HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Logiranje NAT prometa

CCERT-PUBDOC-2006-06-160

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. UVOD 5

2. NAT 6

2.1. VRSTE NAT-OVA 6
2.2. IMPLEMENTACIJA NAT TEHNOLOGIJE 8
2.3. PRIMJENA NAT TEHNOLOGIJE 9
2.4. PREDNOSTI NAT TEHNOLOGIJE 10
2.5. NEDOSTACI NAT TEHNOLOGIJE 10
2.5.1. Protokoli na koje NAT ima negativni utjecaj 11
2.6. MODIFIKACIJE NAT TEHNOLOGIJE 11
2.6.1. STUN 11
2.6.2. TURN 12
2.6.3. ICE 12

3. PROBLEMATIKA LOGIRANJA 12

3.1. VAŽNOST LOGIRANJA NAT PROMETA 13
3.2. CENTRALIZIRANI SUSTAV LOGIRANJA 13
3.2.1. Sigurnost centralnog log poslužitelja 13
3.3. RAZINE VAŽNOSTI LOG ZAPISA 15
3.4. RAZDJELJIVANJE LOG ZAPISA 15
3.5. ARHIVIRANJE LOG ZAPISA 15
3.5.1. Sigurnost arhiviranih log zapisa 16
3.6. *SYSLOG* PROTOKOL I NJEGOVA EVOLUCIJA 16
3.7. PREDNOSTI LOG ZAPISA 17
3.8. NEDOSTACI LOG ZAPISA 17

4. TESTIRANJE RAZLIČITIH NAT IMPLEMENTACIJA 17

4.1. TESTNO OKRUŽENJE 18
4.2. WINDOWS 2003 SERVER 18
4.3. VATROZIDI ZASNOVANI NA IP TABLES ALATU 21
4.3.1. Astaro Security Gateway 6 21
4.3.2. Prototip Linux vatrozida razvijenog na LSS, ZESOI, FER 24
4.4. CISCO PIX 506E 28
4.5. TESTIRANJE VELIČINE NAT LOG ZAPISA NA ASTARO SECURITY GATEWAY 6 VATROZIDU 31

5. MOGUĆA UNAPREĐENJA LOGIRANJA NAT PROMETA 35

5.1. SIGURNOSNI ZAHTJEVI 35
5.1.1. Tajnost podataka 36
5.1.2. Integritet podataka 36
5.1.3. Autentikacija izvora podataka 36
5.1.4. Dostupnost 36
5.2. SUMIRANJE ZAPISA I VIZUALIZACIJA 37
5.3. NORMALIZIRANJE ZAPISA 37
5.4. KORIŠTENJE BAZA PODATAKA 37
5.5. AUTOMATIZIRANA OBRADA LOG ZAPISA 38
5.6. ALARMIRANJE 38
5.7. DEFINIRANJE NAZIVA ZA ODREĐENE VRIJEDNOSTI PARAMETARA LOG ZAPISA 38

6. ZAKLJUČAK 40

7. REFERENCE 40

1. Uvod

NAT (eng. *Network Address Translation*) tehnologija omogućava prepisivanje IP adresa u mrežnim paketima. Pri tome se izvorne IP adrese mijenjaju kad korisnici iz unutarnjih mreža pristupaju vanjskim resursima pa im usmjerivač zamjenjuje izvornu privatnu IP adresu sa svojom javnom IP adresom kako bi se odgovori mogli vratiti s Interneta. Ciljne IP adrese mijenjaju se kad je potrebno preusmjeriti određeni mrežni paket na drugu IP adresu.

U slučajevima kad lokalni korisnici urade određene neovlaštene aktivnosti na udaljenim računalima, na ciljanim računalima nalaze se log zapisi o neovlaštenim aktivnostima koje su napravljene s računala koje ima IP adresu jednaku NAT usmjerivaču. Stoga vlasnici tih resursa smatraju organizaciju odgovornom za neovlaštene aktivnosti. Kako bi se otkrili pravi zlonamjerni korisnici potrebno je logirati NAT promet.

U nastavku dokumenta raspoloživa je detaljna analiza NAT tehnologije pri čemu su navedene glavne vrste, uobičajena implementacija, primjena, prednosti i nedostaci te modifikacije NAT tehnologije. Potom je analizirana problematika logiranja događaja unutar koje je opisana važnost logiranja običnog i NAT prometa, razine važnosti, razdjeljivanje, prednosti i nedostaci te arhiviranje log zapisa. Također, vezano uz logiranje raspoloživ je i opis *syslog* protokola kao i općenitog centralnog sustava logiranja. U dokumentu je raspoloživ i prikaz testiranja NAT logiranja na različitim oblicima NAT implementacija (Windows 2003 Server, Ip Tables vatrozidi, PIX 506E), a na kraju je dan i prijedlog mogućih unapređenja logiranja NAT prometa.

2. NAT

NAT tehnologija definirana RFC 1631 specifikacijom [1] predstavlja prepisivanje izvorne ili ciljne IP adrese u mrežnom paketu s novom tijekom njihovog prelaska preko usmjerivača ili vatrozida. Mnoge organizacije koriste NAT kako bi omogućile "skrivenim" računalima pristup na Internet.
Glavni razlog za uvođenje NAT-a u organizacije nalazi se u nedovoljnom broju IP adresa zasnovanih na IPv4 protokolu. Internet je danas veoma velik, a točna veličina nije niti poznata. Pretpostavke su da postoji preko 100 milijuna računala priključenih na Internet, a broj korisnika na Internetu je preko 350 milijuna. Kako bi računalo moglo komunicirati na Internetu ono mora imati IP adresu čija je veličina 32 bitni broj koji identificira računalo na mreži. Teoretski postoji 2^{32} adresa što je preko 4 milijarde, ali pravi broj je negdje oko 3.2 milijarde zbog načina na koji su IP adrese grupirane u klase, i iz razloga što se neke IP adrese koriste za *multicast*, testiranje i druge specijalne svrhe. Također, većina IP adresa nalazi se rezervirana u SAD-u.
Zbog nedovoljnog broja raspoloživih IP adresa, definirane su tzv. privatne adrese koje se ne mogu pojaviti na Internetu, a RFC 1918 specifikacijom [2] je definirano da su to IP adrese 192.168.x.x, 10.x.x.x i rang od 172.16.x.x do 172.31.x.x. Računalima koja se nalaze u unutarnjim mrežama pridjeljuju se te privatne IP adrese. Usmjerivač ili vatrozid koji povezuje lokalne mreže s Internetom posjeduje minimalno dva mrežna sučelja. Ono koje je spojeno na privatnu mrežu ima IP adresu ili adrese iz domene privatnih IP adresa. Mrežno sučelje koje je spojeno na Internet posjeduje jednu ili više IP adresa iz domene javnih IP adresa.
Ukoliko se na Internetu slučajno i pojavi mrežni paket koji ima ciljnu IP adresu iz skupa privatnih IP adresa, paket će brzo biti odbačen jer nije poznato gdje ga je potrebno poslati. Stoga usmjerivač ili vatrozid treba svim mrežnim paketima koji napuštaju lokalne mreže u kojima se nalaze privatne IP adrese, zamijeniti izvornu IP adresu u mrežnom paketu s jednom od svojih javnih IP adresa. Na taj način će se odgovor u obliku povratnog mrežnog paketa moći vratiti do usmjerivača. Stoga usmjerivač prati neke osnovne informacije o aktivnim vezama (ciljnu IP adresu i ciljni port) kako bi mogao povratne pakete preusmjeriti na pravo računalo iz lokalne mreže. I ukoliko usmjerivač koristi samo jednu javnu IP adresu, računala na Internetu koja dobivaju sve te pakete najčešće nisu svjesna kako su svi ti zahtjevi generirani od više računala.
Često organizacije smještaju svoje poslužitelje u lokalne mreže te isti nisu vidljivi na javnim mrežama. Poslužitelji se najčešće smještaju u zasebnu mrežu koja ima poseban pristup na usmjerivač ili vatrozid, to su tzv. de-militarizirane zone (eng. DMZ – *Demilitarized Zone*). Računala koja se nalaze na Internetu šalju zahtjev za određenim uslugama na vatrozid, a vatrozid po IP adresi i/ili ciljnom portu na koje je zahtjev upućen, preusmjerava mrežne pakete na lokalne poslužitelje.

2.1. Vrste NAT-ova

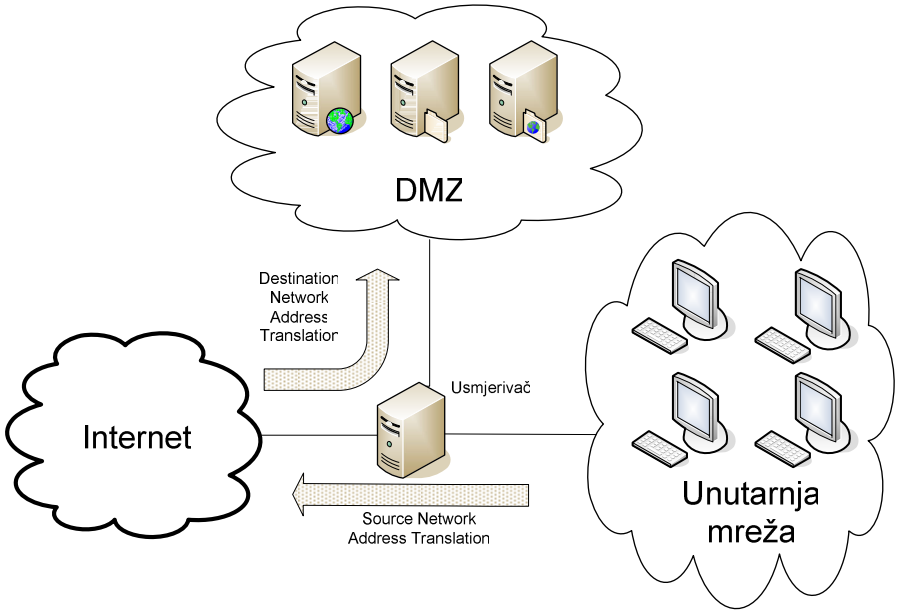
Postoje različiti oblici NAT-a. Od početka se NAT neprestano razvijao, ali jedna od početnih klasifikacija koja se danas u manjoj mjeri primjenjuje:

- Potpuni NAT (eng. *Full Cone NAT*) - svako unutarnje računalo posjeduje svoju privatnu IP adresu, a na NAT uređaju se nalazi rezervirana javna IP adresa za to računalo. Stoga se to računalo iz unutarnje mreže na Internetu prikazuje uvijek s istom IP adresom. Sva računala s Interneta mogu pristupati na to unutarnje računalo, naravno ako je to dozvoljeno sigurnosnom politikom, na način da se spoje na definiranu IP adresu na NAT uređaju i na željeni port. NAT uređaj će potom preusmjeriti taj zahtjev na unutarnje računalo na identični port.
- Ograničeni NAT (eng. *Restricted Cone NAT*) - kao i kod prethodnog potpunog NAT-a, svako unutarnje računalo posjeduje svoju privatnu IP adresu, koja se posredstvom NAT uređaja preslikava u točno definiranu i rezerviranu javnu IP adresu za to računalo. Ipak, računala s Interneta ne mogu pristupati tom unutarnjem računalu, osim ukoliko unutarnje računalo prije toga nije poslalo paket na to udaljeno računalo i uspostavilo vezu.
- Ograničeni NAT prema portovima (eng. *Port Restricted Cone NAT*) - djeluje kao i ograničeni NAT, ali ograničenje se odnosi na portove, što znači da vanjsko računalo može poslati mrežne

pakete na odgovarajuće portove unutarnjeg računala samo ukoliko je to unutarnje računalo prije toga poslalo pakete tom računalu s tih portova.

- Simetrični NAT (eng. *Symmetric NAT*) - svi zahtjevi s unutarnjih IP adresa i portova za specifičnim ciljnim IP adresama i portovima se mapiraju u specifičnu IP adresu i port. Ukoliko isto unutarnje računalo šalje zahtjev s istog porta, koristi se drugo mapiranje. Samo ona vanjska računala koja zaprime zahtjev mogu slati UDP paket nazad unutarnjem računalu koje je započelo komunikaciju.

NAT se može primjenjivati na izvorne i ciljne IP adrese mrežnih paketa. Izvorni NAT (eng. SNAT - *Source NAT*) mijenja izvornu IP adresu u mrežnom paketu, dok ciljni NAT (eng. DNAT - *Destination NAT*) mijenja ciljnu IP adresu. Stoga se SNAT najčešće koristi za lokalne mreže pri čemu mijenja privatne IP adrese u vanjsku javnu IP adresu. S druge strane, DNAT se najčešće koristi za kontrolu pristupa poslužiteljima u de-militariziranoj zoni.



Slika 1: Prikaz zaštićene mreže poslužitelja i unutarnje mreže

Maskiranje IP adresa (eng. *Masquerading*) oblik je NAT-a koji omogućava korisnicima unutarnje mreže koji nemaju javnu IP adresu, komunikaciju preko Interneta. Maskiranje IP adresa zamjena je za SNAT koji mijenja paketima izvornu IP adresu. Razlika je u tome što SNAT zamjenjuje izvornu IP adresu s točno definiranom IP adresom, a proces maskiranja zamjenjuje izvornu IP adresu s IP adresom pridruženom vanjskom sučelju. Stoga se na mrežnom sučelju prema Internetu nalazi samo jedna javna IP adresa. Time je olakšana administracija jer prilikom promjene javne IP adrese NAT usmjerivača, nije potrebno mijenjati i NAT pravila.

U slučaju potrebe za pristupom s javnog Interneta određenoj grupi poslužitelja za koje se provodi DNAT (web, elektronička pošta, DNS te ostali slični servisi) moguća su dva obilka DNAT implementacije:

- Mapirane IP adrese (eng. *Mapped IP address*) - u ovom slučaju definira se prepisivanje adresa "jedan na jedan", gdje se kompletni promet upućen na definiranu javnu IP adresu vatrozida prosljeđuje odabranom unutarnjem računalu. U ovom slučaju potrebno je posebno odvojiti jednu javnu IP adresu koja će na javnom Internetu zastupati odabrano unutarnje računalo. Kada usmjerivač primi paket adresiran na tu javnu adresu, paket se prepisuje i na temelju definiranih NAT tablica prosljeđuje se odgovarajućem unutarnjem računalu.
- Virtualne IP adrese (eng. *Virtual IP address*) - omogućuju preusmjeravanje dolaznog mrežnog prometa na temelju ciljnog porta dolaznog paketa. Na ovaj način moguće je različite pakete za pojedine mrežne servise (npr. web, elektronička pošta, FTP), preusmjeriti na odgovarajuće lokalne poslužitelje koji su zaduženi za navedeni servis. Npr. sav web promet (ciljni port 80) preusmjerava se na web poslužitelj, promet elektroničke pošte (ciljni port 25) preusmjerava

se na poslužitelj za elektroničku poštu, itd... Ovakva konfiguracija upotrebljava se u okolinama gdje su javni servisi raspoređeni na nekoliko različitih lokalnih poslužitelja, a ne postoji dovoljno raspoloživih javnih IP adresa da bi se svaki od njih mapirao "jedan na jedan" kako je to prethodno opisano.

Podjela NAT-a na statički i dinamički

- Statički NAT - broj privatnih IP adresa je jednak broju javnih IP adresa na usmjerivaču. Ovaj oblik je identičan potpunom NAT-u.
- Dinamički NAT - broj privatnih IP adresa nije jednak broju javnih IP adresa u koje se trebaju prepisati. Stoga usmjerivač upravlja procesom dodjeljivanja javnih IP adresa.

Danas većina NAT implementacija unutar sebe uključuje i promjenu ciljnih i izvornih portova u mrežnom paketu. Kad se želi istaknuti da NAT obavlja promjenu portova onda se on naziva NAPT (eng. *Network Address Port Translation*). Potreba za mijenjanjem portova pojavljuje se i kod SNAT-a i kod DNAT-a. Kada unutarnja računala pristupaju vanjskim računalima na Internetu, usmjerivač provodi promjenu ciljne adrese (SNAT). U takvim situacijama usmjerivač često mora mijenjati i izvorni port. To je potrebno u slučajevima kad različita unutarnja računala započinju komunikaciju s istih portova. Također, promjena portova je česta kad se na usmjerivaču nalaze virtualne IP adrese. Naime, organizacija može imati politiku pri kojoj usmjerivač čeka na neke standardne zahtjeve na standardnim portovima, te potom te iste zahtjeve preusmjerava na odgovarajući poslužitelj koji ih može očekivati na nekom drugom portu.

2.2. Implementacija NAT tehnologije

Da bi se implementirao NAT na usmjerivaču, korisnik mora definirati pravila koja će se primjenjivati na dolazne pakete. NAT pravila u sebi mogu sadržavati veći broj definiranih parametara koji moraju biti ispunjeni kako bi se obavila NAT pretvorba. Osnovni oblik pravila definira da se jedna IP adresa (privatna) mapira u drugu IP adresu (javnu). Prošireni oblik NAT pravila može sadržavati i neke od sljedećih potencijalnih parametara:

- Skup IP adresa – umjesto jedne IP adrese moguće je definirati skup IP adresa. Ukoliko se javna IP adresa zamjenjuje sa skupom IP adresa tada će odabir IP adrese biti zasnovan na određenom algoritmu (slučajni odabir, opterećenost i sl.).
- Mrežno sučelje – definiranjem pravila koje specificira da se određene IP adrese moraju pojaviti s točno određenog mrežnog sučelja te da se moraju proslijediti na točno određeno mrežno sučelje, uklanja se rizik koji se pojavljuje ako napadač iz vanjske mreže pošalje mrežni paket na usmjerivač s postavljenom IP adresom iz unutarnje mreže. Naime, u tom slučaju napadač može postići da se mrežni paket proslijedi na neku mrežu kojoj računala s unutarnje mreže smiju slati zahtjeve.
- Portovi – unutar NAT pravila moguće je definirati da se samo određeni portovi dodjeljuju kod preslikavanja mrežnih paketa. Portove je moguće ostaviti onakve kakvi jesu ili ih je moguće promijeniti. Npr. kod ciljnog NAT-a (DNAT) zahtjev zaprimljen od strane usmjerivača na port 80 (HTTP protokol) se može preusmjeriti na port 8080 lokalnog poslužitelja. Također, kod izvornog NAT-a (SNAT) moguće je zadržati izvorni port s kojeg je iniciran zahtjev ili ga je moguće zamijeniti s nekim novim koji može biti točno definiran ili slučajno odabran iz definiranog raspona portova.
- Odredište – kod izvornog NAT-a (SNAT) moguće je definirati da se dozvole samo zahtjevi koji su usmjereni prema određenim odredištima tj. prema određenim ciljnim IP adresama i/ili portovima. Time se korisnici ograničavaju kod svojih aktivnosti jer im može biti dozvoljeno pristupanje samo određenim IP adresama (npr. u kooperativnoj organizaciji) ili samo određenim portovima tj. protokolima (HTTP- port 80, SSH – port 22, itd...).
- Izvorište – kod ciljnog NAT-a (DNAT) moguće je definirati da se dozvole samo zahtjevi s određenih izvorišta, tj. s određenim izvornim IP adresama i/ili portovima. Time se korisnici ograničavaju u svojim aktivnostima zavisno o njihovim privilegijama.

