

**ANALISIS SQUID SERVER MONITORING PADA INTERNET PROTOKOL
VERSI 6 (IPv6) MENGGUNAKAN METODE *ACTIVE QUEUE MANAGEMENT***

(AQM)

JURNAL



DISUSUN OLEH :

ERWIN OKTAF KURNIAWAN WARUWU

1642101468

**PROGRAM STUDI INFORMATIKA
FAKULTAS SAINS DAN KOMPUTER
UNIVERSITAS KRISTEN IMMANUEL**

2020

Analisis Squid Server Monitoring Pada Internet Protocol versi 6 (IPv6) Menggunakan Metode *Active Queue Management* (AQM)

Erwin Oktaf Kurniawan Waruwu¹, Agustinus Rudatyo Himamunanto, S.Si., M.Kom², Febe Maedjaja, B.Sc., M.Sc³

Program Studi Informatika, Fakultas Sains dan Komputer
Universitas Kristen Immanuel Yogyakarta

Jalan Solo Km. 11 PO Box 4 YKAP Yogyakarta ph: (0274) 496256-296247 fax: (0274) 496258
e-mail : ¹erwinoktaf@student.ukrimuniversity.ac.id, ²rudatyo@ukrimuniversity.ac.id,

³febe@ukrimuniversity.ac.id

Abstrak

Server squid monitoring merupakan aplikasi dalam membangun proxy server yang bertugas sebagai koneksi sharing, filtering, caching dan memonitoring aktivitas client dalam jaringan. Penerapan squid server saat ini masih menggunakan pengalamatan Internet Protokol versi 4 (IPv4) yang semakin terbatas, sehingga dibutuhkan suatu standar baru pada routing protocol yang mampu mengakomodasi jumlah pengalamatan alamat IP yang lebih banyak yaitu Internet Protokol versi 6 (IPv6). Menurut statistik dari Google, persentasi pengguna yang mengakses Google melalui IPv6 dari tahun 2009 s/d 2020 mencapai 33.08 %.

Subject dalam penelitian ini adalah menjelaskan tentang analisis perancangan squid server monitoring menggunakan IPv6 serta melakukan pengujian QoS (Quality of Service) berdasarkan parameter delay, jitter, paket loss dan throughput. Dalam penelitian ini dilakukan metode penanganan bufferbloat (kemacetan) menggunakan metode Active Queue Management (AQM) dengan algoritma Random Early Detection (RED).

Berdasarkan hasil analisis squid server monitoring menggunakan IPv6 dan implementasi metode AQM, menurut standar THIPON didapat hasil throughput 21,517 bps dengan kategori “sangat bagus” nilai indek 4, delay 0,119 dengan kategori “sangat bagus” nilai index 4, jitter 0,303 dengan kategori “sangat bagus” nilai indek 4, dan paket loss 0,012 dengan kategori “sangat bagus” nilai indek 4.

Kata kunci: *Server squid, Proxy server, AQM, RED, IPv6, Parameter QoS, THIPON, Bufferbloat.*

Abstract

Squid monitoring server is an application in building a proxy server that functions as connection sharing, filtering, caching and monitoring client activity in the network. The current implementation of Squid Server still uses increasingly limited Internet Protocol version 4 (IPv4) addressing, so that a new standard in the routing protocol is needed that can accommodate more number of IP address addresses, namely Internet Protocol version 6 (IPv6). According to statistics from Google, the percentage of users accessing Google via IPv6 from 2009 to 2020 reached 33.08%.

The subject in this study is to explain the analysis of the design of Squid server monitoring using IPv6 and to perform QoS (Quality of Service) testing based on parameters of delay, jitter, packet loss and throughput. In this study, the method of

handling bufferbloat (congestion) using the Active Queue Management (AQM) method with the Random Early Detection (RED) algorithm.

Based on the results of the Squid server monitoring analysis using IPv6 and the implementation of the AQM method, according to the THIPON standard, the throughput results were 21.517 bps with the category "very good" index value 4, delay 0.119 with the category "very good" index value 4, jitter 0.303 with the "very good" category. "Index value 4, and package loss 0.012 with the category" very good "index value 4.

Keywords: Squid server, Proxy server, AQM, RED, IPv6, QoS parameters, THIPON, Bufferbloat.

