INFOTEH-JAHORINA Vol. 9, Ref. B-II-9, p. 213-217, March 2010.

OBEZBJEĐENJE GRANICE MREŽE VOIP PROVAJDERA UPOTREBOM OPENSBC-a I VYATTA FIREWALL-a
SECURING VOIP PROVIDER'S NETWORK BOUNDARY USING OPENSBC AND VYATTA FIREWALL

Petar Krgušić, Zoran Brajović, Biljana Vuksanović, *PTT Inženjering Podgorica*
Bojana Čavić, *Integral Inženjering Beograd*

Sadržaj - *Predmet analize u radu je konfiguracija VoIP sistema sa realizovanom adekvatnom interkonekcijom sa pristupnim telekom operatorom proširena besplatnom verzijom SBC-a ("OpenSBC") instaliranom na Vyatta firewall-u. Obavljeni testovi pomenute konfiguracije treba da potvrde opravdanost očekivanja da se bez dodatnih ulaganja u skupe SBC uredjaje može rješiti pitanje bezbjedne konekcije SIP korisnika.*

Abstract – *In this tutorial, we have analyzed configuration of VoIP system that has realized interconnection with telecom operator and that is extended with free version of SBC called OpenSBC installed on Vyatta firewall. Test results of mentioned configuration should to confirm our expectation that secure SIP customer's connection can be resolved without investing in expensive SBC devices.*

Ključne riječi: Session Border Controller, User Network Interface, Firewall, Open source

1. UVOD

Prilikom odabira tehničkog rješenja platforme za pružanje usluge prenosa govora preko mreža baziranih na IP protokolu, osim tehničkih pitanja bitnu ulogu igra i cijena odabrane konfiguracije. Cjelovita rješenja sa većinom funkcionalnosti iz ove oblasti su veoma skupa a samim tim i neadekvatna za budućeg VoIP provajdera koji tek treba da se pozicionira na telekomunikacionom tržistu. Obično se kompromis pravi u zavisnosti da li su ciljna grupa VoIP provajdera postojeći PSTN korisnici pristupnog telekomunikacionog operatora ili su to korisnici brzog interneta. Ukoliko su ciljna grupa postojeći PSTN korisnici, nameće se potreba ostvarivanja interkonekcije VoIP provajdera sa pristupnim telekom operatorom, preko E1 linkova. Prilikom realizacije interkonekcijskog linka, dominantni telekom operatori insistiraju na obavljanju seta zahtjevnih testova koje nije moguće proći bez adekvatne opreme. Troškovi proizašli iz realizacije interkonekcijskog linka u drugi plan stavljaju troškove zaštite integriteta mreže VoIP povajdera u konfiguraciji sa SIP korisnicima. Moguće rješenje prilikom ostvarivanja veze izmedju VoIP provajdera i pristupnog telekom operatora kao što je recimo veza preko primarnog ISDN-a ipak ne omogućavaju potrebne funkcionalnosti koje VoIP provajder treba da pruži svojim korisnicima. Jedna od bitnih funkcionalnosti je predstavljanje korisnika koji originira poziv, sa svojim vlastitim brojem (CLI) umjesto sa nekim od brojeva iz opsega primarnog ISDN-a što je slučaj prilikom pomenutog rješenja. Konfiguracija kojom ćemo se baviti u ovom radu je ona u kojoj VoIP provajder ima realizovanu interkonekciju sa pristupnim telekom operatorom preko E1 linkova ali ne i uslove za priključenje SIP korisnika. Kako bi omogućio priključenje SIP korisnika na svoju platformu ali u isto vrijeme i zaštitio integritet svoje mreže, VoIP provajderu je neophodan SBC (Session Border Controller).

