije o ukupnom prenetom saobraćaju razdvojene po protokolima, servisima, hostovima.
- Informacije o spoljašnjim pristupima našoj mreži (protokol, servis, host).
- Detekcija saobraćaja koji je blokiran access listom.
- Detekcija saobraćaja koji je odbačen usled lošeg rutiranja (crne rupe).
- Predikcija ponašanja saobraćaja u budućnosti.
- Komunikacija između autonomnih sistema (AS).
- Informacija o saobraćaju razdvojena po QoS markerima.
- Uvid u karakteristike IPv6 saobraćaja.

Problemi koji se mogu detektovati na ovaj način su:

- Pojava Virus u mreži (velika količina saobraćaja se generiše u izlaznom ili ulaznom smeru, ili ka DNS ili EMAIL serverima).
- Pojava DoS napada.
- Zloupotreba protoka (youtube, facebook, torrent...).
- Pristup zabranjenim sajtovima.
- Pokušaji napada/pristupa zaštićenim mrežnim uređajima.
- Opterećenje linka.

Prednosti:

- Centralizovano prikupljanje podataka.
- Može se koristiti već postojeća oprema.
- Lako se konfigurise.
- Mogućnost prikupljanja i drugih parametara u komunikaciji kao što su kašnjenje, varijacija kašnjenja, izgubljeni paketi (IPFIX).
- Besplatne aplikacije za prikupljanje NetFlow statistike.

Mane:

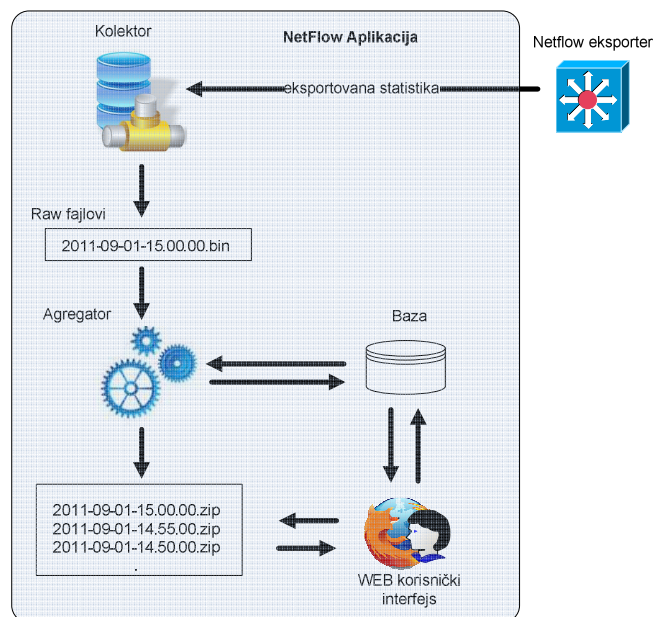
- Aplikacije nemaju mogućnost da same reše problem (blokiranje komunikacije).
- Nakon nastanka problema pa do njegovog uočavanja može proći dosta vremena.
- Mogu se prikupiti samo informacije do L4 sloja.
- Zahtevaju poznavanje mreže da bi se ispravno konfigurisao eksport podataka putem NetFlow protokola.

1.2 Arhitektura sistema za analizu prikupljene NetFlow statistike

Većina sistema za prikupljanje i obradu NetFlow statistike se sastoji od uređaja koji prave statistiku o saobraćaju i eksportuju tu statistiku, i sistema za analizu prikupljene statistike. U mreži najčešće postoji samo jedan sistem za obradu statistike, dok se statistika o saobraćaju može prikupljati sa većeg broja uređaja.

Većina komercijalnog i nekomercijalnog softvera, prilikom kreiranja aplikacije za prikupljanje i obradu NetFlow statistike, koristi komponente koji su prikazani na slici 1.2., a koje su definisane u sledećoj listi:

- Eksporter – Uređaj koji prikuplja statistiku o saobraćaju koji je prošao kroz njega i eksportuj tu statistiku u NetFlow formatu ka sistemu za analizu.
- Kolektor – Deo sistema za analizu koji samo prikuplja NetFlow statistiku sa svih eksportera.
- Agregator – Deo sistema za analizu koji obrađuje prikupljenu NetFlow statistiku prema zadatim kriterijumima i dobijene rezultate čuva u bazi ili na neki drugi način.
- Raw Fajlovi – Binarni fajlovi u kojima sistem za analizu čuva svu prikupljenu NetFlow statistiku.
- Baza – Deo sistema za analizu u kome se čuvaju informacije iz *raw* fajlova obrađene prema predefinisanim zahtevima (Mysql, Oracle, Postgresql...).
- Korisnički interfejs – Web aplikacija koja se koristi prilikom pregleda obrađene statistike.



Slika 1.2 – Komponente sistema za obradu NetFlow statistike

Dalje objašnjenja će biti data imajući u vidu arhitektura ICmyNet.Flow aplikacije koja se koristi za prikupljanje i obradu NetFlow statistike u AMRESu.

Mada se eksportovanje NetFlow statistike ka udaljenom centralnom serveru može vršiti sa više mrežnih uređaja, na slici 1.2 je prikazan primer eksportovanja NetFlow statistike sa jednog uređaja (NetFlow Exportera), i ceo proces obrade kroz koji prolazi primljeni NetFlow podatak. Prva komponenta aplikacije koja se koristi za primanja eksportovane NetFlow statistike sa eksportera, zove se kolektor. Taj deo aplikacije u periodičnim vremenskim intervalima generiše *raw* fajlove, koji sadrže prikupljenu NetFlow statistiku za određeni vremenski interval, i čuva ih u binarnom obliku. Kada kolektor popuni *raw* fajl on ga prosleđuje drugoj komponenti sistema koja se zove agregator. Agregator preuzima fajl od kolektora i obrađuje ga, koristeći predefinisane informacije iz baze. Obradene podatke (agregirane) agregator čuva u bazi. Agregator zatim kompresuje, prethodno dobijeni *raw* fajl od kolektora, i čuva ga u arhivi. Kompresija se koristi da bi se uštedelo na prostoru. Empirijski se pokazalo da je odnos kompresije 1:10.

Korisnički interfejs predstavlja *web* aplikaciju i on nam omogućava da dobijemo informacije o stanju u mreži na osnovu agregiranih podataka iz baze. U slučaju potrebe za detaljnim informacijama o svakoj komunikaciji, korisnik može putem *web*-a otvoriti *raw* fajl za određeni vremenski interval i izvršiti njegovo filtriranje prema željenim kriterijumima.

1.3 Lokacija NetFlow kolektora u mreži

Lokacija kolektora koji prikuplja NetFlow statistiku zavisi od same arhitekture mreže. Količina NetFlow podataka koju mrežni uređaji eksportuju direktno zavisi od količine saobraćaja koja prolazi kroz taj uređaj (eksporter). Empirijski se pokazuje da procenat NetFlow saobraćaja ne prelazi 1% od ukupnog saobraćaja u mreži, tako da ne postoji problem "udaljenosti" servera (kolektora) od mrežnog uređaja koji eksportuje podatke (eksportera). Bitniji parametri su dostupnost i sigurnost servera.

Fizička lokacija servera se obično vezuje za centralno čvorište zato što većina glavnog saobraćaja prolazi kroz to čvorište. Preporučuje se:

- Postavljanje servera u odvojeni Vlan (menadžment vlan).
- Postavljanje zaštite u vidu firewall-a na server.
- U slučaju otkaza pojedinih mrežnih uređaja bitno je da NetFlow server bude dostupan za analizu saobraćaja tako da je potrebno izdvojiti i UPS sistem za neprekidno električno napajanje NetFlow servera.

2 Konfigurisanje NetFlow eksportera

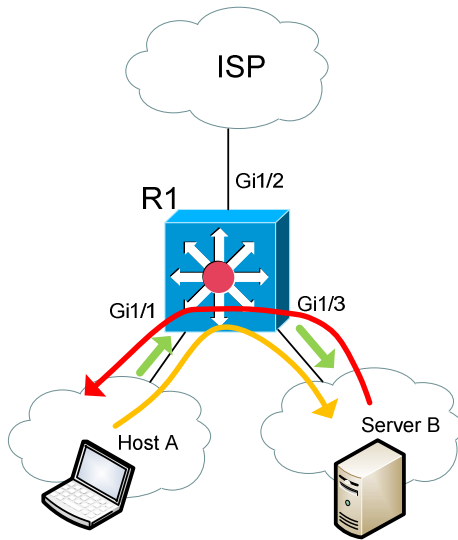
Konfigurisanje eksporta NetFlow statistike na uređajima zavisi od karakteristika samih uređaja, ali i od arhitekture mreže. Na novijim uređajima, prikupljanje i eksport NetFlow statistike moguće je podešavati na nivou interfejsa, i to u jednom od dva smera ulaznom (*in/ingress*) smeru ili izlaznom (*out/egress*) smeru. Pojedini uređaji imaju mogućnost eksporta i u ulaznom i u izlaznom smeru istovremeno. Većina starijih uređaja ima mogućnost prikupljanja i eksportovanja NetFlow statistike istovremeno na svim interfejsima samo u ulaznom smeru.