1. PENDAHULUAN

Pada penerapaa squid server saat ini masih menggunakan teknologi komunikasi berbasis Internet Protokol versi 4 (IPv4) . IPv4 merupakan protocol internet yang dirancang oleh IANA (*Internet Assigned Number Authority*) untuk standar penomoran internet di dunia. IPv4 mengalami masalah keterbatasan pengalamatan IP yang semakin terbatas, keterbatasan jumlah pengalamatan pada IPv4 dibutuhkan suatu standar baru pada routing protokol yang mampu mengakomodasi jumlah pengalamatan alamat IP yang lebih banyak.

Menurut statistik dari Google, persentasi pengguna yang mengakses Google melalui Internet Protokol versi 6 (IPv6) dari tahun 2009 s/d 2020 mencapai 33.08 % (<https://www.google.com/intl/id/ipv6/statistics.html>. Diakses tanggal 1 Mei 2020). Negara-negara di Dunia tidak semua mengadopsi IPv6 dikarenakan faktor ketidaktahuan dan tidak adanya ISP penyedia layanan IPv6. Tunneling broker merupakan penyedia layanan berbasis IPv6 bagi Negara yang masih belum menggunakan IPv6. Metode Tunneling akan membangun jaringan IPv6 dengan memanfaatkan infrastruktur jaringan IPv4 yang sudah ada, dengan metode tunneling protokol IPv6 akan dienkapsulasi pada protokol IPv4. Paket yang terenkapsulasi ini kemudian diteruskan melalui jaringan IPv4 melalui infrastruktur jaringan IPv4.

Bufferbloat merupakan salah satu kondisi buffer dengan ukuran besar yang cenderung selalu penuh dan menyebabkan antrian panjang didalam buffer, jika hal ini terjadi secara terus-menerus maka dapat menyebabkan jeda transmisi data yang sangat tinggi, *bufferbloat* sering terjadi pada aplikasi berbasis *real-time*. *Active Queue Management* (AQM) salah satu cara untuk menangani terjadinya *bufferbloat*, ada banyak algoritma AQM yang bisa digunakan antara lain: *Random Early Detection* (RED) , *First In First Out* (FIFO) dan *Controlled Delay* (CoDel). Dalam penelitian ini, Peneliti menggunakan algoritma RED sebagai solusi penanganan *bufferbloat* pada saat antrian sedang padat.

Dalam penulisan skripsi ini peneliti mengali informasi dari penelitian-penelitian sebelumnya sebagai bahan perbandingan metode yang digunakan, peneliti mengali informasi dari jurnal yang disusun oleh Ulansari Ramadhani pada tahun 2017, Mahasiswa Universitas Respati Indonesia Jurusan Teknik Informatika yang berjudul "Analisis Simulasi Perbandingan Antrean Fifo Dan Red Dengan Menggunakan Network Simulator 2 (Ns2)". Tujuan dari jurnal ini adalah menganalisis perbandingan antrian algoritma FIFO dan RED menggunakan networks simulator 2 (NS2) sehingga dapat memperoleh data berdasarkan pengujian delay, paket loss, throughput dan total yang diterima pada suatu topologi jaringan kabel. Hasil simulasi diketahui antrian RED

terlihat lebih mampu menangani antrian ketika sedang padat sedangkan FIFO lebih unggul ketika menangani antrian berasal dari agent *User Data Protocol* (UDP) ketika antrian tidak terlalu padat.

Dengan demikian, meskipun ada penelitian sebelumnya yang berkaitan dengan penelitian yang akan dilakukan, akan tetapi memiliki perbedaan di beberapa aspek, dari perbedaan tersebut maka akan ada keinginan untuk menggunakan salah satu algoritma yaitu algoritma RED.

Berdasarkan uraian latar belakang di atas Peneliti dapat menarik rumusan masalah pada kasus ini adalah bagaimana merancang squid server monitoring menggunakan IPv6 dan melakukan monitoring jaringan dengan aplikasi squid server serta implementasi metode AQM pada mikrotik.

