TESIS TE-142599

ANALISIS PERFORMANSI INTRUSION DETECTION SYSTEM, FIREWALL, HONEYPOT DAN LOAD BALANCER DALAM RANGKA MITIGASI SERANGAN DOS DAN DDOS PADA LPSE KAB. LUWU TIMUR

SALMAN AKBAR
2214206711

DOSEN PEMBIMBING
Dr.Ir. Endroyono, DEA.
Dr.Adhi Dharma Wibawa S.T., M.T.

PROGRAM MAGISTER
BIDANG KEAHLIAN TELEMATIKA
KONSENTRASI CHIEF INFORMATION OFFICER
JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2016

TESIS TE-142599

PERFORMANCE ANALYSIS OF INTRUSION DETECTION SYSTEM, FIREWALL, HONEYPOT AND LOAD BALANCER TO MITIGATE DOS AND DDOS ATTACK ON THE LPSE OF LUWU TIMUR REGENCY

SALMAN AKBAR
2214206711

SUPERVISOR
Dr.Ir. Endroyono, DEA.
Dr.Adhi Dharma Wibawa S.T., M.T.

MAGISTER PROGRAM
FIELD OF STUDY TELEMATICS
CONCENTRATION CHIEF INFORMATION OFFICER
MAJOR ELECTRICAL ENGINEERING
FACULTY OF INDUSTRIAL TECHNOLOGY
INSTITUTE OF TECHNOLOGY SEPULUH NOPEMBER
SURABAYA
2016

Tesis telah disusun untuk memenuhi salah satu syarat memperoleh gelar

Magister Teknik (MT)

Di
Institut Teknologi Sepuluh Nopember

Oleh : Salman Akbar
NRP : 2214206711

Tanggal Ujian : 23 Juni 2016
Periode Wisuda : September 2016

Disetujui oleh:

1. **Dr. Ir. Endroyono, DEA** **(Pembimbing I)**
   NIP. 19650404 199102 1 001

2. **Dr. Adhi Dharma Wibawa, ST., MT.** **(Pembimbing II)**
   NIP. 19760505 200812 1 003

3. **Dr. Ir. Achmad Affandi, DEA** **(Penguji)**
   NIP. 19651014 199002 1 001

4. **Dr. Surya Sumpeno, ST., M.Sc.** **(Penguji)**
   NIP. 19690613 199702 1 003

5. **Eko Setijadi, ST., MT., Ph.D.** **(Penguji)**
   NIP. 19721001 200312 1 002

Direktur Program Pasca Sarjana,

KEMENTERIAN RISET, TEKNOLOGI DAN PENDIDIKAN TINGGI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
PROGRAM PASCASARJANA

Prof. Ir. Djauhar Manfaat. M.Sc, Ph.D.
NIP. 19601202 198701 1 001

ANALISIS PERFORMANSI INTRUSION DETECTION SYSTEM, FIREWALL, HONEYPOT DAN LOAD BALANCER DALAM RANGKA MITIGASI SERANGAN DOS DAN DDOS PADA LPSE KAB. LUWU TIMUR

Nama	: Salman Akbar
NRP	: 2214206711
Pembimbing 1	: Dr. Ir. Endroyono, DEA
Pembimbing 2	: Dr. Adhi Dharma Wibawa, ST., MT.

ABSTRAK

Internet dewasa ini telah menjadi hal yang penting bagi masyarakat, Internet telah mengubah cara berkomunikasi dan model bisnis, Layanan Pengadaan Secara Elektronik pemerintah yang biasa disebut (LPSE) telah menjadi bagian yang sangat penting bagi instansi pemerintahan pusat dan daerah. LPSE bagi Pemerintah Daerah dapat disebut sebagai salah satu aset yang sangat penting dalam proses pembangunan daerah. Sebagai salah satu aset penting, LPSE harus dilindungi untuk menjamin kelangsungan layanan dan untuk meminimalkan risiko gangguan layanan. Semakin canggih teknologi dan sistem informasi maka ancamannya pun akan menjadi lebih canggih. Serangan DDoS adalah salah satu ancaman yang paling banyak mengancam layanan pengadaan pemerintah. Berdasarkan Laporan Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center (ID-SIRTII/CC) Tahun 2014, pada infrastruktur internet di Indonesia terdapat 40.446 Total Serangan DoS Januari sampai dengan pertengahan Desember 2014. Dalam penelitian ini, penulis mengevaluasi dampak dari serangan DDoS pada infrastruktur jaringan exisiting LPSE Kab. Luwu Timur, juga mengevaluasi mekanisme pertahanan pada jaringan existing seperti *firewall, router* dan *web server*. Penulis juga membandingkan implementasi *Intrusion Detection System, Firewall Server Based, Honeypot Server* dan *Load Balancer* dalam jaringan untuk memitigasi serangan DoS dan DDoS. Selama serangan *UDP Flood* berlangsung pada infrastruktur jaringan Existing hasil penelitian menunjukkan penggunaan *CPU Firewall* mencapai 100% dan pada 500 request ke web server LPSE hanya 30 request yang dapat diproses. Dibandingkan dengan topologi jaringan yang menggunakan *IDS, Firewall Server Based* dan *Honeypot* yang menunjukkan bahwa pada 500 request yang ditujukan ke web Server LPSE terdapat 499 request yang dapat direspon dan penggunaan *CPU firewall* hanya mencapai 15,79 %. Selanjutnya pada topologi jaringan yang menggunakan *IDS, Firewall* dan *Load Balancer*, penggunaan *CPU firewall* hanya 15,70 % namun pada 500 request yang ditujukan ke web Server LPSE hanya terdapat 41 request yang dapat direspon.

Kata Kunci : DDoS, LPSE, IDS, Firewall, Honeypot, Load Balancer.

PERFORMANCE ANALYSIS OF INTRUSION DETECTION SYSTEM, FIREWALL, HONEYPOT AND LOAD BALANCER TO MITIGATE DOS AND DDOS ATTACK ON THE LPSE OF LUWU TIMUR REGENCY

Name : Salman Akbar
NRP : 2214206711
Advisor : Dr. Ir. Endroyono, DEA
: Dr. Adhi Dharma Wibawa, S.T., M.T.

ABSTRACT

The Internet nowadays has become important to current society, it has changed the way of communication and business models, The Electronic Procurement Services to government agencies which is called Layanan Pengadaan Secara Elektronik (LPSE) has become a very important part for central and local government agencies. LPSE for an agency can be termed as one of the most important assets in the process of regional development. As one of the important assets, LPSE must be protected to ensure continuity of services as well as to minimize the risk of service interruption. With the increase of sophisticated information systems and technology, the threat will also become more sophisticated. DDoS attack are one of the most threat to the government procurement services. Based on the Report of Indonesia Security Incident Response Team on Internet and Infrastructure/ Coordination Center (ID-SIRTII / CC) In 2014, there were 40.446 Total DoS attacks at the Indonesian Internet infrastructure from January to mid December 2014. In this research, author evaluated the impact of DDoS attacks on the existing network infrastructure of government procurement service and also evaluates the existing network defense mechanisms such *firewall, router* and *web server*. Author also compared the implementation of *Intrusion Detection system*, *firewall server based*, *honeypot* and *load balancer* in the network to mitigate DoS and DDoS Attack. During *UDP Flood* the results showed that on the existing network infrastructure, *CPU usage* of *integrated firewall* reaching 100 % and at 500 requests to the LPSE web server, there were only 30 requests that could be processed. Comparing to network topology using *IDS, Firewall Server Based* and *Honeypot*, showed only 15,79 % of *CPU usage* of *Firewall* and at 500 requests to the LPSE web server, there were 499 requests that could be responded. Furthermore, the *network topology* using *IDS, Firewall Server Based* and *Load Balancer* showed only 15,70 % *CPU usage* of *Firewall* but at 500 request to LPSE web server there were only 41 requests that could be processed .

Keywords **:** DDoS, LPSE, IDS, Firewall, Honeypot, Load Balancer.

DAFTAR ISI

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dengan diterapkannya Layanan Pengadaan Secara Elektronik (LPSE) secara Nasional oleh Lembaga Kebijakan Pengadaan Barang Dan Jasa Pemerintah (LKPP) RI untuk kegiatan pengadaan barang dan jasa dilingkup instansi pemerintahan, serta terbitnya Peraturan Presiden Nomor 4 Tahun 2015 pasal 106 ayat 1 (satu) yang menyebutkan "Pengadaan Barang/Jasa Pemerintah dilakukan secara elektronik" dengan demikian maka setiap Kementerian/Lembaga/Daerah/Instansi (K/L/D/I) secara aturan wajib mengimplementasikan Sistem Pengadaan Secara Elektronik, tidak terkecuali pada Pemerintahan Kabupaten Luwu Timur. Mengingat bahwa progress percepatan pembangunan daerah sangat tergantung pada efisiensi proses pelelangan barang dan jasa, maka kegiatan ini sangat vital bagi daerah.