Prilikom pokretanja NetFlow protokola najčešće sa mogu pojaviti problemi sa dupliranjem eksportovane NetFlow statistike. U zavisnosti od arhitekture mreže, problemi se mogu svrstati u tri grupe. U daljem tekstu je dat njihov opis kao i opis rešenja.

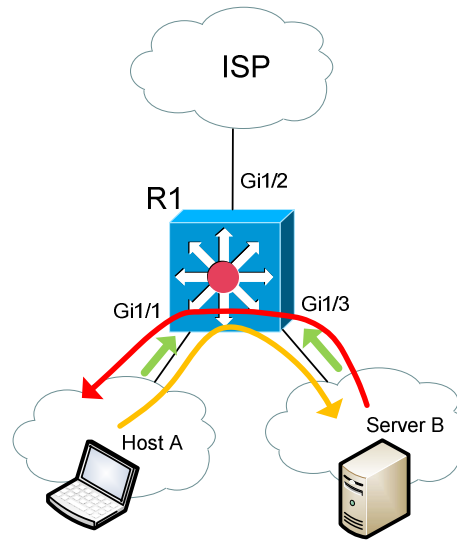
2.1 I Grupa – Samo centralni uređaj podržava NetFlow tehnologiju

Prva grupa problema nastaje u situaciji u kojoj je Netflow pokrenut na centralnom uređaju. To je najčešće jedini uređaj koji podržavaju prikupljanje i eksport NetFlow statistike u manjim kampus mrežama.

Na slici 2.1 je dat primer nepravilnog konfigurisanja NetFlow eksporta, dok je na slici 2.2 dat primer ispravnog pokretanja NetFlow eksporta. Zelenim strelicama označen smer u kome je pokrenut eksport statistike na interfejsima.



Slika 2.1 – Nepravilno pokrenut NetFlow eksport



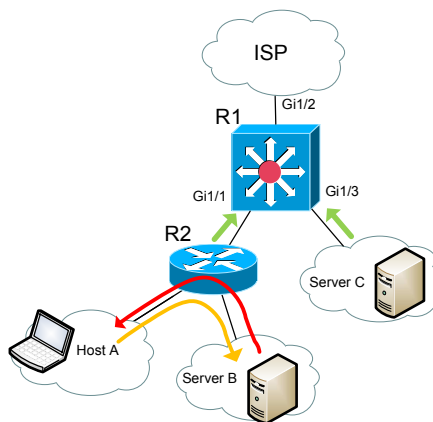
Slika 2.2 – Ispravno pokrenut NetFlow eksport

Konfiguracija prikazana na slici 2.1 je nepravilna, jer će jedan flow, na putu od od hosta A do servera B, biti dva puta obrađen i eksportovan ka NetFlow kolektoru - prvi put prilikom ulaska na interfejs Gi1/1, a drugi put prilikom izlaska na interfejs Gi1/3. Informacija o ovoj komunikaciji će biti duplirana prilikom analize prikupljene NetFlow statistike. U ovom slučaju statistika o komunikaciji koja potiče od tačke B do tačke A neće biti prikupljena.

Da bi se ispravno prikupila statistika potrebno je pokrenuti NetFlow na svim interfejsima u ulaznom ili na svim interfejsima u izlaznom smeru.

Na slici 2.2 je prikazan primer ispravnog prikupljanja NetFlow statistike. Konfigurisano je prikupljanje NetFlow statistike u ulaznom smeru na Gi1/1 i Gi1/3 interfejsima. Statistika o komunikaciji od tačke A do tačke B će biti prikupljena na interfejsu Gi1/1, a statistika o komunikaciji od tačke B do tačke A će biti prikupljena na interfejsu Gi1/3. U ovoj situaciji će se sakupljati i eksportovati statistika o svom saobraćaju koji prolazi kroz centralni uređaj.

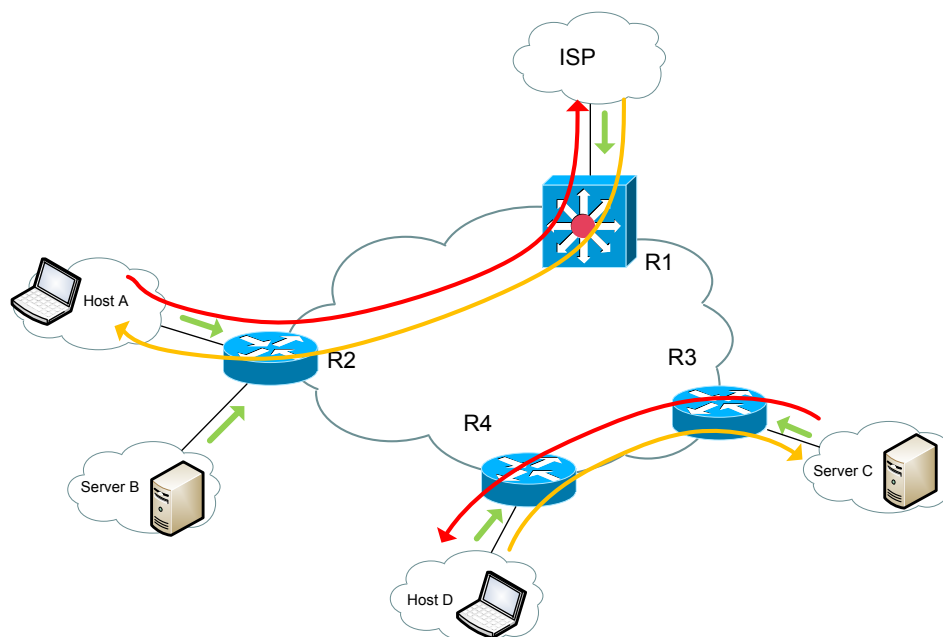
Ako komunikacija između pojedinih subneta u mreži ne prolazi kroz centralni uređaj, kao na slici 2.3, NetFlow statistika o toj komunikaciji se neće prikupiti. Uređaj R2 na slici 2.3 ne podržava NetFlow tehnologiju.



Slika 2.3 – Lokalni saobraćaj čija se statistika ne eksportuje

2.2 II Grupa – Uređaji na obodu mreže podržavaju NetFlow tehnologiju

Na slici 2.4 je prikazana situacija kada uređaji na obodu mreže podržavaju NetFlow tehnologiju. Ovakva arhitektura je karakteristična za institucije koje imaju delove na više lokacija međusobno povezane zakupom servisa preko MPLS mreže telekom provajdera. Tada se preporučuje da se na svim obodnim uređajima pokrene prikupljanje NetFlow statistike i to samo na interfejsima ka krajnjim subnetima. Zelenim strelicama su na slici 2.4 označeni interfejsi na kojima je pokrenuto prikupljanje NetFlow statistike, a smer strelice definiše da li je u pitanju ulazni smer. Potrebno je da smer bude isti za celu mrežu, ili ulazni ili izlazni. Na slici 2.4 je odabran ulazni smer.

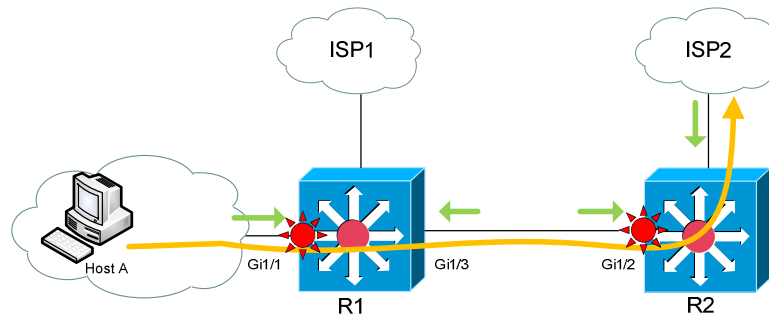


Slika 2.4 - Podešavanje prikupljanja NetFlow statistike na uređajima na obodu mreže

Sa slike 2.4 se može zaključiti da će biti prikupljena statistika o saobraćaju između hosta A i ISP, ali će se takođe prikupiti statistika o saobraćaju između lokalnih sabneta, odnosno komunikacija između hosta D i servera C. U ovom slučaju se podrazumeva da svi mrežni uređaji podržavaju NetFlow tehnologiju, kao i mogućnost definisanja smera u kom će se prikupljati NetFlow statistika na nivou interfejsa.

2.3 III Grupa – Dupliranje saobraćaja

U složenijim mrežnim konfiguracijama, postoje i situacije u kojima je nemoguće izbeći dupliranje NetFlow statistike na hardverskom nivou, odnosno konfiguracijom samog mrežnog uređaja. Na slici 2.5 je dat primer ovakve situacije, sa dva mrežna uređaja u *coru* mreže.