1.1 Landasan Teori

Landasan teori yang digunakan dalam penelitian ini adalah sebagai berikut:

1.1.1 Proxy server

Menurut (Armadya, 2014), Squid adalah *caching proxy* untuk web yang berbasis HTTP, HTTPS, FTP dan masih banyak lagi. Squid dapat mengurangi pemakaian bandwidth dan meningkatkan waktu respon dengan meng-cache. Dan menggunakan halaman web yang sering diminta atau diakses. Squid memiliki banyak jenis penggunaan, mulai dari mempercepat server dengan melakukan caching permintaan yang berulang-ulang, caching DNS, caching situs web, dan caching pencarian komputer di dalam jaringan untuk sekelompok komputer yang menggunakan sumber daya jaringan yang sama, hingga pada membantu keamanan dengan cara melakukan penyaringan (filter) lalu lintas. Versi squid mencakup dukungan protocol IPv6 dan Internet Content Adaption Protocol (ICAP). Squid awalnya dikembangkan oleh Duane Wessels sebagai “Harvest object cache”, yang merupakan bagian dari proyek Harvest yang dikembangkan di University of Colorado at Boulder. Pekerjaan selanjutnya dilakukan hingga selesai di University of California, San Diego dan didanai melalui National Science Foundation. Squid kini hampir secara eksklusif dikembangkan dengan cara usaha sukarela. Squid umumnya didesain untuk berjalan diatas system operasi mirip UNIX, meski squid juga bisa berjalan di atas system operasi Windows. Karena dirilis dibawah lisensi GNU (*General Public License*), maka squid merupakan perangkat lunak bebas.

1.1.2 Bufferbloat

Untuk menangani kondisi seperti bufferbloat, anjuran untuk menggunakan Active Queue Management (AQM) sudah lama direkomendasikan. Bila berbicara mengenai AQM maka hal tersebut tidak lepas dari kongesti. Kongesti adalah kondisi ketika kebutuhan bandwidth melebihi kapasitas link yang tersedia. Akibatnya adalah banyaknya packet loss, utilisasi link yang rendah (throughput rendah), delay queue yang tinggi, dan congestion collapse. Satria Mandala et.al. Menurut (Noer, 2017) Active Queue Management (AQM) Performance. AQM merupakan satu cara congestion control pada closed-loop atau packet switched network yang eksplisit. AQM berperan penting dalam mengatur buffer dan mengurangi latency. Secara umum berfungsi dalam mengontrol queue agar tidak full atau tumbuh terlalu besar dengan memonitor queue paket dengan menandai (marking) atau mendropnya. Pada kenyataannya, AQM tidak banyak digunakan pada router dan benar-benar tidak diterapkan pada banyak perangkat.

1.1.3 Active Queue Management (AQM)

Menurut (Pamungkas, 2018) RED merupakan mekanisme antrian yang dapat melakukan *packet drop* sebelum *buffer* penuh dengan cara menentukan parameter min thresh dan max thresh. Jika data < min thresh maka data dilayani jika data ditandai dan di drop secara random. Jika data > max thresh maka data akan langsung di drop.

Menurut (Gumilang, 2017) Random Early Detection (RED) adalah manajemen antrian dengan menghitung ukuran rata-rata panjang antrian menggunakan low pass filter secara eksponensial. Ukuran rata-rata panjang antrian RED dibatasi oleh batas minimal dan batas maksimal. Ketika ukuran rata-rata antrian kurang dari batas minimal maka paket tidak akan ditandai, pada saat rata-rata antrian melebihi batas maksimal maka paket yang datang akan ditandai. Pada kenyataannya paket-paket yang ditandai akan di buang karena rata-rata panjang antrian melebihi batas maksimal yang telah ditentukan. Ketika rata-rata antrian diantara batas minimal dan batas maksimal maka paket yang datang akan ditandai dengan kemungkinan atau probabilitas P_a , dimana P_a adalah fungsi dari ukuran rata-rata antrian *avg*.

Pada dasarnya, algoritma RED memiliki dua bagian terpisah. Salah satunya adalah untuk menghitung dan mengukur rata-rata antrian yang menentukan tingkat *burstiness* yang akan diizinkan dalam antrian router. Yang lainnya digunakan untuk menghitung kemungkinan paket-paket yang telah ditandai dan kemudian menentukan seberapa sering router menandai paket pada saat terjadi kemacetan antrian.

1.1.4 Tunnel Broker

Menurut (Muhtadi, 2015) *Tunnel broker* adalah wadah koneksi dari user pada jaringan IPv4 untuk melakukan proses pendaftaran dan pengaktifan tunnel. Fungsinya adalah untuk mengatur pembentukan, modifikasi, dan penghapusan tunnel sesuai dengan permintaan dari user. Dalam prakteknya, tunnel broker bertanggung jawab untuk membagi beban jaringan kepada tunnel server, caranya adalah dengan mengirimkan konfigurasi kepada tunnel server yang bersangkutan pada saat tunnel tersebut dibentuk, dimodifikasi, atau dibubarkan. Tunnel broker juga harus mendaftarkan alamat IPv6 user dan memasukkannya ke dalam DNS server.

