Centar Informacijske Sigurnosti

Optimiziranje vatrozid sustava

listopad 2011.

CIS-DOC-2011-10-027

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

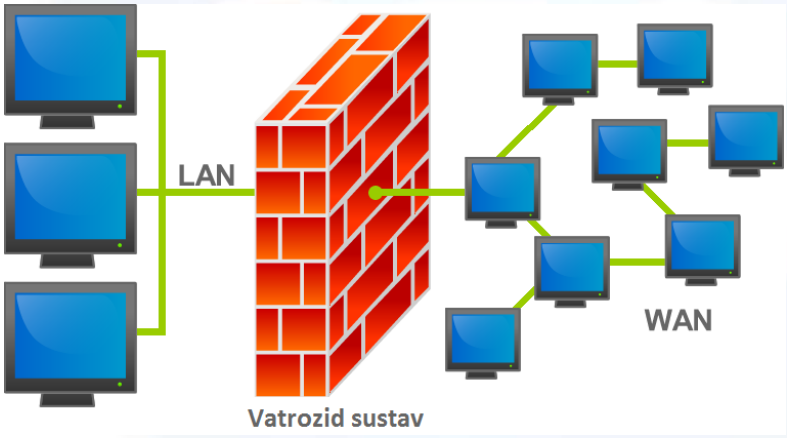
1. Uvod

Vatrozid sustav (eng. *firewall*) je sigurnosni element (mrežni uređaj ili program) smješten između neke lokalne mreže i javne mreže (Interneta), a prikazan je na slici 1. U svom najjednostavnijem obliku ponaša se kao sigurnosna granica koja provjerava pristup mreži dopuštajući ili odbijajući dolazni, odnosno odlazni mrežni promet ovisno o skupu sigurnosnih pravila.

U današnjem globalnom svijetu Interneta vatrozid sustav je postao uistinu ključna tehnologija u borbi za očuvanje sigurnosti na mreži te prva linija obrane protiv napada i prijetnji na mreži. Ipak, s neprestanim rastom Interneta te sve profinjenijim napadima dolazi potreba za sve složenijim dizajnom i održavanjem vatrozid sustava, što za sobom povlači njihovu povećanu potencijalnu ranjivost.

Naime, što je veći skup sigurnosnih pravila to je veći teret postavljen na vatrozid sustav jer za svaki paket koji stigne na vatrozid sustav on mora ispitati svoja pravila i odlučiti hoće li propustiti ili blokirati paket. U tom kontekstu, sigurnost koju pruža vatrozid sustav ne ovisi samo o skupu njegovih pravila nego i o brzini kojom je vatrozid sustav sposoban pronaći odgovarajuće pravilo koje treba primjeniti na određeni paket. Pod napadom ili teškim opterećenjem vatrozid sustav s mnogo sigurnosnih pravila koja nisu optimizirana lako može postati usko grlo. Kako se skup pravila stalno mijenja i raste zbog stalnog povećanja veličine mreže, tako su i sigurnosna pravila u stalnoj potrebi za nadogradnjom, ugađanjem i ispitivanjem (kako bi se optimizirala sigurnost koju pruža vatrozid sustav).

Ovaj dokument će objasniti najčešće anomalije u sigurnosnim pravilima te prikazati 3 vrste metoda koje se koriste u optimizaciji vatrozid sustava. To su: rudarenje podataka (eng. Data Mining Method), *Directed Acyclical Graphs* i metode temeljene na svojstvima mrežnog prometa.



Slika 1. *Ilustracija smještaja vatrozid sustava u mreži*
Izvor: *Wikipedia*

2. Najčešći oblici anomalija u sigurnosnim pravilima

Sigurnosna pravila vatrozid sustava su zapravo uređena lista pravila za filtriranje prometa koja definiraju koja će se akcija izvesti nad paketom koji zadovoljava određene uvjete. Pravilo se sastoji od niza polja po kojima se filtrira promet i od polja koje kaže koju akciju treba izvesti (propustiti ili odbaciti paket).

Najčešće korišteni vatrozid sustavi ispituju barem 5 osnovnih polja u zaglavlju paketa što znači da pravila sadrže barem 5 varijabli o kojima ovisi hoće li vatrozid sustav propustiti ili odbaciti paket [1]. Ona su:

1. protokol,
2. IP adresa izvora,
3. broj priključnice izvora,
4. IP adresa odredišta i
5. broj priključnice odredišta

Paket se propušta ili odbacuje na temelju određenog pravila ako se sve promatrane informacije iz zaglavlja paketa podudaraju sa odgovarajućim poljima u tom pravilu. U suprotnom, ispituje se sljedeće pravilo po redu i taj postupak se ponavlja sve dok se ne pronađe prvo pravilo koje se podudara u potpunosti.

Vatrozid sustav se treba ponašati deterministički (dakle za isti paket treba uvijek izvesti isto pravilo). Mogućnosti za nedeterminističko ponašanje su, na primjer, razni konflikti i anomalije u pravilima. Do anomalija će doći ako

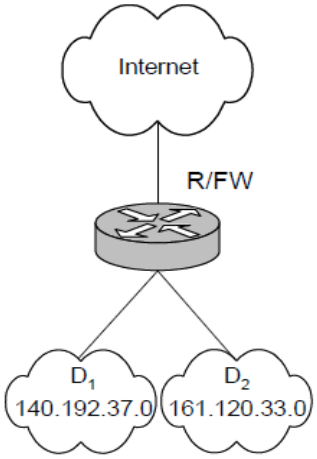
1. dva ili više pravila vrijede za isti paket ili
2. se pravilo ne podudara s nijednim paketom koji prolazi kroz vatrozid sustav.

Kako se broj sigurnosnih pravila povećava, povećava se i vjerojatnost anomalija. Zbog toga je vrlo važno otkriti i ukloniti ove anomalije na vrijeme, barem kako bi skup sigurnosnih pravila bio bez konflikta.

Anomalije se mogu podijeliti u 5 osnovnih razreda [2] :

1. zasjenjivanje (eng. *Shadowing anomaly*),
2. redundancija (eng. *Redundancy anomaly*),
3. korelacija (eng. *Correlation anomaly*),
4. poopćenje (eng. *Generalization anomaly*) i
5. nevažna pravila (eng. *Irrelevance anomaly*)

U nastavku slijedi detaljniji pregled navedenih anomalija pri čemu će se za ilustraciju anomalija koristiti skup sigurnosnih pravila vatrozid sustava sa Slike 2 (Tablica 1).