U sljedećem primjeru pretpostavljeno je postojanje sljedeće SNAT tablice preusmjeravanja koja ne sadrži sve moguće parametre već samo izvorne IP adrese i portove, koji se preslikavaju u vanjske IP adrese i portove:

Izvorni IP	Izvorni port	Vanjski IP	Vanjski port
10.0.1.1/32	0	161.53.1.1	0
10.0.0.1/32	0	161.53.1.2	0
10.0.0.0/24	1030	161.53.1.2	1040
10.0.0.0/24	0	161.53.1.2	0
10.0.1.0/24	0	161.53.1.1	0
10.0.0.0/8	0	161.53.1.3	0

Tablica 1: Primjer definiranja SNAT tablice

Navedena NAT tablica definira pet pravila preslikavanja privatnih IP adresa u javne. Prvo pravilo svim zahtjevima koji imaju izvornu IP adresu 10.0.1.1 i bilo koji port, mijenja izvornu IP adresu u javnu IP adresu 161.53.1.1 bez promjene izvornog porta, osim ako je on već zauzet. Drugo pravilo radi to isto samo što su zamijenjene izvorna i vanjska IP adresa u 10.0.0.1 i 161.53.64.2. Treće pravilo svim mrežnim paketima koji imaju izvornu IP adresu iz mreže 10.0.0.0/24 i izvorni port 1030, mijenja izvornu IP adresu u 161.53.1.2 , a izvorni port u 1040. Zadnja tri pravila definiraju samo mijenjanje IP adresa.
Neka se za dani primjer SNAT tablice na usmjerivaču pojavi mrežni paket sa sljedećim parametrima:

```
Izvorna IP adresa: 10.0.0.5
Izvorni port:      1030
Ciljna IP adresa:  161.53.160.69
Ciljni port:       80
```

Usmjerivač za zadani mrežni paket prolazi kroz definirana SNAT pravila te uočava da mrežni paket zadovoljava treće pravilo. Stoga je potrebno preslikati izvornu IP adresu 10.0.0.5 u 161.53.1.2 i port 1030 u 1040. Ukoliko se pretpostavi da je port 1040 već zauzet, tada će mrežni paket dobiti prvi veći slobodni port, npr. 1041. Sukladno sljedećim promjenama, u internim NAT tablicama zapisuje se obavljeno mapiranje.

Vanjski IP	Vanjski port	Unutarnji IP	Unutarnji port
…	…	….	….
161.53.160.69	1041	10.0.0.5	1030

Tablica 2: Primjer interne NAT tablice s uspostavljenim vezama

Ukoliko usmjerivač primi odgovor s vanjske mreže koji posjeduje izvornu IP adresu 161.53.160.69 i usmjeren je na port 1041, tada će usmjerivač pregledavanjem svojih internih NAT tablica detektirati da taj mrežni paket treba preusmjeriti na unutarnje računalo s IP adresom 10.0.0.5 i to na port 1030 s kojeg je poslan inicijalni zahtjev.

2.3. Primjena NAT tehnologije

NAT tehnologija se primjenjuje od strane brojnih malenih i velikih organizacija. U nastavku slijede mogućnosti primjene NAT tehnologije:

- Prevođenje privatnih IP adresa u javne – glavna funkcionalnost zbog koje se NAT danas najčešće koristi. Dodjeljivanjem privatnih IP adresa organizacije smanjuju svoje troškove na kupovinu javnih IP adresa čiji broj je limitiran.
- Zaštita poslužitelja u sklopu DMZ okruženja – odvajanjem poslužitelja u DMZ, organizacije postižu veću razinu zaštite svojih mreža. Naime, sigurnosna politika mora dozvoliti pristup vanjskim zahtjevima s Interneta do poslužitelja. Ukoliko se poslužitelji nalaze u unutarnjoj mreži, zlonamjerni napadači mogu iskorištavanjem određenih potencijalnih propusta na poslužiteljima steći određene ovlasti na tim poslužiteljima te s njih usmjeriti svoje napade na ostala unutarnja računala.
- Balansiranje opterećenošću (eng. *Load Balancing*) - ciljni NAT može preusmjeravati zahtjeve za određenom uslugom na slučajno odabrani poslužitelj. Npr. ukoliko se koristi određena web usluga, ista se može razdijeliti na više poslužitelja. Stoga usmjerivač ili vatrozid koji obavlja

NAT, može na temelju slučajnog odabira ili specifičnog algoritma, preusmjeravati zahtjeve ravnomjerno na različite poslužitelje te ih time ravnomjerno opteretiti. U tom slučaju NAT predstavlja virtualni poslužitelj jer svi zahtjevi inicijalno dolaze na njega, a potom ih on preusmjerava prema nekom principu na ostala računala. Algoritam koji se koristi za odabir poslužitelja kojem će biti proslijeđen pristigli zahtjev, najčešće prati opterećenost svih poslužitelja. To se može postići mjerenjem brzine prometa u broju paketa po nekoj vremenskoj jedinici, na temelju čega se novi pristigli zahtjev proslijedi na poslužitelj koji ima najmanje opterećenje. Time se postiže ravnomjerno opterećenje sustava. Algoritam za odabir poslužitelja može koristiti i podatke koje može dobivati od svakog od poslužitelja, a tiču se opterećenosti samog poslužitelja. Postoji veliki broj algoritama koji se može koristiti za postizanje optimalne opterećenosti svih poslužitelja koji se mogu međusobno i kombinirati.

- Visoka dostupnost (eng. *High Availability*) - ciljni NAT može biti korišten kako bi se uspostavila usluga koja zahtjeva visoku dostupnost. Ukoliko jedan od poslužitelja padne, i ako usmjerivač detektira da se određeni usmjerivač srušio, usmjerivač može preusmjeravati pristigle zahtjeve na pomoćni poslužitelj.
- Posredne usluge (eng. *proxy*) - NAT može preusmjeravati sve HTTP zahtjeve prema Internetu na posebni HTTP posredni poslužitelj koji može spremati sadržaj tih paketa i filtrirati zahtjeve. Time se unutarnja mreža štiti od virusa i drugih potencijalno zlonamjernih prijetnji. Također, time se postiže i kontrola unutarnjih korisnika kojima se može zabraniti pristupanje određenim web uslugama (pornografija, igrice, itd...). Neki pružatelji Internet usluga koriste tu tehniku kako bi smanjili propusni pojas, a da pri tome klijenti toga nisu niti svjesni. Naime, na posrednom HTTP poslužitelju nalaze se spremljene stranice koje potom više korisnika koristi.
- Zaštita mreže - mnogo je lakše štititi jedan prolaz, nego veliki broj prolaza. Korištenjem NAT-a osigurava se samo jedan prolaz prema lokalnoj mreži. Zaštitom jednog računala koji obavlja NAT preusmjeravanje, štiti se cijela mreža. Također, NAT najčešće omogućava unutarnjim računalima izlaz na Internet te samo povratne pakete s Interneta. Time je napravljen prvi korak u sprečavanju različitih neovlaštenih aktivnosti usmjerenih s Interneta. Naime, potencijalni napadači zbog prepisivanja IP adresa ne znaju koje su stvarne IP adrese unutarnjih računala te im ne mogu tako lako niti pristupiti. Usmjerivači koji obavljaju NAT obično su prošireni sa skupom sigurnosnih politika te time postaju vatrozidima.

2.4. Prednosti NAT tehnologije

Glavna prednost NAT-a je u tome što je riješio problem nedostatka javnih IP adresa. Time su se smanjili i troškovi organizacija koje inače moraju kupovati javne IP adrese. Korištenjem privatnih IP adresa u kombinaciji s NAT-om, organizacijama je dostatna samo jedna IP adresa s kojom će spojiti cijelu organizaciju s Internetom. Mreže koje su prije zahtijevale klasu B adresa ili klasu C adresa s NAT-om mogu koristiti samo jednu jedinu javnu IP adresu. Čak se i nedostatak u obliku nemogućnosti potpunih dvosmjernih veza preko NAT-a može smatrati u određenim uvjetima povećane računalne sigurnosti, prednošću. Naime, zavisnost NAT-a koja zahtjeva od unutarnjeg računala da uspostavi komunikaciju s vanjskim računalom na Internetu, štiti lokalnu mrežu od različitih zlonamjernih aktivnosti koje prijete s Interneta. To može povećati pouzdanost sustava zaustavljajući aktivnosti crva i drugih sličnih zlonamjernih programskih kodova te povećati sigurnost lokalne mreže jer su onemogućeni razni oblici skeniranja iste.
Osim što povećava računalnu sigurnost, NAT također olakšava mrežnu administraciju. Naime, administratori lokalnih mreža mogu slobodno mijenjati IP adrese lokalnih računala bez ikakvih modifikacija na DNS poslužiteljima. Naravno, taj uvjet je ispunjen dok koriste privatne IP adrese.

2.5. Nedostaci NAT tehnologije

Računala koja se nalaze iza usmjerivača nemaju uvijek direktnu vezu do udaljenih računala i ne mogu koristiti sve Internet protokole. Usluge koje zahtijevaju uspostavljanje TCP veze s Interneta ili korištenje UDP protokola kod kojih nema stanja veza, često se ne odvijaju ispravno jer za njih nije podržan NAT. I ukoliko se na NAT usmjerivačima ne provedu određene preinake da bi se podržali takvi problematični protokoli, dolazni paketi ne mogu doći do svojih odredišta. Takav protokol je i FTP (eng.

File Transfer protokol) koji kod prijenosa datoteka koristi aktivni i pasivni način rada, ali pasivni način rada nije podržan od strane NAT-a. Rješenje za taj problem s FTP-om se može pronaći u korištenju APG tehnologije (eng. *Application Layer Gateway*), ali niti ona nije dostatna kad su oba računala zaštićena NAT-om.
Stoga neki stručnjaci smatraju NAT jednim oblikom kvara u računalnim mrežama jer je mogućnost međusobnog spajanja računala jedan od osnovnih principa Interneta. NAT je između ostalog znatno usporio prihvaćanje IPv6 protokola pošto je njime djelomično riješen problem nedostatka javnih IP adresa.
NAT usmjerivač mora kontinuirano pratiti koje veze su aktivne, a koje nisu. Time usmjerivač omogućava povratak mrežnih paketa na prava odredišta. To stanje veze mora nekad postati i neaktivno i usmjerivač ju mora obrisati iz svojih internih tablica. Tu se nalazi problem kad određena veza postaje neaktivna. Naime, Telnet veza ne mora uopće razmjenjivati mrežne pakete, a i dalje je aktivna. Usmjerivač te veze može držati onoliko dugo koliko ima slobodnih portova i IP adresa.

2.5.1. Protokoli na koje NAT ima negativni utjecaj

Neki protokoli višeg nivoa (npr. FTP i SIP) šalju adresu mrežnog računala enkapsuliranu u aplikacijski sadržaj mrežnog paketa. FTP tako npr. u aktivnom načinu rada koristi dvije odvojene konekcije za komandni promet i za podatkovni promet. Kad zaprimi zahtjev za prijenosom datoteka, računalo koje je primilo zahtjev za prijenosom datoteka uspostavlja vezu s udaljenim računalom. Kao rješenje za navedeni slučaj koristi se ALG (eng. *Application Layer Gateway*) čiji modul mora biti ugrađen u usmjerivač ili vatrozid koji obavlja NAT prometa. Taj modul automatski ispravlja aplikacijski sadržaj mrežnog paketa koji bi vezu učinio neispravnom. ALG moduli stoga trebaju razumjeti više protokole koje trebaju popravljati i zbog toga je za svaki protokol koji ima probleme s NAT-om, potrebno koristiti posebni ALG modul.
Drugo rješenje za ovaj problem je korištenje drugih NAT tehnika koristeći protokole poput STUN-a, TURN-a ili ICE-a čije pojašnjenje se nalazi u poglavlju 2.6 Modifikacije NAT tehnologije. Osim opisanih raspoloživi su i drugi protokoli koji rješavaju ove probleme poput RIP (eng. *Realm Specific IP*) definiran RFC 3103 specifikacijom [5] i TIST (eng. *Topology-Insensitive Service Traversal*).
NAT može isto prouzročiti probleme i u slučajevima kad se koristi IPSec enkripcija ili kad je veliki broj uređaja kao što su SIP telefoni locirani unutar lokalne mreže. Telefoni kriptiraju portove što znači da NAPT ne može pristupiti istima i promijeniti izvorni port. U ovakvim slučajevima moguć je samo NAT nad IP adresama što uzrokuje nefunkcioniranje usluge. Jedno od rješenja za spomenuti problem je korištenje TLS (eng. *Transport Layer Security*) kriptografskog protokola koji radi na 4 razini OSI modela i stoga ne maskira broj porta. Drugo rješenje za korištenje IP telefonije je u enkapsuliranju IPSec sadržaja kroz UDP promet.

2.6. Modifikacije NAT tehnologije

Da bi se zaobišli nedostaci povezani s NAT tehnologijom, razvijene su različite nadogradnje koje omogućavaju uklanjanje tih nedostataka.

2.6.1. STUN

STUN (eng. *Simple Traversal of UDP over NATs*) je mrežni protokol koji omogućava klijentima koji se nalaze iza jednog ili više NAT uređaja, pronalazak njegove javne IP adrese, vrstu NAT-a iza kojeg se nalazi i vanjski port dodijeljen od strane NAT uređaja kao i originalni port unutarnjeg računala. Te informacije se koriste za uspostavljanje UDP komunikacije između dva računala koja se oba nalaze iza NAT uređaja. Protokol je definiran RFC 3489 specifikacijom [3].
Jednom kad klijenti posjeduje UDP portove na strani prema Internetu, komunikacija može početi. Ukoliko je NAT potpuni (eng. *Full Cone NAT*) komunikaciju može započeti bilo koje računalo, kako ono na unutarnjoj mreži tako i ono na vanjskoj. Ali ako se tu radi o ograničenom NAT-u, tada obje strane moraju započeti komunikaciju istovremeno.
Protokoli poput SIP-a koriste UDP pakete za prijenos zvuka i/ili slike preko Interneta. Nažalost, ukoliko obje strane koriste NAT, konekcija ne može biti uspostavljena na tradicionalni način.
STUN protokol u sebi uključuje kombiniranje klijenta i poslužitelja. VoIP telefon ili neki drugi program može sadržavati STUN klijent koji šalje zahtjev na STUN poslužitelj. Poslužitelj odgovara klijentu

šaljući mu informacije o vanjskoj IP adresi NAT usmjerivača te o otvorenom vanjskom portu kako bi se dozvolio povratni mrežni promet. Odgovor koji poslužitelj vraća klijentu također sadrži i informaciju o tipu korištenog NAT-a jer različiti tipovi NAT-a upravljaju UDP prometom različito. STUN može raditi samo s tri tipa NAT-a, potpunim, ograničenim i ograničenim prema portovima, dok simetrični NAT nije podržan.

2.6.2. TURN

TURN (eng. *Traversal Using Realy NAT*) je protokol koji omogućava uređajima iza NAT usmjerivača da primaju podatke preko TCP ili UDP veza, a veoma je koristan za uređaje koji se nalaze iza simetričnog NAT-a. TURN ne dozvoljava korisnicima pokretanje poslužitelja na dobro poznatim portovima ukoliko su oni iza NAT-a. Njegova uloga je da omogući uređajima koji se nalaze u unutarnjoj mreži, da budu i završni dio konekcije, a ne samo inicirajući, pri čemu mora biti očuvana sigurnost unutarnje mreže.
STUN to postiže djelomično jer ne omogućava prijenos prometa preko simetričnih NAT-ova. Potpuno rješenje u obliku TURN-a omogućava klijentu dohvaćanje javne IP adrese s koje može dobivati podatke s bilo kojih vanjskih računala na Internetu. To može biti postignuto samo ako se podaci prosljeđuju preko poslužitelja koji je lociran na javnoj mreži.

2.6.3. ICE

ICE (eng. *Interactive Connectivity Establishment*) protokol zasnovan je na algoritmu koji je iterativni proces u kojem dva uređaja, oba smještena iza NAT-a, razmjenjuju adrese u pokušaju međusobne komunikacije. Prvi uređaj započinje sa skupljanjem svih svojih IP adresa koje može pronaći i preko kojih može ostvariti komunikaciju, a potom te IP adrese šalje drugom računalu. Drugo računalo također skuplja sve IP adrese koje može pronaći uključujući i one koje dobije slanjem STUN ili sličnog zahtjeva prvom računalu te skup tih adresa šalje prvom računalu. Nakon što ih prvo računalo dobije, ono pokušava uspostavljanje komunikacije s drugim računalom pri čemu registrira eventualne dodatne IP adrese koje potom šalje drugom računalu. Ova procedura međusobnog pomaganja u obliku slanja IP adresa nastavlja se dok nisu dohvaćene sve IP adrese koje su raspoložive što na kraju treba rezultirati jednim parom IP adresa preko kojeg bi se trebala moći uspostaviti komunikacija.

3. Problematika logiranja

Za informatičke stručnjake log ili dnevnički zapisi se koriste za pohranjivanje podataka o događaju pri čemu se nastoji odgovoriti na standardnih pet pitanja, tzv. W5: *who* - tko, *what* - što, *when* - kada, *where* - gdje i *why* - zašto. Log zapisi generirani su uslijed određenih događaja od strane posebnih procesa, a mogu se prikazivati na zaslonu monitora, slati na uređaj za ispis ili zapisivati u datoteke, bazu podataka ili sl. Najčešći format za zapisivanje log zapisa je ASCII format.
Ukoliko su log zapisi takvi da odgovaraju na standardnih pet pitanja (W5), tada je svrha log zapisa da pruži informatičkim stručnjacima mogućnost praćenja aktivnosti aplikacija ili uređaja kako bi se detektiralo uobičajeno ponašanje i odstupanje od istog. I ukoliko određeni log zapis izostane, a očekivan je, tada se pretpostavlja da je ponašanje sustava iz određenog razloga neispravno. Na isti način, ukoliko nepredviđeni log zapis postoji, a ne bi smio postojati, pretpostavlja se da nešto u sustavu nije ispravno.
Sadržaj log zapisa često nije dovoljno razumljiv. Naime, programeri često u log zapise stavljaju određene tekstove koji samo njima predstavljaju određenu informaciju i ne odgovaraju na 5 standardnih pitanja. To je rezultat neprimjerenog programiranja koje nije prilagođeno krajnjem korisniku. Srećom, većina vatrozida i sličnih programa i uređaja koji obavljaju NAT prilagođeni su krajnjim korisnicima, pri čemu se misli na informatičke stručnjake.
Primjena log zapisa može biti različita:

- kroz praćenje mrežnih aktivnosti moguće je detektirati različite pokušaje napada, virusne ili crvne infekcije, konfiguracijske probleme, sklopovske probleme i tome slično.
- mrežnom analizom moguće je detektirati pokušaje neovlaštenog pristupa osjetljivim informacijama ili resursima, što pomaže osiguranju tajnosti. Moguće je detektirati pokušaje mijenjanja sadržaja datoteka što osigurava integritet. Također, moguće je detektirati bilo koju vrstu problema koji mogu utjecati na dostupnost informacija kao što su napadi

uskraćivanjem resursa (eng. DoS – *Denial of Service*) ili distribuirani napadi uskraćivanjem resursa (eng. *Distributed DoS*).

- kroz praćenje sistemskih log zapisa moguće je detektirati razne aktivnosti na razini sustava koje spadaju u uobičajeno ponašanje, ali i u nepoželjno (kvarovi, virusi, neovlašteni pokušaji upada,...).