Metode *Tunnel broker* akan membangun jaringan IPv6 dengan memanfaatkan infrastruktur jaringan IPv4 yang sudah ada, dengan metode tunneling protokol IPv6 akan dienkapsulasi pada protokol IPv4. Paket yang terenkapsulasi ini kemudian diteruskan melalui jaringan IPv4 melalui infrastruktur jaringan IPv4.

1.1.5 Quality of Service (QoS)

Menurut (Pamungkas dkk, 2018) Quality of Service (QoS) merupakan mekanisme pada jaringan yang menentukan bahwa aplikasi-aplikasi atau layanan dapat beroperasi sesuai dengan standart kualitas layanan yang telah diterapkan. Parameter-parameter Quality of Service (QoS) seperti throughput, latency, jitter, dan packetloss.

Ada Standart Quality of Services (QoS) salah satunya adalah THIPON (Telecommunications and Internet Protocol harmonization Over Network) TR. 101329.V2.1.1.1999-06 yang dikeluarkan oleh ETSI (European telecommunications Standards Institute) nilai Quality of Service (QoS) dapat dilihat pada Tabel 2.1.

Tabel 2. 1 Kategori Standart Nilai QoS

Nilai Indeks	Presentase (%)	Kategori
3,8 – 4	95 - 100%	Sangat Bagus
3 – 3,79	75 - 4,75%	Bagus
2 – 2,99	50 - 74,75%	Sedang
1 – 1,99	25 - 49,75%	Jelek

2. METODE PENELITIAN

2.1 Metode Penelitian

Dalam bab ini metodologi penelitian yang digunakan penulis dalam implementasi squid server monitoring pada IPv6 menggunakan metode AQM adalah sebagai berikut :

2.1.1 Studi Pustaka

Pada Langkah ini penulis mengumpulkan informasi-informasi yang dapat mendukung implementasi squid server monitoring pada IPv6 yakni, mencari Sumber informasi yang berhubungan dengan proxy server, TCP IPv6, algoritma RED pada AQM, tunneling broker dan aplikasi monitoring squid, pengujian parameter QOS dan monitoring client melalui jurnal, paper, skripsi, dan lain-lain.

2.1.2 Tahap Observasi

Pada langkah ini peneliti menentukan spesifikasi perangkat yang dibutuhkan dan topologi jaringan yang akan digunakan untuk membangun *squid server* pada IPv6.

2.1.3 Perancangan

Pada langkah ini peneliti melakukan rancangan skema system jaringan *squid server* serta melakukan instalasi *software* untuk konfigurasi pada router mikrotik dan komputer server. Pada konfigurasi di instal winbox 3.18, komputer server di instal OS Debian Server sedangkan aplikasi untuk melihat log squid adalah aplikasi SARG guna memonitoring *user* dalam jaringan.

2.1.3 Konfigurasi

Pada langkah ini peneliti melakukan konfigurasi tunnel IPv6 to IPv4 di router mikrotik menggunakan winbox untuk menyambungkan jaringan IPv6 dan konfigurasi *proxy server* di komputer server serta melakukan konfigurasi metode AQM.

2.1.4 Squid Server Monitoring

Pada langkah ini peneliti melakukan melakukan monitoring dari seluruh aktivitas *client*.

2.1.5 Pengujian

Pada langkah ini penulis melakukan pengujian system antara lain: pengujian tunnel, pengujian network, pengujian monitoring *client* dan pengujian nilai parameter QoS.

2.1.6 Tahap Dokumentasi

Pada tahap ini dilakukan dokumentasi terhadap proses input serta output berdasarkan paket data system sehingga dapat memudahkan apabila nanti system ini akan dikembangkan menjadi lebih baik lagi.

2.2 Analisis Kebutuhan Perancangan

Perancang squid server monitoring IPv6, kebutuhan dibagi menjadi 2 sebagai berikut:

2.2.1 Kebutuhan Perangkat Keras

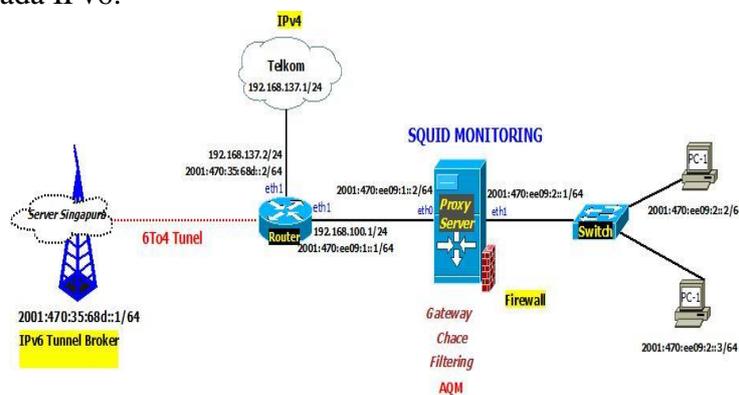
- a. Komputer Server (1 buah)
- b. Komputer Client (2 buah)
- c. Router (1 buah)
- d. Switch (1 buah)
- e. Adapter Ethernet External USB (1 buah)
- f. Kabel UTP (5 Meter)

2.2.2 Kebutuhan Perangkat Lunak

- a. Debian 9
- b. Windows 10
- c. Windows 7
- d. Winbox 3.18
- e. Wireshark 3.2.5
- f. Squid
- g. SARG (Squid Analysis Reports Generator)
- h. Apache2

2.3 Desain System Jaringan

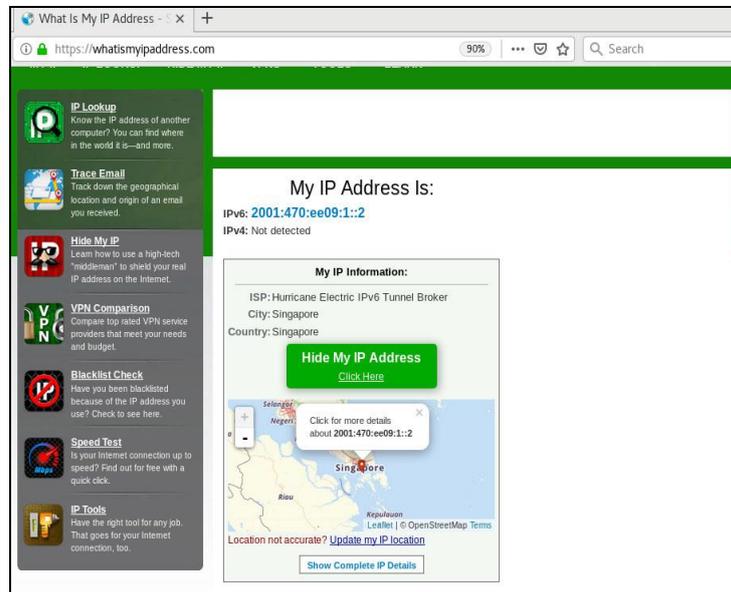
Desain topologi perancangan squid server monitoring pada IPv6 melalui teknik tunnelling menggunakan topologi Star (Topologi Bintang), topologi Star merupakan topologi jaringan komputer yang menghubungkan satu atau lebih komputer dengan control terpusat. Desain topologi squid server monitoring IPv6 tidak jauh beda dengan topologi yang menggunakan IPv4. Server tunnelling IPv6 pada penelitian ini adalah server Singapura. Singapura adalah salah satu Negara maju yang mengadopsi IPv6 di Dunia dibandingkan dengan Negara-negara lain yang masih menggunakan IPv4. Desain topologi jaringan squid server pada IPv6 dapat dilihat pada Gambar 3.1 Desain Topologi Squid Server Pada IPv6:



Gambar 3.1 Desain Topologi Squid Server Pada IPv6

3. HASIL DAN PEMBAHASAN

3.1 Hasil Tunneling IPv6 pada Server



Gambar 4.29 Alamat IP Public Server

Gambar 4.29 di atas adalah Hasil pengujian IP public yang berhasil ditunneling dari server singapura dengan mengecek di alamat link, <https://whatismyipaddress.com/>. ISP dari tunnel broker yaitu, Hurricane Electric IPv6 Tunnel Broker dan IP public server yang sedang terhubung ke internet yaitu, 2001:470:ee09:1::2, kemudian jika dilihat dari lokasi server yang terhubung ke komputer server berada di Singapura.