Slika 2. *Topologija mreže sa vatrozid sustavom*
Izvor: *Al-Shaer, Hamed " Discovery of Policy Anomalies in Distributed Firewalls "*

Red. br.	Protokol	IP izvora	Port izvora	IP odredišta	Port odredišta	Akcija
1.	TCP	140.192.37.20	ANY	*.*.*.*	80	Odbaci
2.	TCP	140.192.37.*	ANY	*.*.*.*	80	Propusti
3.	TCP	*.*.*.*	ANY	161.120.33.40	80	Propusti
4.	TCP	140.192.37.*	ANY	161.120.33.40	80	Odbaci
5.	TCP	140.192.37.30	ANY	*.*.*.*	22	Odbaci
6.	TCP	140.192.37.*	ANY	*.*.*.*	22	Propusti
7.	TCP	140.192.37.*	ANY	161.120.33.40	22	Propusti
8.	TCP	*.*.*.*	ANY	*.*.*.*	ANY	Odbaci
9.	UDP	140.192.37.*	ANY	161.120.33.40	53	Propusti
10.	UDP	*.*.*.*	ANY	161.120.33.40	53	Propusti
11.	UDP	140.192.38.*	ANY	1161.120.35.*	ANY	Propusti
12.	UDP	*.*.*.*	ANY	*.*.*.*	ANY	Odbaci

Tablica 1. *Sigurnosna pravila vatrozid sustava*
Izvor: *Al-Shaer, Hamed " Discovery of Policy Anomalies in Distributed Firewalls "*

2.1. Zasjenjivanje

Pravilo je zasjenjeno kada se neko pravilo ispred njega podudara sa svim paketima s kojima bi se zasjenjeno pravilo podudaralo, a da pri tom pravila ne obavljaju istu akciju. To dovodi do nemogućnosti izvođenja zasjenjenog pravila, što izaziva neregularnost u radu vatrozid sustava.

Kao primjer zasjenjivanja služe pravila 4 i 3 iz Tablice 1. Pravilo 4 je zasjenjeno pravilom 3 i nikada neće biti aktivirano. Svaki paket koji bi se trebao podudariti s pravilom 4 bit će podudaren s pravilom 3 i paket će biti propušten, umjesto da bude odbačen kako je određeno pravilom 4 koje je zasjenjeno.

Ovu vrstu anomalije je jako bitno otkriti na vrijeme i upozoriti adminitratora da promijeni redoslijed pravila.

2.2. Redundancija

Redundantno pravilo obavlja istu akciju nad nekim paketom kao i neko drugo pravilo. Ukoliko se redundantno pravilo ukloni to neće utjecati na sigurnosna pravila i konačan ishod odluke.

Kao primjer redundancije služe pravila 6 i 7 iz Tablice 1. Svi paketi koji se podudaraju s pravilom 7 također se podudaraju s pravilom 6 koje je općenitije, stoga je pravilo 7 višak.

Redundancija se smatra greškom u sigurnosnim pravilima jer redundantno pravilo povećava listu sigurnosnih pravila koju vatrozid sustava mora pretražiti, čime se povećava vrijeme pretrage i nepotrebno zauzima memorijski prostor.

2.3. Korelacija

Dva pravila su u korelaciji ako obavljaju različite akcije i prvo pravilo se podudara s nekim paketima koji se podudaraju s drugim pravilom, dok se drugo pravilo podudara s nekim paketima koji se podudaraju s prvim pravilom. Kako se pravila ne poklapaju u potpunosti nijedno se nemože ukloniti. Ipak, redoslijed provjeravanja podudaranja pravila s paketom utječe na krajnji rezultat za neke pakete.

Kao primjer korelacije služe pravila 1 i 3 iz Tablice 1. Ta dva pravila su u korelaciji jer IP adresa izvora u pravilu 1 se podudara s IP adresom izvora u pravilu 3, dok obrnuto ne vrijedi. IP adresa odredišta u pravilu 3 se podudara s IP adresom odredišta u pravilu 1, dok obrnuto ne vrijedi. Ova dva pravila u ovom redoslijedu impliciraju odbacivanje cijelog prometa koji dolazi sa 140.192.37.20 i ide prema 161.120.33.40. Ukoliko bi pravila bila navedena u obrnutom redoslijedu, sav taj isti promet bi bio prihvaćen.

Korelacija se smatra upozorenjem na anomaliju jer pravila koja su u korelaciji impliciraju akciju koja nije eksplicitno navedena u filtrirajućim pravilima. Kako bi se riješio ovaj konflikt potrebno je istaknuti korelaciju među pravilima administratoru kako bi odabrao koji redoslijed pravila odgovara zahtjevima sigurnosti.

2.4. Poopćenje

Pravilo je poopćenje nekog prethodnog pravila ako pravila imaju različite akcije i drugo pravilo se podudara sa svim pravilima koja se podudaraju s prvim pravilom.

Kao primjer poopćenja služe pravila 2 i 1 iz Tablice 1. Pravilo 2 je poopćenje pravila 1. Ova dva pravila impliciraju prihvaćanje cijelog prometa koji dolazi s adrese 140.192.37.*, osim onog koji dolazi s adrese 140.192.37.20.

Poopćenje se često koristi da se isključi specifični dio prometa iz općenite filtrirajuće akcije. Ovo je samo oblik upozorenja na anomaliju jer specifično pravilo čini iznimku od općenitog pravila. Ovisno o redoslijedu kojim su ova dva pravila navedena, promet koji bi trebao biti prihvaćen može biti blokiran, ali i obrnuto.

2.5. Nevažno pravilo

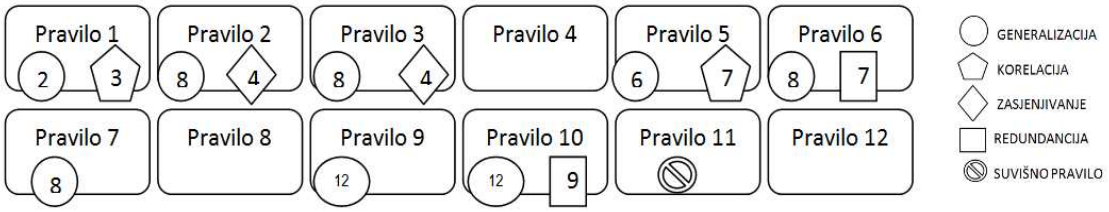
Pravilo koje nikada neće biti podudareno s nekim paketom.