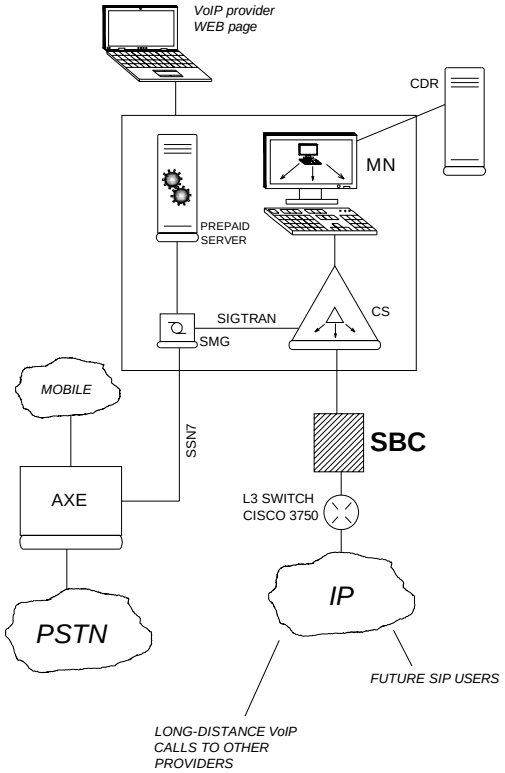
SBC je uređaj koji razumije VoIP sesiju i smješta se na granici mreže gdje služi za kontrolisano propuštanje poziva u nju (mrežu) [2]. Funkcionalno, SBC se dijeli na dvije odvojene logičke cjeline: Signaling SBC funkcija (SBC-SIG) kontroliše pristup VoIP signalnih poruka coru mreže i manipuliše sadržajem ovih poruka djelujući kao Back-to-Back User Agent (B2BUA); Media SBC funkcija (SBC-MEDIA) kontroliše pristup media paketa mreži, obezbjeđuje diferencijaciju servisa i QoS za različite media strimove kao i prevenciju krađe servisa djelujući kao RTP proxy. Na tržištu je prisutan širok spektar SBC uređaja koji se između ostalog razlikuju i po tome koje od funkcionalnosti podržavaju. Funkcije podržane od trenutno aktuelnih SBC uređaja su sledeće: DMZ (Demilitarized Zone) procesiranje; propuštanje VoIP signalnih i media paketa kroz Firewall i NAT (Network Address Translator); CAC (Call Admission Control) i DoS (Denial of Service) zaštita; QoS (Quality of Service); Media bridging; Fault Tolerance; Policy-based rutiranje poziva; Signaling protocol interworking; tarifiranje poziva. Prve dvije od pobrojanih funkcionalnosti podržavaju svi, na tržištu dostupni, SBC uređaji uključujući i besplatnu verziju Session Border Controlera-OpenSBC. Prve dvije funkcionalnosti su predmet našeg interesovanja.

2. TOPOLOGIJA SISTEMA

Matična kompanija autora je postala VoIP provajder krajem 2007. godine. Odabir tehničkog rješenja VoIP platforme uslovila je ciljna grupa potencijalnih korisnika. U to vrijeme, broj PSTN priključaka dominantnog telekom operatora je bio cca 200.000 dok je broj ADSL priključaka bio cca 6.000. Pomenute brojke su uticale na odluku da se za isporučioca opreme odabere kompanija sa bogatim iskustvom u proizvodnji telekomunikacione opreme koja je garantovala uspješno obavljanje testova interkonekcijskog linka sa dominantnim telekom operatorom. Dodatna pogodnost je bila činjenica da je odabrani isporučilac opreme ujedno i jedan od strateških partnera pomenutog telekom operatora u oblasti komutacija. Odabrano tehnicko rješenje je bazirano na

telekomunikacionom sistemu SI3000 MSCN [3]. Trenutno se servis izbora/predizbora (CS/CPS) operatora, preko VoIP sistema, nudi postojećim pretplatnicima fiksne telekomunikacione mreže dominantnog telekom operatora. Sistem pruža mogućnost postpaid i prepaid načina tarifiranja pri cemu su postpaid pretplatnici ugovorno vezani dok se prepaid saobraćaj obavlja sa prepaid karticama u okviru prepaid sistema, koji kao aplikacioni dio predstavlja dio cjelokupnog tehničkog rješenja. Interkonekciono povezivanje sa dominantnim telekom operatorom realizovano je sa 2 E1 linka sa po 30 govornih i jednim signalizacijskim (SSN7) kanalom a međunarodni saobraćaj se usmjerava ka nadprovajderima preko 10 Mbps simetrične internet konekcije.