Penerapan tata kelola keamanan informasi merupakan sebuah kebutuhan dan tuntutan untuk layanan pemerintah kepada publik yang mencerminkan tata kelola pemerintahan yang baik yang membantu pencapaian proses bisnis didalamnya, hal ini tertuang dalam Undang-undang No. 11 Tahun 2008 Pasal 15 ayat 1 "Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya"[1] dan Peraturan Pemerintah No. 82 Tahun 2012 pasal 14 ayat 1 "Penyelenggara Sistem Elektronik wajib memiliki kebijakan tata kelola, prosedur kerja pengoperasian, dan mekanisme audit yang dilakukan berkala terhadap Sistem Elektronik."[2]

Namun demikian masih banyak instansi pemerintah yang memiliki nilai kurang dalam indeks keamanan informasi dan penerapan keamanan informasi, kurang mengedepankan kajian resiko karena lebih mengedepankan implementasi teknologi serta tidak aware terhadap keamanan informasi

khususnya bagi instansi dan atau lembaga yang mengelola Teknologi Informasi dan Komunikasi.

Berdasarkan Laporan Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center (Id-SIRTII/CC) Tahun 2014 pada infrastruktur internet di Indonesia yaitu terdapat 40.446 Total Serangan DoS Januari sampai dengan pertengahan Desember 2014, memiliki rata-rata tingkat keseriusan 78% (High) [3], tidak terkecuali pada LPSE Kab. Luwu Timur dimana dalam kurun waktu 4 Tahun terakhir telah mengalami beberapa kali insiden keamanan informasi yang dicurigai merupakan serangan DoS dan DDoS yang tidak jarang mengakibatkan terhentinya layanan e-procurement pada pemerintah Kabupaten Luwu Timur dan berakibat tertundanya kemajuan pelaksanaan kegiatan penyelenggaraan pemerintahan dan pembangunan daerah pada waktu-waktu tersebut [4].

Dalam Implementasi SPSE, LPSE Kab. Luwu Timur berjalan diatas infrastruktur IT yang dikelola secara mandiri dan tidak memiliki sistem mitigasi DoS dan DDoS sehingga rentan terhadap serangan DoS dan DDoS. Dengan berbagai motif dan kepentingan, tidak jarang LPSE menjadi target serangan dan mengakibatkan operasional layanan LPSE terhenti.

Oleh karena itu diperlukan adanya evaluasi dan sistem mitigasi terhadap ancaman serangan yang dapat mengakibatkan terhentinya layanan LPSE khususnya jenis serangan Denial Of Service (DoS) dan Distributed Denial Of Service (DDoS).

1.2 Rumusan Masalah

Berdasarkan Laporan Evaluasi LPSE Kab. Luwu Timur dalam kurun waktu 4 Tahun terakhir pada infrastruktur jaringan LPSE Kab. Luwu Timur telah mengalami sedikitnya 32 kali insiden keamanan informasi yang merupakan serangan DoS dan DDoS yang tidak jarang mengakibatkan terhentinya layanan e-procurement pada pemerintah Kabupaten Luwu Timur dan mengakibatkan

tertundanya kemajuan pelaksanaan kegiatan penyelenggaraan pemerintahan dan pembangunan daerah pada waktu-waktu tersebut.[4]

Serangan DoS dan DDoS tersebut mengakibatkan pengguna tidak dapat mengakses Web Server LPSE dan perangkat-perangkat lain yang berada dalam jaringan LPSE tidak dapat terkoneksi ke internet dikarenakan resource perangkat pada jaringan LPSE telah dipenuhi paket-paket yang berasal dari serangan DoS dan DDoS. Oleh karena itu kami merumuskan belum terdapat strategi mitigasi yang mumpuni disiapkan oleh pihak pengelola LPSE Kab. Luwu Timur untuk menghadapi serangan Dos dan DDoS.

1.3 Batasan Masalah/Ruang Lingkup

Pada penelitian ini akan di uji coba mensimulasikan serangan DoS dan DDoS dengan Jenis UDP Flood dan TCP Flood, dan menggunakan Intrusion Detection System, Honeypot yang bersifat Open Source dan Load Balancer untuk mengurangi downtime Web Server LPSE akibat dampak serangan Dos dan DDoS.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk mengidentifikasi dan memitigasi serangan DoS dan DDoS dengan penerapan IDS, Firewall Server Based, Honeypot dan Load Balancer sebagai bentuk penanganan dan mitigasi terhadap serangan DoS dan DDoS pada Infrastruktur LPSE Kab. Luwu Timur. Penelitian ini juga dilakukan dalam rangka mengurangi resiko downtime akibat serangan Dos dan DDoS terhadap Infrastruktur serta menjaga kualitas ketersediaan layanan Jaringan LPSE Kab. Luwu Timur.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah dengan dilakukannya uji coba serangan DoS dan DDoS pengelola LPSE dapat mengidentifikasi dan mengetahui kerentanan keamanan informasi akibat serangan DoS dan DDoS serta meningkatkan

perlindungan terhadap infrastruktur Jaringan dan Sistem Informasi LPSE Kab. Luwu Timur dengan penerapan IDS dan Load Balancer untuk mitigasinya. Selain hal tersebut penelitian ini dapat memberikan kontribusi berupa rekomendasi perbaikan dan mitigasi serangan DoS dan DDoS untuk meningkatkan ketersediaan akses jaringan LPSE, dengan demikian pihak pemangku kepentingan LPSE dapat mengambil kebijakan dalam rangka melakukan evaluasi, perbaikan dan peningkatan layanan LPSE di seluruh Indonesia.

BAB II
LANDASAN TEORI

2.1 Intrusion Detection System (IDS)

Intrusion Detection System adalah sistem yang dirancang untuk membantu mempersiapkan dan menghadapi serangan dengan mengumpulkan informasi dari berbagai sumber dalam suatu sistem dan jaringan dan kemudian menganalisa informasi tersebut untuk mendefinisikan berbagai kemungkinan masalah keamanan informasi berdasarkan informasi tersebut.[13]

Intrusion Detection System menyediakan fasilitas sebagai berikut :

- Pemantauan dan analisis pengguna dan aktivitas sistem
- Audit konfigurasi sistem dan kerentanan
- Penilaian integritas pada sistem yang kritikal/penting dan data file
- Analisis statistik dari pola aktivitas berdasarkan pencocokan terhadap serangan yang diketahui
- Analisis aktivitas abnormal
- Audit sistem operasi

Dalam Intrusion Detection System Terdapat tiga komponen utama yaitu :

1. Network Intrusion Detection system (NIDS) - aktivitas analisis untuk data yang melewati sebuah lalu lintas pada seluruh subnet dalam jaringan. Bekerja dalam mode promiscuous, dan mencocokan lalu lintas yang telah lewat pada subnet dengan libbrary jenis serangan. Setelah serangan itu diidentifikasi, atau perilaku abnormal dirasakan, IDS akan mengirim peringatan ke administrator.

2. Network Node Intrusion Detection system (NNIDS) – aktivitas analisis lalu lintas data yang melewati jaringan ke host tertentu. Perbedaan antara NIDS dan NNIDS adalah bahwa lalu lintas yang dipantau pada host tunggal saja dan tidak untuk seluruh subnet. Contoh NNIDS akan, menginstal pada

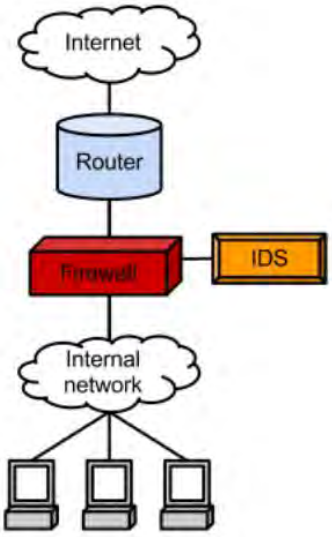
perangkat VPN, untuk memeriksa lalu lintas setelah itu didekripsi. Dengan cara ini Anda dapat melihat apakah seseorang mencoba masuk ke perangkat VPN Anda Layanan Pengadaan Secara Elektronik.

3. Host Intrusion Detection System (HIDS) – mengcapture file dari sistem yang ada dan dan mencocokannya ke file system sebelumnya. Jika file sistem penting yang dimodifikasi atau dihapus, peringatan tersebut dikirim ke administrator untuk diselidiki. Contoh dari HIDS dapat dilihat pada Device kritikal/penting, yang tidak diharapkan mengubah konfigurasi mereka.

Pada berbagai penelitian sebelumnya tentang implementasi IDS, solusi open source telah banyak digunakan di seluruh dunia, dan beberapa dari software IDS open source yang masih aktif dikembangkan dan cukup populer sampai dengan saat ini antara lain adalah [14] :

- Snort
  Snort adalah sebuah IDS open-source yang dikembangkan oleh Sourcefire. Snort diciptakan pada tahun 1998 oleh Martin Roesch. Snort mampu melakukan analisis lalu lintas real-time dan paket logging pada jaringan IP. Snort kompatibel dengan sebagian besar sistem operasi (misalnya Linux, Mac OS X, FreeBSD, OpenBSD, UNIX dan Windows).
- Suricata
  The Suricata adalah mesin IDS open source yang cukup baru dirilis versi beta 1 Januari 2010, dikembangkan oleh Open Information Security Foundation (OISF), yang merupakan yayasan non-profit didukung oleh US Department of Homeland Security (DHS) dan sejumlah perusahaan swasta. Suricata kompatibel dengan sebagian besar sistem operasi (misalnya Linux, Mac, FreeBSD, UNIX dan Windows).
- Bro
  Bro IDS berfokus pada keamanan jaringan, tetapi juga menyediakan platform yang komprehensif untuk analisis yang lebih dalam pada lalu

lintas jaringan umum. Bro telah dikembangkan lebih dari 15 tahun. Bro diciptakan oleh Vern Paxson, yang masih memimpin proyek bersama-sama dengan tim peneliti dan pengembang di Komputer Internasional Science Institute (ICSI) di Berkeley dan Pusat Nasional Aplikasi untuk Supercomputing di Urbana-Champaign. Bro juga kompatibel dengan sebagian besar sistem operasi (misalnya Linux, Mac, FreeBSD, UNIX).