Kao primjer nevažnog pravila služi pravilo 11 iz Tablice 1. Promet koji ide od izvorišta (140.192.38.*) do odredišta (161.120.35.*) ne prolazi kroz vatrozid sustav.

Pravilo iz skupa sigurnosnih pravila je nevažno ako se ne može podudariti s nijednim paketom koji može proći kroz vatrozid sustav. Do toga dolazi ako put od adrese izvora do adrese odredišta navedenih u pravilu ne prolazi kroz vatrozid sustav. Dakle, ovo pravilo nema nikakav utjecaj na ishod filtriranja i smatra se anomalijom jer nepotrebno dodaje posao vatrozid sustavu tijekom filtriranja paketa.

Održavanje tablice s pravilima za filtriranje što manjom pomaže u ukupnom poboljšanju performansi vatrozid sustava.Upravo zbog toga otkrivanje i izbacivanje nevažnih pravila je jako bitan zadatak administratora mrežne sigurnosti.

Potpuni popis svih anomalija na skupu sigurnosnih pravila danih u Tablici 1 prikazan je na Slici 3.



***Slika 3**. Sve anomalije na skupu sigurnosnih pravila*
***Izvor:** CIS*

3. Zavisnosti između sigurnosnih pravila

U svrhu izgradnje korisnog skupa pravila za filtriranje prometa potrebno je poznavati zavisnosti ili odnose koji mogu postojati među sigurnosnim pravilima. U nastavku slijedi prikaz svih mogućih odnosa između sigurnosnih pravila koja se utvrđuju na temelju usporedbe prije spomenutog niza polja na temelju kojih se filtrira promet [2].

- **Potpuno razdvojena pravila** (eng. *completely disjoint*)

  Ako dva pravila X i Y nemaju dodirnih točaka, tj. svako polje pravila X nije niti podskup, niti nadskup niti je jednako odgovarajućem polju iz pravila Y, kažemo da su pravila X i Y potpuno razdvojena pravila.
- **Identična pravila** (eng. *exactly matching*)

  Ako je svako polje pravila X jednako odgovarajućem polju pravila Y kažemo da su pravila X i Y identična.
- **Uključivo podudarajuća pravila** (eng. *inclusively matching*)

  Ako se dva pravila X i Y ne podudaraju u potpunosti, već je svako polje pravila X podskup ili je jednako odgovarajućem polju pravila Y, kažemo da se pravilo X uključivo podudara s pravilom Y.

  (primjer iz Tablice 1 : pravilo 1 uključivo se podudara s pravilom 2)
- **Dijelomično radvojena pravila** (ili dijelomično podudarajuća) (eng. *partially disjoint/partially matching)*

  Ako postoji barem jedno polje u pravilu X koje je podskup ili nadskup ili je jednako odgovarajućem polju pravila Y i ako postoji barem jedno polje pravila X koje nije ni nadskup, ni podskup niti je jednako odgovarajućem polju pravila Y, kažemo da su pravila X i Y dijelomično razdvojena pravila.

  (primjer iz Tablice 1 : pravila 2 i 6 su dijelomično razdvojena)
- **Pravila u korelaciji** (eng. *correlated*)

  Ako su neka polja iz pravila X podskup ili jednaka odgovarajućim poljima pravila Y, a ostatak polja pravila X su nadskupovi odgovarajućih polja pravila Y, kažemo da su pravila X i Y u korelaciji.

  (primjer iz Tablice 1 : pravila 1 i 3 su u korelaciji)

Ovdje navedene relacije su međusobno odvojene (samo jedna relacija može vezati pravila X i Y) i čine potpun skup (ne postoji više nijedna relacija osim ovdje navedenih).

Redoslijed pravila za filtriranje je jako bitan jer se proces filtriranja provodi na način da se paket slijedno uspoređuje s pravilima za filtriranje sve dok ne dođe do podudaranja. Ako su pravila potpuno razdvojena njihov redoslijed nije bitan. U praksi je česta pojava pravila koja se podudaraju na neki način. U tom slučaju, ako redoslijed nije pažljivo odabran, neka pravila mogu biti zasjenjena drugim pravilima što dovodi do nepravilnosti u radu vatrozid sustava. Nadalje, što je skup pravila za filtriranje

veći, to je veća vjerojatost pojave konflikata ili suvišnih pravila, a sve to skupa narušava rad vatrozid sustava.

4. Optimiziranje korištenjem *Data Mining*-a

Jedan od zanimljivijih problema kada su u pitanju sigurnosna pravila vatrozid sustava je i pitanje koliko su pravila korisna i dobro organizirana te jesu li u skladu s trenutnim svojstvima mrežnih paketa. Na primjer, praćenjem trenda u mreženom prometu može se pokazati da su neka pravila zastarjela ili nisu korištena u posljednje vrijeme, što može biti poticaj administratoru kako bi uklonio ili razmjestio takva pravila u svrhu optimiziranja učinkovitosti vatrozid sustava.

Prvi korak u uklanjanju potencijalnog neslaganja između onog što piše u sigurnosnim pravilima i onog što se stvarno događa na mreži je analiza prometa i log datoteka korištenjem tehnika *Data Mining*-a.

4.1. Tehnike Data Mining-a

Data Mining je metoda kojom se pretražuje ogromna količina podataka kako bi se pronašao neki trend ili uzorak u tim podacima koji bi olakšao i usmjerio daljnju analizu i rad s tim podacima. Postoji nekoliko pristupa *Data Mining*-a kao što su stablo odluka (eng. *Decision tree*) i rudarenje pravila pridruživanja (eng.Association Rule Mining, ARM).

4.1.1. Stablo odluka

Stablo odluka je prediktivni model koji može biti prikazan kao stablo. Stablo nastaje grananjem kao posljedica ispunjenja uvjeta klasifikacijskih pitanja. Svako pitanje će podjeliti podatke u podskupine koje su homogenije nego viša skupina. Ako pitanje ima dva odgovora, tada će kao odgovor na pitanje nastati dvije podskupine (binarno stablo). Općenito, koliko pitanje ima odgovora toliko će podskupina nastati. Samim time obavlja se klasificiranje pojedinih podataka.

Svaki čvor stabla predstavlja atribut, svaka grana stabla predstavlja usporedbu vrijednosti, a svaki list stabla predstavlja jednu klasifikacijsku skupinu.