Za dvije godine broj postpaid korisnika sistema je dostigao cca 2000 dok je broj mjesečno aktiviranih prepaid kartica u prosjeku cca 1000. Relativno mala iskorištenost sistema, porast broja ADSL priključaka sa 6.000 na cca 50.000, aktiviranje 7.000 WiMAX priključaka od strane drugog telekom operatora kao i sve veći broj korisnika kablovskog interneta aktualizovali su potencijalne SIP korisnike opisanog sistema. Obzirom da priključenje SIP korisnika nije preporučljivo bez zaštite integriteta mreže VoIP provajdera, to je i nabavka SBC uređaja postala neminovna. Nemogućnost dodatnog investiranja usmjerila nas je na OpenSBC. Prije eventualne konekcije potencijalnih SIP korisnika na VoIP sistem proširen OpenSBC-om, neophodno je detaljno testiranje OpenSBC-a u pomenutom okruženju. Na Slici .1 je prikazan opisani VoIP sistem. Na istoj slici je prikazan server sa instaliranim Vyatta Firewall-om i OpenSBC-om čije se funkcionisanje želi testirati u prikazanoj konfiguraciji..



Slika 1:VoIP sistem proširen SBC-om

3. INSTALACIJA VYATTA-e

Vyatta je provajder "open source" mrežnog softvera. Vyatta Community Edition 5 (VC5) je besplatni ruter i firewall softver baziran na Linux-u, koji smo iskoristili za transformisanje našeg PC-a u ruter koji može podnijeti mrežnu infrastrukturu u opsegu od DSL-a do 10-Gigabitnog Etherneta.

Nakon download-a Vyatta live CD ISO sa www.vayatta.org/downloads i snimanja istog na CD, procedura je sledeća:
1. Boot PC sa Vyatta Live CD ISO.
2. Kod logovanja, unijeti username kao 'root' i password kao 'vyatta'.
3. Ukucati 'install-system'
4. Konfigurisati prema vlastitim potrebama [5].
U radu ćemo opisati samo karakteristične dijelove konfiguracije.

Firewall spriječava ulazak neželjenog saobraćaja u mrežu kao i izlazak istog iz mreže. To se obavlja kroz ispitivanje paketovog vodiča bez potrebe razumjevanja ostalih djelova paketa. Ispod su prikazani isječci iz konfiguracije koji omogućavaju SIP Signalni Saobraćaj i RTP (voice) Saobraćaj.

Omogućavanje SIP Signalnog Saobraćaja

```
rule 40 {
    action accept
    destination {
        port 5060
    }
    log enable
    protocol udp
}
rule 41 {
    action accept
    destination {
        port 5060
    }
    log enable
    protocol tcp
}
```

Omogućavanje RTP (voice) Saobraćaja

```
rule 42 {
    action accept
    destination {
        port 10000-20000
    }
    log enable
    protocol udp
}
```

Postojeći VoIP sistem koji proširujemo SBC-om je u funkciji tako da nam je cilj, u prvoj fazi testiranja OpenSBC-a, bio ne mjenjanje postojeće postavke po pitanju već unešenih

parametara. U postojećoj konfiguraciji, statička IP adresa, dobijena od Internet provajdera kod kojeg je zakupljen simetrični internet, je iskorištena za konekciju sa nadprovajderima. Da bismo novu statičku IP adresu dobijenu od istog Internet provajdera iskoristili kao izlaznu sa SBC-a, bila je neophodna rekonfiguracija Cisco rutera (slika 1). Navedeno je uslovilo da smo se odlučili testirati OpenSBC pomoću softphone-ova (X-lite) konektovanih na SBC-om prošireni VoIP sistem preko ADSL konekcije dobijene od drugog Internet provajdera. U radu ćemo adrese koje ne mogu biti javno objavljene, radi zaštite konfiguracije, obilježavati sa X.X.X.X ili sl.