Gambar 2.1 Contoh Penempatan IDS pada Jaringan [14]

2.2 Honeypot

Sebuah Honeypot didefinisikan sebagai server yang terpasang di Internet yang bertindak sebagai umpan, untuk mengelabui kegiatan hacking untuk mempelajari kegiatan mereka dan memantau bagaimana mereka dapat masuk ke sebuah system.

Berdasarkan aktivitas interaksinya Honeypots dapat diklasifikan sebagai berikut[15] :

- Low-Interaction

  Pada honeypots Low Interactions, alat dipasang meniru sistem operasi dan layanan dan kemudian berinteraksi dengan penyerang dengan kode berbahaya. Selain itu, jenis honeypot ini memiliki resiko kecil untuk terganggu dan ideal untuk jaringan. Honeypots bekerja sepenuhnya

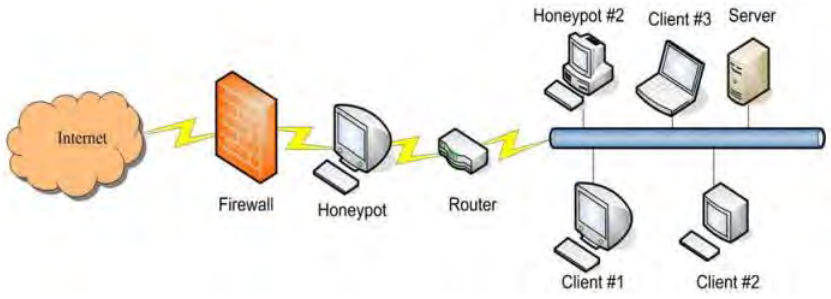
meniru sistem operasi dan layanan. Kegiatan Penyerang terbatas pada honeypot dan kualitas emulasi honeypot.

- High-Interaction

  Dalam klasifikasi Honeypot tingkat interaksi paling maju dan final dari honeypots adalah jenis honeypots High Interaction. Jenis honeypot ini benar-benar memakan waktu untuk dirancang, oleh karena itu sulit untuk mengelola dan memeliharanya. honeypot ini memiliki lebih banyak risiko dan kompleksitas karena melibatkan sistem operasi yang nyata dengan aplikasi nyata namun demikian informasi dan bukti terkumpul untuk analisis juga melimpah dan manfaatnya juga semakin meningkat.

- Medium-interaction

  Honeypot jenis ini merupakan tipe dari honeypot yang menggabungkan manfaat dari kedua pendekatan yaitu high interaction dan medium interaction, Honeypots ini sedikit lebih maju dari honeypots low interaction, tetapi sedikit kurang rumit dari honeypots high interaction. Pada honeypot ini Tidak ada operasi yang nyata disediakan sistem selain virtualisasi lapisan aplikasi. jenis honeypots Ini tidak bertujuan sepenuhnya untuk simulasi, lingkungan sistem beroperasi penuh, juga tidak menerapkan semua rincian protokol aplikasi, jenis honeypots ini tidak memberikan respon yang memadai untuk exploit yang diketahui menunggu pada port tertentu yang akan mengelabui dengan mengirimkan payload penyerang [16].



Gambar 2.2 Contoh Penempatan Honeypot pada Jaringan [14]

2.3 Load Balancer

Load Balancer adalah sebuah perangkat yang mendsitribusikan jaringan dan atau lalu lintas aplikasi pada sejumlah server, load balancer digunakan untuk meningkatkan (concurrent user) pengguna dalam waktu yang bersamaan dan realibility aplikasi, perangkat ini meningkatkan kinerja aplikasi dengan mengurangi beban pada server.[14]

Secara umum Load Balancer terbagi menjadi dua kategori yaitu :

1. Layer 4

   Load balancer ini mendistribusikan permintaan berdasarkan data yang ditemukan dalam jaringan dan transportasi protokol lapisan (IP, TCP, FTP, UDP).

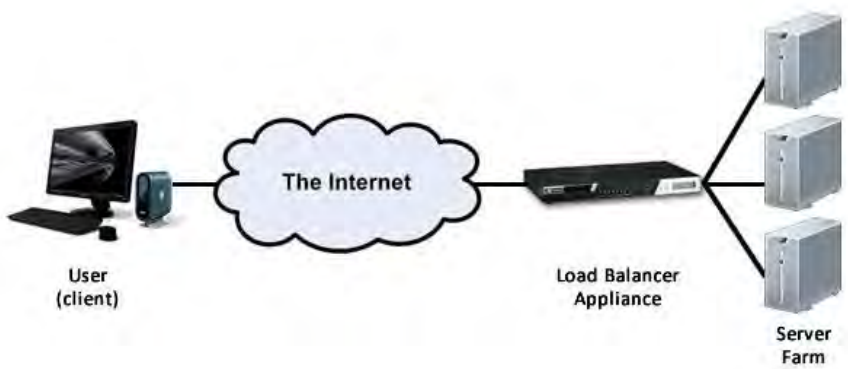
2. Layer 7

   Load balancer ini Mendistribusikan permintaan berdasarkan data yang ditemukan pada Aplication Layer Protocol seperti HTTP.

Requests yang diterima oleh kedua jenis load balancer ini didistribusikan ke server-server tertentu berdasarkan algoritma yang telah dikonfigurasi. algoritma industri standar tersebut adalah:

- Round robin
- Weighted round robin
- Least connections
- Least response time

Load balancer memastikan keandalan dan ketersediaan dengan memantau "kesehatan" dari aplikasi dan hanya mengirim permintaan ke server dan aplikasi yang dapat merespon secara tepat waktu.

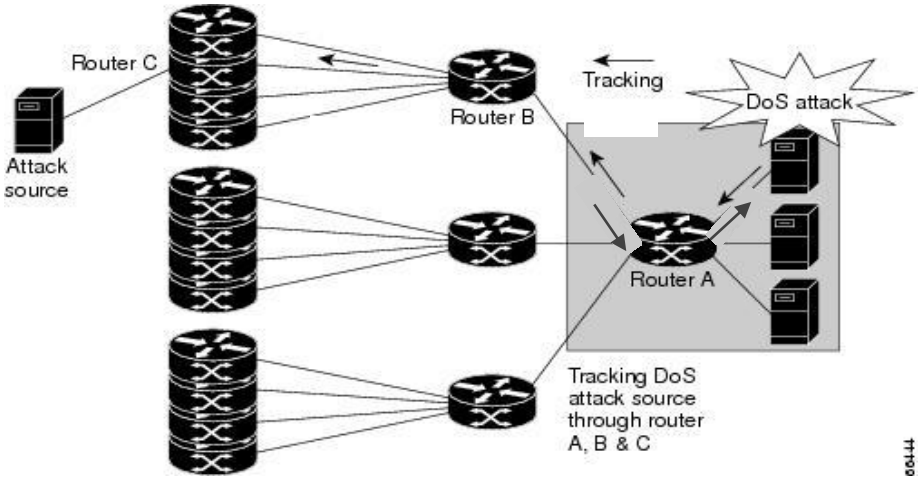


Gambar 2.3 Contoh Penempatan Load Balancer pada Jaringan
(sumber cloudleverage.com)

2.4 DoS – Denial of Service Attack

Serangan DoS adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut [10]. Dalam sebuah serangan Denial of Service, si penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap sistem atau jaringan dengan menggunakan beberapa cara, yakni sebagai berikut:

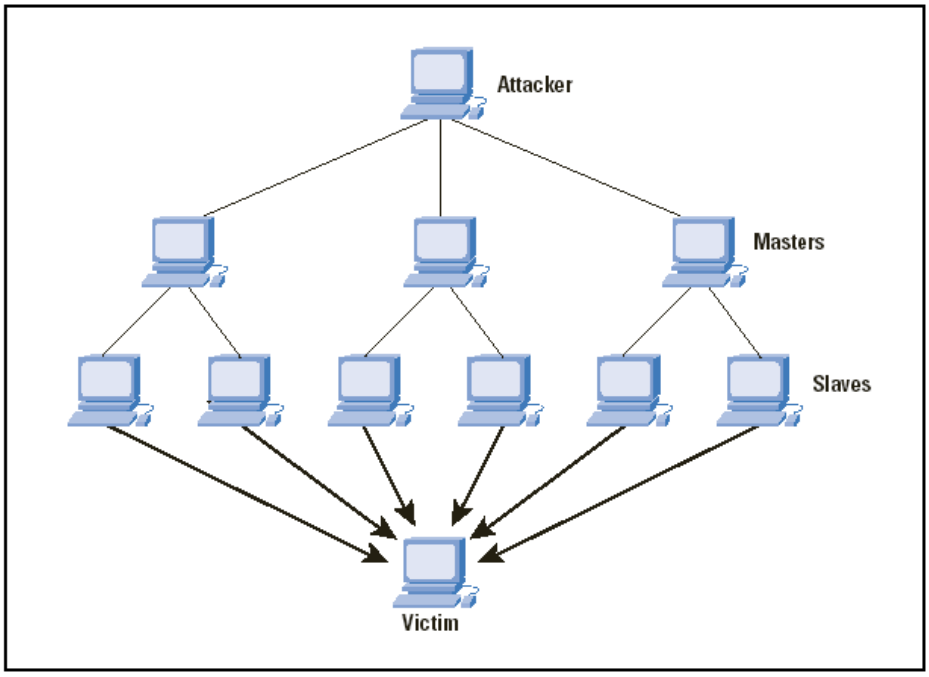
- Membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Teknik ini disebut sebagai traffic flooding.
- Membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disediakan oleh sebuah host sehingga request yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini disebut sebagai request flooding.
- Mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan server.