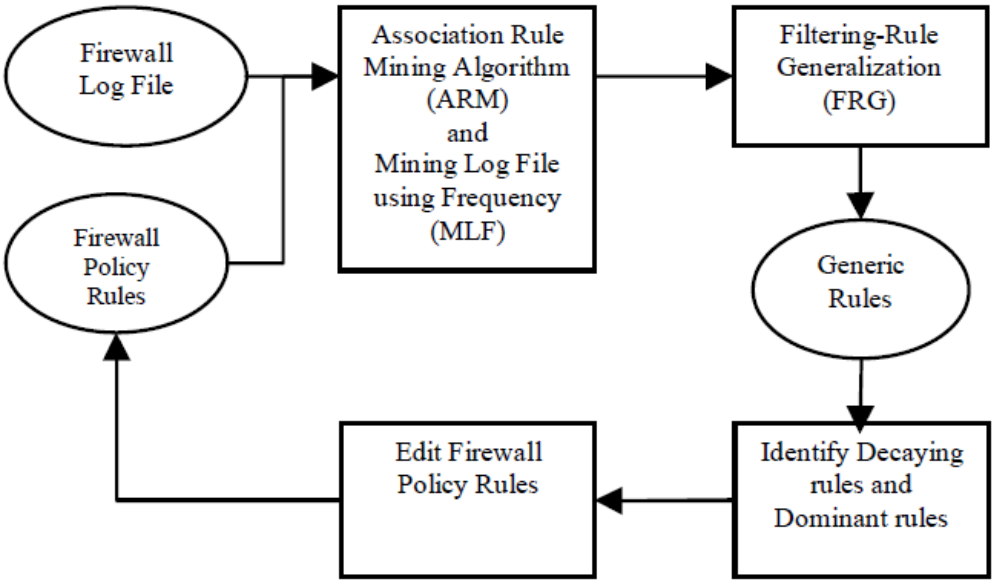
4.1.2. Association Rule Mining (ARM)

ARM je jedna od najvažnijih i najistraženijih tehnika *Data Mining*-a. Cilj joj je izvući zanimljive korelacije, česte uzorke ponašanja ili veze iz raznih skupova podataka. Pravila pridruživanja su često korištena u raznim područjima kao što su telekomunikacijske mreže, ekonomija i slično.

ARM se kod optimizacije vatrozid sustava može koristiti za pronalazak uzoraka ponašanja u skupu sigurnosnih pravila, nakon čega se taj uzorak ponašanja može oblikovati u novi skup pravila, detaljnjiji od početnog skupa sigurnosnih pravila.

4.2. Primjer optimizacije pomoću metoda Data Mining-a

Jedan od pristupa optimizacije vatrozid sustava pomoću *Data Mining*-a dan je u primjeru navedenom u dodatnoj literaturi [3]. U tom pristupu *Data Mining* tehnika se koristi kako bi se iz log datoteke vatrozid sustava dobio novi skup sigurnosnih pravila. Taj skup se potom grupira u skup općenitijih pravila, filtrira i dodaje već postojećem skupu pravila nakon čega se uklanjaju suvišna pravila i moguće anomalije kako bi se dobio optimalan skup sigurnosnih pravila (Slika 8).



Slika 4. *Dijagram toka optimizacije vatrozid sustava korištenjem Data Mining-a*
Izvor: *Golnabi, Min, Khan "Analysis of Firewall Policy Rules Using Data Mining Techniques"*

Dakle, opisana metoda optimizacije vatrozid sustava podrazumijeva sljedeće korake :

1. Stvoriti log datoteku vatrozid sustava korištenjem početnog skupa sigurnosnih pravila.
2. Pomoću metode rudarenja log datoteke vatrozid sustava korištenjem učestalosti pojavljivanja (eng.Mining Firewall Log using Frequency,MLF) potrebno je iz log datoteke izvući jedinstvene kombinacije atributa i broj pojavljivanja svake kombinacije u čitavoj log datoteci. Time se dobiva novi, opsežni skup pravila.
3. Generalizirati dobivena pravila pomoću algoritma poopćavanja skupa pravila za filtriranje prometa (eng.Filtring-Rule Generalization, FRG)[1] kako bi se smanjio broj pravila.
4. Kombinirati dobivena generalizirana pravila s početnim skupom sigurnosnih pravila.
5. Detektirati anomalije u tako dobivenom skupu pravila i ispraviti ih.
6. Na temelju frekvencije pojavljivanja pojedinog pravila (frekvencija se dobije tako da se broj pojavljivanja svakog pravila dobiven iz koraka 2 i 3 podijeli s ukupnim brojem zapisa u log datoteci) donese se zaključak o tom je li pravilo beskorisno, zastarjelo ili dominira u ukupnom prometu.
7. U skladu sa donesenim zaključcima mijenja se skup sigurnosnih pravila.

U ovom poglavlju opisana je tehnika *Data Mining*-a koja se može koristiti prilikom optimizacije vatrozid sustava (koraci 1 i 2). Ta tehnika predstavlja samo prvi korak u optimizaciji, kojim se dobiju sigurnosna pravila koja su učinkovita pri radu vatrozid sustava. Ta pravila potrebno je generalizirati (više detaljnijih pravila povezati u jedno općenitije pravilo) kako bi se smanjio broj

[1] Algoritam FGR koristi stablo odluke kako bi ispitao svako pravilo iz početnog skupa. Svako pravilo se analizira i pokušava grupirati s nekim drugim pravilom na temelju sličnih polja kako bi se dobio nadskup općenitijih pravila, gdje se svako općenitije pravilo podudara sa nekim skupom jedinstvenih pravila.

pravila. Generalizirana pravila se zatim spajaju s početnim pravilima, čime se dobije novi i potpuniji skup sigurnosnih pravila.

Iz tog skupa zatim je potrebno ukloniti anomalije. Nakon uklanjanja anomalija preporuča se primjena neke metode dodatne optimizacije, koja bi optimizirala redoslijed ispitivanja ovako dobivenih sigurnosnih pravila. U primjeru iz [3] koristi se znanje stečeno *Data Mining*-om o frekvenciji podudaranja pojedinog pravila.

4.2.1. Mining Firewall Log using Frequency (MLF)

Algoritam *Data Mining*-a korišten kao prvi korak pri optimizaciji vatrozid sustava iz primjera pod [3] jest algoritam „Mining Firewall Log using Frequency“. Navedeni algoritam čita liniju po liniju log datoteke, izvlači atribute koji se koriste u sigurnosnim pravilima (npr. protokol, smjer paketa, IP adresa izvora, priključnica izvora, IP adresu odredišta, priključnica odredišta, akciju) za svaki log zapis te broji pojavljivanje takve kombinacije promatranih atributa u cijelom logu. Svako pravilo zapisano u log datoteci smatra se primitivnim pravilom jer su vrijednosti svih atributa točno definirane.