3.1. Važnost logiranja NAT prometa

NAT tehnologija omogućava različitim korisnicima, bilo unutarnjim ili vanjskim, pristupanje različitim resursima s IP adresom koja nije njihova već od usmjerivača koji obavlja NAT nad njihovim privatnim IP adresama. Lokalni korisnici pristupaju različitim računalima na Internetu pri čemu ta računala znaju samo IP adresu usmjerivača organizacije. I ukoliko lokalni korisnici izvrše određene neovlaštene i zabranjene aktivnosti, vlasnici oštećenih resursa smatrat će odgovornom organizaciju u kojoj lokalni korisnik djeluje. Stoga organizacije imaju dužnost praćenja NAT prometa kako bi u svakom trenutku mogle detektirati koji korisnici su u kojem vremenu pristupali određenim resursima. Organizacije ne moraju te podatke znati samo kako bi mogle detektirati korisnike u slučaju prijava njihovih neovlaštenih aktivnosti. Naime, ukoliko organizacija ne koristi vatrozid za definiranje određenih sigurnosnih politika zabrane pristupa određenim Internet resursima ili im raspoloživi vatrozid to ne omogućava, tada ona može praćenjem NAT zapisa detektirati kojim zabranjenim web stranicama te drugim zabranjenim resursima su njihovi zaposlenici pristupali.

Praćenjem NAT prometa moguće je detektirati i nekakve neuobičajene aktivnosti, kako lokalnih korisnika tako i udaljenih korisnika. Naime, ukoliko se na određenom unutarnjem računalu instalira određeni *spyware*, trojanski konj, crv ili neki drugi oblik zlonamjernog programa, tada je praćenjem mrežne aktivnosti moguće uočiti da je promet s nekog računala neuobičajeno velik ili to računalo pristupa određenim IP adresama kojima nikad prije nije pristupalo ili im pristupa u „previše" jednolikim vremenskim razmacima i sl. Da bi se mogle detektirati ovakve aktivnosti koje mogu biti uzrokovane zlonamjernim programima, tada je potrebno koristiti analizator log zapisa koji će moći detektirati sve elemente koji označavaju određene oblike neispravnog ponašanja unutarnjeg računala.

3.2. Centralizirani sustav logiranja

Centralizirani sustav logiranja je vrlo važan dio svake sigurnosne politike kao i centralizirano nadgledanje mreže. Ono omogućava lakše i brže upravljanje i administraciju organizacijom. U tu svrhu potrebno je koristiti udaljeni centralni log poslužitelj.

Važnost upotrebe udaljenog log poslužitelja je višestruka. Bez poslužitelja konfiguriranog na ovakav način, vjerojatnost detekcije neovlaštenih aktivnosti u mreži je smanjena. Naime, ukoliko napadač posjeduje mogućnost provaljivanja na određeno računalo, tada on posjeduje i mogućnost modificiranja postojećih log zapisa te uništavanja dokaza koji identificiraju njegove neovlaštene aktivnosti. Stoga su korištenjem udaljenog log poslužitelja log zapisi zapisani na dvije lokacije, na klijentu i log poslužitelju čime se smanjuje mogućnost gubitka važnih informacija.

Velike organizacije često posjeduju različite mreže za koje koriste različite odvojene NAT uređaje. Time se osigurava veća propusnost nego kad bi sav promet svih mreža išao samo preko jednog NAT uređaja. Svi ti NAT uređaji mogu slati svoje log zapise o ostvarenom NAT prometu na jedinstveni centralni poslužitelj. Pri tome je potrebno paziti na sigurnost tog poslužitelja kako bi podaci bili zaštićeni, ali i vjerodostojni.

Jedan od razloga za korištenje centralnog poslužitelja za prikupljanje NAT log zapisa je i u činjenici da najčešće nije dovoljno iz NAT log zapisa detektirati nekakve nedopuštene aktivnosti. Stoga se na centralni log uređaj ne šalju samo NAT log zapisi nego i ostali log zapisi pri čemu se prvenstveno misli na sistemske log zapise generirane od uređaja koji sudjeluju u mrežnom prometu. Njihovim zajedničkim povezivanjem u jednu kompaktnu cjelinu moguće je pronaći određene zavisnosti između različitih log zapisa te na temelju tih zavisnosti detektirati određene događaje u mreži.

3.2.1. Sigurnost centralnog log poslužitelja

Centralni poslužitelj na koji se šalju log zapisi je potrebno zaštiti iz više razloga. Jedan od glavnih razloga za podizanje sigurnosti samog centralnog log poslužitelja je uklanjanje zapisa koji označavaju

određene neovlaštene aktivnosti. Ukoliko se centralni log poslužitelj ne zaštiti, tada napadač koji je izvršio određeni oblik napada može upasti i na centralni log poslužitelj te ukloniti log zapise koji identificiraju njegove zlonamjerne aktivnosti. Time je naknadno nemoguće saznati tko je izvršio koji napad ili kad je napad izvršen i sl. Kako bi se zaštitio poslužitelj koji registrira log zapise potrebno je da isti bude zaštićen vlastitim vatrozidom, zaporkama, sustavom za detekciju neovlaštenih aktivnosti (eng. IDS – *Intrusion Detection System*), sustavom za sprečavanje neovlaštenih aktivnosti (eng. IPS – *Intrusion Prevention System*) te različitim elementima programske sigurnosti (anti-virusni programi i sl.).

Kao što na centralni log poslužitelj mogu neovlašteno upasti udaljeni napadači, tako isto na njega mogu još jednostavnije upasti i lokalni korisnici koji se bave određenim neovlaštenim aktivnostima. Naime, ukoliko lokalni korisnici posjeduju određena tehnička znanja tada isti mogu lakše provaliti na centralni log poslužitelj koji se najčešće nalazi u istoj mreži kao i njihova računala.

Prilikom postavljanja sustava koji je baziran na jednom centralnom log poslužitelju, potrebno je pripaziti na određene kritične elemente koji su povezani s raspodijeljenim sustavima. Neki osnovni sigurnosni koncepti:

- Osnovna zaštita zasnovana je na korištenju zaporki na "svakom koraku". Zaporka pri tome mora zadovoljavati određene sigurnosne zahtjeve: minimalna duljina, određena kombinacija znakova uključujući mala i velika slova, brojeve, simbole i sl. Također, moguće je zaporke podesiti s politikom regularnog mijenjanja na vremenskoj bazi. Sigurnost zaporki dodatno se podiže ukoliko se ne koriste riječi koje se koriste i u stvarnom životu. Naime, *brute force* napadi za razbijanje zaporki često prvo isprobavaju riječi iz svojih rječnika.
- Minimiziranje količine instaliranih programa na poslužitelju. Razlog tomu je što većina programskih paketa posjeduju nepoznate sigurnosne propuste koji se svakodnevno otkrivaju. U takvom okruženju, postavljeni poslužitelj za prikupljanje log zapisa bi lako bio kompromitiran. Stoga je potrebno minimizirati broj instaliranih programa na one koji su neophodni jer se sa smanjenjem instaliranih programa smanjuje i broj potencijalnih sigurnosnih rupa.
- Mrežna sigurnost samog poslužitelja mora biti na visokoj razini. Naime, poslužitelj za log zapise ne smije biti na tzv. "otvorenoj" mreži na koju mogu pristupiti udaljeni napadači. To je potrebno iz razloga što napadač može razbiti zaporku te se neovlašteno prijaviti na napadnuti poslužitelj. Ujedno, čak i da ne uspije razbiti zaporku i prijaviti se na sustav, napadač i dalje može izvesti napad uskraćivanja resursa (DOS) te onemogućiti poslužitelja u primanju log zapisa i adekvatnoj obradi istih. Stoga je poslužitelj potrebno zaštititi i na jednoj mrežnoj razini pri čemu se preporuča korištenje IP adresa iz raspona privatnih IP adresa. Također, poželjno je da se centralni log poslužitelj odvoji iz mreže u kojoj se nalaze lokalni korisnici. Naime, opasnost modificiranja log zapisa ne postoji samo od udaljenih napadača, nego i od lokalnih korisnika koji s malo tehničkog znanja mogu lakše doprijeti do centralnog log poslužitelja ako se isti nalazi u njihovoj mreži.
- Kako bi se osiguralo očuvanje log zapisa u svim uvjetima, potrebno je osigurati dovoljnu količinu memorijskog prostora na disku na koji se log zapisi spremaju. Time se povećava sigurnost da će i u slučaju povećanja količine log zapisa isti biti sačuvani, a sam poslužitelj se neće srušiti uslijed nedovoljnih memorijskih resursa.
- Ukoliko se koristi jedan log poslužitelj za registriranje svih log zapisa tada je potrebno osigurati identičnost sistemskih vremena na svim generatorima log zapisa. Time će se naknadno moći definirati koji događaji su slijedili prije/nakon kojih i administrator će biti u mogućnosti saznati pravi slijed događaja koji je nastao unutar mreže. U tu svrhu preporuča se korištenje NTP-a (eng. *Network Time Protocol*) koji omogućava sinkronizaciju vremena na ciljanim računalima. NTP protokol omogućava uređajima sinkroniziranje sa centralnim vremenskim poslužiteljem koji je sam sinkroniziran s GPS-om (eng. *Global Positioning Sattelites*). Time je vremenska usklađenost unutar jedne zone točna do razine milisekunde.
- Ukoliko je na poslužitelju potrebno odobriti udaljeno spajanje tada je potrebno koristiti sigurne protokole kao što je SSH. Uz to, potrebno je i ograničiti mogućnost spajanja na poslužitelj sa samo točno određenih IP adresa.
- Kako bi se osigurao integritet podataka u log zapisima potrebno je testirati ispravnost tih podataka. Do neispravnosti može doći ukoliko zlonamjerni napadač uspije provaliti na

poslužitelj te modificirati log zapise. U tu svrhu potrebno je koristiti određeni IDS na samom računalu kako bi detektirao neovlaštene promjene na samom računalu ili u samim zapisima.

3.3. Razine važnosti log zapisa

Na sustavima postoji više različitih tipova log zapisa koje označavaju važnost samih log zapisa. Npr. *syslog* poruka generirana od strane sustava može biti u jednoj od sljedećih 7 razina važnosti:

- Hitnost (eng. *Emergency*) – označava postojeću ili očekivanu neuporabljivost sustava ili nekih njegovih elemenata,
- Upozorenje (eng. *Alert*) – označava važne situacije koje bi trebale biti sređene što ranije, a inače će najvjerojatnije doći do većih problema sustava,
- Kritični događaji (eng. *Critical*) – označavaju kritične događaje koji bi mogli završiti u neispravnom stanju,
- Pogreške u radu (eng. *Error*) – označava pogreške u radu sustava ili određenih elemenata koje nisu ispravne, ali se zbog njih najvjerojatnije neće srušiti sustav,
- Upozorenja (eng. *Warning*) – označavaju događaje koji upozoravaju na ponašanje koje nije uobičajeno,
- Obavijesti (eng. *Notice*) – označavaju događaje koji nisu pogrešni, ali predstavljaju značajan događaj pa ih je potrebno registrirati i eventualno naknadno analizirati,
- Informativno (eng. *Informational*) – označava događaje koji predstavljaju normalan rad sustava i
- Detaljni (eng. *Debug*) – označava detaljni prikaz događaja.

Razina log zapisa je važan parametar koji mora biti uzet u razmatranje. Administratori uvijek nastoje odabrati minimum informacija koji će im pružiti dovoljnu količinu informacija. Odabir prave razine logiranja pomaže kod održavanja stabilnosti mreže i kod osiguranja da neće biti gubitka informacija. Npr. ukoliko se odabere najdetaljniji nivo logiranja - *Debug*, postojat će veliki broj log poruka koje zahtijevaju određeni dio diska, visoke performanse sustava i odgovarajuća propusnost mreže (osobito ukoliko se radi o udaljenom prikupljanju log zapisa). S druge strane, ukoliko se odabere *Error* ili viša razina, tada vjerojatno neće biti raspoloživo dovoljno podataka za otkrivanje pravog ponašanja u mreži. Postojat će obavijesti o neispravnim ponašanjima, ali neće biti raspoložive informacije iz kojih bi se moglo zaključiti zašto je do neispravnog ponašanja došlo, tko je odgovoran, itd…

3.4. Razdjeljivanje log zapisa

Spremanje svih log zapisa na jedno mjesto omogućava postojanje cjeline i neprekinutog niza gdje određeni događaji koji se sastoje od više zapisa nisu prekinuti. Ipak, korištenje takvog neprekinutog niza posjeduje i svoje nedostatke u obliku nemogućnosti jednostavnog pregledavanja velikih količina informacija (zapisa). Stoga se log zapisi često razdjeljuju na manje dijelove pri čemu je osnova uglavnom vremenska, a jedinice su uglavnom sati, dani, tjedni ili mjeseci. U trenutku kad treba doći do preusmjeravanja log zapisa na drugu lokaciju (najčešće datoteku), potrebno je osigurati da to minimalno utječe na postojeći proces zapisivanja log zapisa. I pošto su te promjene zapisivanja ovisne o vremenu, vrlo je važno da uređaji koji generiraju log zapise budu vremenski sinkronizirani. U suprotnom se ne može napraviti dovoljno precizan rez između log zapisa. U tu svrhu potrebno je koristiti NTP protokol za sinkronizaciju uređaja koji generiraju log zapise.

Sve nove kolekcije log zapisa moraju biti efikasno imenovane kako bi imale određeno značenje za računalne stručnjake. Uobičajeno se te datoteke nazivaju po vremenima koje sadrže unutar sebe. Tako nazivi mogu biti zasnovani na danima (npr. 2006-05-31-NAT_promet.log) ili na danima i vremenu (npr. 2006-05-31-11-30-00-NAT_promet.log).

Kad se log zapisi razdjeljuju na manje dijelove na vremenskoj osnovi, moguće je provesti kontrolu nad tim vremenskim odsječcima. Naime, moguće je pratiti veličine tih zapisa u tim odsječcima te detektirati nagla povećanja mrežnog prometa i log zapisa. Ili izostajanje samih log zapisa.

3.5. Arhiviranje log zapisa

Log poslužitelji moraju posjedovati dovoljno velike dovoljne količine memorijskog prostora kako bi spremile sve potrebne podatke. Ipak, i u slučaju posjedovanja najvećeg postojećeg diska opet je

potrebno nakon nekog vremena isprazniti isti. U suprotnom će doći do prepunjenja diska log poslužitelja što će uzrokovati trajni gubitak novih log zapisa, a vjerojatno i rušenje samog poslužitelja. Korištenjem CD medija ili ZIP disketa u kombinaciji s nekom od tehnologija kompresije (RAR, ZIP,...) moguće je na jednostavan način arhivirati stare log zapise.

3.5.1. Sigurnost arhiviranih log zapisa

Nakon što se kreira arhiva log zapisa, istu je potrebno i zaštititi. Kako bi se arhiva sačuvala od eventualnih slučajnih modifikacija ili od virusa i sličnih zlonamjernih programa, arhive je potrebno spremati samo s ovlastima čitanja (*read only status*). To je moguće izvesti na tvrdom disku, ali preporuča se korištenje CD-R i DVD-R medija koji dozvoljavaju samo zapisivanje podataka, ne i modificiranje. Ostali mediji poput CD-RW ili ZIP dozvoljavaju i modificiranje spremljenih podataka. Ipak, CD-R i DVD-R mediji u usporedbi s trakama imaju 10 godina kraći vijek trajanja. To je uzrokovano prvenstveno lakim oštećenjima medija (ogrebotine, prljavština, korozija i sl.). Stoga se za dugo čuvanje log zapisa ne preporuča njihovo korištenje. Usprkos svim nedostacima CD-R i DVD-R medija, oni su ipak najefektivnije rješenje za organizacije pa ih organizacije najčešće i koriste.
Jedna od nedostataka CD-R i DVD-R medija za arhiviranje je što je podatke s medija moguće neovlašteno čitati. Stoga je potrebno koristiti određene enkripcijske metode kao što je PGP (eng. *Pretty Good Privacy*) koje će zaštititi log zapise od neovlaštenog čitanja.
Dodatna preporuka kod arhiviranja log zapisa je i spremanja arhiva na fizički odvojeno mjesto. Time se podaci osiguravaju od različitih općenitih rizika. Kako onih uzrokovanih ljudskim faktorom (krađe, teroristički napadi,...), tako i od različitih prirodnih nepogoda (poplave, požari, potresi,...).

3.6. *Syslog* protokol i njegova evolucija

Syslog poslužitelj je poslužitelj koji prikuplja različite log zapise s različitih poslužitelja. Korištenjem *syslog* poslužitelja moguće je uspostaviti centralizirani sustav logiranja. RFC 3164 specifikacija [4] u tu svrhu definira *syslog* kao transportni protokol koji omogućava računalu slanje poruka preko IP mreže do *syslog* poslužitelja. Pri tome se koristi UDP transportni protokol, a uobičajeno je korištenje porta 514 na *syslog* poslužitelju za primanje poruka. Primjer *syslog* poslužitelja je Kiwi Syslog Daemon koji prihvaća, registrira, prikazuje i prosljeđuje log zapise.
Syslog protokol je razvijen od Computer Science Research Group (CSRG) s University of California-Berkley, a njegova namjena je pružanje usluge izvještavanja o događajima na Linux ili UNIX operacijskom sustavu. Proces koji se izvršava na UNIX sustavu naziva se *syslogd* poslužitelj i on generira log zapise i šalje ih drugom *syslog* poslužitelju koji ih prikuplja i arhivira na neki od mogućih načina (datoteke, monitor, baza,...).
Iako se *syslog* najčešće koristi za registraciju NAT prometa na Linux ili UNIX operacijskim sustavima, isti ima i određene nedostatke. Glavni nedostatak *syslog* protokola je u tome što se log zapisi šalju nekriptirani u običnom tekstu. Stoga ih je moguće korištenjem odgovarajućih mrežnih analizatora prisluškivati. Također, mrežni administrator ne može biti siguran ukoliko su log zapisi putem bili modificirani. To je rezultat korištenja nekriptiranog UDP protokola za prijenos log zapisa čime se mrežni paketi ne mogu osigurati od modificiranja. Naime, *syslog* protokol ne posjeduje mehanizam autentikacije koji bi potvrdio vjerodostojnost podataka.
Zbog navedenih nedostataka, razvijene su nadogradnje *syslog* protokola koje bi uklonile problematične elemente *syslog* protokola. Jedan oblik unapređenja syslog protokola je tzv. modularni (eng. *modular*) *syslog* protokol koji unutar sebe uključuje module koji se ugrađuju na generator log zapisa kao i na primatelja istih sa svrhom provjere integriteta podataka koji se prenose *syslog* protokolom. Time će administrator biti u stanju detektirati modificirane log zapise.
Jedan drugi oblik nadogradnje *syslog* protokola je *nsyslog* koji za razliku od *syslog* protokola ne koristi UDP pakete za prijenos već TCP koji zahtijevaju potvrdu primitka paketa. Također, protokol je proširen i s mogućnošću kriptiranja sadržaja paketa pri čemu se koristi SSL (eng. *Secure Socket Layer*) kriptografski protokol.

3.7. Prednosti log zapisa

Posjedovanje log zapisa administratorima uvelike olakšava posao administriranja računalnom mrežom i pojedinim računalima. To je osobito ispunjeno ukoliko je sustav logiranja organiziran s nekim centralnim log poslužiteljem. Administratori mogu na jednostavan način detektirati koja računala su aktivna, koliko dugo su aktivna, kojim resursima lokalni korisnici najčešće pristupaju, iz kojih država se najviše pristupa web stranicama organizacije, itd…

Korištenjem log zapisa moguće je detektirati različite nepravilnosti u radu kao i zlonamjerne aktivnosti koje inače ne bi bile detektirane. Organizacije sve češće koriste različite sustave za detekciju neovlaštenih aktivnosti (IDS) koji mogu biti takvi da prate aktivnosti na pojedinom računalu (eng. HIDS – *Host IDS*) ili na cijeloj mreži (eng. NIDS – *Network IDS*). Time oni izvještavaju o nastalim problemima, a centralni log poslužitelj te informacije povezuje i detektira određenu neovlaštenu aktivnost u sustavu. Pri tome mora biti ispunjen uvjet sinkroniziranosti različitih uređaja. Jedan oblik IDS uređaja je i vatrozid koji može uz zabranjivanje određenih zlonamjernih aktivnosti kao što su napadi uskraćivanjem resursa ili skeniranje portova, o istima slati i izvještaj u obliku log zapisa.