Konfigurisanje Ethernet Interfejsa

```
interfaces {
   ethernet eth0 {
      address X.X.X.X/28
      description unutrasnja
      duplex auto
      hw-id 00:21:85:96:2a:0b
      mtu 1500
      speed auto
   }
   ethernet eth1 {
      description spoljasnja
      duplex auto
      hw-id 00:19:e0:0d:10:ea
      speed auto
   }
   ethernet eth2 {
      address 192.168.1.101/24
      duplex auto
      hw-id 00:23:cd:b1:5b:9e
      speed auto
   }
   loopback lo {
   }
}
```

Dodjeljivanje hostname-a homeunix.com za pristup sistemu preko ADSL-a

```
system {
   domain-name sbc.homeunix.com
   gateway-address 192.168.1.1
   host-name vyatta
   login {
      user root {
         authentication {
            encrypted-password
$1$xDAXjOeC$9LUWxQ1voqD9lscz87iAH.
         }
         level admin
      }
      user vyatta {
         authentication {
            encrypted-password
$1$v74A/fEO$O9./I5OD6Xc8IWXOjOZtG
         }
         level admin
      }
   }
```

4. INSTALACIJA OpenSBC-a

Koristeći Open Source SBC poznat kao OpenSBC (www.opensourcesip.org) i Open Source firewall poznat kao Vyatta (www.vyatta.org), kreirali smo potpuno funkcionalan SIP Session Border Controller na jednom serveru. Procedura kreiranja je sledeća [5] :

-Download/Instaliraj Stavke potrebne za OpenSBC Kompilaciju:

1. Loguj se na Firewall kao user 'vyatta'
2. cd /etc/apt
3. su
4. Password: (unesi root password)
5. nano -w sources.list
6. Dodaj liniju: "deb ftp://ftp.us.debian.org/debian/ lenny main contrib non-free"
7. Ctrl-X i Y za prepis
8. apt-get update
9. apt-get install -y mc autoconf automake cvs flex expat libexpat1-dev libtool build-essential libxml2 libxml2-dev libtiff4 libtiff4-dev php5 php5-cli php5-mysql php5 php5-cli php5-mysql php5-gd mysql-server libmysqlclient15-dev php-pear php-db curl sox apache2 libssl-dev libncurses5-dev bison libaudiofile-dev subversion libnewt-dev libcurl3-dev libnet-ssleay-perl openssl ssl-cert libauthen-pam-perl libio-pty-perl libmd5-perl libpg-perl libdbd-pg-perl php5-pgsql sqlite3 libsqlite3-dev openssl ssl-cert libapache2-mod-php5 php5-cli php5-common phpMyAdmin php5-mcrypt mcrypt phppgadmin apache2 libmcrypt-dev

-Dobij OpenSipStack i OpenSBC sa CVS-a:

1. cd/usr/src
2. cvs –d:pserver:anonymous@opensipstack.cvs.sourceforge.net:/cvsroot/opensipstack login
3. cvs -z3 -d:pserver:anonymous@opensipstack.cvs.sourceforge.net:/cvsroot/opensipstack co –P opensipstack
4. cvs -z3 -d:pserver:anonymous@opensipstack.cvs.sourceforge.net:/cvsroot/opensipstack co –P opensbc

-Kompiliraj/Sačini OpenSipStack i OpenSBC:

1. cd /usr/src/opensipstack
2. chmod +x ./configure
3. ./configure
4. make bothnoshared
5. cd ../opensbc
6. chmod +x ./configure
7. ./configure
8. make bothnoshared
9. make distrib