3.2 Hasil Networking Server dan Client

Pada ping antar server-client dan sebaliknya, serta melakukan uji koneksi internet apakah sudah berhasil terhubung atau tidak. Server akan ping IP address client yang terdiri dari 2 IP yakni, 2001:4860:ee09:2::2 (client1) dan 2001:470:ee09:2::3 (client 2) sedangkan IP Server yakni, 2001:470:ee09:2::1. Pengujian dapat dibuktikan dengan melihat hasil ping yang keluar, jika hasil ping muncul “reply....” Maka koneksi antara server dan client sudah terhubung, pada pengujian koneksi internet dapat dilakukan dengan ping IPv6 DNS google yaitu, 2001:4860:4860::8844. Jika hasil ping muncul “64 bytes from...” maka koneksi internet di komputer sudah terhubung. Adapun hasil pengujian networking server dan client sebagai berikut:

```

erwin@debian: ~
Berkas Sunting Tampilan Cari Terminal Bantuan
root@debian:/home/erwin# ping 2001:470:ee09:2::2
PING 2001:470:ee09:2::2(2001:470:ee09:2::2) 56 data bytes
64 bytes from 2001:470:ee09:2::2: icmp_seq=1 ttl=128 time=1.12 ms
64 bytes from 2001:470:ee09:2::2: icmp_seq=2 ttl=128 time=1.07 ms
64 bytes from 2001:470:ee09:2::2: icmp_seq=3 ttl=128 time=1.38 ms
64 bytes from 2001:470:ee09:2::2: icmp_seq=4 ttl=128 time=1.07 ms
64 bytes from 2001:470:ee09:2::2: icmp_seq=5 ttl=128 time=1.35 ms
^C
--- 2001:470:ee09:2::2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.074/1.203/1.383/0.140 ms
root@debian:/home/erwin#

```

Gambar 4.31 Ping IP Address Komputer Client-1

```

erwin@debian: ~
Berkas Sunting Tampilan Cari Terminal Bantuan
root@debian:/home/erwin# ping 2001:470:ee09:2::3
PING 2001:470:ee09:2::3(2001:470:ee09:2::3) 56 data bytes
64 bytes from 2001:470:ee09:2::3: icmp_seq=1 ttl=128 time=0.932 ms
64 bytes from 2001:470:ee09:2::3: icmp_seq=2 ttl=128 time=1.32 ms
64 bytes from 2001:470:ee09:2::3: icmp_seq=3 ttl=128 time=1.34 ms
64 bytes from 2001:470:ee09:2::3: icmp_seq=4 ttl=128 time=0.936 ms
^C
--- 2001:470:ee09:2::3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.932/1.133/1.347/0.204 ms
root@debian:/home/erwin#

```

Gambar 4.32 Ping IP Address Komputer Client-2

```

erwin@debian: ~
Berkas Sunting Tampilan Cari Terminal Bantuan
root@debian:/home/erwin# ping 2001:4860:4860::8844
PING 2001:4860:4860::8844(2001:4860:4860::8844) 56 data bytes
64 bytes from 2001:4860:4860::8844: icmp_seq=1 ttl=120 time=31.6 ms
64 bytes from 2001:4860:4860::8844: icmp_seq=2 ttl=120 time=39.3 ms
64 bytes from 2001:4860:4860::8844: icmp_seq=3 ttl=120 time=42.2 ms
64 bytes from 2001:4860:4860::8844: icmp_seq=4 ttl=120 time=27.9 ms
64 bytes from 2001:4860:4860::8844: icmp_seq=5 ttl=120 time=29.4 ms
^C
--- 2001:4860:4860::8844 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 27.990/34.141/42.233/5.626 ms
root@debian:/home/erwin#

```

Gambar 4.33 Ping IP DNS Google

3.1 Hasil Analisis Squid Server Monitoring

monitoring aktivitas client menggunakan aplikasi SARG dengan cara mengakses <localhost/squid-reports/> melalui web server. Hasil monitoring jaringan dapat dilihat pada Gambar 4.36:

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
2020Jul12-2020Jul12	Min 12 Jul 2020 04:21:37 WIB	2	27.31M	13.65M
2020Jul11-2020Jul12	Min 12 Jul 2020 02:38:20 WIB	4	191.51M	47.87M
2020Jul11-2020Jul11	Sab 11 Jul 2020 04:23:06 WIB	3	333.51K	111.17K
2020Jul07-2020Jul07	Sel 07 Jul 2020 03:29:18 WIB	2	11.13M	5.56M
2020Jul06-2020Jul06	Sen 06 Jul 2020 11:04:57 WIB	5	2.45M	491.72K
2020Jul01-2020Jul01	Rab 01 Jul 2020 07:39:40 WIB	1	84.10M	84.10M

Generated by sarg-2.3.10 Apr-12-2015 on Jul/12/2020 16:21

Gambar 4.36 Squid Access Reports IPv6

Pada Gambar di atas terlihat laporan harian aktivitas client mulai dari laporan: file cache, hari, tanggal, jumlah user, ukuran dan rata-rata bandwidth yang dipakai client selama 1 hari.