Dakle, cilj MLF metode je pronaći sve postojeće kombinacije promatranih atributa u log datoteci i broj pojavljivanja svake kombinacije. Algoritam MLF metode prikazan je u nastavku.

```
Algoritam MLF
Ulaz: log datoteka vatrozid sustava
Izlaz: jedinstvena pravila i njihova frekvencija

Broj_paketa <- 0
FOR EACH linija u log datoteci
      Pravilo[Broj_paketa]<- protokol,smjer,IP_izvor,Port_izvor,
                        IP_odredište,Port_odredište,akcija
      Broj_paketa++
END FOR

FOR EACH i WHERE 0<=i<Broj_paketa
      Frekvencija<-0
      FOR EACH j WHERE i<j<Broj_paketa
            IF Pravilo[i]=Pravilo[j]
                  Frekvancija++
            ENF IF
      END FOR

      IF Pravilo[i] NOT prije otkriveno
            zapiši Pravilo[i] i Frekvencija
      ELSE Continue
      END IF
END FOR
```

Jedno od ograničenja ovakvog pristupa rudarenju podataka s ciljem izvlačenja IP adresa i brojeva priključnica jest u tom što je rezultat u konačnici vezan samo za ono što je sadržano u log datoteci, a zapravo bi trebao biti upravljan sigurnosnom politikom koju vatrozid sustav treba poštivati. Naime, osim u idealnoj situaciji, log datoteka neće prikazivati sve moguće IP adrese koje se mogu pojaviti tijekom rada vatrozid sustava, pa skup pravila stvorenih pomoću ove tehnike i daljnje generalizacije tako dobivenih pravila zapravo predstavlja tek podskup sigurnosnih pravila. Zbog toga je generalizirana pravila potrebno kombinirati s početnim skupom sigurnosnih pravila. Nakon toga potrebno je iskoristiti znanje dobiveno iz rudarenja log datoteke o učestalosti pojavljivanja pojedinog pravila kako bi se pokušao promijeniti redoslijed ispitivanja sigurnosnih pravila s ciljem da pravila s većom frekvencijom pojavljivanja budu ispitana ranije.

5. Optimiziranje korištenjem *Directed Acyclical Graphs* tehnike

Jedan od načina optimiziranja vatrozid sustava s listom sigurnosnih pravila jest metoda predstavljena u dodatnoj literaturi pod [4]. Temelji se na promjeni redoslijeda pravila u listi kako bi se minimizirao broj potrebnih usporedbi pri traženju akcije koju treba izvesti za neki paket. Pri tome se postavlja uvjet da se sačuva integritet početne liste sigurnosnih pravila. Integritet je sačuvan ako izmjenjena i izvorna lista dolaze do iste akcije za isti paket. Prilikom izmjene redoslijeda pravila koriste se usmjereni aciklički grafovi (eng. *Directed Acyclical Graphs*, DAG).

5.1. Oblikovanje sigurnosnih pravila

Kao što je već prije opisano, skup sigurnosnih pravila vatrozid sustava je zapravo lista od n pravila, koju zapisujemo kao $R = \{r_1, r_2,...,r_n\}$. Paket d koji dolazi na vatrozid sustav se slijedno uspoređuje sa pravilima r_i, počevši od prvog, dok ne dođe do podudaranja ($d => r_i$) nakon čega vatrozid izvede akciju naznačenu u podudarenom pravilu. Do podudaranja dolazi ako je svako promatrano polje paketa podskup odgovarajućeg polja pravila.

Kao što je prikazano u poglavlju 2, postoji uvjet na redoslijed pravila u listi. Pojedina pravila se moraju pojaviti prije nekih drugih pravila kako bi se sačuvao integritet liste i kako bi vatrozid sustav funkcionirao u skladu sa postavljenim zahtjevima. Taj oblik ovisnosti nekog pravila o drugom naziva se **odnos prvenstva** (eng. *precedence relationship*). Pravila među kojima ne postoji odnos prvenstva (potpuno razdvojena pravila) dozvoljavaju međusobni razmještaj bez utjecaja na integritet vatrozid sustava.

Metoda optimizacije pomoću Directed Acyclical Graphs tehnike pretpostavlja ovakav tip pravila navedenih u nekom redoslijedu među kojima postoji bilo kakva razina međusobne ovisnosti (odnosa prvenstva). Stoga se prilikom optimizacije putem mijenjanja redoslijeda pravila mora obratiti pažnja kako se ne bi narušili odnosi prvenstva.

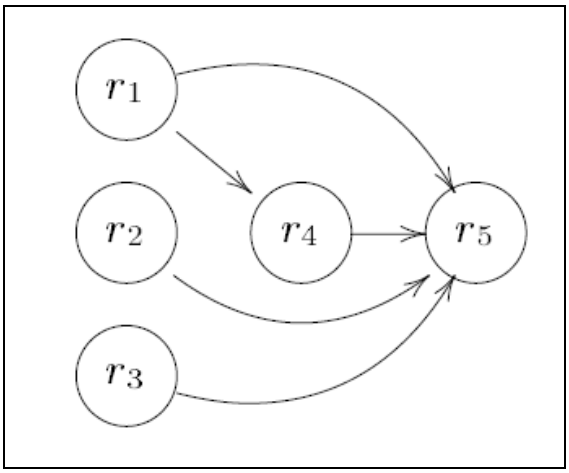
Za ilustraciju metode koristit će se skup sigurnosnih pravila iz Tablice 2.