Slika 2.5 – Dupliranje NetFlow statistike

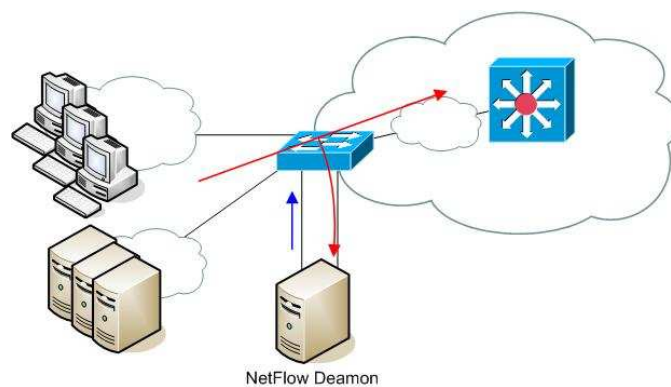
Na slici 2.5 je dat prikaz situacije u kojoj centralni uređaji R1 i R2 imaju mogućnost prikupljanja NetFlow statistike na svim interfejsima, ali samo u ulaznom smeru. Komunikacija od hosta A ka ISP2 će biti dva puta obrađena, prvi put prilikom ulaska u uređaj R1 na interfejsu G1/1, a drugi put prilikom ulaska u uređaj R2 na interfejsu G1/2. Komunikacija od ISP2 ka hostu A će takođe biti dva puta obrađena. Kako nije moguće zaustaviti dupliranje statistike na hardverskom nivou potrebno je detektovati dupliranje saobraćaja pomoću aplikacije koja analizira NetFlow statistiku. Postoji više načina pomoću kojih je moguće to uraditi.

Prvo rešenje ovog problema zahteva da sama aplikacija koja prikuplja statistiku detektuje duplirane informacije i odbaci ih. Duplirane informacije će imati ista pojedina NetFlow polja (*src* i *dst* ip adrese, protokol, *src* i *dst* portove) tako da je na osnovu toga moguće izvršiti detekciju dupliranja.

Drugo rešenje zahteva da aplikacija koja prikuplja statistiku mora da ima mogućnost filtriranja prikupljene statistike. Kako se u eksportovanoj NetFlow statistici nalazi informacija o ip adresi eksportera i ulaznom i izlaznom interfejsu kroz taj eksporter za svaki flow, moguće je iskoristiti ta polja za filtriranje. U primeru na slici 2.5 je moguće isključiti iz analize (filtrirati) saobraćaj, koji prolazi preko linka između uređaja R1 i R2, jer se na njemu vrši dupliranje. Problem dupliranja ćemo rešiti tako što ćemo iz analize isključiti svu NetFlow statistiku koju je generisao eksporter R1 i koja ima ulazni interfejs Gi1/3 i svu NetFlow statistiku koju je generisao eksporter R2 i koja ima ulazni interfejs Gi1/2.

3 Eksportovanje NetFlow statistike sa L2 segmenta

U situaciji kada ni jedan uređaj na mrežnom segmentu ne podržava NetFlow protokol može se primeniti sledeće rešenje. Na serveru je potrebno instalirati odgovarajući softver i pokrenuti NetFlow sondu (demon) koji vrši analizu primljenog saobraćaja i generiše NetFlow statistiku. Zatim konfigurisati mrežni uređaj i saobraćaj sa njegovih portova preusmeriti na server. Na slici 3.1 je prikazana ova situacija.



Slika 3.1 - Preusmeravanje saobraćaja ka NetFlow serveru

Na slici 3.2 je dat detaljniji prikaz preusmeravanja saobraćaja (port mirroring) sa uplink porta Ge0/0 na Ge0/1 port. Ovakvo rešenje nam pruža statistiku o saobraćaju koji je ušao na bilo koji Fa0/X interfejs L2 uređaja i izašao na Gi0/0 interfejs, kao i statistiku o saobraćaju koji je ušao na Gi0/0 interfejs. Statistiku o lokalnom saobraćaju između Fa0/X i Fa0/Y porta nećemo moći prikupiti.

U manjoj kamus mreži, kao server se može koristiti računar standardnih karakteristika za radnu stanicu. Potrebno je da server ima dve mrežne kartice.

Softver koji se instalira na server da bi prikupljao statistiku o saobraćaju se naziva NetFlow sonda. Primer besplatne sonde je softflowd sonda (<http://code.google.com/p/softflowd/>). Ova sonda se može pokrenuti i na Windows i na Linux platformama. Besplatni softver za rad sa NetFlow statistikom se može pronaći na <http://www.switch.ch/network/projects/completed/TF-NGN/floma/software.html> sajtu. U tabeli 3.1 je dat primer pokretanja softflowd aplikacije.

```
[root@linuxserver /]# softflowd -i eth2.4 -n 192.168.99.6:2055 -v 5 -t  
udp=1m30s -t tcp=1m30s -t maxlife=4m -m 6553
```

Tabela 3.1 – Primer pokretanja softflowd aplikacije

U tabelama 3.2 i 3.3 je dat primer konfigurisanja port mirroringa saobraćaja na Cisco i Juniper uređaju.

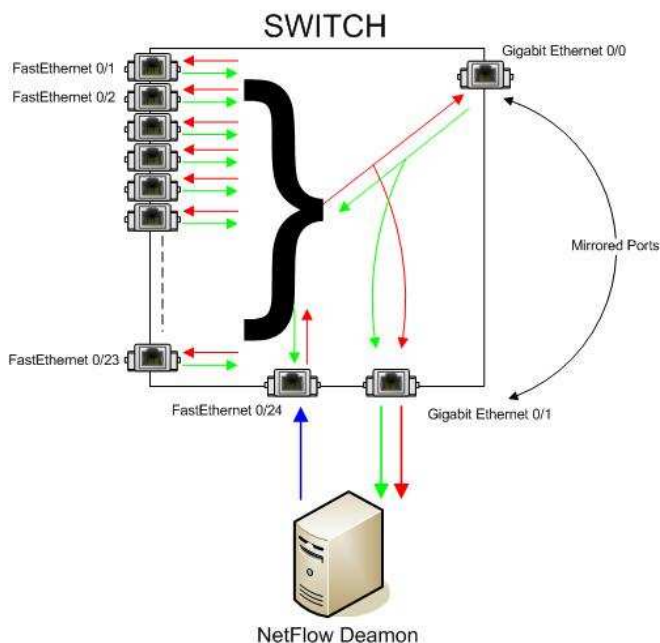
```
switch#(config)# monitor session 1 source interface GigabitEthernet 0/0
switch#(config)# monitor session 1 destination interface gigabitEthernet 0/1
```

Tabela 3.2 – Primer konfiguracije kopiranja saobraćaja na Cisco uređaju

```
ivke@branch#edit ethernet-switching-options
ivke@branch#set analyzer my-monitor input ingress interface ge-0/0/0.0
ivke@branch#set analyzer my-monitor input egress interface ge-0/0/0.0
ivke@branch#set analyzer my-monitor ratio 1
ivke@branch#set analyzer my-monitor output interface ge-0/0/10.0
```

Tabela 3.3 – Primer konfiguracije kopiranja saobraćaja na Juniper uređaju

Da ne bi došlo do odbacivanja saobraćaja prilikom kopiranja, potrebno je da portovi koji se koriste za kopiranje budu istih karakteristika. Takođe je potrebno da port na serveru, na koji se prosleđuje duplirani saobraćaj, bude istih karakteristika kao i port na sviču. Na slici 3.2 se za prikljupljanje statistike koriste Gigabit Ethernet portovi - dva na sviču i jedan Gigabit Ethernet priključak na serveru. Druga mrežna kartica u serveru (u ovom slučaju FastEthernet) koristi za povezivanje servera u mrežu i redovnu komunikaciju sa serverom.

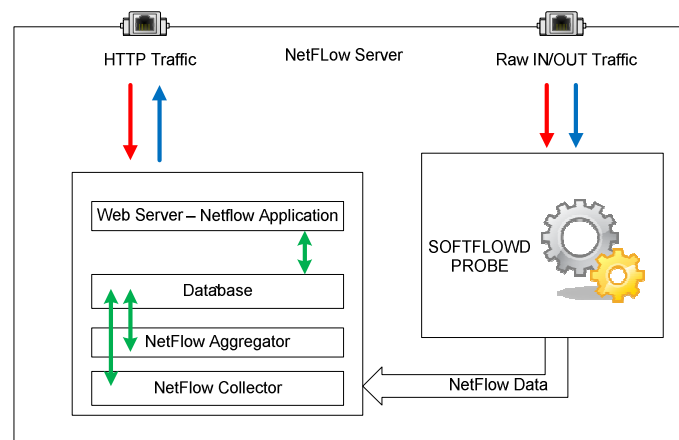


Slika 3.2 - Detaljniji prikaz postavljanja servera i povezivanja portova

Na slikama 3.1 i 3.2 se vidi da je izvršeno dupliranje saobraćaja ka serveru gde je pokrenuta NetFlow sonda. Kada se pokrene dupliranje saobraćaja na sviču, interfejs ka kome se sav saobraćaj prosleđuje (Gi0/1), odnosno duplira, postaje neupotrebljiv za normalnu komunikaciju između uređaja. On samo prosleđuje sav ulazni i izlazni saobraćaj sa interfejsa na kom je konfigurisano dupliranje saobraćaja. Problem je kako eksportovati NetFlow statistiku ako je interfejs na koji je povezan server sa NetFlow sondom neupotrebljiv za normalnu ip komunikaciju. Rešenje je dodavanje još jedne mrežne kartice na server i njeno povezivanje na svič. Na slici 3.2 je plavom strelicom prikazan eksport NetFlow statistike sa druge mrežne kartice sa servera. Ovakvom konfiguracijom je omogućeno da se vrši eksport NetFlow statistike i sa L2 uređaja.