Jika ingin melihat aktivitas client pada tanggal tertentu, bisa dibuka dengan mengklik salah satu tanggal yang ada ditabel file/period. Contoh tanggal 07 Juli 2020 terdapat 2 user dengan yang mengakses situs pada hari tersebut. Laporan squid tanggal 07 Juli 2020 dapat dilihat pada gambar: sedangkan untuk menampilkan semua log situs web yang diakses oleh setiap user dapat ditampilkan dengan mengklik salah satu IP user. Laporan log akses situs web user dapat dilihat pada Gambar 4.38.

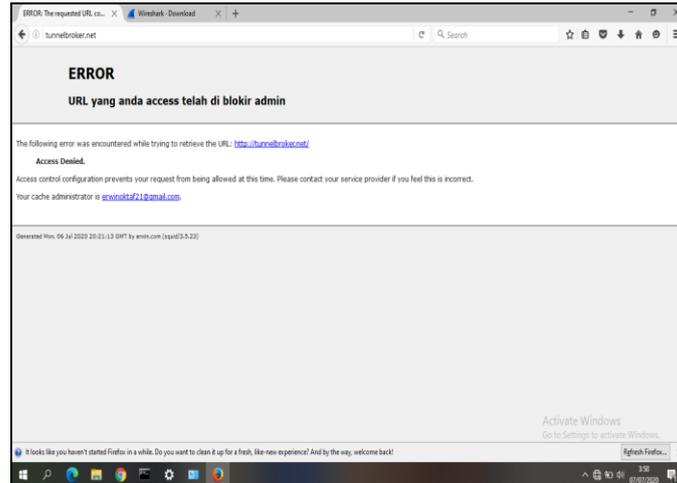
ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILLISEC	%TIME
www.speedtest.com.sg	26	10.89M	99.23%	0.00%	100.00%	00:01:08	68.381 12.43%
ds.download.windowsupdate.com	2	25.03K	0.23%	0.00%	100.00%	00:00:39	39.705 7.22%
r10--sn-3c27n7s.gvt1.com	3	16.91K	0.15%	0.00%	100.00%	00:00:41	41.026 7.46%
storage.googleapis.com	3	15.35K	0.14%	0.00%	100.00%	00:00:35	35.153 6.39%
r16--sn-3c27n7e.gvt1.com	3	15.01K	0.14%	0.00%	100.00%	00:00:36	36.148 6.57%
redirector.gvt1.com	6	6.27K	0.06%	0.00%	100.00%	00:01:13	73.194 13.30%
www.google.com	2	2.02K	0.02%	0.00%	100.00%	00:01:10	70.967 12.90%
gs.microsoft.com	2	1.00K	0.01%	0.00%	100.00%	00:01:12	72.834 13.24%
cr1pk1.goog	1	914	0.01%	0.00%	100.00%	00:00:39	39.205 7.12%
tunnelbroker.net	2	748	0.01%	100.00%	0.00%	00:00:38	38.131 6.93% DENIED
cdn1.windowsupdate.com	1	420	0.00%	0.00%	100.00%	00:00:35	35.503 6.45%
debian.org	1	374	0.00%	100.00%	0.00%	00:00:00	2 0.00% DENIED
TOTAL	52	10.98M	98.64%	0.01%	99.99%	00:09:10	550,249 49.74%
AVERAGE	0	5.56M				00:09:13	553,119 50.00%

Generated by sarg-2.3.10 Apr-12-2015 on Jul/07/2020 03:29

Gambar 4.1 Laporan Log Akses Situs Web User

3.4 Hasil Pemblokiran Situs

Pengujian pemblokiran situs squid server dapat di uji pada salah satu client dengan melakukan akses situs web ke tunnelbroker.net dan debian.org, sesuai perintah pemblokiran situs. Jika pemblokiran situs berhasil maka akan muncul tampilan error “url yang anda akses telah diakses oleh admin”, kode error pemblokiran dapat diubah kapan saja di server squid. Hasil pemblokiran situs dapat dilihat pada Gambar 4.39:



Gambar 4.2 Error Situs tunnelbroker.net

3.5 Pengujian Parameter QoS

Berdasarkan Tabel. Hasil pengukuran parameter QoS menurut standart THIPON di dapat hasil throughput 21,517 bps dengan kategori “sangat bagus” dan nilai indek 4. Delay 0,119 dengan kategori “sangat bagus” dan nilai indek 4. Jitter 0,303 dengan kategori “sangat bagus” dan nilai indek 4. Paket loss 0,012 dengan kategori “sangat bagus” dan nilai indek 4. Pengukuran QoS menurut THIPON dapat dilihat pada Tabel 4.3.