Gambar 2.4 Serangan DoS (www.cisco.com)

2.5 DDoS – Distributed Denial of Service Attack

Serangan DDoS adalah jenis serangan DoS terhadap sebuah komputer atau server di dalam Serangan DoS dengan upaya untuk menguras sumber daya korban secara terdistribusi. Sumber daya ini dapat berupa bandwidth jaringan, daya komputasi, atau struktur data sistem operasi. Untuk menjalankan serangan DDoS pengguna membangun jaringan komputer yang akan mereka gunakan untuk menghasilkan volume lalu lintas yang diperlukan untuk melakukan serangan DDoS kepada pengguna komputer. Untuk membuat serangan ini, penyerang mencari situs rentan atau host pada jaringan, host yang rentan biasanya tidak menjalankan perangkat lunak antivirus atau out-of-date, atau terdapat kerentanan yang belum ditambal dengan benar, host tersebut kemudian dieksploitasi oleh penyerang yang menggunakan kerentanan mereka untuk mendapatkan akses ke host ini. Langkah berikutnya untuk penyerang adalah dengan menginstal program baru (dikenal sebagai alat serangan) pada beberapa host tersebut. Host yang menjalankan alat serangan ini dikenal sebagai zombie, dan mereka dapat melakukan serangan di bawah kendali penyerang. Banyak zombie bersama-sama membentuk apa yang disebut *Army.[11]*



Gambar 2.5 Serangan DDoS (www.cisco.com)

Jenis serangan DDoS

Secara umum Serangan DDoS dapat dibagi menjadi 3 (tiga) kategori[11] yaitu :

1. Volume Based Attacks yaitu jenis serangan yang bertujuan menghabiskan resource bandwith target/korban, dengan cara membanjiri target dengan paket-paket seperti ICMP floods, UDP floods and other spoofed packet attacks. Besarnya serangan diukur dalam bits per second's (bps).
2. Protocol Based Attacks yaitu jenis serangan yang Tujuan utama dari penyerangnya adalah untuk mengkonsumsi sumber daya server yang sebenarnya seperti perangkat firewall. Contoh aplikasi yang digunakan yaitu SYN floods, fragmented packet attacks, Ping of death, Smurf attack dan lain-lain. Besarnya serangan diukur dalam Packet per second's (pps)
3. Application Layer Based Attacks yaitu jenis serangan yang Tujuan utama dari penyerangnya adalah untuk mencari dan memanfaatkan celah kerentanan sistem seperti Apache, Windows dan Open BSD dan lainnya. Contoh serangan yaitu Zero-day attack, Slowloris dan lain-lain.

2.6 Jaringan Komputer

Jaringan Komputer adalah dua atau lebih komputer yang terhubung dengan kabel atau dengan koneksi radio nirkabel sehingga mereka dapat saling bertukar informasi. Jaringan komputer sederhana dapat dibangun dengan mengaitkan komputer-komputer dengan kabel dan menggunakan antarmuka jaringan komputer. Jaringan memungkinkan berbagai pihak untuk berbagi informasi dengan komputer lain pada jaringan tergantung pada bagaimana pengaturan pada jaringan tersebut. Dalam kasus yang sederhana , beberapa pihak dapat berbagi file dengan pihak lainnya yang terhubung dalam satu jaringan .Dengan cara yang berbeda , dapat mengirim file dari satu komputer secara langsung ke komputer lain dengan melampirkan file ke e-mail pesan , atau dengan

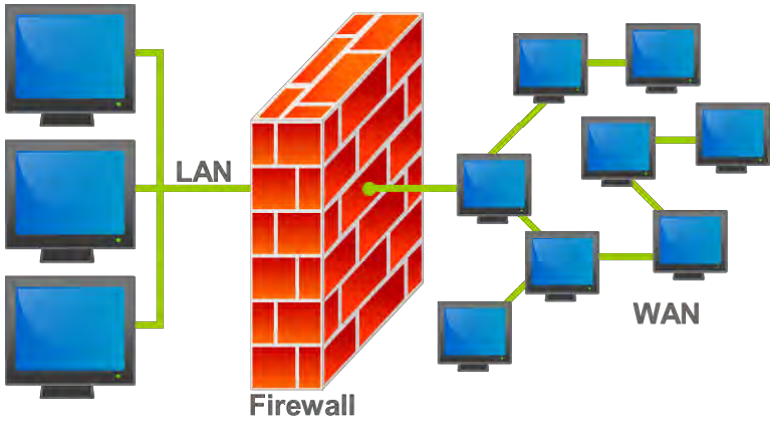
membiarkan pihak lain dapat mengakses komputer melalui jaringan sehingga pihak tersebut dapat mengambil file langsung dari storage. Jaringan komputer yang berisi storage, printer, dan sumber lainnya yang dibagi dengan komputer jaringan lain disebut server. Hanya dua jenis komputer di jaringan: server dan klien. Dalam beberapa jaringan, komputer server adalah sebuah komputer server dan tidak ada yang lain. Ini didedikasikan untuk tugas tunggal menyediakan sumber daya bersama, seperti hard drive dan printer, untuk diakses oleh komputer klien jaringan. Beberapa jaringan yang lebih kecil mengambil pendekatan alternatif dengan memungkinkan komputer pada jaringan berfungsi baik sebagai klien dan server. Dengan demikian, setiap komputer dapat berbagi sumber dengan komputer lain pada jaringan.Sementara ketika komputer bekerja sebagai server, komputer yang sama masih bisa digunakan untuk fungsi-fungsi lainnya [7].

Gambar 2.6 Jaringan Komputer (www.itdirec.com)

2.7 Firewall

Firewall merupakan alat untuk mengimplementasikan kebijakan security (security policy). Sedangkan kebijakan security, dibuat berdasarkan perimbangan antara fasilitas yang disediakan dengan implikasi security-nya. Semakin ketat kebijakan security, semakin kompleks konfigurasi layanan informasi atau semakin sedikit fasilitas yang tersedia di jaringan. Sebaliknya, dengan semakin banyak fasilitas yang tersedia atau sedemikian sederhananya konfigurasi yang diterapkan, maka semakin mudah orang orang 'usil' dari luar

masuk kedalam sistem (akibat langsung dari lemahnya kebijakan security). Dalam terminologi internet, istilah "firewall" didefinisikan sebagai sebuah titik diantara dua/lebih jaringan dimana semua lalu lintas (trafik) harus melaluinya (chooke point); trafik dapat dikendalikan oleh dan diautentifikasi melalui sautu perangkat, dan seluruh trafik selalu dalam kondisi tercatat (logged). Dengan kata lain, "firewall adalah penghalang (barrier) antara 'kita' dan 'mereka' dengan nilai yang diatur (arbitrary) pada 'mereka'[8].



Gambar 2.7 Firewall (en.wikipedia.org)

1. Fungsi Dasar Firewall

Ketika traffic sampai di firewall, firewall akan memutuskan traffic mana yang diijinkan dan mana yang tidak, berdasarkan pada aturan yang telah didefinisikan sebelumnya. Adapun fungsi dasar dari suatu firewall adalah :

- Mengatur dan mengontrol traffic jaringan
- Melakukan autentifikasi terhadap akses
- Melindungi sumber daya dalam jaringan privat
- Mencatat semua kejadian dan melaporkan kepada administrator

Selain itu, ada pula fungsi lain dari firewall yaitu :

1. Packet Filtering

Seluruh header dari paket data yang melewati firewall akan diperiksa, kemudian firewall akan membuat keputusan apakah paket tersebut diizinkan masuk atau harus diblok.

2. Network Address Translation (NAT)

   Dunia luar hanya akan melihat satu alamat IP dibalik firewall, sedangkan komputer-komputer di jaringan internal dapat menggunakan alamat IP apapun yang diperbolehkan di jaringan internal, alamat sumber dan tujuan dari paket yang melalui jaringan secara otomatis diubah (diarahkan) ke komputer tujuan (client misalnya) yang ada di jaringan internal oleh firewall.