Red.br.	Protokol	IP izvora	Port izvora	IP odredišta	Port odredišta	Akcija	Vjerojatnost podudaranja
1.	UDP	1.1.*	*	*	80	Odbaci	0.01
2.	TCP	1.*	*	1.*	90	Prihvati	0.02
3.	TCP	2.*	*	2.*	20	Prihvati	0.25
4.	UDP	1.*	*	*	*	Prihvati	0.22
5.	*	*	*	*	*	Odbaci	0.50

Tablica 2. *Lista sigurnosnih pravila koja se koriste prilikom ilustracije DAG metode*
Izvor: *Fulp " Optimization of Network Firewall Policies using Directed Acyclical Graphs"*

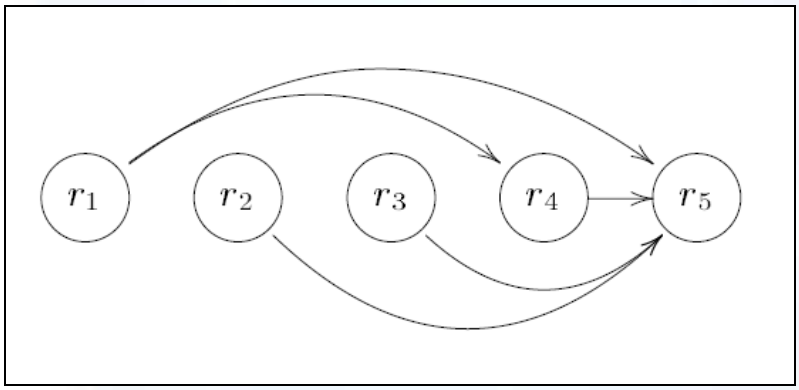
5.2. Modeliranje odnosa prvenstva

Neka je $G = \{R, E\}$ DAG za skup pravila R pri čemu su vrhovi grafa pravila, a bridovi E pokazuju da među pravilima koja dotični brid spaja postoji odnos prvenstva. Odnos prvenstva postoji među pravilima r_i i r_j ako je $i<j$ i pravila su ovisna (svako polje pravila i se siječe s odgovarajućim poljem pravila j). Na ovaj način stvara se DAG za skup pravila iz Tablice 2 (Slika 4).



Slika 5. *DAG za pravila iz Tablice 2*
Izvor: *Fulp " Optimization of Network Firewall Policies using Directed Acyclical Graphs"*

Koristeći prikaz sigurnosnih pravila preko DAG-a pokušava se pronaći linearan raspored pravila koji bi poboljšao performanse vatrozid sustava. Linearan raspored je zapravo lista vrhova DAG-a gdje se svi sljedbenici nekog vrha pojavljuju u slijedu nakon tog vrha (Slika 5). Dakle, linearan raspored DAG-a predstavlja zapravo redoslijed ispitivanja pravila ako se vrhovi čitaju s lijeva na desno. Nadalje, dokazano je (dodatna literatura [4]) da bilo koji linearni raspored DAG-a zadržava integritet vatrozid sustava.



Slika 6. *Početni izgled linearnog rasporeda DAGa koji odgovara početnom redoslijedu pravila u Tablici 2*
Izvor: *Fulp " Optimization of Network Firewall Policies using Directed Acyclical Graphs"*

5.3. Optimizacija liste sigurnosnih pravila

U postupku optimizacije vatrozid sustava DAG se koristi kako bi se očuvao integritet sustava. Kako bi se optimizirao rad samog sustava potrebno je pronaći linearan raspored DAG-a koji će imati najmanji broj potrebnih usporedbi paketa s pravilima. Neka sigurnosna pravila imaju veću vjerojatnost podudaranja s paketom od drugih. Stoga je tijekom vremena moguće razviti profil pravila (eng. *policy profile*) koji kazuje frekvenciju podudaranja paketa s pravilom.

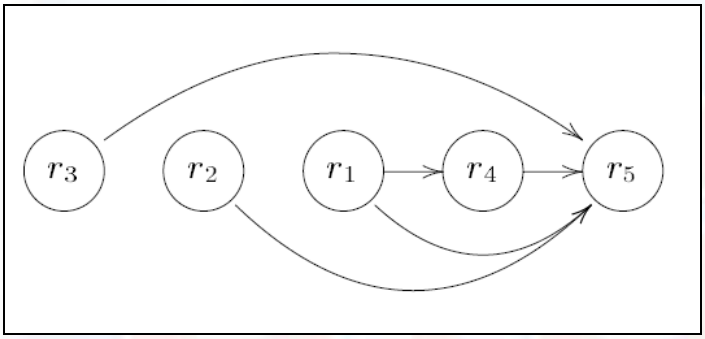
Recimo da je $P = \{p_1,p_2,...p_n\}$ profil pravila u kojem p_i predstavlja vjerojatnost da će se paket podudariti s pravilom *i*. Pomoću početnog DAG-a i profila pravila *P* traži se onaj linearan raspored pravila koji bi rezultirao najmanjim vremenom uspoređivanja paketa s pravilima. Ako ne postoji niti jedan odnos prvenstva u cijelom skupu pravila, prosječno vrijeme traženja podudaranja je najmanje ako su pravila složena u skladu s opadajućim vjerojatnostima podudaranja. Ako postoji odnos prvenstva stvar se komplicira. U tom slučaju traženje optimalnog redoslijeda sigurnosnih pravila postaje NP-težak problem.

5.3.1. Jednostavan algoritam za slaganje pravila

Iako je traženje optimalnog redoslijeda sigurnosnih pravila NP-težak problem, uz algoritam u nastavku moguće je smanjiti vrijeme traženja podudarajućeg pravila. Algoritam slaže susjedna pravila po opadajućim vjerojatnostima podudaranja uz uvjet da do zamjene mjesta među susjednim pravilima ne dolazi ako se pravila preklapaju (tj. u DAGu postoji brid E među vrhovima koji predstavljaju dotična pravila), čime je integritet očuvan.

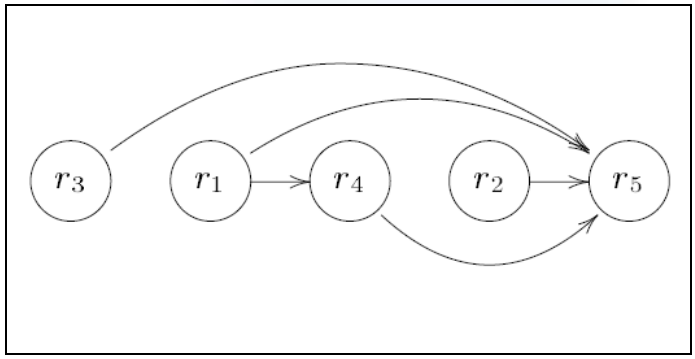
```
done = false
while(!done)
     done = true
     for(i=1;i<n;i++)
           if(p_i< p_i+1 AND r_i∩r_i+1) then
                 zamijeni mjesta pravilima i vjerojatnostima
                 done = false
           endif
     endfor
endwhile
```

Primjenom algoritma na skup pravila iz Tablice 2 dobije se linearan raspored DAG-a kao na Slici 6. pri čemu je broj usporedbi pri traženju podudarajućeg pravila smanjen za 11% u odnosu na prosjek.