Tabel 4.3 Tabel Indeks QoS

No	Quality of Service (QoS)	Keterangan		
		Nilai	Indeks	Kategori
1	Troughput	21,517 bps	4	Sangat Bagus
2	Delay	118 ms	4	Sangat Bagus
3	Jitter	300 ms	1	Jelek
4	Packetloss	0,012 %	4	Sangat Bagus
Rata-Rata Indeks			3,25	Bagus

4. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan dapat diambil kesimpulan bahwa:

1. Pengukuran parameter QoS didapat hasil throughput 21,517 bps dengan kategori “sangat bagus”, delay 118 dengan kategori “sangat bagus”, jitter 300 dengan kategori “jelek” dan nilai indek 1, dan paket loss 0,012 dengan kategori “sangat bagus”
2. Hasil Pengukuran QoS dari implementasi squid server monitoring pada Ipv6 menggunakan metode AQM menurut standar THIPON didapat hasil indek 3,25 dengan kategori “bagus”.
3. Pada penelitian ini, peneliti telah mampu membangun squid server monitoring menggunakan IPv6 dengan metode AQM
4. Fasilitas cache dapat menyimpan akses dari internet ke dalam harddisk pada proxy server
5. Aplikasi monitoring dapat memberi fasilitas untuk pengadministrasian bagi admin jaringan.

5. SARAN

Dalam melaksanakan tugas akhir ini, penulis memberikan saran untuk perbaikan adalah dibuatkan perintah reload otomatis setelah penambahan data pada aplikasi monitoring melalui website, sehingga tidak direpotkan untuk reload secara manual melalui terminal.

DAFTAR PUSTAKA

- [1] Armadya. 2014. *Perancangan dan Penerapan Server Akses Monitoring Menggunakan Linux Ubuntu Pada SMA Negeri 1 Pemali*. Pangkalpinang: sekolah tinggi Manajemen Informatika dan Komputer.
- [2] Arjuni, S. 2012. *Perancangan Dan Implemtasi Proxy Server Dan Manajemen Bandwidth Menggunakan Linux Ubuntu Server (Studi Kasus di Kantor Manajemen PT. Wisma Bumiputera Bandung*. Polytechnic TELKOM.
- [3] Gumilang, A.C. 2017. *Analisis Perbandingan Unjuk Kerja Congestion Control TCP TAHOE dan TCP NEWRENO pada Antrian Random Early Detecetion dan Drop Tail*. Skripsi: Sains dan Teknologi Jurusan Teknik Informatika Universitas Sanata Dharma, Yogyakarta.
- [4] Khilmy,Zulfa. 2013. *Wireshark*.<https://www.kompasiana.com/ikujuki/552fa1f86ea83403048b45b1/pengenalan-wireshark>. Diakses tanggal 30 Juli 2020.
- [5] Noer, Muhamad, I. 2017. *Analisis Active Queue Management (AQM) Berbasis Algoritma Control Delay (CoDel) pada Streaming User Datagram Protocol (UDP)*. Bandung: Universitas Telkom
- [6] Pamungkas, G. W., Yahya, W., & Nurwarsito, H. 2018. *Analisis Perbandingan Kinerja TCP Vegas Dan TCP New Reno Menggunakan Antrian Random Early Detection Dan Droptail*. 2(10), 3239–3248
- [7] Pamungkas, S. W., & Pramono, E. 2018. *Analisis Quality of Service (QoS) Pada Jaringan Hotspot SMA Negeri XYZ"*. 7(2), 142–152.
- [8] Ulansari, Ramadhani. 2017. *Analisis Simulasi Perbandingan Antrean FIFO dan RED Dengan Menggunakan Network Simulator 2 (Ns2)*. Jurnal: Universitas Respati Indonesia Jurusan Teknik Informatika.
- [9] Usman. 2020. *SARG Squid Analysis Report Generator*. <https://www.opinikoe.id/sarg-squid-analysis-report-generator/>. Diakses tanggal 30 Juli 2020.