3. Application Proxy

   Firewall mampu memeriksa lebih dari sekedar header suatu paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protocol aplikasi tertentu yang spesifik.

4. Pemantauan dan pencatatan traffic

   Pemantauan dan pencatatan traffic bisa membantu kita untuk memperkirakan kemungkinan penjebolan keamanan atau memberikan umpan balik yang berguna tentang kinerja firewall.

2. Klasifikasi Firewall

Fungsi dasar firewall adalah untuk melindungi komputer internal dari dunia luar. Firewall tersedia dalam berbagai ukuran dan rasa, seperti misalnya sistem yang didesain khusus atau merupakan perangkat yang berada diantara dua jaringan yang berfungsi memisahkan jaringan internal dan external[9].

Firewall diklasifikasikan dalam dua jenis umum yaitu :

1. Desktop atau Personal Firewall
2. Network Firewall

Perbedaan utama antara kedua jenis adalah kapasitas jumlah host yang dapat dilindungi. Firewall ini tersedia dalam bentuk perangkat lunak, Perangkat Keras dan *Integrated Firewall.*

a. Desktop Atau Personal Firewall

Personal Firewall dirancang untuk melindungi satu komputer dari akses yang tidak sah dan serangan eksternal, firewall ini hanya melindungi host di mana ia terinstal. Saat ini firewall pribadi hari telah terintegrasi dengan kemampuan tambahan seperti pemantauan perangkat lunak antivirus, analisis perilaku dan *intrusion detection* untuk meningkatkan perlindungan perangkat. Firewall ini umumnya digunakan di pasar SOHO (Small Office And Home Office) dan pengguna rumahan karena memberikan perlindungan akhir kepada pengguna dan kontrol kebijakan kontrol akses. Beberapa firewall pribadi yang populer adalah *Cisco Security Agent, Personal Firewall Symantec dan Microsoft Internet Connection Firewall.*

b. Network Firewall

Network Firewall dirancang untuk melindungi seluruh jaringan dari akses yang tidak sah dan serangan eksternal. Firewall jenis ini memberikan perlindungan yang maksimal dan fleksibilitas untuk pengguna enterprise. Seperti halnya firewall pribadi jenis ini juga telah terintegrasi fitur tambahan seperti *Intrution Detection* dan kemampuan pencegahan dan pemutusan *Virtual Private Network*. Fitur andalan lain yang diperkenalkan pada *network firewall* pemeriksaan paket yang mendalam, dengan fitur ini firewall jenis ini dapat memeriksa lalu lintas jaringan pada layer aplikasi dan dapat memutuskan cara terbaik untuk menangani arus lalu lintas.

c. Software Firewall

Software Firewall berjalan di atas sistem operasi komersial yang tersedia di pasar seperti *Windows* dan *Sun Solaris*. Satu layanan dapat mengkonfigurasi firewall software menjadi serbaguna. Sebagai contoh, firewall jenis ini dapat berfungsi sebagai server Domain Name System (DNS) atau dapat menjadi filter *spam*, konfigurasi sebagai sistem multiguna jauh lebih mudah daripada *Dedicated Appliance Firewall*. Beberapa *Software Firewall* populer antara lain *Sun Screen firewall, Microsoft ISA Server , IPTables*

Linux dan FreeBSD. Firewall Jenis ini tidak sebaik fungsi firewall yang berupa perangkat atau *Appliance Firewall*, tetapi jenis ini lebih murah dan berguna untuk pengguna rumah.

d. Appliance Firewall

Appliance Firewall adalah perangkat yang dirancang khusus yang memiliki hardware dan sistem operasi *Custom*. Hardware dan sistem operasi firewall ini dibangun secara *Custom* dan telah mengintegrasikan fungsi filter, inspeksi perangkat lunak dan perangkat keras dan menyediakan layanan firewall ke jaringan. *Appliance Firewall* menawarkan kinerja yang lebih baik dibandingkan dengan software firewall karena firewall jenis ini telah dikustomisasi dengan sistem operasi, prosesor khusus dan *application specific integrated circuits (ASICs)* untuk pengolahan data. Dengan menggunakan *Asics*, firewall ini telah menghilangkan kebutuhan part-part seperti hard disk yang diperlukan dalam *software firewall*. Namun demikian pada perangkat berbasis *Appliance firewall* sulit untuk menyediakan fitur tambahan seperti filter spam, yang merupakan tugas sepele Dalam kasus *software firewall*.

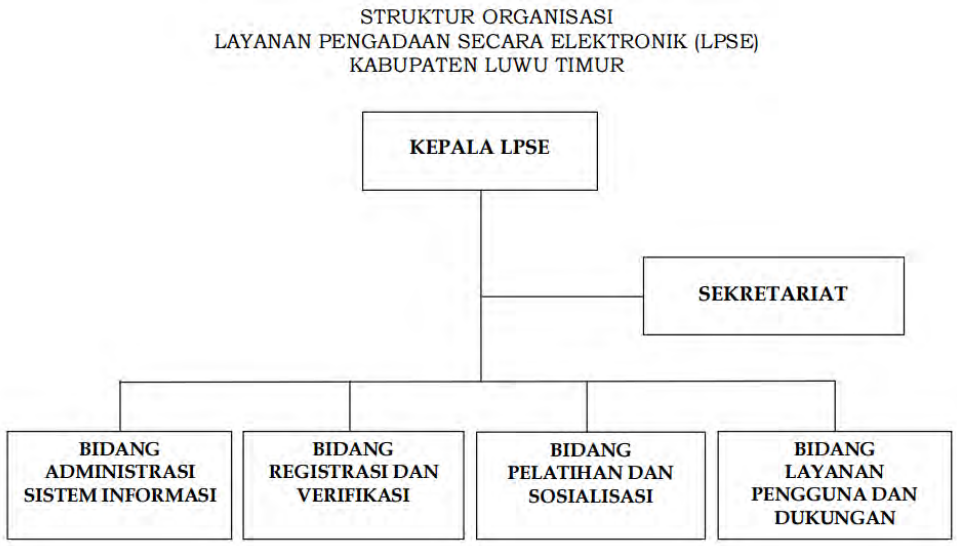
e. Integrated Firewall

Integrated Firewall adalah perangkat firewall serbaguna yang menawarkan banyak layanan jaringan untuk pengguna jaringan. Firewall Ini telah menggabungkan fitur firewall tradisional dengan fitur tambahan lainnya seperti remote-akses VPN, LAN ke LAN VPN, *Intrusion detection and Prevention, spam filtering and antivirus filtering*. Perangkat ini dibuat dengan menggabungkan banyak perangkat ke dalam satu perangkat dan dikenal sebagai "All In One" untuk keamanan jaringan yang lengkap. Keuntungan pertama dari firewall ini adalah bahwa hal itu membuat desain jaringan jadi lebih sederhana dengan mengurangi jumlah perangkat jaringan yang memerlukan proses administrasi, yang mengurangi beban administrasi oleh staf jaringan. Keuntungan yang lain adalah biaya yang kurang

dibandingkan dengan beberapa perangkat dari beberapa vendor . Tapi firewall ini merupakan titik kegagalan, jika firewall ini dalam kondisi *network fail* firewall ini membiarkan jaringan tidak terlindungi dan mengakibatkan beberapa celah jaringan terbuka.

2.8 Layanan Pengadaan Secara Elektronik (LPSE)

Layanan Pengadaaan Secara Elektronik yang selanjutnya disebut LPSE adalah unit kerja Kementerian/Lembaga/Daerah/Instansi yang dibentuk untuk menyelenggarakan sistem pelayanan Pengadaan Barang/Jasa secara elektronik[5]. Dalam struktur organisasi LPSE terdapat 4 (empat) bidang, yang bekerja dibawah koordinasi Kepala LPSE dan Sekretariat sesuai gambar 2.2 berikut :



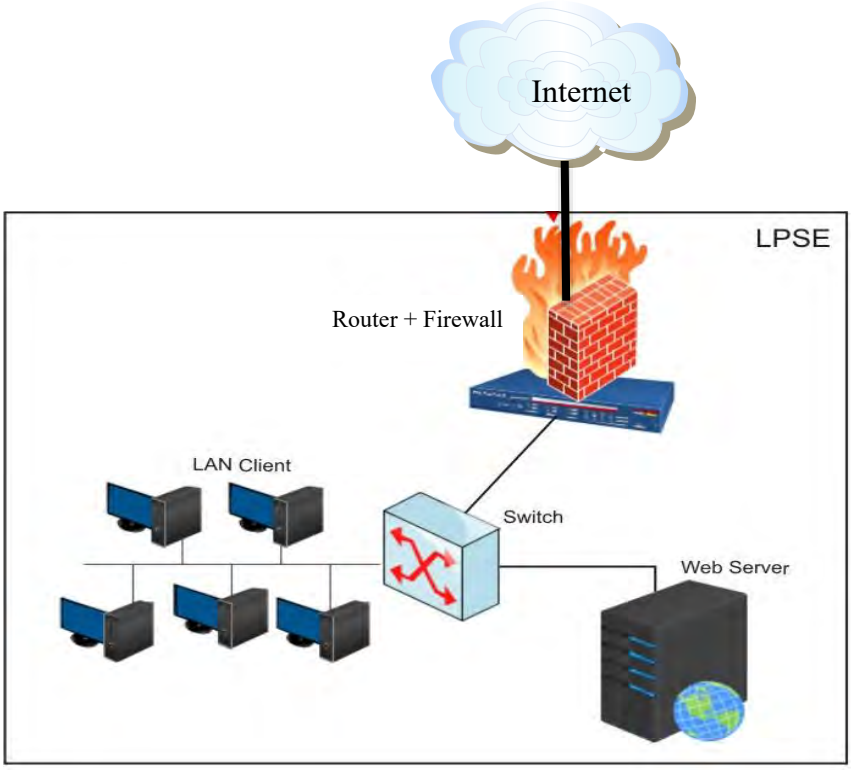
Gambar 2.8 Struktur Organisasi LPSE Kab. Luwu Timur