Mana ovakvog rešenja je dodatno zauzimanje portova na sviču i potreba za dodatnim serverom. Prilikom eksporta prikupljene statistike na ovaj način pojedine informacije koje su standardne za NetFlow protokol će se izgubiti. Informacija o as brojevima, ip adresi eksportera, next-hop ip adresi i ulaznim i izlaznim interfejsima na eksporteru neće više biti dostupne. Aplikacije za analizu prikupljene NetFlow statistike koje analizu baziraju na ip adresi eksportera i ulaznim i izlaznim interfejsima se ne mogu koristiti u ovoj situaciji pošto ove informacije postaju nedostupne prilikom ovakvog eksporta NetFlow statistike.

Rešenje na slici 3.2 nam omogućuje da eksportujemo prikupljenu statistiku ka centralnom NetFlow serveru koji se može nalaziti bilo gde u mreži. Ako se u mreži ne koristi centralizovano prikupljanje NetFlow statistike, server na slici 3.2 se može iskoristiti i kao lokacija za instalaciju aplikacije koja obrađuje NetFlow statistiku. Na slici 3.3 je dat ovaj primer. Jedino je potrebno da se NetFlow sonda konfigurise tako da statistiku eksportuje lokalno na 127.0.0.1 ip adresu. Na ovaj način administratori izolovanih lokacija mogu imati uvid u karakteristiku saobraćaja koji prolazi kroz njihov svič



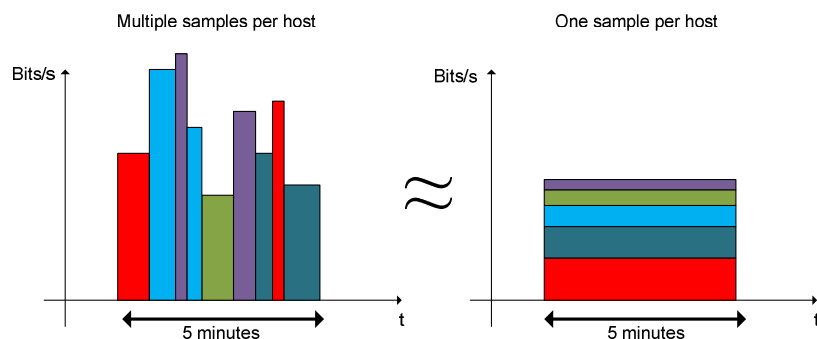
Slika 3.3 – Primer lokalnog eksporta podataka

4 Pravilno definisanje vremenskih intervala za eksport

Aplikacije koje obrađuju NetFlow statistiku na dva načina procesuiraju podatak o vremenskom trenutak kada se određeni flow u mreži pojavio i koliko dugo je trajao.

1. Prvi način utvđuje vreme iz NetFlow *raw* formata, odnosno očitavanjem *timestamp* polje. U suštini ta informacija daje tačan trenutak kada je flow počeo i koliko dugo je trajao.

2. Aplikacije koje su pravljene da podrže ogromnu količinu eksportovanih podataka ne mogu prilikom analize da očitavaju NetFlow *timestamp* polje za svaki flow, jer bi takva analiza dosta usporila rad aplikacije i povećala veličinu baze u kojoj se te informacije čuvaju nakon obrade. Takve aplikacije definišu i koriste minimalni vremenski interval, recimo 5 minuta, a agregirana statistika prikupljena u poslednjem vremenskom intervalu od 5 minuta za svaki pojedini host će se sačuvati kao jedan 5 minutni odbirak u bazi. Primer je dat na slici 4.1.



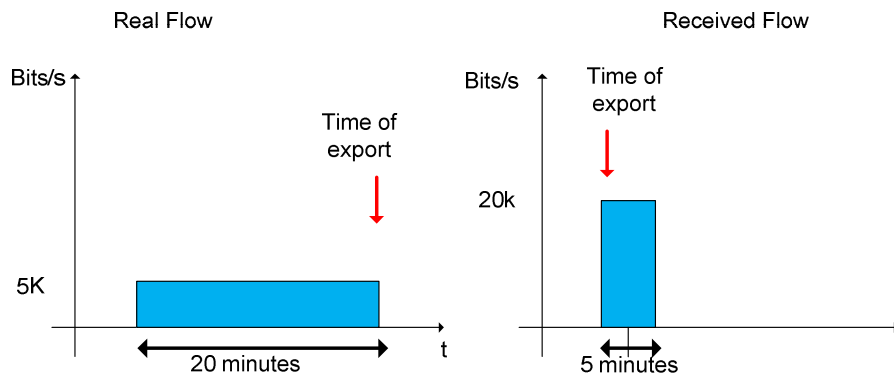
Slika 4.1 – Primer čuvanja statistike u bazi

Na slici 4.1 su različitim bojama prikazani različiti hostovi (ip adrese). U toku 5 minuta su hostovi mogli jednom ili više puta da generišu različite tokove podataka. Umesto da se u bazi za svakog hosta pojedinačno čuva informacija o svim tokovima podataka i vremenskim intervalima kada je koristio mrežu, čuvaće se samo ukupna (sumarna) informacija o tome koliko je saobraćaja preneo u toku 5 minuta. Uvodi se usrednjavanje prikupljene statistike na zadatom vremenskom intervalu. U primeru na slici 4.1 taj vremenski interval iznosi 5 minuta.

Kada se koriste aplikacije za obradu koje usrednjavaju prikupljenu NetFlow statistiku na zadatom vremenskom intervalu, obratiti pažnju da vremeneni interval (u kome se eksportuju *netflow* informacija), na eksporterima treba podesiti tako da bude manji ili jednak vremenskom intervalu usrednjavanja koji aplikacija koristi.

Drugi razlog, koji zahteva podešavanje vremena za eksport informacija sa NetFlow exporteru je da bi se dobile tačne informacije o događajima u mreži u slučaju vremenski dugačkih tokova podataka ili u slučaju suviše kratkih tokova podataka.

Na slici 4.2 je prikazana situacija kada u mreži postoji tok podataka koji traje duži vremenski interval (20 minuta). Tek po završetku tog toka podataka eksporter će poslati prikupljenu NetFlow statistiku ka kolektoru. Ako aplikacija koja obrađuje statistiku ne koristi *timestamp* polje, koje se nalazi u primljenim podacima, ona će pretpostaviti da se taj događaj odigrao u poslednjih 5 minuta i u bazi će se sačuvati informacija o količini prenetih podataka kao da je tok trajao 5 minuta, a ne 20 minuta. Samim tim će se prikazati i veći protok, što nije tačno.



Slika 4.2 – Primer nepravilnog prikupljanja NetFlow statistike

Na uređajima postoje tri vrste tajmera za zastarevanje prikupljene statistike i u tabeli 4.1 je dat primer konfigurisanja tajmera na Cisco uređajima.

- Normalno zastarevanje je predefinisano tako da iznosi 5 minuta.
- Brzo zastarevanje podataka je potrebno podesiti na kraći vremenski interval nego što koristi normalno zastarevanja. Ono se koristi u kombinaciji sa kriterijumom o prenetoj količini paketa da bi se flow proglasio završen. Ideja je da se kratki upiti kao što su DNS ili ping što pre proglaše završenim, zastare i eksportuju ka kolektoru. Na taj način se brzo može detektovati napad u mreži.
- Dugo zastarevanje se koristi da bi se dugi tokovi podataka proglasili završenim i eksportovali ka kolektoru. Primer ove situacije je dat na slici 4.2.

```
branch#(config)#mls aging fast time 30 threshold 100
branch#(config)#mls aging normal 300
branch#(config)#mls aging long 300
```

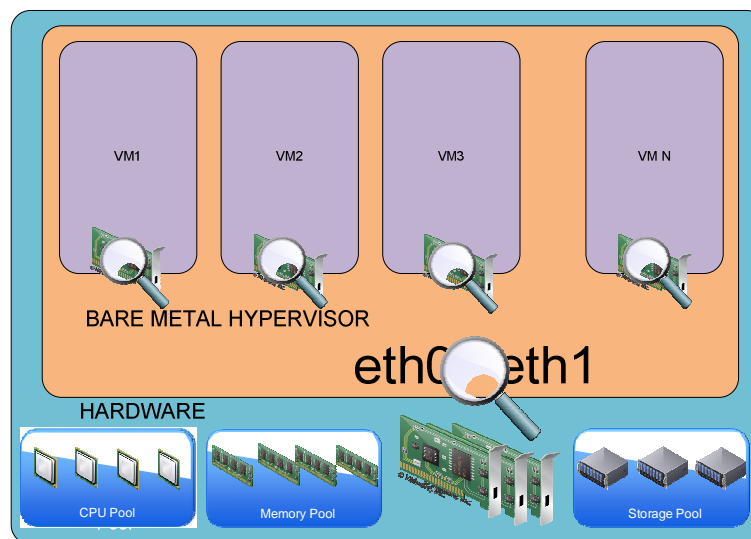
Tabela 4.1 – Primer podešavanja tajmera na Cisco uređajima

Preporuka je da se ovi tajmeri ispravno podese zbog samog rada eksportera. Generisanje DOS napada (*ping sweep*, *dns sweep*) može za kratak vremenski interval popuniti memoriju u kojoj se čuva NetFlow statistika na eksporteru. Kada se prepuni memorija za sakupljenje NetFlow statistike eksporter počne da zastareva sve informacije i eksportuje ih ka kolektoru bez obzira da li su se ti tokovi podataka završili ili ne. Na taj način eksporter oslobađa memoriju. Ova pojava može dosta da optereti sam procesor uređaja. Brzo zastarevanje NetFlow podataka nam omogućuje da eksporter kratkotrajne upite brzo zastari, eksportuje i izbriše iz memorije i na taj način oslobodi memoriju za novu NetFlow statistiku.