-Relociraj Executables

1. cp /usr/src/opensbc/distrib/* /usr/local/bin

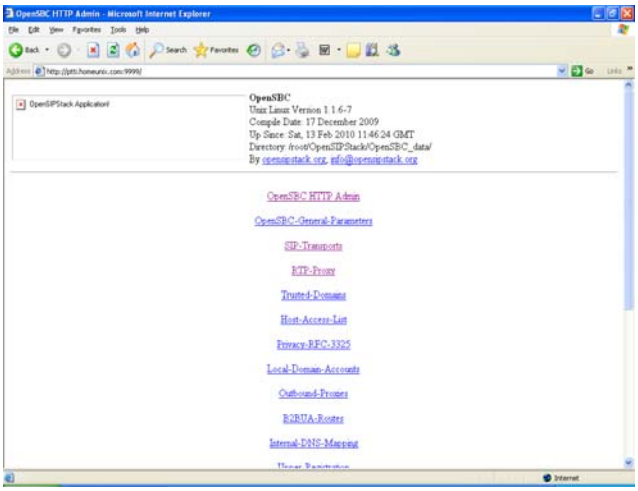
-Fiksiraj Shell Skripte

1. Edit /usr/local/bin/startup.sh (koristili smo 'nano -w /usr/local/bin/startup.sh')
2. Modifikuj startup komandu u: ./opensbc -d -p /var/run/opensbc.pid -H 65536 -C 1024000
3. Modifikuj shutdown komandu u: ./opensbc -k -p /var/run/opensbc.pid

-Podesi startovanje OpenSBC-a pri Startup-u

1. copy startup.sh to /etc/init.d (cp /usr/local/bin/startup.sh /etc/init.d/opensbc.sh
2. Modifikuj opensbc.sh da bi se startovao kao root i mogao pronaći aplikaciju.
   a. nano -w /etc/init.d/opensbc.sh
   b. Sačini liniju: /usr/local/bin/opensbc -u root -d -p /var/run/opensbc.pid -H 65536-C 1024000
3. ln -fs /etc/init.d/opensbc.sh /etc/rc2.d/S92opebsbc

Nakon uspješne konfiguracije OpenSBC-a, HTTP admin je dostupan preko porta 9999 servera na kojem je OpenSBC startovan [7]. Slika 2 prikazuje glavnu HTTP admin stranicu.



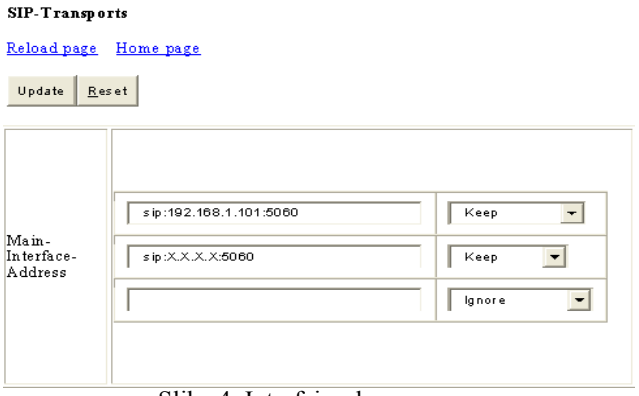
Slika 2: OpenSBC stranica za administriranje

U radu ćemo opisati samo karakteristične dijelove konfiguracije.

Otvaranje "OpenSBC General Parameters" linka omogućava nam podešavanje različitih parametera. U radu ćemo spomenuti samo neke od njih: Log-File-Prefix (Po default-u Log-File-Prefix je `b2bua`. Isti se može promijeniti u bilo koju vrijednost koja se ne podudara sa setom karaktera u imenima fajlova za specifični host operativni sistem.); User-Agent-Name (Postavljanje ovog parametra uzrokuje da OpenSBC šalje postavljeni User-Agent ili Server header u odlaznim SIP Header-ima.); SBC-Application-Mode (Arhitektura OpenSBC-a omogućava mu da djeluje kao B2BUA i kao Registar. Biranje funkcionalnosti se obavlja kroz postavljanje SBC-Application-Mode parametra.); Enable-Trunk-Port (OpenSBC ima mogućnost da prevodi SIP account-e iz internog domena u ITSP koji zahtjeva registraciju za obavljanje telefonskih poziva.). Slika 3 prikazuje opisane parametre.