Mogućnost definiranja razine važnosti log zapisa omogućava administratorima orijentiranje na tzv. „važnije“ log zapise koji sadrže značajnije informacije o sustavima. Ta osobina većine generatora log zapisa je veoma korisna osobito iz razloga jer u sustavima uglavnom postoji velika količina log zapisa koji nisu toliko važni.

Na temelju log zapisa moguće je obavljati i poslovanje organizacije. Tako se npr. u telekomunikacijskim organizacijama log zapisi koriste za naplaćivanje različitih sadržaja. Naime, krajnji korisnik ne potpisuje nikakav ugovor na temelju kojeg bi mogao poslati određenu SMS poruku, uspostaviti određeni poziv, iskoristiti određenu uslugu i tome slično. Jedini dokaz da je krajnji korisnik zaista koristio određenu uslugu nalazi se u log zapisima koje organizacija bilježi u vezi njegovih aktivnosti. Na sličnom principu bazira se i naplaćivanje korištenjem Internet bankarstva te druge slične *on-line* usluge.

3.8. Nedostaci log zapisa

Pošto se log zapisi uglavnom šalju na centralni log poslužitelj, smanjuje se širina raspoloživog propusnog linka mreže. Ovaj nedostatak osobito je uočljiv u slučajevima kad je na log generatorima uključen detaljni prikaz log zapisa, tzv. *debug* način rada. U tom i sličnim oblicima načina rada ne pojavljuje se samo problem smanjivanja propusnosti mreže već se i performanse sustava koji generira log zapise smanjuju.

Iako log zapisi prikazuju stanje mreže i pojedinih računala, ipak u slučajevima nedovoljne sigurnosne zaštite ti podaci ne moraju biti vjerodostojni. Nažalost, sigurnosti log zapisa se uglavnom ne posvećuje dovoljna pažnja pa stoga određeni zlonamjerni korisnici ili napadači mogu izmijeniti te log zapise. Stoga se preporuča kriptiranje log zapisa.

Često se u sustavima generiraju „prevelike“ količine log zapisa, ili barem administratori koji ih trebaju analizirati tako smatraju. Naime, ukoliko ne postoji dobar sustav sažimanja i pregledavanja log zapisa, administratori često moraju pregledati velike količine u potrazi za određenim slijedom događaja. Iako su sve te informacije u osnovi važne jer predstavljaju dio određenih informacija, ipak tijekom pretrage za točno određenim log zapisima koji predstavljaju dijelove događaja, mogu stvoriti skup nepreglednih informacija. Također, iz tako velikih skupova informacija često je poprilično teško detektirati određene anomalije u ponašanju. Rješenje za ove probleme je u korištenju specijaliziranih alata koji trebaju biti prilagođeni za točno određene vrste log zapisa.

Sadržaj log zapisa često, po mišljenju administratora, ima ili previše informacija ili premalo informacija. Nažalost, količina sadržaja u log zapisima je rijetko idealna i to ovisi o iskustvu i znanju administratora da postavi pravu razinu važnosti log zapisa te da razumije log zapise.

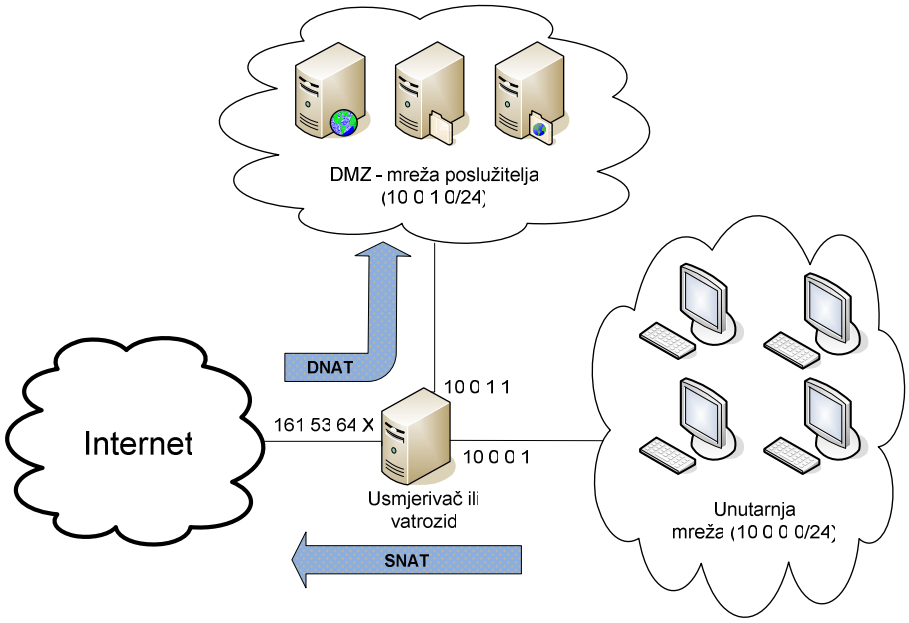
4. Testiranje različitih NAT implementacija

U ovom poglavlju prikazani su rezultati testiranja različitih NAT implementacija. Prva implementacija je Windows 2003 Server koji je danas veoma čest među korisnicima zbog svoje jednostavne administracije u odnosu na neka Linux ili UNIX rješenja. Potom su obrađena rješenja bazirana na IP Tables alatu otvorenog koda (eng. *open source*), pri čemu je odabran Astaro Security Gateway 6 te

Linux vatrozid koji je razvijan na LSS, ZESOI, FER. Na kraju je prikazana analiza Cisco-ovog PIX 506E hardverskog vatrozida.

4.1. Testno okruženje

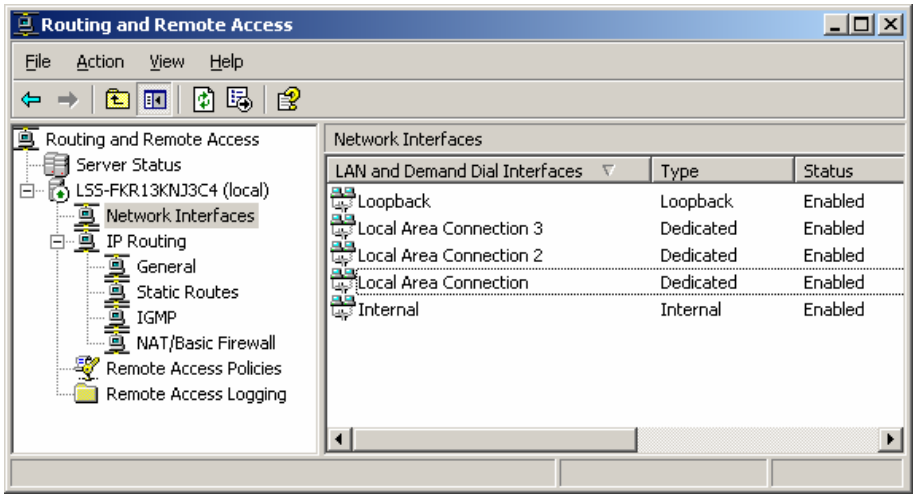
Prilikom testiranja korištene su dvije lokalne mreže. Jedna predstavlja unutarnju mrežu u kojoj se nalaze lokalni korisnici, a druga DMZ unutar kojeg se nalaze poslužitelji. Time je omogućeno testiranje dva oblika NAT-a: ciljni NAT (DNAT) i izvorni NAT (SNAT).



Slika 2: Testno okruženje

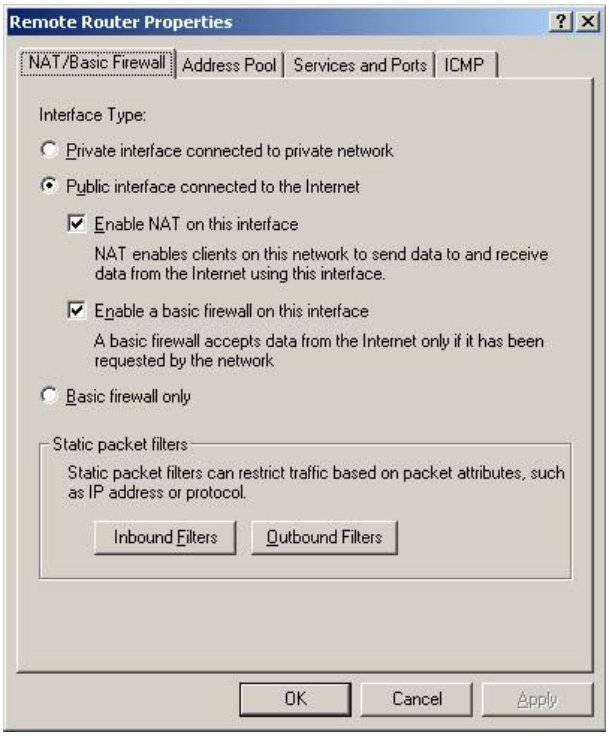
4.2. Windows 2003 Server

Iako mu to nije osnovna svrha, Windows 2003 Server se može koristiti kao usmjerivač pri čemu spomenuti operacijski sustav ima podršku za statički i dinamički NAT. Windows 2003 Server posjeduje brojne funkcionalnosti poslužitelja, a kao NAT uređaj pruža podršku i za IPSec veze.
Podešavanje Windows 2003 Server operacijskog sustava kao NAT poslužitelja je relativno jednostavan i brz postupak. Prvo je potrebno podesiti ulogu poslužitelja da bude RRAS (eng. *Routing and Remode Access*) / VPN (eng. *Virtual Private Network*) poslužitelj, a nakon toga je potrebno preko administrativnog alata *Routing and Remote Access* podesiti NAT. Moguće je podešavati sve opcije, od statičkih ruta pa do SNAT i DNAT pravila.



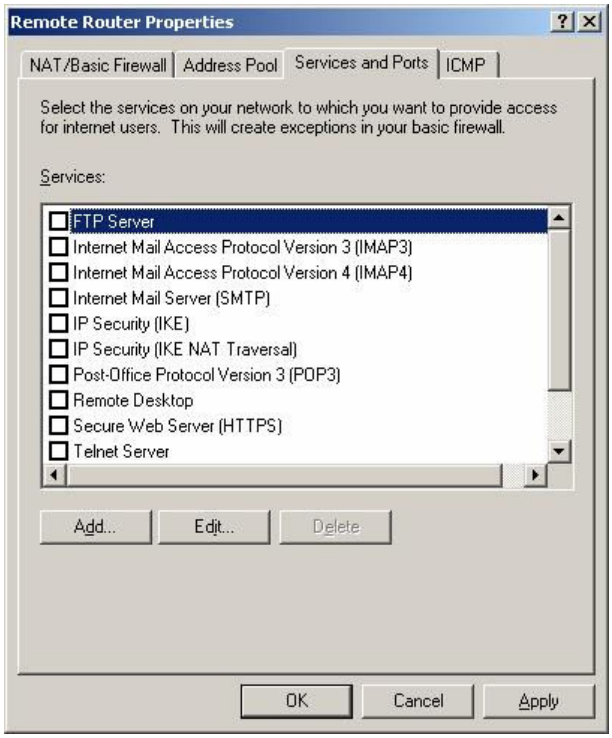
Slika 3: *Routing and Remote Access* administracijsko sučelje

Unutar opcije *NAT/Basic Firewall* RRAS sučelja moguće je aktivirati NAT funkcionalnost. Također, u tom dijelu se operacijski sustav može pretvoriti i u jedan osnovni oblik vatrozida. *NAT/Basic Firewall* sučelje prikazano je na sljedećoj slici.



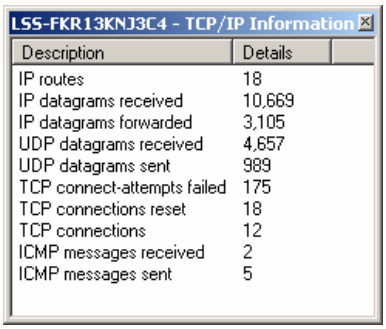
Slika 4: Uključivanje NAT funkcionalnosti

Windows 2003 Server omogućava administratorima jednostavno odabiranje protokola koji će biti podržani tijekom NAT preusmjeravanja za Internet korisnike. Pod opcijom *Service and Ports* (Slika 5) raspoloživi su određeni protokoli, a administrator može i sam definirati željene protokole specificiranjem ulaznih i izlaznih portova za konekcije. Odabiranjem pojedinih protokola, kreiraju se posebna pravila (iznimke) u osnovnom vatrozidu.



Slika 5: Odabiranje dozvoljenih protokola u NAT prometu za Internet korisnike

Nažalost NAT ugrađen u sam Windows 2003 Server nema mogućnost logiranja pojedinih veza i u tu svrhu je potrebno koristiti neki od drugih dostupnih vatrozida. Ipak, Windows 2003 Server omogućava pregledavanje trenutne statistike vezane uz broj ruta, broj uspostavljenih veza, kao i broj primljenih, poslanih i proslijeđenih TCP, UDP i ICMP paketa.



Slika 6: Statistički podaci NAT usmjerivača

Također, moguće je s malim vremenskim odmakom pratiti koje su veze u tijeku, odnosno koje veze su trenutno translatirane. Na slici Slika 7 dan je primjer dvije izlazne veze preko DNAT-a te jedne dolazne veze preko SNAT-a. Računalo s IP adresom 10.0.0.2 se nalazi u unutarnjoj mreži, a prilikom pristupanju Internetu prelazi preko usmjerivača koji ima IP adresu 161.53.64.X, a IP adrese različitih Internet resursa doznaje preko DNS poslužitelja na IP adresi 161.53.56.Y. S druge strane na IP adresi 10.0.1.2 nalazi se lokalni web poslužitelj kojem udaljeni Internet korisnici pristupaju.
Nažalost, iz prikazanih podataka nije lako zaključiti o kojim vezama se radi, a također bez dodatnih programa nije moguće niti sačuvati ove podatke u vidu log datoteke kako bi se kasnije mogli detaljnije analizirati.

LS5-FKR13KNJ3C4 - IP Address Translations

Address	Index	Type	Physical address
161.53.64.X	65,541	Dynamic	00 0B CD 1B 95 3E
161.53.64.Y	65,541	Dynamic	00 09 B7 6A C2 FF
10.0.1.2	65,540	Dynamic	00 00 F8 06 97 DA
10.0.0.2	65,539	Dynamic	00 E0 7D 7F 01 27

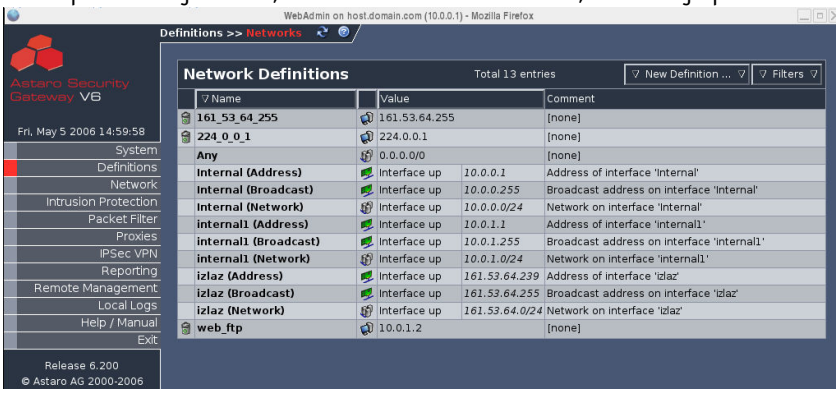
Slika 7: Prikaz trenutno aktivnih računala

4.3. Vatrozidi zasnovani na IP Tables alatu

IP Tables alat dio je Netfilter projekta, a predstavlja unaprijeđenu verziju IP Chains alata. IP Tables omogućava definiranje naredbi filtriranja na Linux operacijskim sustavima kao i definiranje naredbi prepisivanja IP adresa i portova. Korištenjem IP Tables paketa moguće je izgraditi vatrozide koji rade u tzv. dinamičkom načinu rada filtriranja prometa (eng. *stateful inspection*) koji omogućava započinjanje komunikacije samo s jedne mreže dok su s druge mreže dozvoljeni samo odgovori na upite iz prve mreže. Taj način rada se bazira na kontinuiranom praćenju i analizi pojedinih segmenata paketa koji prolaze kroz vatrozid, kako bi se na temelju njih u stvarnom vremenu mogle donositi pravilne odluke o filtriranju paketa. Ovakav način filtriranja dodatno podiže sigurnosni nivo sustava jer smanjuje broj nepotrebno otvorenih portova na vatrozidu. Drugi način rada, tzv. statičko filtriranje prometa (eng. *stateless inspection*) drži neprekidno „otvorenim" portove kako bi se povratni paketi mogli vratiti.

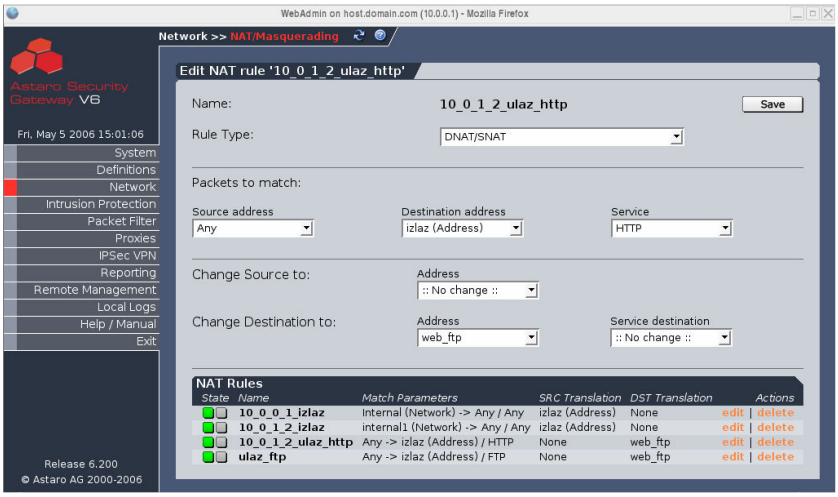
4.3.1. Astaro Security Gateway 6

Astaro Security Gateway je mrežni sigurnosni operacijski sustav otvorenog koda koji u sebi sadrži vatrozid, detekciju i prevenciju neovlaštenih aktivnosti, antivirusnu zaštitu, zaštitu od spama, filtriranje URL-a, VPN funkcionalnost i podršku za virtualne lokalne računalne mreže (VLAN).
Cijeli sustav se administrira preko web sučelja pa je prilikom instalacije potrebno odrediti preko kojeg mrežnog sučelja će se obavljati administracija sustava. Web sučelje za kontrolu je jednostavno i intuitivno tako da podešavanje NAT-a, ali i ostalih funkcionalnosti, ne iziskuje puno truda.