2.7.1 Sistem Pengadaan Secara Elektronik

Aplikasi SPSE adalah aplikasi perangkat lunak Sistem Pengadaan Secara Elektronik (SPSE) berbasis web yang terpasang di server Layanan Pengadaan Secara Elektronik (LPSE) atau server Lembaga Kebijakan Pengadaan

Barang/Jasa Pemerintah (LKPP) yang dapat diakses melalui website LPSE atau Portal Pengadaan Nasional[6].

Secara umum topologi jaringan LPSE pada Pemerintah kabupaten Luwu Timur dapat dilihat pada gambar dibawah ini :



Gambar 2.9 Topologi Jaringan LPSE Kab. Luwu Timur

2.9 Penelitian Yang Telah Dilakukan

Beberapa penelitian yang pernah dilakukan tentang penerapan IDS, Honeypot, Load Balancer, Firewall dan serangan DDoS dan mitigasinya diantaranya adalah :

Muhammad Zamrudi AH (2006) dengan judul "analisa mekanisme pertahanan DOS dan DDOS (Distributed Denial Of Service) pada virtual machine menggunakan IDS Center" dari penelitian ini menyimpulkan bahwa tingkat keamanan tidak berbanding lurus dengan kemudahan

penggunaan dan fungsionalitas dari sistem tersebut, semakin tinggi tingkat keamanan suatu sistem maka akan semakin sulit digunakan dan semakin terbatas fungsinya. Dari hasil simulasi serangan yang telah dilakukan nilai rata-rata response time pada sistem pertahanan ini adalah 1753 ms.

Pratomo, Baskoro Adi (2011) dengan judul "Pengalihan Paket Ke Honeypot Pada Linux Virtual Server Untuk Mengatasi Serangan DDOS" dari hasil pengamatan dan proses uji coba perangkat lunak yang dilakukan dengan menggunakan sistem ini, failed request mengalami penurunan rata-rata sebanyak 0.97% dibandingkan Linux Virtual Server standar.

Ioannis Vordos, 2009, dengan judul "Mitigating Distributed Denial of Service Attacks with Multi-Protocol Label Switching—Traffic Engineering (MPLS-TE)" ketika traffic flow berada diatas 8,5 Mbps, beban CPU dari router inti melebihi ambang batas aman (80%), dan dalam waktu yang singkat (kurang dari 1 menit) koneksi antar router menjadi tidak stabil, oleh karena itu adalah penting dalam jaringan untuk memiliki sumber daya yang cukup untuk menangani sejumlah besar traffic data yang berbahaya ketika sinkhole method digunakan.

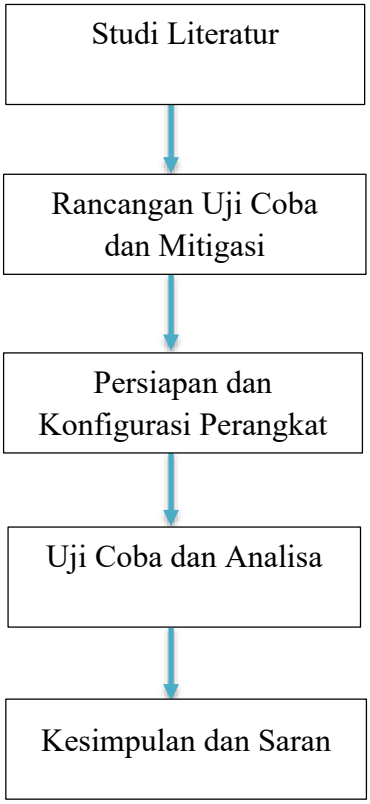
Qian Zhou, 2013, dengan judul "Comparing Dedicated and Integrated Firewall Performance" menyimpulkan bahwa Pada dasarnya, perbedaan latency dan packet lost tidak jelas ketika ukuran paket dengan jumlah kecil namun ketika ukuran paket berjumlah menengah, router dengan fitur firewall memiliki delay yang lebih kecil dibandingkan dengan jaringan dengan SmoothWall dalam router.

Sardar Muhammad Sulaman, 2011, "An Analysis and Comparison of The Security Features of Firewalls and IDSs" menyimpulkan bahwa Firewall dan Intrusion Detection System saja tidak bisa menawarkan perlindungan lengkap terhadap serangan, mereka harus digunakan bersama-sama untuk meningkatkan pertahanan mendalam atau pengamanan berlapis.

BAB III
METODOLOGI

3.1. Metode Penelitian

Secara umum metode penelitian dapat dilihat pada Gambar 3.1 berikut :



Gambar 3.1 Alur Metodologi Penelitian

Keterangan :

1. Studi Literature

Dalam penelitian ini langkah awal dilakukan pengumpulan dan pembelajaran literature terkait Intrusion Detection System, Load Balancer, Networking, Firewall, Load Balancer, serangan DoS dan DDoS beserta mekanisme pertahanan dan Mitigasinya yang bersumber dari buku-buku, *ebook,* jurnal-jurnal ilmiah nasional dan internasional serta berbagai referensi lainnya.

2. Rancangan Ujicoba Dan Mitigasi

Pada tahap ini dilakukan perancangan arsiktektur skenario uji coba serangan Dos dan DDoS dan mitigasinya dimana pada desain mitigasi terdapat IDS dan Load Balancer.

3. Persiapan dan Konfigurasi Perangkat

Pada Tahap ini dilakukan proses setup dan konfigurasi pada perangkat-perangkat yang terdapat pada infrastruktur LPSE guna kepentingan penelitian, antara lain :

- Instalasi Sistem Operasi Linux Debian, Ubuntu, Centos pada server-server yang akan digunakan dalam uji coba.
- Konfigurasi Routing dan Firewall pada server yang bertindak sebagai IDS dan Firewall.
- Instalasi Aplikasi Engine IDS Suricata pada Server yang diperuntukkan sebagai IDS.
- Instalasi aplikasi-aplikasi pendukung seperti Apache Webserver, Java, dan SPSE pada Server yang diperuntukan sebagai Server LPSE dan Honeypot.
- Instalasi Apache Web Server pada Server yang diperuntukan sebagai Honeypot.
- Konfigurasi Load Balancer.
- Instalasi dan konfigurasi Aplikasi GCC dan Perl untuk mengenerate Packet DoS dan DDoS pada komputer Client yang bertindak sebagai Attacker.
- Instalasi Aplikasi Uji Fungsionalitas dan Performa seperti Httperf dan Sysstat pada Server-Server yang bertindak Sebagai IDS-Firewall, Honeypot, dan Web Server LPSE, Attacker Client dan Real Client.
- Instalasi Aplikasi Putty pada Real Client untuk memudahkan meremote Server-Server yang akan digunakan dan Winbox untuk meremote Router Mikrotik.
- Setup Switch unmanageable dan Cabling.

4. Uji Coba dan Analisa

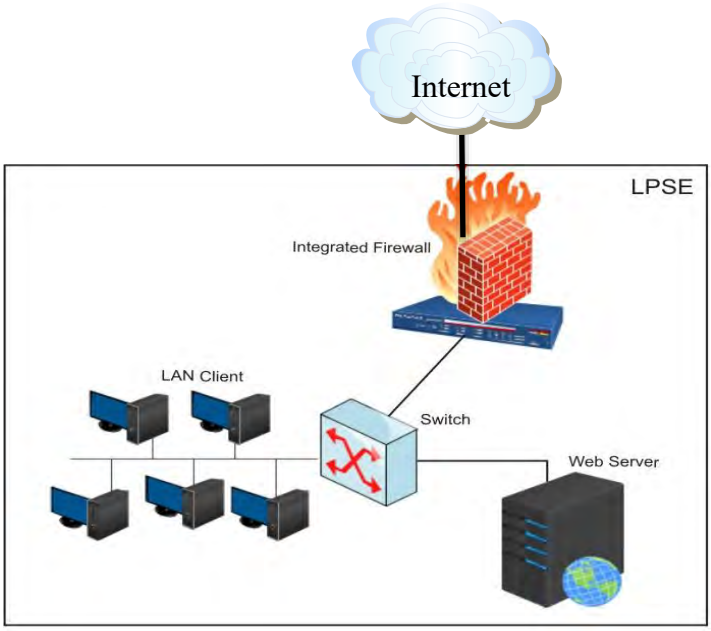
Pada tahap ini dilakukan proses pengujian atau simulasi serangan DDoS terhadap infrastruktur LPSE dengan topologi jaringan existing, topologi jaringan setelah penerapan IDS, Firewall Server Based, Honeypot dan Load Balancer, selang pengujian dilakukan maka akan diamati dan dicatat beberapa parameter penting pada jaringan terkait fungsionalitas dan performansi pada perangkat yang terdapat pada infrastruktur jaringan LPSE.