5 Virtuelizacija i NetFlow protokol

Kod pojedinih proizvođača softvera za virtuelizaciju (Citrix, VmWare) se takođe može primeniti metoda postavljanja NetFlow sonde koja je opisana u glavi 3.

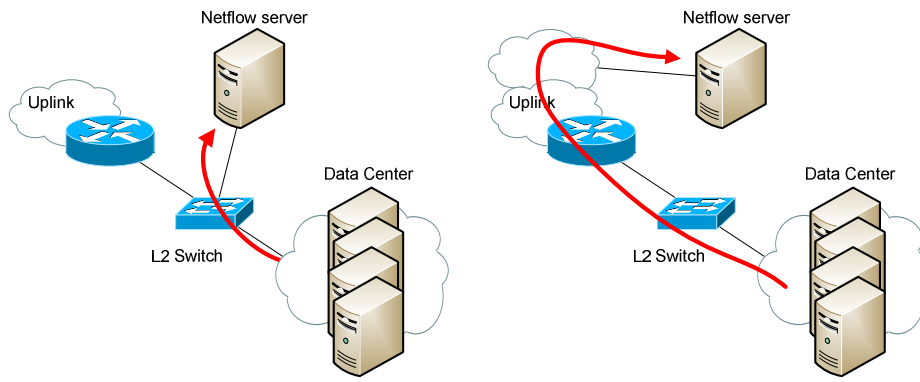
Na slici 5.1 je dat primer postavljanja softflowd sonde.



Slika 5.1 – Postavljanje NetFlow sonde na virtuelno okruženje

Na slici 5.1 se može videti da se sonde mogu postaviti na same virtuelne mašine, ili na još niži sloj (bare metal). U prvom slučaju se postavljaju na virtuelne interfejs dok u drugom na same fizičke kartice.

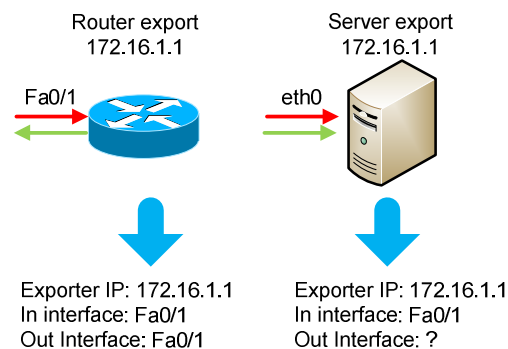
Na ovaj način se mogu sakupiti informacije o ulazno/izlaznom saobraćaju servera u slučaju da na postoji mogućnost prikupljanja statistike na mrežnim uređajima. Slika 5.1 opisuje takav primer. Prikupljena statistika se može zatim eksportovati na sistem za prikupljanje NetFlow statistike čija lokacija može biti u lokalnoj mreži ili na udaljenoj lokaciji kao što je prikazano na slici 5.2.



Slika 5.2 Prikupljanje statistike sa farme servera

6 Analiza NetFlow statistike pomoću ICmyNet.Flow aplikacije

Većina dostupnih aplikacija za obradu NetFlow statistike, analizu saobraćaja bazira na podacima o ulazno/izlaznom interfejsima i ip adresi eksportera. Kada se prikupljanje statistike saobraćaja vrši pomoću NetFlow sonde, odnosno kada se koristi dupliranje saobraćaja (port mirroring), te informacije se gube. Prilikom eksportovanja NetFlow statistike, sonda u polje eksportera upisuje ip adresu interfejsa sa koga sonda šalje statistiku (ip adresa servera na kome je instalirana). Informacija o ulazno/izlaznom interfejsu se takođe gubi, jer sav preusmereni saobraćaj ulazi na jedan interfejs servera. Na slici 6.1 su radi poređenja dati podaci eksportovani sa rutera i podaci eksportovani sa NetFlow sonde instalirane na serveru.



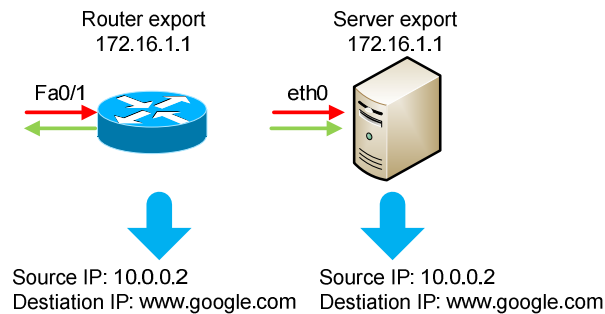
Slika 6.1 – Problem prilikom korišćenja “port mirroring” opcije

U slučaju sa serverom kao eksporterom, na slici 6.1, vidi se da aplikacija ne može da otkrije koji je dolazni a koji odlazni saobraćaj. Sa stanovišta aplikacije sav saobraćaj je dolazni, pošto dolazi do servera. U slučaju sa ruterom kao eksporterom, na slici 6.1, aplikacija može da razlikuje odlazni i dolazni saobraćaj, pošto prilikom eksporta dobija informaciju o eksporteru, i informacije o ulazno/izlaznim interfejsima za svaki flow.

Da bi prikupili i ispravno analizirali saobraćaj koji je eksportovan putem “mirroring” metode, potrebno je modifikovati pristup za analize prikupljenih podataka. Analiza saobraćaja se ne može bazirati na podacima o ulazno/izlaznom interfejsima i ip adresi eksportera. Aplikacije mora izvršiti analizu na osnovu drugih parametara u eksportovanoj NetFlow statistici. Jedna od aplikacija koja omogućava analizu po drugim parametrima (*source* i *destination* ip adresama saobraćaja) je ICmyNet.Flow aplikacija.

ICmyNet.Flow aplikacija se koristi u AMRES-u kao deo sistema za monitoring mrežne infrastrukture. Aplikacija je besplatna za sve akademske institucije. U daljem tekstu će biti opisano kako se ICmyNet.Flow aplikacija koristi za prikupljanje i analizu NetFlow statistike.

ICmyNet.Flow aplikacija, omogućava da se analiza NetFlow statistike bazira na npr. *source* i *destination* ip adresama saobraćaja. Kada se koristi kriterijum *source* i *destination* ip adresa, za svaki flow može da se definiše odakle je došao i gde ide. Slika 6.2 opisuje ovaj primer.



Slika 6.2 – Primer analize na osnovu src/dst ip adresa

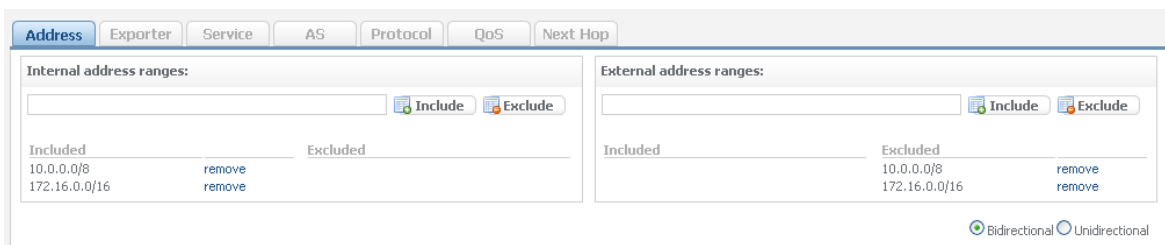
ICmyNet.Flow aplikacija za analizu prikupljene statistike koristi logički element koji se zove Traffic Pattern. Ovaj logički element se formira tako što se definiše mrežni opseg (lokalni adresni opseg) koji obuhvata adresni prostor za mrežu od interesa. Eventualno se definiše i eksterna mreža ka kojoj želimo da posmatramo saobraćaj. Time se dobija osnovna potrebna konfiguracija za Traffic Pattern, a dalje se mogu definisati i dodatni kriterijumi za filtriranje kao što su:

- IP address – IP adresa eksportera
- Service – Posmatraju se TCP ili UDP portovi
- AS – Source ili Destination AS
- Protocol – L3 protokol
- QoS – QoS Markeri
- Next Hop – Next Hop ip adresa

6.1 Konfiguracija i rezultati analize

Za kampus mreže je karakteristična potreba da posmatramo saobraćaj iz naše lokalne mreže ka internetu i obrnuto, te smo kroz ovaj primer objasnili konfiguraciju aplikacije i analizu NetFlow statistike.