Slika 3: OpenSBC-Osnovni-Parametri

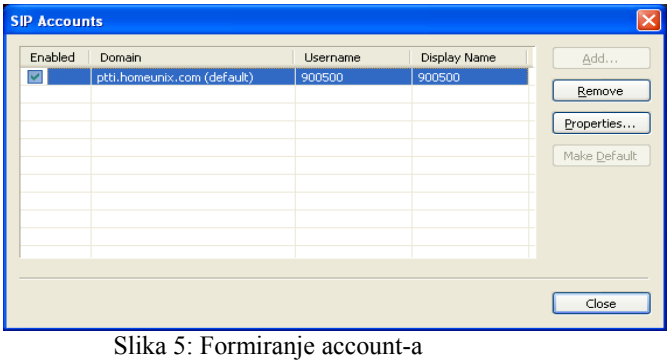
Otvaranje "SIP-Transport" linka omogućava nam postavljanje adresa različitih interfejsa. Jedna od njih je Main-Interface-Adress i to je adresa interfejsa (u SIP URI formatu) na kojem OpenSBC treba da veže svog glavnog transport listener-a. Ako se ova adresa na unese, po default-u je ista sip:*:5060 i na nju se vežu svi dostupni interfejsi. Mijenjanje njene vrijednosti zahtjeva restart kako bi promjena postala efektivna. Slika 4 prikazuje Main-Interface-Address.



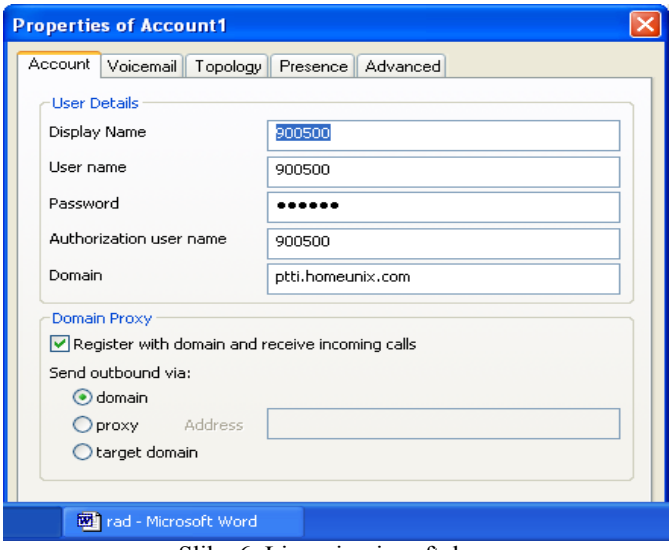
Slika 4: Interfejs adresa

5. TESTIRANJE SISTEMA

Testiranje VoIP sistema proširenog OpenSBC-om smo obavili upotrebom softphone-a tipa X-lite. Nakon download-a X-lite-a i instalacije istog na PC izvršili smo kreiranje SIP klijenta. Na slikama 5 i 6 prikazano je otvaranje account-a na softphone-u i licenciranje istog za obavljanje poziva preko VoIP sistema.