5. Kesimpulan dan Saran

Tahap ini merupakan proses akhir, dalam proses ini pembuatan kesimpulan dan laporan terhadap perbandingan kondisi existing dan kondisi setelah dilakukan mitigasi dengan topologi yang berbeda, yang mencakup kualitas pertahanan perangkat-perangkat yang terdapat pada LPSE, analisa fungsionalitas dan performa LPSE web server terhadap serangan DDoS beserta dampaknya terhadap perangkat dan operasional layanan LPSE dan rekomendasi perbaikan infrastruktur LPSE.

3.2. Kondisi Existing Infrastruktur LPSE Kab. Luwu Timur

Secara umum kondisi existing infrastruktur dan jaringan LPSE Kab. Luwu Timur dapat dilihat pada gambar 3.12 dibawah ini :

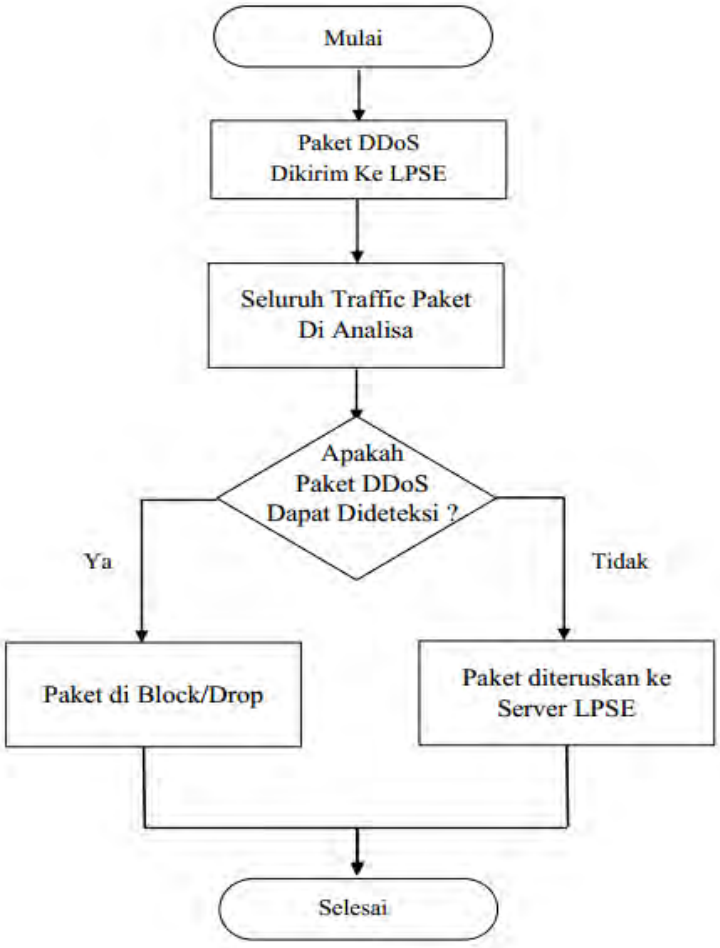


Gambar 3.2 Infrastruktur dan Jaringan Existing LPSE Kab. Luwu Timur

Sesuai laporan tahunan LPSE Kab. Luwu TImur tahun 2015, pada infrastruktur existing LPSE kab. Luwu Timur dalam empat tahun terakhir tercatat telah terjadi 32 kali insiden gangguan keamanan informasi yang merupakan serangan DoS dan atau DDoS dan mengakibatkan tertundanya kegiatan lelang pengadaan barang dan jasa pada LPSE. Berdasarkan hal tersebut dapat dilihat bahwa dengan infrastruktur, topologi jaringan dan metode mitigasi yang terdapat pada kondisi existing ini belum mampu memitigasi serangan DoS dan DDoS dengan baik.

3.3. Strategi dan Metode Mitigasi Serangan DoS dan DDoS Menggunakan Integrated Firewall pada Jaringan Existing LPSE Kab. Luwu Timur.

Alur Metode Mitigasi Dos dan DDoS dapat dilihat pada gambar 3.13 dibawah ini ·



Gambar 3.3 Metode Mitigasi Serangan DoS dan DDoS Menggunakan Integrated Firewall

Strategi mitigasi yang diterapkan pada kondisi existing jaringan LPSE Kab. Luwu Timur yaitu dengan menggunakan Mikrotik Firewall sebagai perlindungan terhadap serangan DoS dan DDos. Dimana firewall ini berfungsi sebagai benteng atau lapisan terluar dalam memfilter traffic paket-paket DoS dan DDoS yang mengarah ke infrastruktur LPSE, sehingga jika terdapat serangan Dos dan DDoS tidak secara langsung mengarah ke Server LPSE. Dengan demikian server LPSE tidak menerima beban traffic yang besar dari serangan Dos dan DDoS secara langsung sehingga diharapkan dapat mengurangi beban traffic paket DDoS dan resiko crash pada Server LPSE.

Keterangan :

3.3.1. Paket DoS dan DDoS Dikirim Ke Server LPSE

Jenis Paket DDoS yang digenerate dan dikirimkan ke Jaringan LPSE adalah paket DDoS UDP dengan menggunakan script UDP yang dicompile dan dijalankan dengan aplikasi GNU Compiler Colection dan paket DDoS Http Flood melalui script slowloris yang dicompile dan dijalankan dengan aplikasi Perl. Serangan-serangan DDoS tersebut bersumber dari dua (2) unit PC attacker client dan satu (1) unit attacker Sever dalam jaringan internal LPSE.

3.3.2. Analisa Paket dan Bloking Firewall

Firewall Mikrotik akan memeriksa dan menganalisa seluruh paket yang melalui jaringan LPSE, apabila terdapat paket yang sesuai dengan rule yang telah didefinisikan pada firewall sebagai paket DoS dan DDoS maka IP sumber paket tersebut akan di Black List, kemudian paket akan di blok.

3.3.3. Firewall

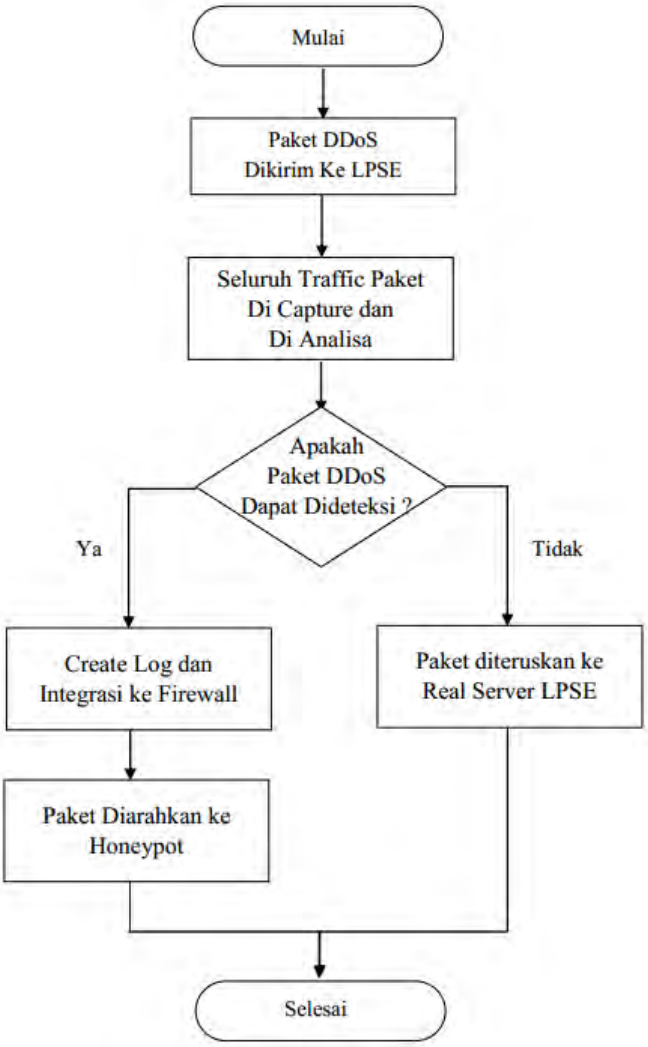
Pada Metode ini perangkat yang berfungsi sebagai firewall adalah Mikrotik RB1200 perangkat ini merupakan integrated firewall dimana dalam perangkat ini terdapat fungsi switching dan routing.