Slika 8: Web administracijsko sučelje Astaro vatrozida

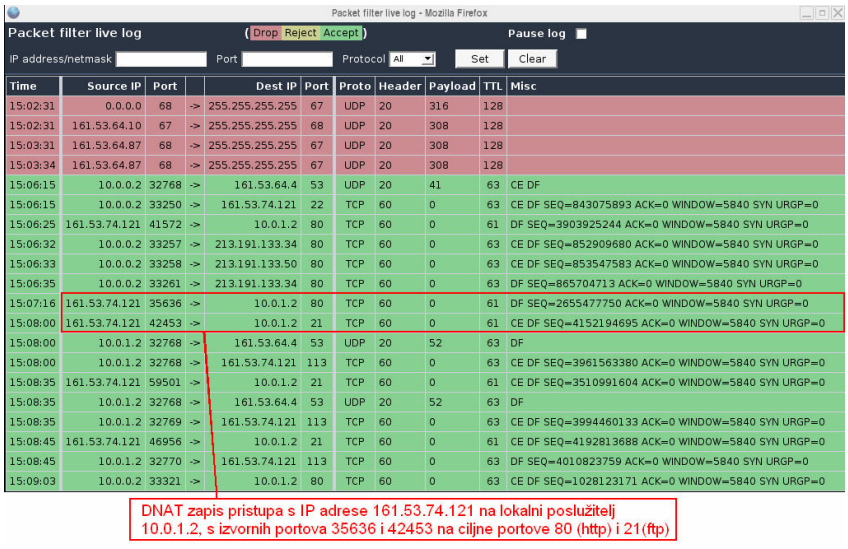
Na početku je potrebno definirati sve mreže, IP adrese mrežnih sučelja te IP adrese servisa koji trebaju biti dostupni iz vanjske mreže. U idućem koraku potrebno je definirati pravila NAT-a odnosno odrediti kriterije za prevođenje, kako privatnih IP adresa u javne tako i obrnuto. Kako bi se mrežni paketi mogli preusmjeravati potrebno je definirati i politike filtriranja koje će to dozvoliti. Prilikom definiranja pravila filtriranja potrebno je uključiti logiranje za pravila koja su sukladna pravilima NAT-a. Naime nad pojedinim NAT pravilima nije moguće aktivirati logiranje pa je to potrebno napraviti prilikom definiranja pravila koje dozvoljavaju NAT promet.



Slika 9: Modificiranje postojećeg DNAT pravila

Astaro nudi mogućnost pregledavanja log zapisa iz web preglednika u stvarnom vremenu tj. moguće je pratiti kako se kreiraju novi log zapisi. Svi log zapisi su u čistom tekstualnom obliku i nalaze se u `/var/log/` direktoriju. Za svaku novu vezu bilježi se vrijeme uspostavljanja, izvorna IP adresa i port, ciljna IP adresa i port, protokol te još neke druge manje važne informacije. U samim log zapisima bilježe se i MAC adrese sučelja preko kojih putuju paketi, ali ta informacija nije vidljiva u praćenju log zapisa iz web preglednika.

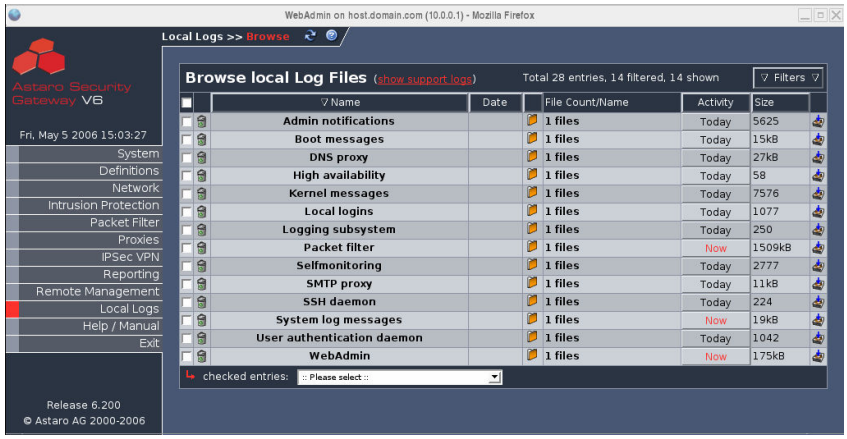
Na slici *Slika 10* vidljiv je prikaz log zapisa u web pregledniku. Posebno je označena veza prevedena DNAT-om.Vidljivo je da je s vanjske IP adrese 161.53.74.121 s porta 35636 uspostavljena veza na lokalnu mrežu na lokalni poslužitelj s IP adresom 10.0.1.2 na portu 80 (HTTP), a odmah zatim i s iste IP adrese i s porta 42453 nova veza na isti poslužitelj, ali na port 21 (FTP). Zelenom bojom označene su dozvoljene komunikacije, dok su crvenom bojom označeni odbačeni paketi. Ovakav način praćenja logova u nekoj aktivnijoj mreži bez dodatnih filtriranja nije praktičan zbog prevelike količine podataka i brzine kojom se novi zapisi dodaju u logove. Stoga se preporuča korištenje udaljenog *syslog* log poslužitelja ili pregledavanje lokalnih log datoteka.



Slika 10: Pregled log zapisa u stvarnom vremenu korištenjem web preglednika

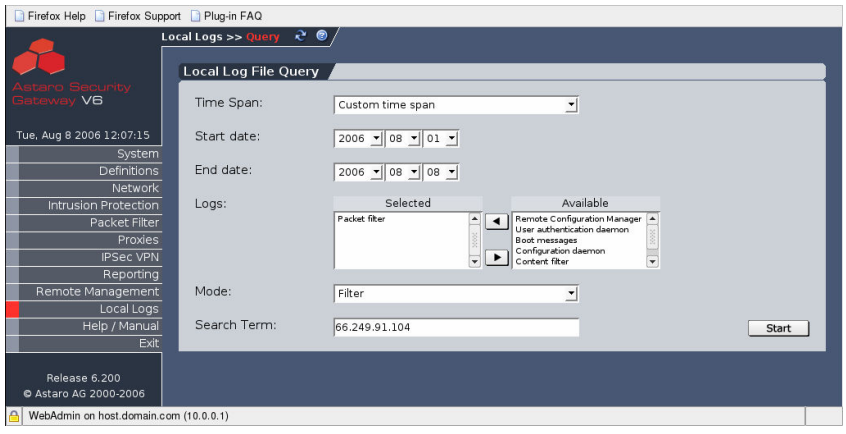
Log zapisi na Astaro vatrozidu prikazuju različite aktivnosti i ponašanja kao što su sistemske poruke registrirane prilikom podizanja sustava, poruke generirane od strane jezgre operacijskog sustava, aktivnosti alata za prevenciju neovlaštenih aktivnosti, poruke o pojedinim blokiranim ili propuštenim mrežnim paketima, izvještaji o kontroli integriteta vezano uz performanse, sigurnost, funkcionalnost,

itd... Na sljedećoj slici prikazano je osnovno web administracijsko sučelje preko kojeg se pregledavaju različiti oblici log zapisa.



Slika 11: Osnovno web sučelje s različitim log zapisima

Na Astaro vatrozidu, svi log zapisi se razdvajaju po danu nastanka u odvojene datoteke. Nažalost, nije moguće kreiranje različitih log datoteka za različite oblike mrežnog prometa kao što je DNAT, SNAT i sl. Stoga će u mrežama gdje postoji veći broj klijentskih računala iza NAT-a, kao i u mrežama gdje je promet preko NAT-a intenzivniji, log datoteke biti velike što će dodatno otežati njihovo pregledavanje i pretraživanje. Ovaj problem će biti još izraženiji ukoliko je vatrozid podešen da logira i druge vrste prometa osim NAT-a što je najčešće slučaj.log datoteke za jedan dan sadrže velike količine log zapisa. Ipak, Astaro vatrozid posjeduje mogućnost pretraživanja log zapisa kako se ne bi pojavljivali svi log zapisi. Odabirom *Local logs -> Querry* u web sučelju Astaro vatrozida moguće je izravno pretraživati postojeće logove. Prilikom pretraživanja moguće je odabrati vremensko razdoblje, vrstu log zapisa, metodu prikaza i traženi izraz. Kao vremensko razdoblje moguće je odabrati neko predefinirano (danas, jučer, zadnjih 7 dana, zadnjih mjesec dana) ili odabrati vremenski period postavljenjem početnog i završnog datuma. Prilikom odabira log datoteke koju je potrebno pretražiti, moguće je odabrati više vrsta log zapisa koje će biti istovremeno pretražene (*Packet filter*, *Boot messages*, itd....). Rezultati pretrage mogu biti prikazani na dva načina. Moguće je filtrirati log datoteke i prikazati samo zapise koji sadrže traženi izraz ili prikazati cijele log datoteke u kojima će posebno biti označeno pojavljivanje traženog pojma. Nažalost, prilikom zadavanja traženog izraza nije moguće korištenje logičkih operatora (I, ILI), kao ni zamjenskih znakova (*,?). Prikaz web sučelja za definiranje parametara pretrage log zapisa prikazano je na sljedećoj slici.



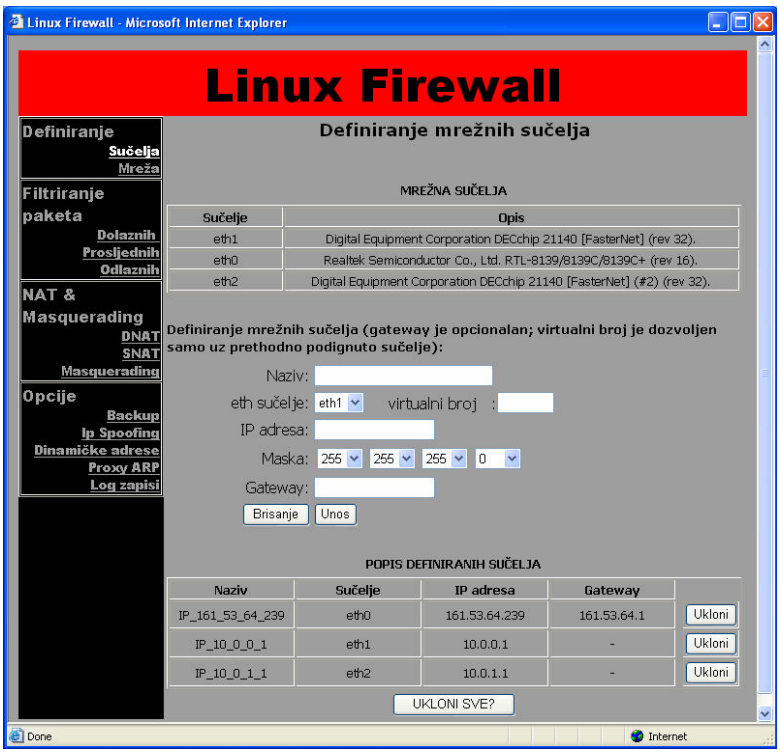
Slika 12: Definiranje parametara pregledavanja log zapisa na Astaro vatrozidu

Korištenjem web sučelja za pretragu log zapisa ne mogu se izdvojiti samo SNAT ili DNAT log zapisi. Ipak, kod traženja lokalnog korisnika koji je na određeni dan pristupao određenom računalu na Internetu moguće je unijeti IP adresu odredišta te odabirom dana dobiti sve log zapise koji su

povezani s tom IP adresom na taj dan te se time djelomično olakšava pronalazak točno određenog zapisa.

4.3.2. Prototip Linux vatrozida razvijenog na LSS, ZESOI, FER

Linux vatrozid razvijen na LSS, ZESOI, FER još je u ranoj fazi razvoja, a trenutno radi samo na Linux operacijskim sustavima. Vatrozid je zasnovan na IP Tables alatu pa radi u dinamičkom načinu filtriranja paketa (eng. *stateful inspection*), a podržava i NAT te *Masquerading* oblike prepisivanja IP adresa. Također, vatrozid podržava i Proxy ARP (eng. *Address Resolution Protocol*) funkcionalnost kao i funkcionalnost virtualnih lokalnih računalnih mreža (eng. VLAN – *Virtual Local Area Networks*) prema IEEE 802.11Q standardu. Administracija vatrozidom omogućena je kroz web sučelje izrađeno u PHP programskom jeziku koje se izvršava kroz Apache web poslužitelj, a iza kojeg se nalaze C++ izvršni programi. Korištenjem web sučelja moguće je pregledavati i log zapise. Razvijani vatrozid trenutno posjeduje zaštitu od nekoliko osnovnih vrsta neovlaštenih aktivnosti (*IP Spoofing*, *Smurf* napad uskraćivanja resursa, *Syn-Flood* napad uskraćivanja resursa, *ICMP flood* napad uskraćivanja resursa, *UDP flood* napad uskraćivanja resursa, *Ping-of-Death*, *Land* napad, skeniranje portova).

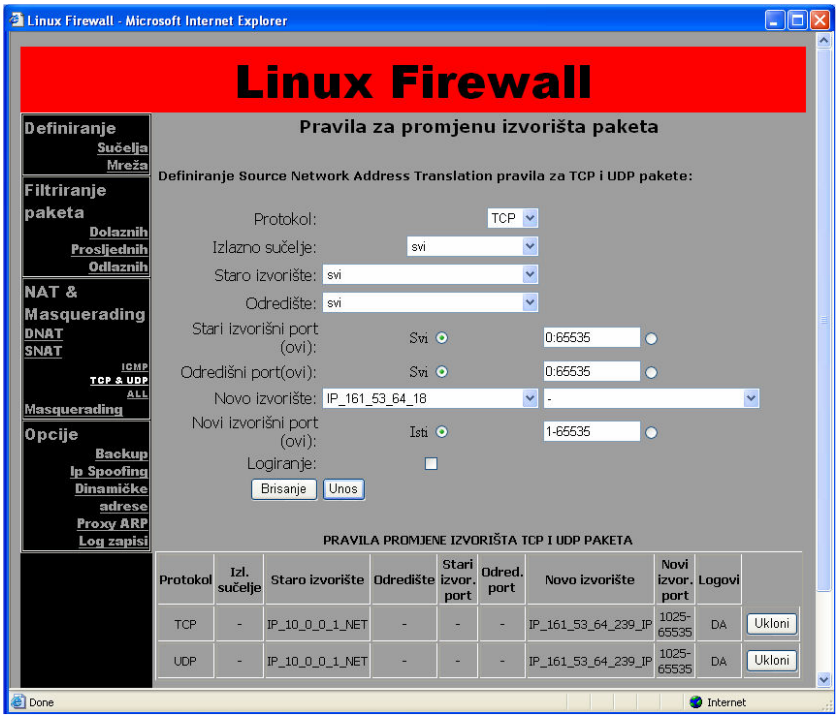


Slika 13: Web administracijsko sučelje vatrozida razvijanog na LSS, ZESOI, FER

Prilikom promjena i maskiranja IP adresa svi paketi mogu se obrađivati prema ICMP protokolu, TCP i UDP protokolu, ili prema svim protokolima. Zbog toga su promjene ciljnih (DNAT) i izvornih (SNAT i *Masquerading*) IP adresa raščlanjene prema protokolima: ICMP, TCP i UDP i svi. Obrada prema TCP i UDP protokolima posebno je izdvojena jer omogućava promjenu IP adresa paketa prema izvornim i ciljnim portovima, kao i mijenjanje istih. Na sljedećoj slici vidljiv je prikaz svih DNAT naredbi koje je moguće uklanjati pojedinačno ili skupno pri čemu modificiranje trenutno nije omogućeno.

Slika 14: Osnovna stranica za pregled svih DNAT naredbi

Na istom principu kao i za DNAT, i za SNAT i *Masquerading* postoji prikaz svih definiranih pravila. Prilikom definiranja jednog pravila prepisivanja IP adrese za sve protokole zajedno, moguće je definirati mrežna sučelja te IP adrese. Nasuprot tome kod definiranja pravila prepisivanja IP adresa za TCP i UDP protokole moguće je definirati i izvorne i ciljne portove, a kod definiranja pravila za ICMP moguće je definirati ICMP broj. Također, za sva pravila koja definiraju prepisivanje IP adresa određuje se ukoliko je potrebno registrirati log zapise za njih ili ne. Na sljedećoj slici vidljivo je web sučelje za definiranje SNAT pravila za TCP i UDP pakete.

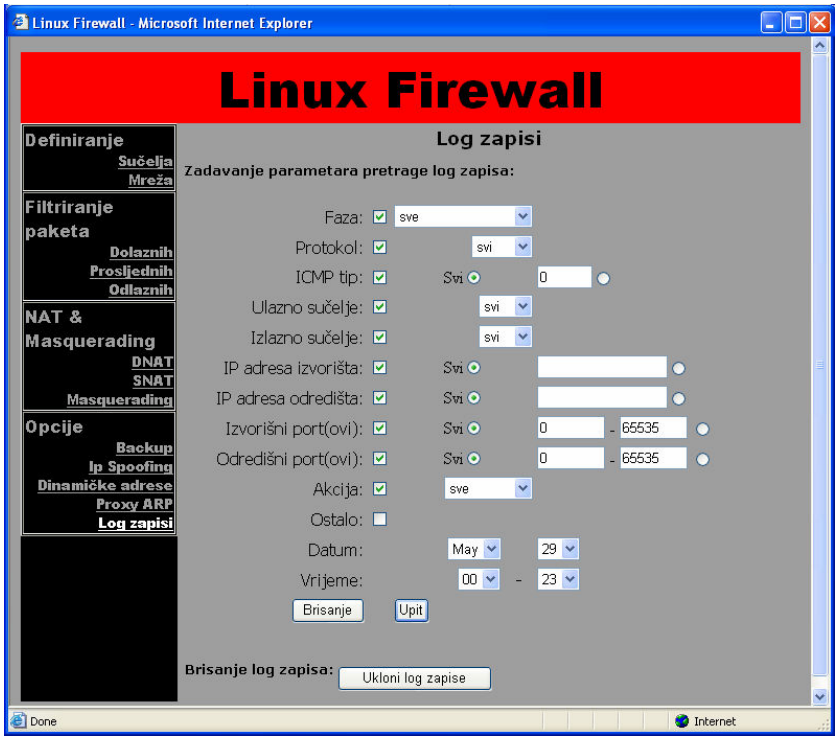


Slika 15: Definiranje SNAT pravila za TCP i UDP pakete

Prilikom definiranja svih NAT naredbi potrebno je pripaziti da se mrežnim paketima kojima se mijenjaju IP adrese dozvoli prolazak preko vatrozida u dijelu za filtriranje mrežnog prometa. Ovo nije samo karakteristika razvijenog vatrozida već svih vatrozida općenito.
Nakon što su definirane sva pravila prepisivanja IP adresa u mrežnim paketima s omogućenim registriranjem mrežnih paketa u obliku log zapisa i nakon što je vatrozid priključen na mrežu, moguće je pratiti log zapise preko web sučelja.
Na slici Slika 16 vidljivo je da se log zapisi mogu pretraživati prema sljedećim opcijama:

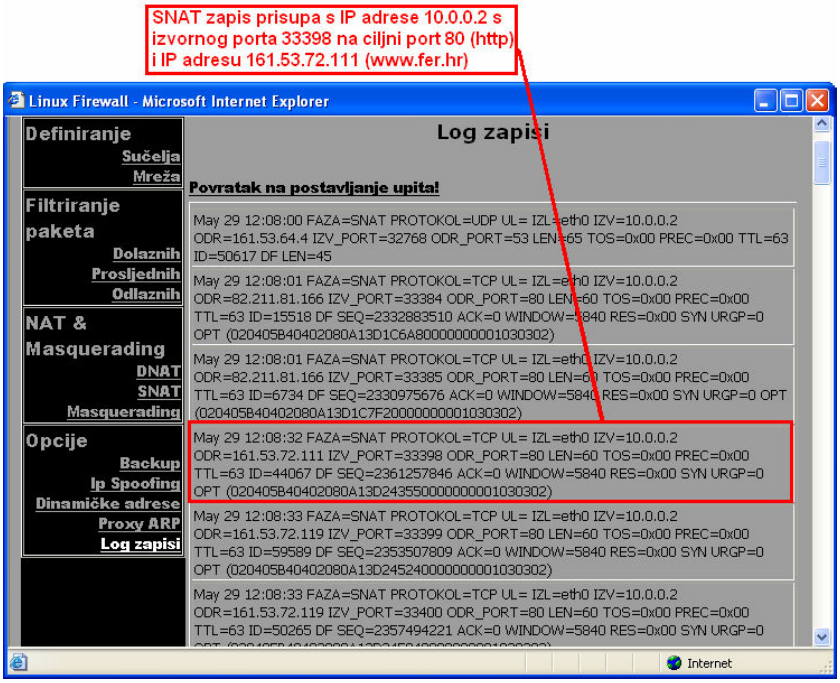
- faza obrade – može biti INPUT za pakete koji su namijenjeni vatrozidu, FORWARD za prosljeđivane pakete, OUTPUT za odlazne pakete generirane od strane vatrozida, DNAT za pakete kojima je promijenjena ciljna IP adresa, SNAT i MASQUERADING za pakete kojima je promijenjena ili zamaskirana izvorna IP adresa, a moguće je odabrati i opciju **„svi"** koja označava pretraživanje svih faza obrade,
- protokol – može biti TCP, UDP, ICMP ili svi protokoli zajedno,
- ICMP broj – može biti točno određeni ICMP broj ili svi, a koristi se uz ICMP odabrani protokol,
- ulazno sučelje – može biti točno određeno mrežno sučelje preko kojeg je mrežni paket dospio do vatrozida, ali mogu se odabrati i sva sučelja,
- izlazno sučelje – može biti točno određeno mrežno sučelje preko kojeg je mrežni paket napustio vatrozid, ali mogu se odabrati i sva sučelja,
- izvorna IP adresa – mogu biti sve moguće izvorne IP adrese ili točno određena IP adresa, ali ne postoji mogućnost pretrage po definiranim mrežama,
- ciljna IP adresa – kao i u prethodnoj opciji, mogu biti sve moguće ciljne IP adrese ili točno određena IP adresa, ali ne postoji mogućnost pretrage po definiranim mrežama,
- izvorni port(ovi) – može biti jedan specifični port, određeni rang portova ili svi mogući,
- ciljni port(ovi) – kao i u prethodnoj opciji, može biti jedan specifični port, određeni rang portova ili svi mogući,
- akcija – pretraživanje za INPUT, FORWARD i OUTPUT fazu obrade može biti po svim akcijama ili samo po akcijama odbacivanja (eng. *Drop*) tj. prihvaćanja (eng. *Accept*),
- datum – moguće je odabrati samo jedan dan u željenom mjesecu i
- vrijeme – moguće je odabrati vremensko razdoblje u satima koje je inicijalno postavljeno na cijeli dan.