Definisali smo interni adresni opseg 172.16.0.0/16, kao opseg koji se koristi na našem lokalnom sabnetu. Kao eksterni opseg se može definisati bilo koji drugi adresni opseg, tj. ne može se definisati ono što odgovara lokalnom subnetu (u našem slučaju, to je sve osim adresnog opsega 172.16.0.0/16). Na taj način smo ubuhvatili sav saobraćaj koji potiče iz naše mreže i završava u nekoj drugoj mreži koja nije naša lokalna mreža. Na slici 6.1 je dat primer za lokalnu mrežu sa dva sabneta, odnosno dva adresna opsega 10.0.0.0/8 i 172.16.0.0/16. Na ovaj način moguće je prikupiti statistiku za saobraćaj koji potiče iz mreže 10.0.0.0/8 i/ili 172.16.0.0/16 i završava u nekoj drugoj mreži koja nije 10.0.0.0/8 ili 172.16.0.0/16 mreža.



Slika 6.1 – Primer konfiguracije aplikacije koja treba da analizira razmenu saobraćaj ka internetu

Na sledećih par slika je dat prikaz rezultata analize prikupljene statistike po različitim parametrima, subnetima, hostovima, servisima, protokolima, QoS markerima, i sl.

Na slici 6.2 je dat prikaz analize prikupljene NetFlow statistike po subnetima. Da bi se dobio detaljan prikaz saobraćaja po svakom od sabneta u internoj mreži prethodno je potrebno definisati sve podmreže u toj mreži.



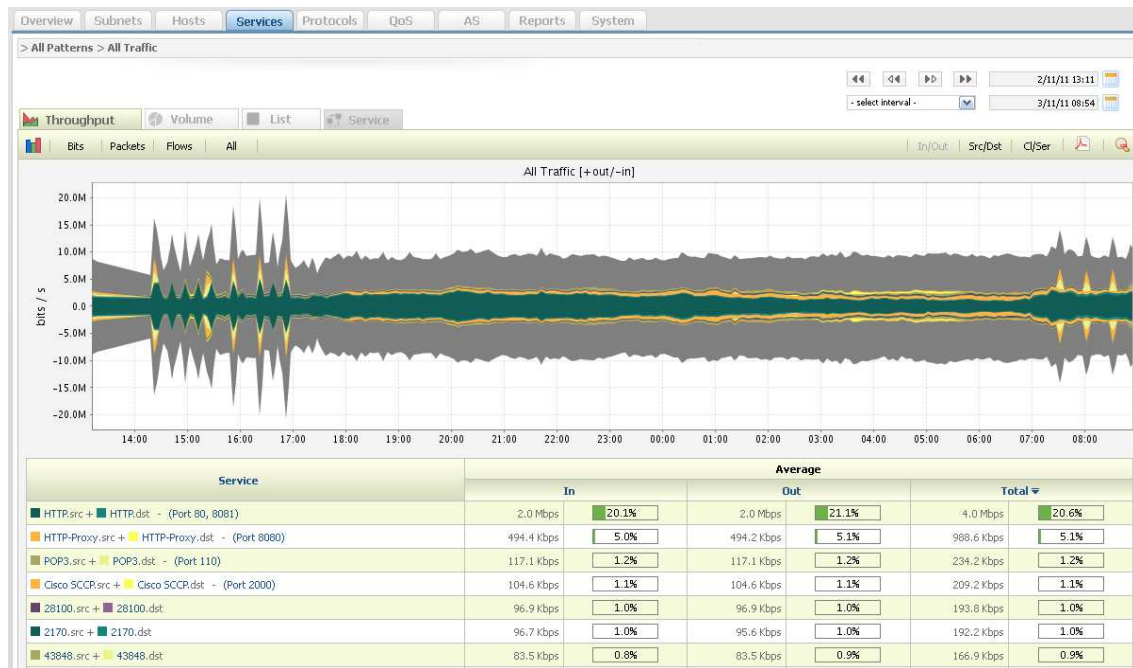
Slika 6.2 – Prikaz rezultata analize po sabnetima

Na slici 6.3 je dat prikaz analize prikupljene NetFlow statistike po hostovima. U pozitivnom delu y ose na graficima je prikazan saobraćaj koji napušta internu mrežu, a u negativnom delu y ose saobraćaj koji ulazi u internu mrežu.



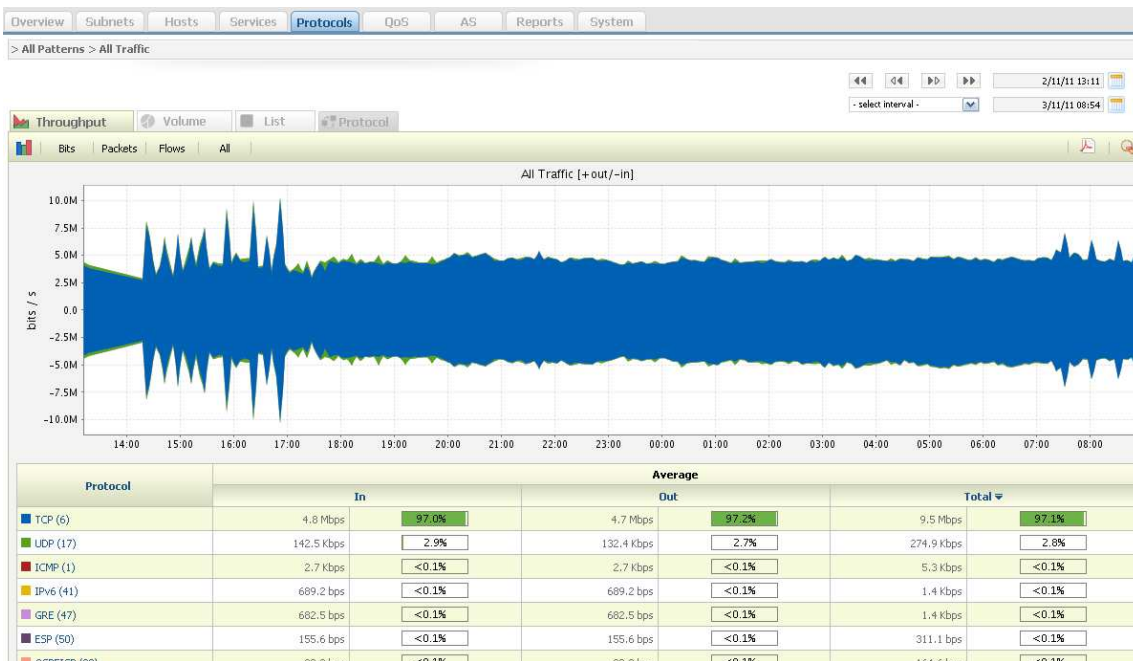
Slika 6.3 – Prikaz rezultata analize po hostovima

Na slici 6.4 je dat prikaz analize prikupljene NetFlow statistike po servisima.



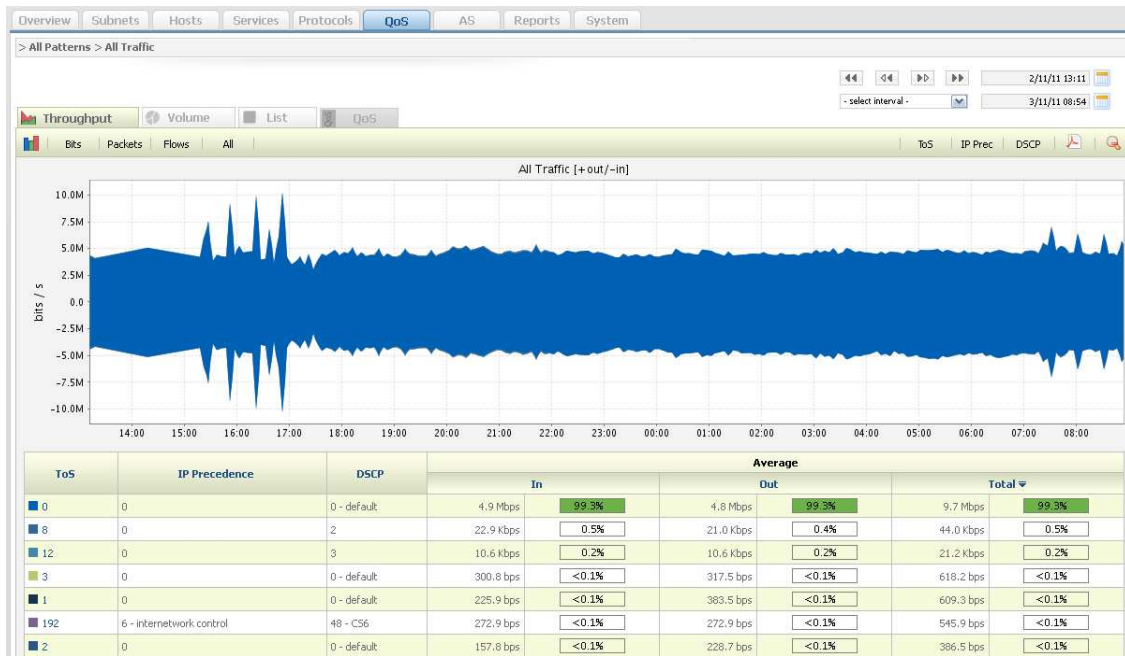
Slika 6.4 – Prikaz rezultata analize po servisima

Na slici 6.5 je dat prikaz analize prikupljene NetFlow statistike po protokolima.