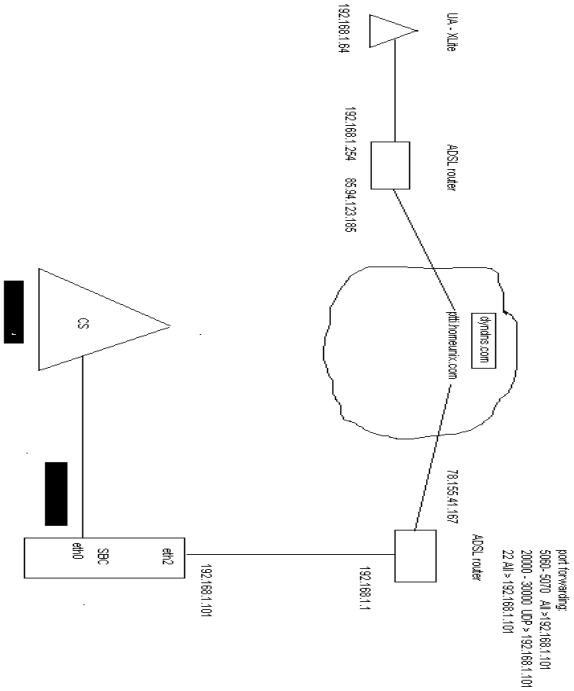


Slika 5: Formiranje account-a



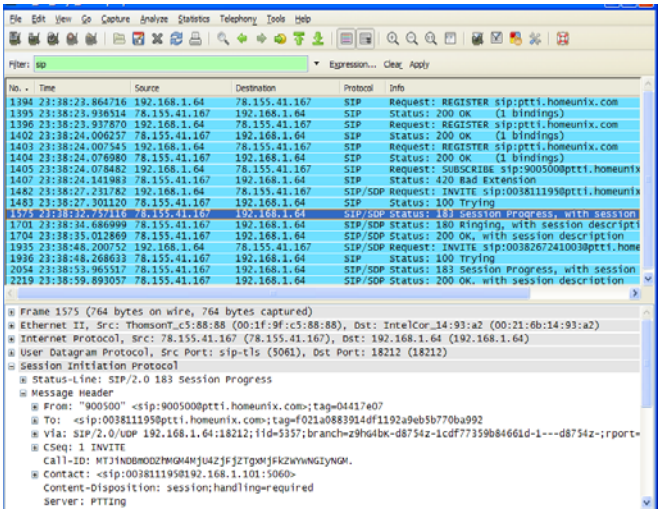
Slika 6: Licenciranje softphone-a

Na slici 7 je prikazan tok poziva po IP adresama obavljen sa softphone-a u konfiguraciji kada je softphone konektovan na VoIP sistem iz mreže koja na izlazu ima ADSL ruter. Na slici su prikazane IP adrese (dinamičke) na ADSL ruterima koje su bile važeće u trenutku obavljanja poziva. Također je na istoj slici opisan port forwarding koji je izvršen na ADSL ruteru preko kojeg se vrši konekcija SIP klijenata na VoIP system. Tamno zasjenčena polja se odnose na statičke IP adrese Call Servera i Ethernet kartice Eth0 koje ne možemo prikazati radi zaštite konfiguracije VoIP sistema. Sakrivena IP adresa kartice Eth0 je inače u konfiguraciji interfejsa na Vyatta-i prikazana sa X.X.X.X a također je na slici 4 prikazana na isti način.



Slika 7: Tok poziva po IP adresama

Wireshark-om smo skinuli trejs poziva na PC-u sa kojeg je poziv obavljen. Pomenuti trejs je prikazan na slici 8 i na istom je vidljivo da UA (User Agent) sa slike 7 koji obavlja poziv ne može vidjeti statičku IP adresu Call servera što je i bio osnovni motiv testiranja OpenSBC-a.



Slika 8: Trejs na UA-u

6. ZAKLJUČAK

Testiranje OpenSBC-a u konfiguraciji u kojoj se SIP klijenti povezuju na VoIP sistem preko ADSL konekcije je opravdalo naša očekivanja. Pozivi preko rutera na strani korisnika su obavljeni uspješno što je osnovni preduslov za konekciju potencijalnih SIP klijenata. Takođe, SIP klijent ne može vidjeti statičku IP adresu Call Servera što predstavlja drugi potreban uslov za konekciju SIP klijenta na Call server. Prije potpisivanja ugovora sa potencijalnim SIP klijentima, izvršiće se rekonfiguracija Cisco rutera na ulazu u VoIP sistem i omogućiće se konekcija OpenSBC-a na simetrični internet preko nove statičke IP adrese

7. LITERATURA

1. „ Implementing Service Quality in IP Networks“; Vilho R¨ais¨anen; John Wiley & Sons, Ltd; 2003
2. „Enabling the VoIP revolution“ ; Jon Hardwick; Data Connection Limited; 2005
3. „NGN Soutions“; Iskratel; 2003.
4. „ Glavni projekat SI300MSCN-PTT Inženjering “; 2007
5. „ Install OpenSBC on Vayatta firewall “; Michal W. Picher; January 2009
6. „Vyatta-My Basic Setap Guide“;
7. „OpenSBC Manual“