Prilikom definiranja parametara pretrage moguće je definirati i koji od navedenih elemenata trebaju biti navedeni u rezultatima pretrage. Naime, administratorima često nisu potrebni svi podaci već npr. samo ciljna IP adresa, ciljni port i izvorna IP adresa u određenom vremenskom razmaku. Uz navedene parametre moguće je omogućiti i prikaz ostalih elemenata mrežnih paketa u koje spadaju elementi TOS (eng. *Type of Service*), LEN (eng. *Length of UDP Packet*), TTL (eng. *Time to Live*), SEQ (eng. *Sequence Number*), itd...



Slika 16: Definiranje uvjeta pregleda log zapisa

Na sljedećoj slici raspoloživ je prikaz SNAT log zapisa. Kao primjer odabran je zapis koji pokazuje pristupanje http stranici www.fer.hr koja ima IP adresu 161.53.72.111. Iz log zapisa moguće je saznati s kojeg porta je ta veza uspostavljena, u koje točno vrijeme te ostale manje bitne podatke.



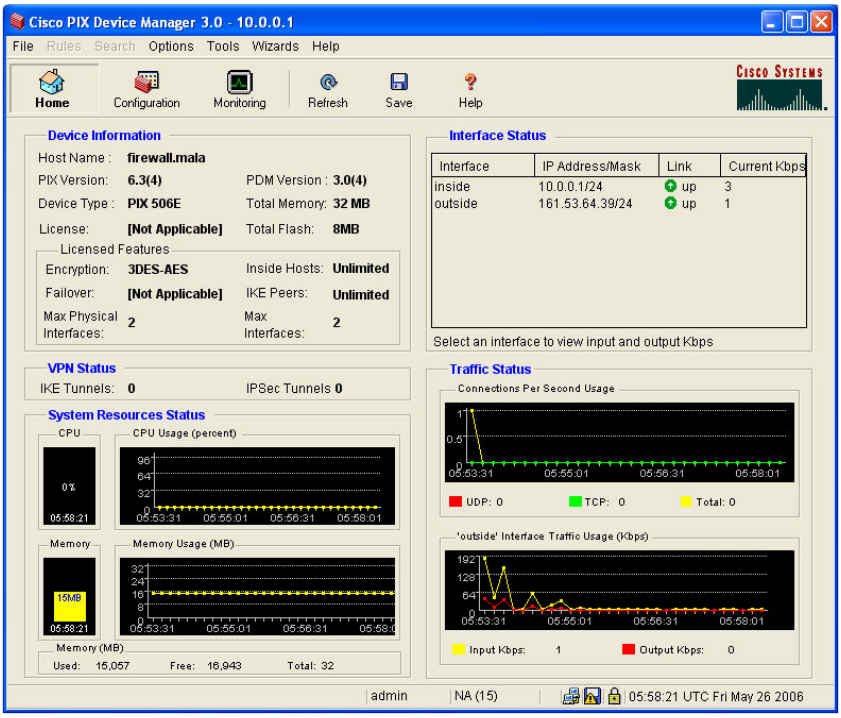
Slika 17: SNAT log zapisi

Tijekom testiranja ustanovljeno je da vatrozid ispravno registrira mrežne pakete nad kojima se obavlja NAT. Računala koja se nalaze u lokalnoj unutarnjoj mreži neometano su pristupala web sadržajima, a Internet računala su pri tome neometano pristupala lokalnom web poslužitelju u DMZ-u. Za pristup

poslužitelju iz DMZ zone, na vatrozidu je rezerviran port 10000 koji je preusmjeravao sve zahtjeve na port 80 ciljanog web poslužitelja.
Pregledavanje log zapisa na razvijanom vatrozidu može biti relativno jednostavno čak i kad se ne prati samo NAT promet. Naime, kod pregledavanja log zapisa na većini vatrozida, glavni nedostatak kod detektiranja pojedinih NAT veza je velika količina log zapisa od kojih se teško uočavaju tražene veze. Stoga je na razvijanom vatrozidu u svrhu jednostavnijeg pronalaska traženih log zapisa moguće odabrati željenu fazu obrade (DNAT, SNAT, *Masquerading*) te time smanjiti količinu prikazanih log zapisa. Problematika detektiranja pojedinih NAT zapisa zbog velikih količina log zapisa dodatno je olakšana jer se tijekom rada vatrozida log zapisi automatski razdjeljuju u odvojene datoteke temeljene na vremenu. Svaka log datoteka sadrži zapise ostvarene na određeni dan u određeni sat.
Također, pretraga log zapisa je dodatno olakšana jer administratorima često nisu potrebni svi podaci o uspostavljenim konekcijama. Stoga je na razvijanom vatrozidu moguće uključiti željene parametre koje je potrebno prikazati kao rezultat pretrage. Time je dodatno pojednostavljeno detektiranje traženih NAT zapisa jer administratori pregledavaju samo parametre koji ih zanimaju (ciljni port i IP adresa, izvorni port i IP adresa, i sl.).
U budućem razvoju vatrozida nastojat će se implementirati automatska obrada log zapisa u vidu detekcije neovlaštenih aktivnosti, ali i prevencije neovlaštenih aktivnosti. Na temelju detektiranih neovlaštenih aktivnosti, vatrozid će automatski mijenjati sigurnosne politike.

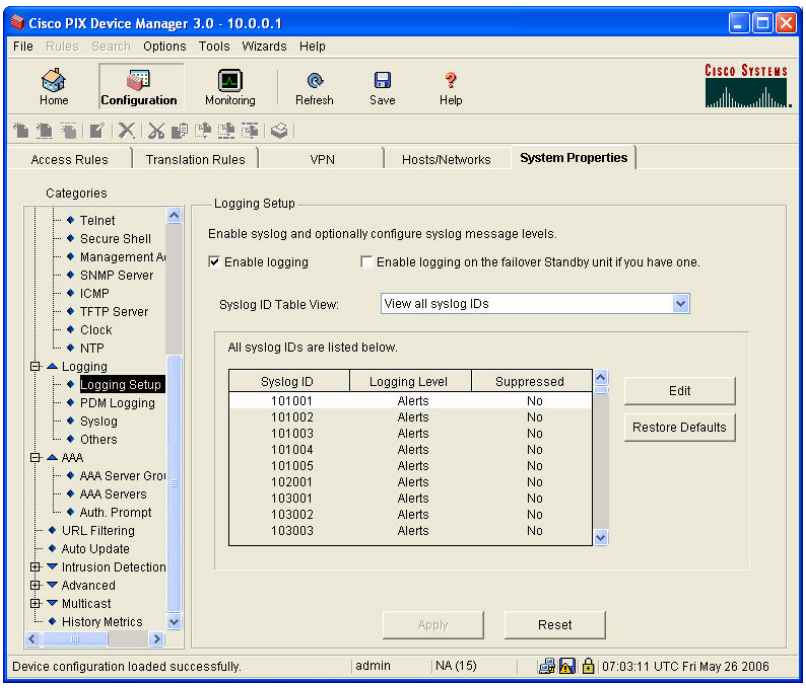
4.4. Cisco PIX 506E

Cisco PIX 506E je hardverski vatrozid koji nije implementiran na klasičnom računalu već na hardverskoj platformi izrađenoj posebno za tu namjenu. Nivo sigurnosti je značajno podignut zbog korištenja specifičnog operativnog sustava. Hardverska platforma vatrozida PIX 506E zasnovana je na procesoru Intel Celeron, 300 MHz s 128 kB L2 među-spremničke (ang. c*ache*) memorije. U vatrozid je ugrađeno 32 MB RAM-a i 16 MB *flash* memoije, a korištena je PCI sabirnica brzine 33 MHz.
PIX 506E uređaj može se administrirati na nekoliko načina. Najjednostavniji način pristupanja konfiguraciji vatrozida predstavlja onaj preko komandne linije (eng. *Command Line Interface* - CLI) kojem se može pristupiti lokalno putem konzole vatrozida ili s udaljenog računala korištenjem telnet protokola ili SSH protokola za pristup. Kao poseban paket uz vatrozid dolazi i PDM (engl. *PIX Device Manager*) koji predstavlja Java bazirano grafičko sučelje za konfiguraciju dostupno putem HTTPS protokola. Testirani vatrozid posjeduje samo dva mrežna sučelja pa se stoga s njim nije koristio DMZ za smještaj lokalnih poslužitelja te se nije testirao DNAT.
Inicijalno je vatrozidu moguće pristupiti samo putem konzole. Svi ostali načini pristupa (telnet, SSH i HTTPS) moraju se posebno omogućiti nakon inicijalne konfiguracije sučelja. Tijekom testiranja korišten je PDM paket za administriranje vatrozida. Na slici Slika 18 vidljivo je PDM administracijsko sučelje.



Slika 18: PDM administracijsko sučelje

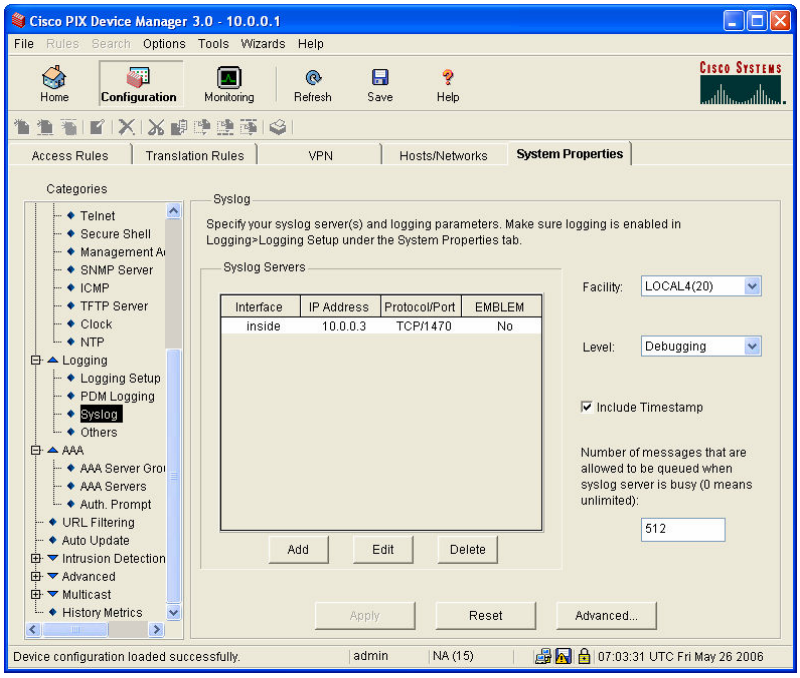
Logiranje mrežnih paketa nije predefinirana opcija na testiranom PIX vatrozidu. Stoga je logiranje mrežnih paketa i drugih zanimljivih događaja potrebno uključiti na samom vatrozidu jednostavnim uključivanjem opcije „*Enable logging*".



Slika 19: Uključivanje logiranja sistemskih događaja

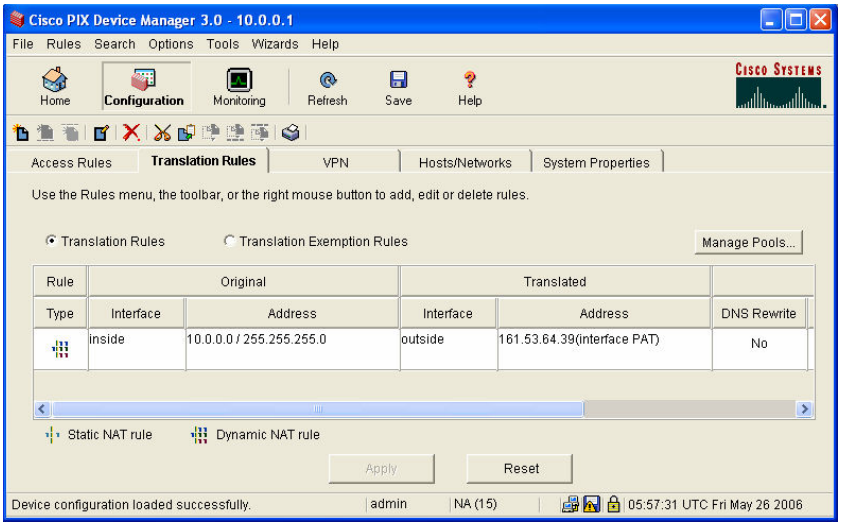
Nakon što se uključi logiranje, potrebno je definirati parametre *syslog* protokola. Preko web administracijskog sučelja (Slika 20) definira se *syslog* poslužitelj koji mora biti smješten na unutarnjoj mreži. Prilikom definiranja samog *syslog* poslužitelja definira se i protokol u kojem je potrebno slati log zapise na poslužitelj, kao i port na koji će log zapisi biti slani. Tokom testiranja odabrano je računalo s IP adresom 10.0.0.3, TCP protokol i port 1470. Prilikom definiranja parametara *syslog*

protokola potrebno je odabrati i razinu važnosti log poruka koje je potrebno slati na *syslog* poslužitelj. U primjeru sa slike odabran je *Debugging* razina obavijesti koja pruža najdetaljnije log informacije generirane od strane vatrozida. PIX vatrozid posjeduje 7 razina logiranja identičnih onim opisanim u poglavlju 3.3 ovog dokumenta.



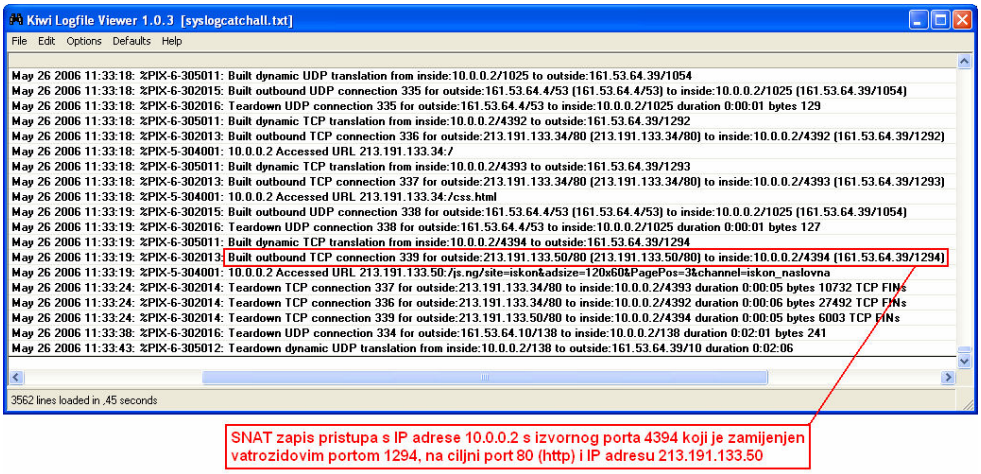
Slika 20: Podešavanje Syslog parametara

Nažalost, da bi se prikazali log zapisi koji pokazuju NAT mrežni promet, potrebno je uključiti informativnu (eng. *Informational*) razinu prijavljivanja od koje jedino detaljna razina generira veće količine prometa. Stoga administratori koji žele pratiti samo NAT promet moraju pretraživati relativno velike količine log zapisa kako bi pronašli željene zapise. U tu svrhu potrebno je tada izraditi određeni analizator log zapisa s kojim će se navedena pretraga, ali i sve ostale, ubrzati.
Na sljedećoj slici prikazano je NAT definirano pravilo koje mrežnim paketima pristiglih s unutarnjeg mrežnog sučelja (eng. *inside*) mijenja originalne IP adrese iz mreže 10.0.0.0/24 u IP adresu pridijeljenu vanjskom mrežnom sučelju (eng. *outside*) – 161.53.64.39.



Slika 21: Definiranje SNAT pravila

Tijekom testiranja korišten je Kiwi Syslog Daemon poslužitelj za primanje log zapisa. Uz tu opciju korištenja *syslog* poslužitelja, moguće je promatrati log zapise i u stvarnom vremenu korištenjem PDM Log Viewer sučelja. Na sljedećoj slici prikazani su registrirani log zapisi korištenjem Kiwi Logfile Viewer programa.



Slika 22: Log zapisi primljeni Kiwi Syslog Daemon poslužiteljem

Na prethodnoj slici vidljiv je SNAT zapis koji označava uspostavljanje HTTP veze prema poslužitelju na IP adresi 213.191.133.50 s unutarnjeg računala na IP adresi 10.0.0.2 pri čemu je vatrozid za tu vezu koristio svoj port 1294. Podaci iz log zapisa označavaju kako se tu radi o TCP vezi koja je uspostavljena 26.05.2006 u 11:33:19.