Slika 6.5 – Prikaz rezultata analize po protokolima

Na slici 6.6 je dat prikaz analize prikupljene NetFlow statistike po QoS markerima.



Slika 6.6 – Prikaz rezultata analize po QoS markerima

Na slici 6.7 je dat prikaz analize prikupljene NetFlow statistike po AS sistemima. Da bi mogao da popuni AS polja prilikom eksporta NetFlow statistike, potrebno je da eksporter ima pokrenut BGP protokol i da ima celu BGP tabelu.



Slika 6.7 – Prikaz rezultata analize po AS vrednostima

Sa prethodnih slika se mogu dobiti informacije o saobraćaju koji je generisan iz interne mreže i saobraćaju koji je generisan ka internoj mreži. Nedostaje informacija o eksternim ip adresama ka kojima je generisan saobraćaj, ili sa kojih je generisan saobraćaj ka našoj mreži. Te informacije se mogu dobiti direktnim očitavanjem raw fajlova, kao što je prikazano na slici 6.8. Slika daje uvid u detalje NetFlow statistike prikupljene za svaku

generisanu komunikaciju koja je prošla kroz određeni eksporter. Dalja analiza ove statistike je moguća pomoću filtera koji se mogu postaviti na početku svake kolone u tabeli na slici 6.8.

Princip rada sa aplikacijom je sledeći. Kada se na graficima koji analiziraju saobraćaj po nekom od parametara (poput onih na slikama 6.1 do 6.7) uoči bilo kakva anomalija u saobraćaju, prvo se analizira problem pomoću dostupnih grafičkih rezultata, a zatim se na osnovu prikupljenim informacijama sa grafika izvrši dodatno vrlo detaljno filtriranje raw NetFlow statistike, da bi se pronašao uzrok anomalije.

Start time	End time	Duration	Source	Source port	Destination	Destination Port	Protocol	TOS
03-11-2011 16:04:55.96	03-11-2011 16:05:19.928	24.832 sec	bidirectional					
03-11-2011 16:04:55.608	03-11-2011 16:09:59.416	303.808 sec		237	55859	7.136	52735	6
03-11-2011 16:04:55.608	03-11-2011 16:09:59.352	303.744 sec		3.51	1300	1.45	8080	6
03-11-2011 16:04:55.608	03-11-2011 16:09:31.960	276.352 sec		209	38678	04.74	57398	6
03-11-2011 16:04:55.608	03-11-2011 16:09:59.160	303.552 sec		1.11	16328	8.178	57437	17
03-11-2011 16:04:55.608	03-11-2011 16:06:40.824	105.216 sec		3.20	23121	1.109	48561	17
03-11-2011 16:04:55.416	03-11-2011 16:09:59.288	303.872 sec		7.29	48936	0.145	56971	17
03-11-2011 16:04:56.248	03-11-2011 16:07:17.560	141.312 sec		7.28	1026	49.18	53760	17
03-11-2011 16:04:55.416	03-11-2011 16:09:58.72	302.656 sec		3.97	21414	03.18	31151	17
03-11-2011 16:04:55.480	03-11-2011 16:09:49.008	288.128 sec		3.20	23121	9.111	64361	17

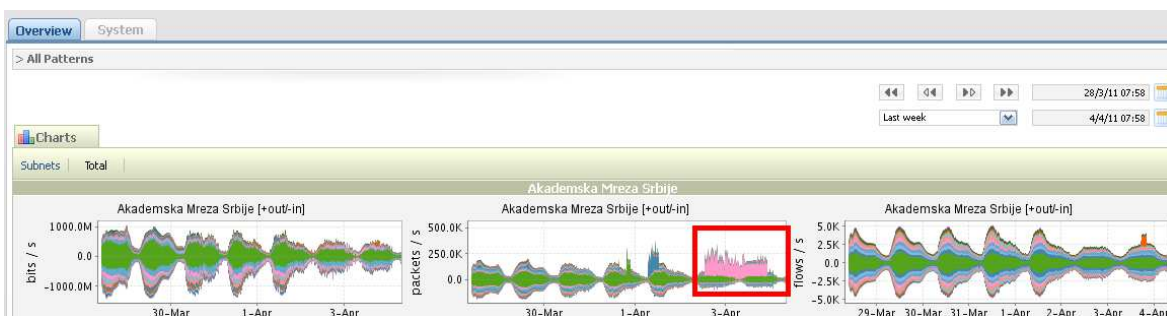
TCP Flags	Packets	Bytes	Throughput	Exporter	Interface In	Interface Out	Next Hop	Source AS	Destination AS
none	809	37,214	12.0 Kbps		85		3	0	3356
none	2,035	1,515,994	39.9 Kbps		174		3	0	42145
none	9,169	428,052	11.3 Kbps		234		252	0	0
none	733	871,678	25.2 Kbps		184		3	0	9808
none	1,157	66,373	1.7 Kbps		179		3	0	27699
none	968	71,927	5.5 Kbps		179		3	0	7922
none	2,430	3,232,591	85.1 Kbps		174		3	0	3215
none	518	723,359	41.0 Kbps		174		3	0	1241
none	701	37,555	992.7 bps		179		3	0	1759
none	733	61,406	1.7 Kbps		179		3	0	7922

Slika 6.8 – Pregled i detaljna analiza prikupljene statistike pomoću filtera

7 Primeri iz prakse

7.1 Analiza pomoću grafičkog prikaza

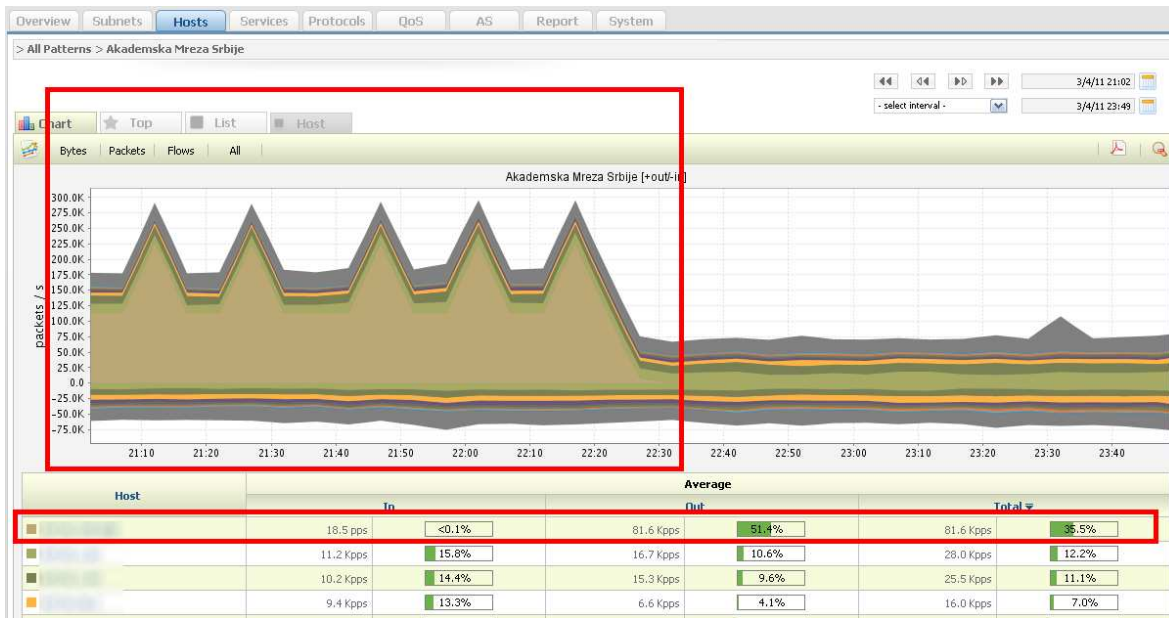
U sledećem primeru je objašnjena analiza napada koji se javio u AMRES-u. Koristi se ICmyNet.Flow aplikacija. Početna stanica ICmyNet.Flow aplikacije je prikazana na slici 7.3. Stranica sadrži grafike iz kojih se vidi da je ovaj konkretni napad došao iz interne mreže.