Slika 7. *Sortirani redoslijed pravila dobiven primjenom danog algoritma*
Izvor: *Fulp " Optimization of Network Firewall Policies using Directed Acyclical Graphs"*

Ipak, kod upotrebe danog algoritma postoji mogućnost da neko pravilo spriječi premještanje nekog drugog pravila (na primjeru Tablice 1 pravilo 1 spriječilo je premještaj pravila 4). Optimalan redoslijed pravila za primjer skupa sigurnosnih pravila danog u tablici 1 prikazan je na Slici 7.



Slika 8. *Optimalan redoslijed pravila iz Tablice 2*
Izvor: *Fulp " Optimization of Network Firewall Policies using Directed Acyclical Graphs"*

6. Optimiziranje na temelju karakteristika mrežnog prometa

Iako je pristup iz primjera u literaturi [3] opisan u poglavlju 4 također koristio optimiziranje na temelju karakteristika mrežnog prometa, pristup opisan u primjeru [5] donosi puno detaljniji način ovakve optimizacije vatrozid sustava. Također, valja istaknuti da se ovaj pristup koristi za više-dimenzijska sigurnosna pravila (IP izvora ili IP odredišta može imati više od jedne vrijednosti, pri čemu su vrijednosti jasno definirane, a ne predstavljaju raspon).

Prvi korak je uklanjanje svih suvišnih pravila iz skupa sigurnosnih pravila (redundantna i nevažna pravila). Nakon njega slijede dvije važne komponente cijelog sustava koje će biti opisane u nastavku.

6.1. Optimizacija na temelju skupa pravila

Prvi korak prilikom optimizacije jest optimizacija samog skupa sigurnosnih pravila s ciljem uklanjanja svih ovisnosti među pravilima kako bi se omogućilo nesmetano razmiještanje pravila prilikom drugog dijela optimizacije temeljenog na karakteristikama samog prometa.

Prvo je potrebno od ulaznog skupa pravila, koji sadrži ovisnosti među pravilima, stvoriti skup pravila koji će sadržavati potpuno razdvojena pravila. Ovaj postupak može rezultirati u povećanju dimenzija skupa pravila budući da može biti potrebno više pravila koja će nadomjestiti dva međusobno zavisna pravila.

Nakon što se dobije skup potpuno razdvojenih pravila potrebno je pokušati spojiti više pravila u jedno zajedničko ako je to moguće, kako bi se smanjio broj pravila. Spajanje dvaju pravila u jedno obavlja se na temelju iste akcije, pod uvjetom da je najviše jedno polje ima različite vrijednosti.

Na primjeru ulaznog skupa sigurnosnih pravila iz Tablice 3 vidi se da su pravila R_1 i R_2 međusobno ovisna, jer polje izvora i odredišta pravila R_2 se siječe s vrijednostima odgovarajućih polja pravila R_1, dok su akcije koje izazivaju ova pravila različite. Ova pravila se mogu učiniti potpuno razdvojenim ako R_1 ne mijenjamo, a R_2 podijelimo na 2 nova pravila (Tablica 4) čime se dobije skup potpuno razdvojenih pravila. Taj skup se dalje može dodatno optimizirati spajanjem pravila $R_{2,2}$ i R_3 u novo pravilo R_4, čime se dobije konačan skup sigurnosnih pravila koji se dalje optimizira na temelju karakteristika mrežnog prometa.

Pravilo	Izvor	Odredište	Akcija
R_1	s_1,s_2,s_3	d_1,d_2,d_3	Odbaci
R_2	s_2,s_3,s_4	d_2,d_3,d_4	Prihvati
R_3	s_5	d_4	Prihvati

Tablica 3. *Ulazni skup sigurnosnih pravila*
Izvor: *Acharya, Wang, Ge, Znati,Greenberg "Traffic-Aware Firewall Optimization Strategies"*

Pravilo	Izvor	Odredište	Akcija
R_1	s_1,s_2,s_3	d_1,d_2,d_3	Odbaci
$R_{2,1}$	s_4	d_2,d_3,d_4	Prihvati
$R_{2,2}$	s_2,s_3	d_4	Prihvati
R_3	s_5	d_4	Prihvati

Tablica 4. *Skup potpuno razdvojenih pravila*
Izvor: *Acharya, Wang, Ge, Znati,Greenberg "Traffic-Aware Firewall Optimization Strategies"*

Pravilo	Izvor	Odredište	Akcija
R_1	s_1,s_2,s_3	d_1,d_2,d_3	Odbaci
$R_{2,1}$	s_4	d_2,d_3,d_4	Prihvati
R_4	s_2,s_3,s_5	d_4	Prihvati

Tablica 5. *Konačan skup sigurnosnih pravila*
Izvor: *Acharya, Wang, Ge, Znati,Greenberg "Traffic-Aware Firewall Optimization Strategies"*

6.2. Optimiziranje na temelju karakteristika mrežnog prometa

Prethodno optimiziran skup potpuno razdvojenih pravila predstavlja ulaz u drugi korak optimizacije temeljen na karakteristikama mrežnog prometa. U postizanju tog cilja koriste se 4 sheme:

1. ***Hot caching***: Cilj je pronaći mali skup "vrućih" pravila, tj. pravila koja imaju najveći broj podudaranja, i staviti ih na početak liste. Tim se postiže da se u većini slučajeva podudaranje pronađe odmah na početku pretrage, čime se smanjuje samo vrijeme traženja. U usporedbi s metodom opisanom u [3] ovdje je situacija uvelike olakšana činjenicom da su pravila potpuno razdvojena pa ne treba voditi računa o ovisnosti među pravilima.
2. ***Total re-ordering***: Ovaj pristup u obzir ne uzima samo frekvenciju pojavljivanja podudaranja pojedinog pravila, nego i njegovu veličinu. Točnije, pravilo se ispituje prije ako mu je omjer broja pogodaka i veličine veći.
3. ***Default proxy***: Temelji se na činjenici da se jako često paket podudara sa zadanim pravilom čija akcija jest odbiti paket. Zadano pravilo se poziva ako se paket nije podudario s nijednim pravilom iz skupa pravila. Ova shema rješava taj problem stvaranjem novog skupa pravila čija akcija je Odbaci, a koji se stvara na način da se pravilo doda u skup ako se dotični pakat odbacio podudarivši se sa zadanim pravilom.
4. ***Online adaptation***: Koristi dvije metode. Pomoću prve metode stvara se dugoročni profil podudaranja pravila na temelju karakteristika mrežnog prometa. Taj profil se zatim uspoređuje s kratkoročnim uzorkom prometa. Ako postoji veliko odstupanje među njima (koje može dovesti do krivog rada vatrozid sustava) sigunosna pravila se mijenjaju. Ova shema povezuje znanje dobiveno iz statične log datoteke sa dinamičkim zbivanjem na mreži, a u skladu s tim potencijalo optimizira skup sigurnosnih pravila.