Nažalost, pregledavanje log zapisa generiranih od strane PIX vatrozida nije jednostavno iz više razloga. Prilikom definiranja razine važnosti log zapisa koji će biti generirati od strane vatrozida, potrebno je odabrati informativnu razinu koja uključuje podatke o uspostavljenim NAT vezama, ali također uključuje i velike količine raznih ostalih informacija. Stoga jednostavnost pregledavanje NAT log zapisa ovisi prvenstveno o mogućnostima alata za primanje i pregledavanje log zapisa. Odabrani Kiwi Logfile Viewer ne posjeduje nikakve napredne mogućnosti pregledavanja log zapisa pa je stoga u kombinaciji s PIX vatrozidom potrebno koristiti neki napredni log preglednik ili razviti vlastiti.

4.5. Testiranje veličine NAT log zapisa na Astaro Security Gateway 6 vatrozidu

U svrhu testiranja veličina log zapisa koji se kreiraju tijekom NAT transakcija, odabran je Astaro Security Gateway 6 vatrozid. Ostali uređaji nisu odabrani iz razloga što Linux vatrozid razvijan na FER, ZESOI, LSS-u trenutno ne posjeduje mogućnost kompresije log zapisa, Windows 2003 ne posjeduje mogućnost efikasnog zapisivanja log zapisa, a slična je situacija i s Cisco PIX 506E vatrozidom koji koristi eksterne programe za prikupljanje log zapisa. Također, pošto kod Cisco PIX 506E vatrozida nije moguće odabrati logiranje isključivo NAT prometa već je potrebo odabrati razinu na kojoj se logira NAT promet, a koja ne uključuje samo NAT promet, količine log zapisa su veće nego što je to u slučaju kad je moguće odabrati logiranje samo NAT prometa.

Prilikom testiranja odabrani su različiti protokoli: HTTP (eng. *Hyper Text Tranfer Protocol*), SSH (eng. *Secure Shell*), FTP (eng. *File Transfer Protocol*), TFTP (eng. *Trivial FTP*) te P2P (eng. *Peer To Peer*) koji se koristi za skidanje različitih datoteka. Testiranje je izvođeno s dva računala locirana u unutarnjoj mreži koja su preko preklopnika spojena na vatrozid.

Tijekom testiranja, vatrozid je bio smješten unutar mreže unutar koje se nalazilo oko 100 računala koji su generirali mrežni promet na *broadcast* domenu pa su ti paketi dolazili i na vanjsko sučelje vatrozida. Pošto je Astaro konfiguriran tako da registrira odbačene mrežne pakete koji nisu dio uspostavljenih sjednica, dnevno se registrira oko 8 MB standardno odbačenog (eng. *DROP*) mrežnog prometa koji komprimirano iznosi oko 400KB. Tijekom sat vremena registrira se oko 1500 DROP log zapisa, pri čemu jedan DROP log zapis sadrži oko 220 okteta (eng. *bytes*). Primjer DROP zapisa:

```
2006:06:23-13:58:16 (none) ulogd[2394]: DROP: IN=eth0 OUT=
MAC=ff:ff:ff:ff:d5:45:00:11:d8:bf:5c:46:08:00  SRC=161.53.64.223
DST=161.53.64.255 LEN=215 TOS=00 PREC=0x00 TTL=128 ID=54336 CE PROTO=UDP
SPT=138 DPT=138 LEN=195
```

Prilikom testiranja HTTP protokola korištena su dva oblika testiranja. Prvi je uključivao izradu skripte koja korištenjem `wget` naredbe skida sadržaj različitih hrvatskih stranica. Linkovi na hrvatske web stranice dobiveni su preko VIDI natječaja za najbolje hrvatske web stranice za godinu 2005. HTTP je odabran za testiranje iz razloga što je to često korišten protokol koji je najčešće povezan s DNS (eng. *Domain Name Server*) upitima. Također, HTTP spada u TCP grupu protokola za koje vatrozid ne bilježi sve pakete već samo pakete koji započinju konekciju. DNS protokol može biti zasnovan na TCP ili UDP protokolu.
Testiranje HTTP protokola korištenjem automatizirane skripte za skidanje web stranica trajalo je dvadeset minuta, a tijekom tog vremena skinuto je 821 web stranica od čega je 83 bilo praznog sadržaja. Ukupni broj zapisa koji su se odnosili na započinjanje HTTP sjednica je 948 (ACCEPT log zapisi). Naime, često pojedine web stranice uključuju u svoj sadržaj i elemente nekih drugih web stranica pa je broj ACCEPT log zapisa veći od broja skinutih web stranica. U odnosu na broj zapisa koji se odnose na započinjanje HTTP sjednica, broj log zapisa koji se odnose na DNS upite je relativno malen, a tijekom testiranja je iznosio 24 log zapisa. Također, u rezultate su uključeni i DROP log zapisi kojih je u tih 20 minuta bilo oko 516. Prosječna veličina jednog ACCEPT log zapisa iznosi 260 okteta, a u nastavku slijedi primjer jednog ACCEPT log zapisa:

```
2006:06:23-14:56:54 (none) ulogd[2394]: ACCEPT: IN=eth1 OUT=eth0
MAC=00:00:f8:02:ec:6d:00:e0:7d:7f:01:27:08:00  SRC=10.0.0.2
DST=69.41.243.226 LEN=60 TOS=00 PREC=0x00 TTL=63 ID=44102 CE DF PROTO=TCP
SPT=37754 DPT=80 SEQ=54690773 ACK=0 WINDOW=5840 SYN URGP=0
```

U sljedećoj tablici prikazane su procjene potrošnje diska za slučaj testiranja korištenjem automatske HTTP skripte. Važno je napomenuti kako Astaro razdjeljuje svoje log zapise prema danima, a nad svakim dnevnim log zapisom se obavlja kompresija koja je zahvaljujući jednostavnim i sličnim zapisima relativno visoka i iznosi oko 1:20.

Protokol:	HTTP
Način izvođenja:	automatska skripta (821 web stranica)
Vrijeme trajanja testa:	20 minuta
Povećanje NAT log zapisa:	352 KB
	1488 log zapisa
Procjena povećanja log zapisa na 24h za jedno računalo:	25 MB nekomprimirano
	1.25 MB komprimirano
Procjena povećanja log zapisa na 24h za mrežu od 50 računala:	1.22 GB nekomprimirano
	62.5 MB komprimirano

Tablica 3: Rezultat testiranja korištenjem automatske HTTP skripte

HTTP testiranje provedeno je i na drugačiji način. Naime, tijekom 20 minuta ručno su se otvarale web stranice koje su dobivene slučajnom pretragom korištenjem http://www.google.com tražilice. Tijekom tih 20 minuta otvarane su uglavnom međunarodne web stranice, ali iste nisu čitane kako bi se ostvarila što veća brzina učitavanja. Također, otvaranje web stranica je izvođeno paralelno što znači da se tijekom testiranja nije čekalo da se jedna web stranica otvori do kraja prije otvaranja druge stranice. Kod prethodnog testiranja to pravilo nije korišteno pa su se web stranice skidale slijedno.
Broj ACCEPT log zapisa usmjerenih prema HTTP portovima (ciljni port 80) različitih poslužitelja je 1417, a broj DNS upita 297 (ciljni port 53). Broj DROP log zapisa iznosi 501.

Protokol:	HTTP
Način izvođenja:	ručno pregledavanje web stranica
Vrijeme trajanja testa:	20 minuta
Povećanje NAT log zapisa:	534 KB
	2215 log zapisa
Procjena povećanja log zapisa na 24h za jedno računalo:	37.5 MB nekomprimirano
	1.88 MB komprimirano
Procjena povećanja log zapisa na 24h za mrežu od 50 računala:	1.83 GB nekomprimirano
	93.75 MB komprimirano

Tablica 4: Rezultat testiranja ručnog skidanja HTTP stranica

Vezano uz HTTP testiranje, važno je napomenuti kako prethodni oblici posjećivanja web stranica nisu uobičajeni, a nije uobičajeno niti 24satno „surfanje" web stranicama. Ipak, u svrhu reprezentativnog testiranja, odabrani su uvjeti koji osiguravaju maksimalnu potrošnju diskovnog prostora.
Prilikom testiranja SSH funkcionalnosti, unutarnje računalo se spajalo na jedno udaljeno računalo. Kao rezultat te akcije, u log zapisima se pronalazi samo jedan log zapis povezan sa SSH konekcijom. Iako se korištenjem SSH ili HTTP konekcija mogu prenositi vrlo velike datoteke (npr. 1 GB), u log zapisima pravilno konfiguriranog *stateful inspection* vatrozida, u pravilu se pronalazi samo jedan log zapis. U slučaju pucanja konekcije, moguć je pronalazak većeg broja konekcija. Primjer jedne uspostavljene SSH konekcije:

```
2006:06:15-11:33:23 (none) ulogd[2644]: ACCEPT: IN=eth1 OUT=eth0
MAC=00:00:f8:02:ec:6d:00:05:5d:a1:3b:71:08:00  SRC=10.0.0.5
DST=151.63.54.13 LEN=48 TOS=00 PREC=0x00 TTL=127 ID=64794 CE DF PROTO=TCP
SPT=2101 DPT=22 SEQ=190593264 ACK=0 WINDOW=65535 SYN URGP=0
```

Testiranje P2P protokola uključivalo je korištenje eMule i Azureus programa koji je zasnovan na korištenju `.torrent` datoteka. Testiranje oba programa trajalo je po dva sata.
Tijekom dvosatnog testiranja eMule aplikacije s Interneta je skinuto 57 MB, a na Internet je poslano (eng. *upload*) 20 MB. eMule koristi isključivo TCP protokol za komunikaciju između korisnika. Kako se prilikom skidanja datoteka klijent računalo spaja na veliki broj udaljenih računala, generira se i veliki broj log zapisa. Tijekom dva sata zabilježeno je 17749 ACCEPT pristupa pojedinim udaljenim računalima, među kojima je pronađeno 6040 različitih IP adresa. Pojedine IP adrese kojima je testno računalo pristupalo, pronađene su i u DROP zapisima. Naime, računala kojima klijent pristupa sa ciljem skidanja željenih datoteka, također pristupaju i klijent računalu s istom namjerom. Ali ukoliko ih vatrozid ne prihvati kao dio uspostavljene konekcije, iste bivaju odbačene.
Ukupni broj DROP zapisa tijekom dva sata je 8627, od čega je 413 usmjereno prema klijent računalu. Unutar tih 413 zapisa nalazi se 208 različitih izvornih IP adresa, a čak prema 196 IP adresa klijent računalo je prethodno otvaralo konekciju. Ipak, zbog određenih razloga i nakon nekog vremena, vatrozid je prestao držati te konekcije u svojim internim tablicama uspostavljenih konekcija.

Protokol:	P2P (eMule)
Način izvođenja:	skidanje 10ak datoteka prosječne veličine 700MB
Vrijeme trajanja testa:	2 sata
Povećanje NAT log zapisa:	6,25 MB
	26376 log zapisa
Procjena povećanja log zapisa na 24h za jedno računalo:	75 MB nekomprimirano
	3.75 MB komprimirano
Procjena povećanja log zapisa na 24h za mrežu od 50 računala:	3.67 GB nekomprimirano
	187.5 MB komprimirano

Tablica 5: Rezultat testiranja P2P korištenjem eMule programa

Testiranje Azureus aplikacije trajalo je dva sata kao i prethodno testiranje, a nakon čega je utvrđeno kako je skinuto 633.4 MB s Interneta dok je prenošenje datoteka na Internet ograničeno na maksimalnu brzinu od 50 KB/s što je uglavnom bilo maksimalno iskorišteno.
Unutar log zapisa detektirano je 15268 ACCEPT log zapisa pri čemu ih je 30% preko TCP protokola, a ostatak preko UDP protokola. Od toga ih je 7193 usmjereno prema različitim IP adresama. Uslijed većih brzina skidanja datoteka i prenošenja istih na Internet, povećao se i broj DROP log zapisa s Interneta. Ukupni broj DROP zapisa povećao se na 45582 log zapisa. Od toga je standardnih zapisa 9825, a broj log zapisa koji su usmjereni prema klijent računalu je 35757, a generirani su od strane računala s 924 različite IP adrese. Kako Azureus funkcionira i na TCP i na UDP protokolu, tako se među odbačenim paketima nalazi 4436 UDP paketa, 31241 TCP paketa pa čak i 80 ICMP paketa.

Protokol:	P2P (Azureus)
Način izvođenja:	skidanje 10ak datoteka prosječne veličine 350MB
Vrijeme trajanja testa:	2 sata
Povećanje NAT log zapisa:	14,5 MB
	60850 log zapisa
Procjena povećanja log zapisa na 24h za jedno računalo:	174,1 MB nekomprimirano
	8.7 MB komprimirano
Procjena povećanja log zapisa na 24h za mrežu od 50 računala:	8.5 GB nekomprimirano
	435.2 MB komprimirano

Tablica 6: Rezultat testiranja P2P korištenjem Azureus programa

Uslijed velikih količina log zapisa koji se odnose na P2P aplikacije, administratorima sustava se preporuča onemogućavanje P2P protokola ili izbjegavanje definiranja pravila prema kojima bi se P2P mrežni paketi zapisivali u log zapise. Rješenje bi bilo i kad bi se mogli ne zapisivati odbačeni mrežni paketi, ali iz sigurnosnih razloga to se ne preporuča, a na web administracijskom sučelju Astaro Security Gateway 6 vatrozida nije pronađena opcija kojom bi se ta funkcionalnost isključila. Ipak, to se može isključiti izravnim modificiranjem IP Tables naredbi kroz komandnu liniju. Web administracijsko sučelje ne posjeduje niti mogućnost ograničavanja brzine propuštanja pojedinih mrežnih paketa (protokola), iako je ta funkcionalnost omogućena IP Tables alatom.
Korištenjem Astaro Security Gateway 6 vatrozida testirane su i potrošnje diskovnog prostora za FTP i TFTP protokole namijenjene prijenosu datoteka s/na udaljeno računalo pri čemu je FTP zasnovan na TCP protokolu, a TFTP na UDP protokolu. Ta dva protokola potrebno je zasebno omogućiti u *Connection Tracking Helpers* dijelu web administracijskog sučelja. Uz njih raspoloživi su i:

- H323 - skup protokola specificiran od ITU udruge (engl. International Telecomunication Union) koji definira multimedijsku komunikaciju preko lokalnih računalnih mreža,
- PPTP (eng. *Point-to-point tunneling protocol*) – protokol za implementaciju VPN-a,
- MMS (eng. *Microsoft Media Services*) – protokol za prijenos multimedijalnih datoteka i
- IRC (eng. *Internet Relay Chat*) – protokol koji omogućava trenutnu komunikaciju preko Interneta.

Uključivanjem TFTP funkcionalnosti, moguće je prenijeti datoteke neograničene veličine na udaljeno računalo pri čemu u log zapisima ostaje samo jedan ACCEPT log zapis:

```
2006:06:15-17:50:38 (none) ulogd[2644]: ACCEPT: IN=eth1 OUT=eth0
MAC=00:00:f8:02:ec:6d:00:12:79:be:91:d9:08:00  SRC=10.0.0.10
DST=151.53.64.33 LEN=45 TOS=00 PREC=0x00 TTL=127 ID=51215 CE PROTO=UDP
SPT=1325 DPT=69 LEN=25
```

Isti rezultat se dobije ukoliko se uključi FTP funkcionalnost:

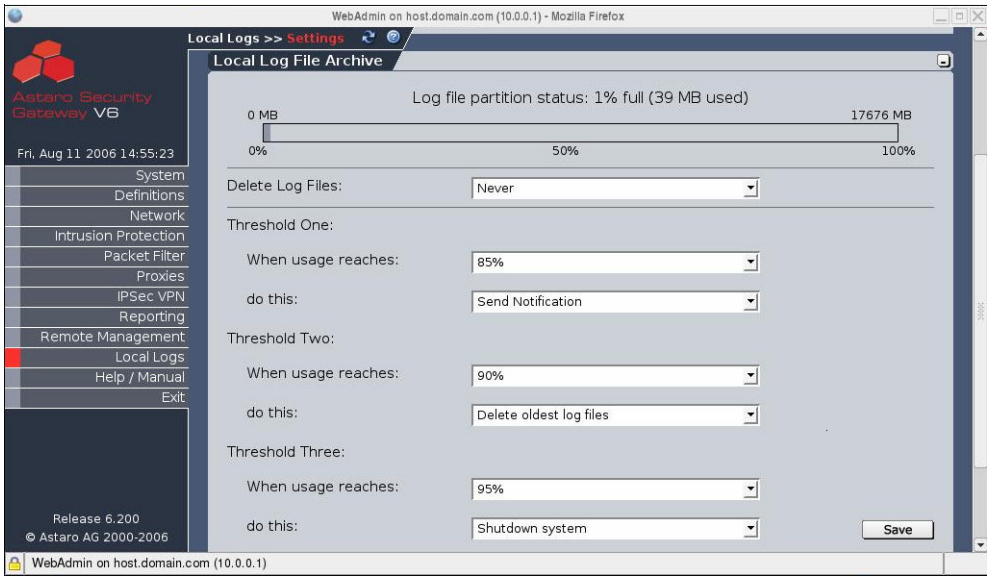
```
2006:06:15-17:54:16 (none) ulogd[2644]: ACCEPT: IN=eth1 OUT=eth0
MAC=00:00:f8:02:ec:6d:00:12:79:be:91:d9:08:00  SRC=10.0.0.10
DST=151.53.64.33 LEN=48 TOS=00 PREC=0x00 TTL=127 ID=34654 CE DF PROTO=TCP
SPT=1329 DPT=21 SEQ=723421547 ACK=0 WINDOW=65535 SYN URGP=0
```

Ipak, ukoliko se u web administracijskom sučelju uključi opcija „*Log FTP Data Connections*“, tada će se u log zapisima pronaći i sljedeća linija koja opisuje otvaranje podatkovnog kanala u FTP konekcijama, a opisana je kao FTP_DATA:

```
2006:06:15-18:11:48 (none) ulogd[2644]: FTP_DATA: IN=eth0 OUT=
MAC=00:50:bf:ee:be:bc:00:ee:b1:04:2a:83:08:00  SRC=161.53.64.13
DST=161.53.64.34 LEN=60 TOS=00 PREC=0x00 TTL=64 ID=13141 DF PROTO=TCP
SPT=20 DPT=1344 SEQ=2828409841 ACK=0 WINDOW=5840 SYN URGP=0
```

Astaro Security Gateway 6 je multifunkcionalni vatrozid pa tako posjeduje jednu funkciju koja može biti prilično korisna za rad sustava vezano uz količinu raspoloživog diskovnog prostora. Naime, na Astaro Security Gateway 6 vatrozidu raspoloživo je sučelje preko kojeg se na temelju količine potrošenog diskovnog prostora definiraju akcije koje je potrebno poduzeti. Moguće akcije su:

- *Send Notification* – akcija definira slanje obavijesti administratoru o potrošnji diskovnog prostora,
- *Delete oldest log files* – akcija definira automatsko pokretanje uklanjanja najstarijih log zapisa, te
- *Shutdown system* – akcija definira gašenje sustava.



Slika 23: Definiranje akcija na temelju veličina potrošenog diskovnog prostora

5. Moguća unapređenja logiranja NAT prometa

Ovisno o odabranom rješenju za obavljanje prepisivanja IP adresa i portova nad mrežnim paketima i logiranju tih aktivnosti, organizacije imaju određene funkcionalnosti koje im u većoj ili manjoj mjeri olakšavaju administraciju i kontrolu mreža. Zavisno o odabranim implementacijama i o zahtjevima organizacije, potrebno je osigurati određene nepodržane funkcionalnosti. U nastavku ovog poglavlja navedene su određene funkcionalnosti koje bi veće organizacije trebale osigurati. Manjim organizacijama često sve te funkcionalnosti nisu potrebne što je s jedne strane rezultat malenog broja računala iz čega proizlazi i malena količina administracije i kontrole, a s druge strane skupim iznosima ostvarivanja svih potencijalno korisnih funkcionalnosti.