Slika 7.3 – Inicijalna stranica u ICmyNet.Flow aplikaciji

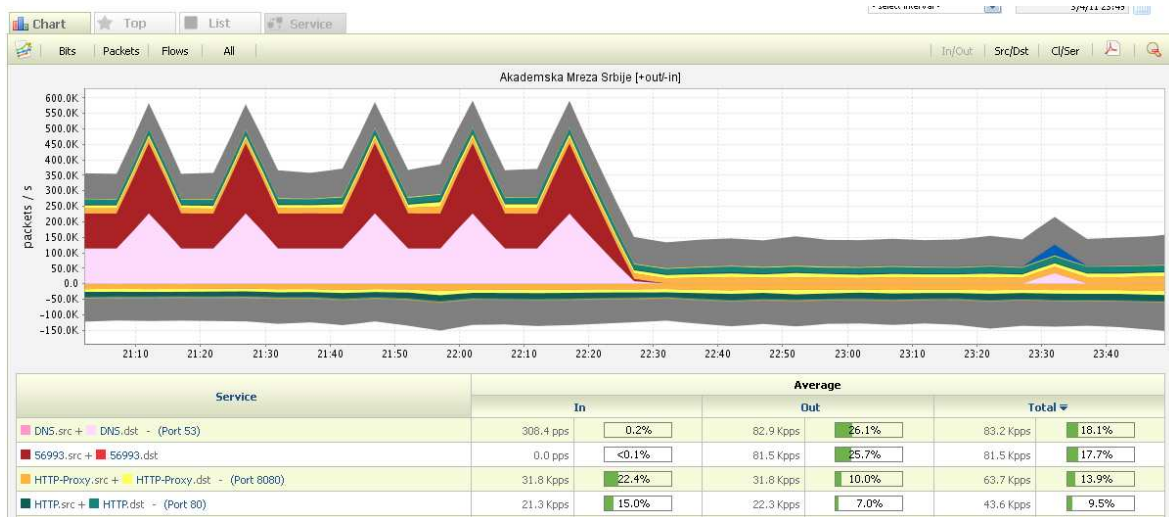
Na slici 7.3 se odmah može uočiti neregularnost na grafiku koji prikazuje količinu prenetih paketa. Crvenom bojom je označena anomalija koja je primećena. Anomalija se nalazi u pozitivnom delu y ose na grafiku koji prikazuje ukupnu količinu paketa po sekundi, iz čega zaključujemo da je u pitanju saobraćaj koji potiče iz naše interne mreže.

Da bi dobili informaciju o hostu koji je generisao taj saobraćaj, kao i količini saobraćaja za vremenski period odabran na grafiku, treba da selektujemo host prikaz. Na slici 7.4 je dat prikaz host opcije.



Slika 7.4 – Informacije o hostu koji je generisao veliku količinu saobraćaja

Ako nas zanima ka kom servisu su generisani ovi podaci možemo selektovati services tab i dobiti tu informaciju. Na slici 7.5 je dat prikaz raspodele saobraćaja po servisima.



Slika 7.5 – Raspodela saobraćaja po servisima

Sa slike 7.5 se može zaključiti da je u pitanju DNS servis. Sada nedostaje jedino informacija o serveru ka kome je upućen ovaj saobraćaj. Da bi smo tu informaciju dobili potrebno je izvršiti filtriranje svih prikupljenih NetFlow podataka prema predhodnim informacijama koje smo uspeli da prikupimo analizom grafika. Dakle, potrebno je da se izvrši filtriranje (nekog od raw fajlova iz uočenog vremenkom opsegu) po identifikovanoj source ip adresi iz interne mreže i destinacionog porta 53. Na slici 7.6 je dat rezultat filtriranja.

No.	Date / Time	Source		Destination		Protocol			Counter		
		IP	Port	IP	Port	Number	TOS	Flags	Flows	Packets	Bytes
1	03-04-2011 21:55:28	192.168.1.10	56993	192.168.1.4	DNS	UDP	0	none	1	33,925,354	1,560,566,284

Exporter		
IP	Int. In	Int. Out
192.168.1.10	Vl172	Vl101

Slika 7.6 – Rezultat filtriranja raw fajlova

Za selektovani petominutni fajl se dobija informacija da je iz interne mreže generisano oko ~1.5GB podataka i ~33M paketa. Sa slike 7.3 se može videti da ovaj napad traje duže od jednog dana tako da je preneto više od 430GB podataka. Sa slike 7.6 se takođe može videti da ovaj saobraćaj nije zabranjen access listama odnosno da je prošao ka drugom AS peer-u, pošto izlazni interfejs ove konekcije nije 0 već vl101.

7.2 Direktna analiza raw fajlova

Upotreba direktne analize raw fajlova je pokazana na još jednom jednostavnom primeru. Radi se o vrlo učestaloj vrsti napada. To je napad, koji u mreži generiše male količine podataka, tako da se na graficima (koji pokazuju saobraćaj iskazan u bajtovima) ne može uočiti nešto što bi ukazivalo na napad. Međutim ako se izvrši filtriranje raw fajlova prema logičkim kriterijumima koji odgovaraju opisu napada dobijaju se interesantni rezultati. U ovom primeru je korišćen je raw fajl koji sadrži NetFlow informacije prikupljene u vremenskom intervalu od 5 minuta.

U primeru je korišćena pretpostavka da mnogi napadi koji potiču iz interne mreže i koriste tcp protokol mogu da budu zaustavljeni na access listama, definisanim u nekom delu mreže. Ako, u internoj mreži, postoje virusi i bootovi koji konstantno pokušavaju da izvrše napad, u raw fajlovima bi trebalo da se pojavi dosta bezuspešnih pokušaja da se uspostavi tcp konekcija, odnosno da bude registrovano dosta saobraćaja koji ima postavljen tcp syn fleg.

Slika 7.1 prikazuje rezultat filtriranja saobraćaja po kriterijumu kojim se traže samo konekcije sa postavljenim syn flagom, a pri tome se vrši njihovo grupisanje po source IP adresi, kao i sortiranje po prenetim paketima. Radi boljeg prikaza izdvojeno je samo prvih pet redova iz table.

Source	Destination	Destination Port	Protocol	TCP Flags	Packets	Bytes	Throughput	Exporter	Interface In	Interface Out	
2.2	-	445	-	6	5	12,237	587,376	15.4 kbps	24	179	0
45	-	445	-	6	5	3,908	187,584	4.9 kbps	24	174	0
63	-	445	-	6	5	1,605	77,040	2.0 kbps	24	174	0
60	-	445	-	6	5	1,311	62,928	1.7 kbps	24	174	0
43	-	-	-	6	5	1,299	69,048	1.7 kbps	24	252	0

Slika 7.1 – Primer filtriranja raw fajlova

Na slici 7.1 se vidi da su na vrh liste isplivale adrese iz lokalne mreže koje pokušavaju da uspostave konekciju na više destinacionih ip adresa po tcp portu 445, ali su blokirane access listom (pojavljuje se 0 za interface out). Interface 0 znači da je eksporter odbacio taj flow, odnosno blokirao ga je access listom.

Ako se zatim uzme neka od adresa iz liste na slici 7.1, npr. prva source ip adrese iz te liste, i izvrši filtriranje njenih konekcija sa tcp flagom postavljenim na *syn*, kao i sortiranje po destinacionim ip adresama, dobija se rezultat prikazan na slici 7.2. Vidi se da je sa odabrane source adrese ka različitim ip adresama generisan po jedan paket veličine 48 bajta. Slika 7.1 pokazuje da ukupan broj generisanih paketa iznosi 12237, iz čega se se zaključuje da je prva ip adresa sa liste generisala ogromnu količinu paketa ka približno 12000 različitih ip adresa po tcp portu 445. Konačni zaključak je da je uređaj iz lokalne mreže zaražen takvom vrstom virusa, koji konstantno pokušava da pronađe uređaj koji ima otvoren tcp port 445 i da izvrši napad.

Source	Source port	Destination	Destination Port	Protocol	TCP Flags	Packets	Bytes
.2	2871	223.	445	6	S	1	48
.2	4809	223.	445	6	S	1	48
.2	4325	223.	445	6	S	1	48
.2	2730	223.	445	6	S	1	48
.2	3289	223.	445	6	S	1	48
.2	2711	223.	445	6	S	1	48
.2	3141	223.	445	6	S	1	48
.2	2567	223.	445	6	S	1	48
.2	3427	223.	445	6	S	1	48
.2	3194	223.	445	6	S	1	48
.2	3504	223.	445	6	S	2	96
.2	2745	223.	445	6	S	1	48
.2	1557	223.	445	6	S	1	48
.2	4101	223.	445	6	S	1	48
.2	3738	223.	445	6	S	2	96
.2	1602	223.	445	6	S	1	48
.2	3039	223.	445	6	S	1	48
.2	4260	223.	445	6	S	1	48

Slika 7.2 – Filtriranje po adresi inficirane mašine (prvih 18 redova)

8 Reference

- [1] Introduction to Cisco IOS NetFlow - A Technical Overview.
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.html
- [2] NetFlow Version 9 Flow - Record Format.
http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9_ps6601_Products_White_Paper.html
- [3] Netflow sonda Softflowd. <http://code.google.com/p/softflowd/>

9 Rečnik

AMRES	Akadska mreža Srbije
AS	Autonomni sistem
BPD	Best Practice Document
DNS	Domain Name Service
DoS	Denial Of Service
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IPFIX	IP Flow Information Export
IPS	Intrusion Prevention System
ISP	Internet Service Provider
MPLS	Multiprotocol Label Switching
NMS	Network Monitoring System
NREN	National research and education network
QoS	Quality of service
TCP	Transmission Control Protocol
UDP	User Datagram Protocol