Dakle, skup pravila dobiven nakon provođenja optimizacija na temelju karakteristika mrežnog prometa koristi se u radu vatrozid sustava sve dok ne dođe do promjena u karakteristici mrežnog prometa. U tom trenutku pokreće se ponovno stvaranje optimiziranog skupa sigurnosnih pravila na temelju karakteristika mrežnog prometa (tj. provodi se drugi korak procesa, mijenjanje rasporeda pravila kako bi odgovarao trenutnoj situaciji na mreži).

7. Zaključak

Postoji velik broj različitih metoda za optimiziranje vatrozid sustava. U osnovi ih možemo podijeliti na dvije skupine. Prvu skupinu čine metode koje se koriste samo jednom, pri promjeni pravila. Spomenute metode sadrže algoritme koji nastoje izbaciti suvišna pravila i postići što optimalniji redoslijed pravila. Drugu skupinu čine metode koje nastoje saznati kakav je promet na mreži i u skladu s njim promijeniti redoslijed pravila.

Pri tom valja istaknuti da je korisno prije bilo koje optimizacijske metode iskoristiti neku od metoda za smanjenje veličine skupa sigurnosnih pravila. Na pitanje koju metodu optimizacije je najbolje (nakon toga) upotrijebiti ne postoji jedinstven (a pri tom i najbolji) odgovor. Neki algoritmi se zasnivaju na smanjenju iskorištavanja memorije, dok drugi na skraćivanju vremena traženja podudaranja.

Ovdje prikazane metode optimizacije imaju svoje prednosti i nedostatke. Metoda „Directed Acyclical Graphsa“ daje odlične rezultate ako se primjenjuje na veliki skup sigurnosnih pravila u kojem ima malo odnosa prvenstva. S druge strane, *data mining* tehnike se sve češće koriste prilikom optimizacije vatrozid sustava, osobito na log datotekama kako bi se na temelju karakteristika prometa optimizirao skup sigurnosnih pravila, a time i sam rad vatrozid sustava. Iako je to relativno nova metoda u optimizaciji vatrozid sustava, pokazuje jako dobre rezultate.

Samo gledanjem teoretske pozadine svakog algoritma ne može se pronaći pobjednik, stoga on ovisi o stvarnoj situaciji, a metodu optimizacije vatrozid sustava treba izabrati u skladu s potrebama i karakteristikama danog vatrozid sustava.

8. Leksikon pojmova

Data Mining

Relativno mlado i interdisciplinarno područje računarske znanosti koje se bavi otkrivanjem novih znanja u skupovima podataka.

http://en.wikipedia.org/wiki/Data_Mining

Directed Acyclical Graphs (DAG)

U matematici i računarskoj znanosti pojam predstavlja usmjereni graf bez ciklusa.

http://en.wikipedia.org/wiki/Directed_acyclic_graph

Filtring-Rule Generalization (FGR)

Algoritam poopćavanja skupa pravila za filtriranje prometa, opisan u [3]. Koristi se za smanjenje veličine skupa sigurnosnih pravila.

http://www.docstoc.com/docs/2363901/Analysis-of-Firewall-Policy-Rule-Using-Data-Mining-Techniques

IP protokol - Internet Protocol

IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

Mining Firewall Log using Frequency (MLF)

Metoda rudarenja log datoteke vatrozid sustava korištenjem učestalosti pojavljivanja sigurnosnih pravila, opisana u [3]. Koristi se kao metoda optimizacije vatrozid sustava.

http://www.arc.uncc.edu/pubs/noms06-mining.pdf

Priključnica

Brojčane vrijednosti temeljem kojih računalo po prihvatu podataka zna koju uslužnu programsku potporu (servise) mora aktivirati te na koji način razmjenjivati podatke na transportnom sloju.

http://www.iana.org/assignments/port-numbers

Payload

Na području informacijske sigurnosti, koristan teret označava odsječak koda pomoću kojeg se iskorištava određeni propust računala mete. Na primjer, koristan teret računalnog crva može sadržati modul za širenje vlastite kopije putem globalne mreže Internet.

http://searchsecurity.techtarget.com/definition/payload

Transmission Control Protocol (TCP)

Jedan od dva protokola usmjeravanja koja se koriste u Internetu, uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos. TCP se nalazi na transportnom sloju OSI modela. - Jedan od dva protokola usmjeravanja koja se koriste u Internetu. Uspostavlja logičku vezu između krajnjih računala i osigurava pouzdani prijenos.

http://www.webopedia.com/TERM/T/TCP.html

Vatrozid sustav

Uređaj čija je uloga zaštititi mrežu od neovlaštenog pristupa blokiranjem i zabranom prometa prema pravilima koje korisnik sam određuje.

http://en.wikipedia.org/wiki/Firewall(computing)

9. Reference

[1] Anssi Kolehmainen: Optimizing firewall performance
http://www.tml.tkk.fi/Publications/C/23/papers/Kolehmainen_final.pdf, listopad 2011.

[2] Ehab S. Al-Shaer; Hazem H. Hamed: Discovery of Policy Anomalies in Distributed Firewalls
http://www.ieee-infocom.org/2004/Papers/54_3.PDF, listopad 2011.

[3] Korosh Golnabi, Richard K. Min, Latifur Khan: Analysis of Firewall Policy Rules Using Data Mining Techniques
http://www.arc.uncc.edu/pubs/noms06-mining.pdf,listopad 2011.

[4] Errin W. Fulp: Optimization of Network Firewall Policies using Directed Acyclical Graphs
http://www.google.hr/url?sa=t&source=web&cd=1&ved=0CBUQFjAA&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.74.685%26rep%3Drep1%26type%3Dpdf&rct=j&q=firewall%20optimization%20Directed%20Acyclical%20Graphs&ei=QP8_TKOHLdahOMbapaUN&usg=AFQjCNHjkctU1dV7UG_igbVP3ZDdO2aYqA,
listopad 2011.

[5] Subrata Acharya; Jia Wang; Zihui Ge; Taieb F. Znati; Albert Greenberg: Traffic-Aware Firewall Optimization Strategies
http://www2.research.att.com/~jiawang/icc06.pdf, listopad 2011.