5.1. Sigurnosni zahtjevi

Sigurnost log zapisa je potrebna i u slučajevima kad se log zapisi šalju na udaljeni log poslužitelj i kad se log zapisi pohranjuju lokalno, na uređaju na kojem su i generirani. Ukoliko zlonamjerni lokalni korisnici ili udaljeni napadači mogu modificirati log zapise koji se šalju na log poslužitelj ili mogu

provaliti na računalo na kojem se nalaze pohranjeni log zapisi i modificirati te iste log zapise, tada oni gube na vrijednosti. Udaljeni napadači tako mogu skriti svoje neovlaštene aktivnosti isto kao i zlonamjerni lokalni korisnici.
U sljedeća četiri poglavlja opisani su osnovni sigurnosni zahtjevi koji se postavljaju kako pred logiranje NAT prometa, tako i pred logiranje svih ostalih drugih događaja:

- tajnost podataka,
- integritet podataka,
- autentikacija izvora podataka i
- dostupnost podataka.

Također, u narednim poglavljima opisane su i moguće implementacije pomoću kojih se ostvaruju navedeni sigurnosni zahtjevi.

5.1.1. Tajnost podataka

Osiguravanje tajnosti podataka mora biti obavljeno već na računalu na kojem log zapisi bivaju generirani. To je potrebno postići primjenom osnovnih sigurnosnih politika na samo računalo (sigurne zaporke, alati za detekciju i prevenciju neovlaštenih aktivnosti, vatrozidi, kriptiranje log zapisa, itd…). Tajnost sadržaja mora biti osigurana i tokom eventualnog prijenosa na drugo računalo. Postoji više načina na koji se to može osigurati, a ovo su neki od raspoloživih:

- slanje log zapisa korištenjem SSH protokola,
- korištenje STunnel metodologije na temelju koje se podaci enkapsuliraju u SSL protokol,
- kriptiranje prometa korištenjem IPSec protokola (eng. *IP Security Protocol*), itd…

Ukoliko se log zapisi samo pohranjuju na računalo na kojem su i generirani tada se preporuča kriptirati log zapise korištenjem nekog asimetričnog algoritma. Na taj način, ukoliko napadač i provali na sustav, moći će saznati ključ s kojim se log zapisi kriptiraju, ali ih neće moći dekriptirati pa će podaci ostati tajni.

5.1.2. Integritet podataka

Integritet podataka osobito je važno osigurati u slučajevima kad se log zapisi šalju na udaljeni log poslužitelj, ali i u slučajevima kad se log zapisi samo spremaju na računalo na kojem su generirani. Prilikom slanja log zapisa na udaljeni poslužitelj, zlonamjerni napadač može modificirati log zapise ili ubacivati neke koje je sam kreirao.
Veliki problem za integritet kod udaljenog slanja log zapisa je korištenje UDP protokola koji ne osigurava prijem log zapisa. Stoga je potrebno koristiti TCP protokol koji zahtjeva potvrdu o prijemu. Nažalost tu i dalje ostaje opasnost modificiranja podataka. Stoga je potrebno nad podacima izračunavati određeni sažetak (eng. *hash*) koji se izračunava jednosmjerno kako bi se potvrdila ispravnost podataka.
Integritet log zapisa na računalu na kojem su generirani je poprilično teško osigurati. Naime, ukoliko napadač uspije preuzeti kontrolu nad računalom tada on može saznati i ključ koji se koristi za kreiranje sažetka nad log zapisima. Stoga je potrebno koristiti određeni alat koji će detektirati, a u idealnim situacijama i onemogućiti, sve neovlaštene aktivnosti.

5.1.3. Autentikacija izvora podataka

Kako bi se osigurao stvarni izvor podataka, tj. kako bi se osiguralo od slučajeva gdje zlonamjerni korisnici izmisle podatke i pošalju ih log poslužitelju, potrebno je koristiti neke od metoda koje su opisane u prethodnim poglavljima. Potvrda autentičnosti na udaljenom poslužitelju osigurava se korištenjem SSH protokola pri čemu je potrebno osigurati računala s kojih se generiraju log zapisi na prethodno opisane načine (sustavi za detekciju i prevenciju neovlaštenih aktivnosti, vatrozidi). Također, na log poslužitelju je potrebno koristiti sigurne zaporke koje se ne mogu jednostavno razbiti.

5.1.4. Dostupnost

Pod dostupnošću podataka prvenstveno se misli na mogućnost slanja i primanja log zapisa na udaljeni log poslužitelj ili na mogućnost zapisivanja log zapisa na disk. Naime, ukoliko napadač može izvesti određeni oblik napada uskraćivanja resursa na računala koja šalju log zapise ili na poslužitelj koji

prima log zapise, tada će log zapisi najvjerojatnije biti izgubljeni. S druge strane, ukoliko napadač uspije dobiti ovlasti za rad na računalu koje zapisuje log zapise na disk tada namjernim okupiranjem diska s nepotrebnim podacima može onemogućiti određene programe u zapisivanju log zapisa. Također, u određenim uvjetima napadač može srušiti procese koji generiraju log zapise.
U slučaju kad se log zapisi šalju s jednog računala na poslužitelj, potrebno je koristiti dva oblika zaštite:

- mrežna zaštita - osigurava detekciju i onemogućavanje zlonamjernih aktivnosti, kako od strane udaljenih napadača, tako i od strane lokalnih korisnika i tu svrhu potrebno je koristiti mrežne vatrozide i sustave za prevenciju neovlaštenih aktivnosti;
- dvostruko zapisivanje log zapisa – log zapise je potrebno zapisivati kako na poslužitelju tako i na računalu koje generira log zapise jer ako napadač onemogući slanje log zapisa od strane generatora ili primanje log zapisa od strane udaljenog poslužitelja, log zapisi će i dalje postojati na računalu na koje su i generirani.

Za zaštitu računala na koja se zapisuju log zapisi potrebno je koristiti neke od mehanizama opisanih u prethodnim poglavljima.

5.2. Sumiranje zapisa i vizualizacija

Prilikom rada administratori često imaju problema kod uočavanja određenih događaja. Naime, velike količine uglavnom nepotrebnih log zapisa onemogućavaju detektiranje nekih nepredviđenih događaja. Stoga se log zapisi često trebaju sumirati po određenim parametrima. Na taj način administratori mogu jednostavnije uočiti određene nepravilnosti nego u slučajevima koji zahtijevaju detaljnu analizu velikih količina log zapisa.
Dodatno poboljšanje u otkrivanju pojedinih događaja unutar log zapisa je u vizualizaciji sumiranih log zapisa u obliku različitih dijagrama. Naime, iako tablični prikazi mogu poslužiti kod detekcije odstupanja od uobičajenog ponašanja, ipak se u grafičkom prikazu odstupanja jasnije uočavaju.
Kod ciljnog NAT prometa sumiranje je moguće obavljati prema danima, prema ciljnim IP adresama ili mrežama i prema korištenim protokolima. Time je moguće detektirati kojim resursima zaposlenici najčešće pristupaju, odnosno koliko udio od ukupnog mrežnog prometa je potrošen u neke aktivnosti koje nisu povezane s radom.
S druge strane kod izvornog NAT prometa, uprava organizacije može detektirati iz kojih područja svijeta se najviše pristupa njihovim npr. web stranicama. Na temelju tih podataka organizacija se može odlučiti na određene poslovne aktivnosti kao što su npr. otvaranje zastupništva u određenim državama, usmjeravanje marketinga prema određenim državama i tome sl.

5.3. Normaliziranje zapisa

Zapisi koji bivaju generirani od različitih uređaja najčešće imaju i različite formate zapisa. Pojedini log zapisi su različito odijeljeni, koriste različite načine zapisivanja brojeva (decimalni, binarni, heksadecimalni), iste vrijednosti su različito nazvane i sl. Ta raznolikost može postojati čak i kad se koriste uređaji koji imaju istu namjenu, ali su im proizvođači različiti.
Ako se ovakvi različiti log zapisi koriste od strane različitih aplikacija tada ta različitost nije toliko niti važna. Ali, ukoliko se ovako različiti log zapisi trebaju objediniti u cjelinu i biti obrađivani od strane jednog programa tada ih je potrebno normalizirati na nekakav standard. Stoga je potrebno izraditi program koji bi trebao usklađivati različite formate log zapisa.

5.4. Korištenje baza podataka

Najčešći oblik zapisivanja log podatka je u obliku datoteka. Nažalost, ukoliko je naknadno potrebno provoditi određene operacije nad podacima, datoteke najčešće nisu najsretnije rješenje za tu svrhu. Korištenjem baza podataka moguće je koristiti neke postojeće programe koji mogu na jednostavan način pristupati i postavljati različite, manje ili više komplicirane upite nad velikim količinama podataka. Time je moguće detektirati zavisnosti između log zapisa koji nisu vremenski blizu.
Primjena baze podataka može biti raznolika pa se tako jednim SELECT upitom pregledavanja podataka mogu jednostavno dobiti svi NAT zapisi ili svi NAT zapisi u određenom vremenskom intervalu. Također, na jednostavan način je moguće detektirati i sve veze uspostavljene prema određenom ciljnom

računalu ili uspostavljene s određenog unutarnjeg računala. Pri svim tim upitima administrator može odrediti koji će parametri biti prikazani kao rezultat pretrage.
Nasuprot brojnim mogućnostima pretrage korištenjem baza podataka, unutar datoteka je log zapise moguće prvenstveno analizirati na vremenskoj osnovi. Zapisi se nalaze jedan iza drugog onako kako su generirani, tj. u nekom vremenskom slijedu i veoma je teško pronalaziti zavisnosti između log zapisa koji se nalaze u vremenski dalekim log datotekama. Implementiranje svih mogućnosti koje pružaju baze podataka gotovo je nemoguće bez velikih ulaganja organizacije, a s druge strane i neisplativo jer su baze podataka obično višestruko optimizirane.

5.5. Automatizirana obrada log zapisa

Oslanjanje na detektiranje određenih poremećaja od strane administratora često je nerealno. Naime, administratori oslonjeni samo na svoje iskustvo koje je uglavnom nedostatno i svoje ipak ograničene sposobnosti detektiranja anomalija, ne mogu obaviti kompleksne operacije nad podacima kao što to mogu računalni programi. Također, administratori najčešće ne dežuraju nad podacima cijelo vrijeme u potrazi za određenim aktivnostima, a ponekad je važna što hitnija reakcija na određene događaje. Stoga je poželjno posjedovati programe pomoću kojih će se obavljati automatizirana obrada podatka.
Primjer programa koji posjeduju alate za automatiziranu obradu log zapisa je program za detektiranje i onemogućavanje neovlaštenih aktivnosti. Nažalost, organizacijama ponekad nisu dovoljno dobri postojeći automatizirani alati za obradu log zapisa. Stoga razvijanje vlastitih programa za automatiziranu obradu log zapisa ovisi prvenstveno o mogućnostima organizacije u razvijanje vlastitog programa za obradu log zapisa te o područjima njihove djelatnosti.
Danas postoje brojni programi koji traže određena ponašanja u velikim količinama zapisa. Ti programi nazivaju se programima za povezivanje različitih događaja (eng. *Event Correlation Engine*). Korisnici mogu pomoću tih programa sami definirati određene zavisnosti između različitih događaja koje predstavljaju određeno ponašanje (eng. *behaviour*). Takvi programi nisu jednostavni i korisnici ih moraju dobro upoznati kako bi ih mogli (is)koristiti. Ipak, isti su raspoloživi u različitim verzijama, pa i u obliku otvorenog koda kao što je Simple Event Correlator [19].

5.6. Alarmiranje

Administratorima je često potrebna pravovremena obavijest o određenim definiranim događajima. Pri tome nisu svi događaji iste važnosti. Veoma je korisna opcija kad administratori mogu definirati oblik izvještavanja za pojedine događaje. Tako je npr. za manje važne događaje dovoljna obavijest elektroničkom poštom, dok je za neke alarmantne događaje potrebno slanje SMS poruke ili obavijesti putem *pager*-a. Primjeri kad je potrebno alarmirati administratora:

- izostanak mrežnog prometa – računala kontinuirano šalju određene signale međusobno, a u organizacijama su česti i programi koji samostalno rade pa stoga izostanak prometa predstavlja neuobičajeno ponašanje koje je potencijalno neispravno,
- detektirane neovlaštene aktivnosti u obliku skeniranja portova što je obično uvod u veće napade,
- povećanje iskorištenja diska iznad određenog postotka, npr. iznad 90% čime je moguće onemogućavanje zapisivanja novih log zapisa,
- pristupanje lokalnih korisnika neovlaštenim resursima ili web stranicama,
- svi log zapisi koji posjeduju oznaku hitnosti (eng. *Emergency*), itd…

Ukoliko se definira alarmiranje najviše razine, potrebno je obavijest o alarmantnom događaju isporučiti na sve moguće oblike. Naime, ukoliko je problem nastao zbog pada nekog mrežnog uređaja moguće je da SMS poruka neće uspjeti doći do SMS poslužitelja. Isto vrijedi i za elektroničku poštu koja može neplanirano završiti na zagušenom mail poslužitelju ili biti neopravdano dijagnosticirana kao spam poruka.

5.7. Definiranje naziva za određene vrijednosti parametara log zapisa

Prilikom pregledavanja log zapisa brojne IP adrese i brojevi protokola često administratorima ne predstavljaju nikakav važan podatak. To je osobito izraženo kod velikih organizacija gdje je broj IP adresa izrazito velik. Stoga je jedna poželjna funkcionalnost uređaja koji generira ili obrađuje log

zapise, mogućnost definiranja naziva pojedinih IP adresa. Većina uređaja posjeduje mogućnost preuzimanja naziva povezanih s IP adresama s DNS poslužitelja, ali administratorima unatoč tome nije jednostavno povezati određeni DNS naziv s određenim računalom. To je osobito ispunjeno u slučajevima kad se koriste privatne IP adrese koje nemaju DNS naziv. U tim slučajevima je neophodno da administrator definira nazive.

Uređaji koji u log zapise zapisuju i portove obično posjeduju određene nazive za određene portove (npr. HTTP=80, FTP=20-21, SSH=22, DNS=53, itd...), ali često korisnici definiraju vlastite korištene portove pa je zbog toga potrebno posjedovati mogućnost definiranja naziva pojedinih portova tj. protokola.

6. Zaključak

Logiranje mrežnog prometa omogućava administratorima nadziranje i kontroliranje ispravnog rada računalne mreže. Detektiranje neispravnog rada mreže moguće je otkriti nemogućnošću korištenja iste ili pravovremenim uočavanjem mogućih problema pregledavanjem log zapisa.

NAT tehnologija pruža organizacijama brojne pogodnosti u obliku smanjenog broja korištenih javnih IP adresa, povećanoj zaštiti lokalnih računala i poslužitelja, balansiranjem opterećenosti većeg broja poslužitelja, olakšanom administracijom mreže bez javnih IP adresa, i sl. Nažalost, NAT tehnologija omogućava lokalnim korisnicima pristupanje različitim Internet resursima i izvršavanje različitih ilegalnih aktivnosti pod zaštitom NAT uređaja koji obavlja prepisivanje njihove privatne IP adrese u svoju javnu. Time vlasnici Internet resursa ne mogu detektirati pravi izvor zlonamjernih aktivnosti i kao odgovornom smatraju najčešće računalo preko kojeg se obavlja NAT. Stoga organizacije moraju moći preko log zapisa detektirati korisnike koji su u određenom vremenu pristupali određenoj IP adresi i portu.

Svi oblici testiranih NAT implementacija posjeduju određene prednosti i nedostatke. Windows 2003 Server je jedno jednostavno rješenje s minimalnom potrebnom konfiguracijom, ali bez ikakvih log zapisa koji bi administratorima pomogli u radu. Vatrozidi bazirani na IP Tables alatu posjeduju veći ili manji opseg funkcionalnosti između kojih je i NAT koji je veoma dobro riješen kao i logiranje istog. Prednost vatrozida razvijanog na LSS, ZESOI, FER je u razdjeljivanju propuštenog prometa na ciljni i izvorni NAT, dok su kod Astaro Security Gateway operacijskog sustava svi log zapisi koji označavaju proslijeđene mrežne pakete, zajedno. Cisco-ov PIX je jedno profesionalno rješenje koje posjeduje efikasan sustav logiranja mrežnog prometa sa sedam razina važnosti pri čemu je jedini nedostatak nemogućnost uključivanja/isključivanja logiranja za pojedine vrste NAT konekcija.

Iako su za uspostavljanje uspješnog sustava logiranja kako NAT prometa, tako i svog ostalog mrežnog prometa, potrebni relativno visoki resursi, ipak je to danas neophodno. To osobito vrijedi za velike organizacije gdje je zbog velikih količina log zapisa potrebno uložiti veći trud za detektiranje određenih znanih ili neznanih događaja nego kod manjih organizacija koje zbog manjeg broja računala imaju i manje količine log zapisa koje je potrebno analizirati.

7. Reference

[1] RFC 1631, The IP Network Address Translator (NAT), http://www.ietf.org/rfc/rfc1631.txt, lipanj 2006.

[2] RFC 1918, Address Allocation for Private Internets, http://www.ietf.org/rfc/rfc1918.txt, lipanj 2006.

[3] RFC 3489, STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), http://www.ietf.org/rfc/rfc3489.txt, lipanj 2006.

[4] RFC 3164, The BSD syslog Protocol, http://www.ietf.org/rfc/rfc3164.txt, lipanj 2006.

[5] RFC 3103, Realm Specific IP: Protocol Specification, http://www.ietf.org/rfc/rfc3103.txt, lipanj 2006.

[6] The TIST (Topology-Insensitive Service Traversal) Protocol, http://mirrors.isc.org/pub/www.watersprings.org/pub/id/draft-shore-tist-prot-00.txt, lipanj 2006.

[7] Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for the Session Initiation Protocol (SIP), http://www.jdrosen.net/papers/draft-rosenberg-sipping-ice-00.html, lipanj 2006.

[8] Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Multimedia Session Establishment Protocols, http://www.softarmor.com/wgdb/docs/draft-ietf-mmusic-ice-00.html, lipanj 2006.

[9] Netfilter, http://www.netfilter.org, lipanj 2006.

[10] Cisco PIX 506E Security Appliance, http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b13.html, lipanj 2006.

[11] Astaro Security Gateway, http://www.astaro.com, lipanj 2006.

[12] Nathaniel Hall: Creating A Secure Linux Logging System, kolovoz 2004.
[13] Seham Mohamed GadAllah: The Importance of Logging and Traffic Monitoring for Information Security, prosinac 2003.
[14] Kenneth E. Nawyn: A Security Analysis of System Event Logging with Syslog, svibanj 2003.
[15] Ian Eaton: The Ins and Outs of System Logging Using Syslog, veljača 2003.
[16] Gregory Lalla: Centralizing Event Logs on Windows 2000, veljača 2003.
[17] Newport Networks: NAT Traversal for Multimedia over IP, lipanj 2006.
[18] Saikat Guha, Paul Francis: Characterization and Measurement of TCP Traversal through NATs and Firewalls, Cornell University, 2005.
[19] Simple Event Correlator, http://kodu.neti.ee/~risto/sec/ , lipanj 2006.
[20] Web stranice eMule projekta, http://www.emule-project.net/, lipanj 2006.
[21] Web stranice Azureus projekta, http://azureus.sourceforge.net/, lipanj 2006.