3.3.4. Server LPSE

Server LPSE adalah server yang didalamnya terdapat aplikasi SPSE yang berfungsi sebagai server production atau Web Server LPSE

3.4. Metode Mitigasi Serangan DoS dan DDoS Menggunakan IDS, Firewall Server Based dan Honeypot

Alur Metode Mitigasi DoS dan DDoS dapat dilihat pada gambar 3.13 dibawah ini :



Gambar 3.4 Metode Mitigasi Serangan DDoS Menggunakan IDS, Firewall Server Based dan Honeypot

Metode mitigasi ini adalah metode yang menggunakan IDS, Firewall Server dan Honeypot, dimana dalam hal ini IDS akan mengcapture dan menganalisa seluruh traffic paket yang melalui jaringan LPSE. Jika terdapat serangan DoS dan DDoS terhadap infrastruktur LPSE yang diidentifikasi IDS maka akan diintegrasikan alert ke firewall untuk mengalihkan paket-paket DoS dan DDoS

tersebut ke honeypot server tiruan atau honeypot, sehingga beban traffic paket-paket DoS dan DDoS tersebut tidak menumpuk pada firewall dan tidak mengarah ke Server LPSE, sehingga diharapkan dapat menutupi kekurangan yang terdapat pada strategi mitigasi pada jaringan existing LPSE.

Keterangan :

3.4.1. Paket DoS dan DDoS Dikirim Ke Server LPSE

Jenis Paket DDoS yang digenerate dan dikirimkan ke Jaringan LPSE adalah paket DDoS UDP dengan menggunakan script UDP yang dicompile dan dijalankan dengan aplikasi GNU Compiler Colection dan paket DDoS Http Flood melalui script slowloris yang dicompile dan dijalankan dengan aplikasi Perl. Serangan-serangan DDoS tersebut bersumber dari dua (2) unit PC attacker client dan satu (1) unit attacker Sever dalam jaringan internal LPSE.

3.4.2. IDS dan Analisa Paket DDoS

Pada metode ini aplikasi Intrusion Detection System yang diinstall pada server yang terintegrasi ke Firewall dalam jaringan Internal LPSE, berfungsi untuk memonitoring, mengcapture dan menganalisa setiap lalu lintas paket yang lewat pada infrastruktur jaringan LPSE.

Dalam mendeteksi serangan DoS dan DDoS IDS ini menggunakan parameter Rule/List Based on Signature dan Based On Behaviour.

a. Based On Signature
   Adalah pendeteksian dengan mencocokan konten traffic pada lalu lintas jaringan dengan Rule/List yang terdapat pada IDS, yang mana rule/list ini merupakan hasil analisa dari para security analyst.
b. Based On Behaviour
   Adalah pendeteksian dengan menilai berdasarkan anomali tertentu paket (suspicius) pada lalu lintas jaringan dengan memadukan IDS dengan Plugin alogaritma AIEngine.

Selain itu, IDS membuat Log paket yang terdeteksi sebagai paket DoS dan DDoS serta mengintegrasikan alert ke firewall untuk memblok sumber atau paket yang berhasil terdeteksi.

3.4.3. Firewall dan Honeypot

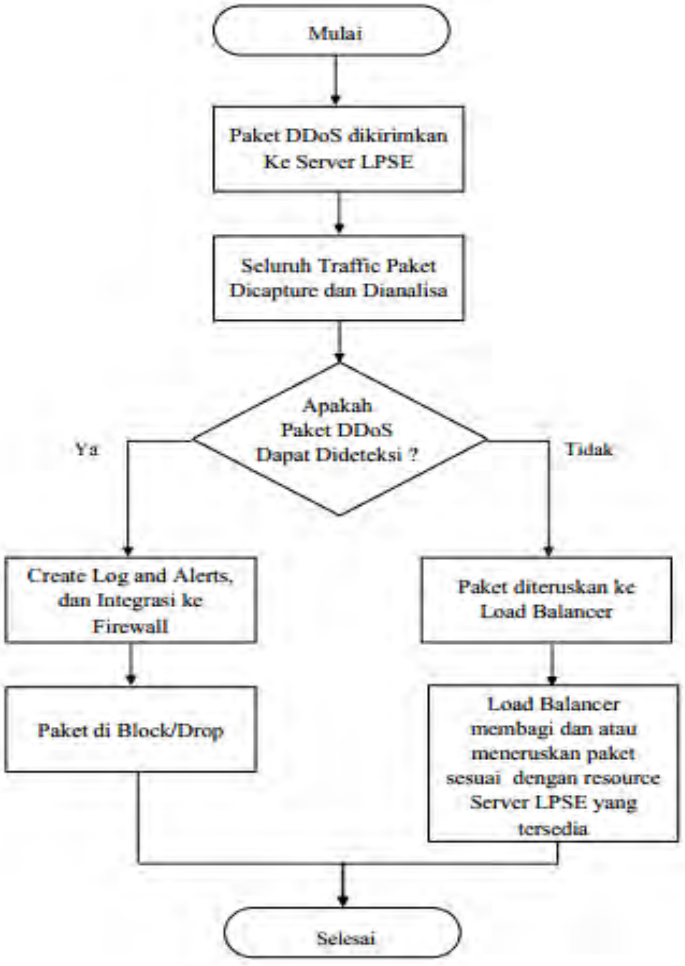
Pada Metode ini perangkat yang berfungsi sebagai firewall adalah server linux yang didalamnya terdapat tools Iptables yang terintegrasi dengan IDS Suricata, sehingga jika IDS mendeteksi paket DDoS maka Firewall akan langsung mengarahkan paket tersebut ke server honeypot atau server tiruan, sehingga paket-paket DDoS tersebut tidak mengarah ke server LPSE.

3.4.4. Server LPSE

Pada metode ini digunakan server LPSE yang didalamnya terdapat aplikasi SPSE yang berfungsi sebagai server production atau Web Server LPSE

3.5. Metode Mitigasi Serangan DoS dan DDoS Menggunakan IDS, Firewall Server Based dan Load Balancer

Alur Metode Mitigasi DoS dan DDoS dapat dilihat pada gambar 3.14 dibawah ini :



Gambar 3.5 Metode Mitigasi Serangan DDoS Menggunakan IDS, Firewall dan Load Balancer

Metode mitigasi ini adalah metode yang menggunakan IDS, Firewall Server dan Load Balancer, dimana dalam hal ini IDS akan mengcapture dan menganalisa seluruh traffic paket yang melalui jaringan LPSE. Jika terdapat serangan DoS dan DDoS terhadap infrastruktur LPSE maka IDS akan mengintegrasikan alert ke firewall untuk memblock paket-paket DoS dan DDoS tersebut. Namun apabila IDS tidak dapat mendeteksi serangan tersebut maka paket DoS dan DDoS ke server tiruan atau honeypot sehingga beban traffic paket-paket DoS dan DDoS tersebut tidak menumpuk pada firewall dan tidak mengarah ke Server LPSE, sehingga diharapkan metode ini dapat menutupi kekurangan pada Strategi mitigasi pada kondisi exsiting LPSE dan metode mitigasi yang menggunakan honeypot sebagai pengalihan paket DoS dan DDoS.

Keterangan :

3.5.1. Paket DoS dan DDoS Dikirim Ke Server LPSE

Jenis Paket DDoS yang digenerate dan dikirimkan ke Server LPSE adalah paket DDoS UDP dan Http yang bersumber dari dua (2) PC attacker client dan satu (1) server dalam jaringan internal LPSE. Dimana Attacker Client menggunakan aplikasi Loic sementara Script UDP dan Http dijalankan menggunakan GCC dan aplikasi perl pada attacker server. Server LPSE berjumlah 2 (unit) ke dua server tersebut up dimana beban traffic nantinya akan ditentukan oleh Load Balancer.

3.5.2. Intrusion Detection System dan Paket DDoS

Aplikasi Intrusion Detection System yang diinstall pada server tersendiri namun terintegrasi dengan Router Firewall dan Jaringan Internal LPSE, berfungsi untuk memonitoring, mengcapture dan menganalisa setiap lalu lintas paket yang lewat pada infrastruktur jaringan LPSE.

Dalam mendeteksi serangan DoS dan DDoS IDS Suricata menggunakan parameter Rule/List Based on Signature dan Based On Behaviour.

a. Based On Signature

Adalah pendeteksian dengan mencocokan konten traffic pada lalu lintas jaringan dengan Rule/List yang terdapat pada IDS, yang mana rule/list ini merupakan hasil analisa dari para security analyst.

b. Based On Behaviour

Adalah pendeteksian dengan menilai berdasarkan anomali tertentu paket (suspicius) pada lalu lintas jaringan dengan memadukan IDS dengan Plugin alogaritma AIEngine.

Selain itu, IDS membuat Log paket yang terdeteksi sebagai paket DDoS serta mengintegrasikan alert ke firewall untuk memblok sumber atau paket DDoS yang berhasil terdeteksi.

3.5.3. Load Balancer Meneruskan Paket Ke Server LPSE

Load Balancer dikonfigurasi dan terkoneksi untuk meringankan beban ke dua Server LPSE dengan membagi beban traffic berdasarkan alogaritma yang terdapat pada Load Balancer sehingga jika serangan DoS dan DDoS tidak terdeteksi oleh IDS dan Firewall maka Load Balancer akan membagi beban traffic ke server utama dan cadangan sehingga tidak terjadi penumpukan paket pada server-server tersebut, selain itu load balancer terintegrasi dengan Router dan Firewall pada jaringan internal LPSE.

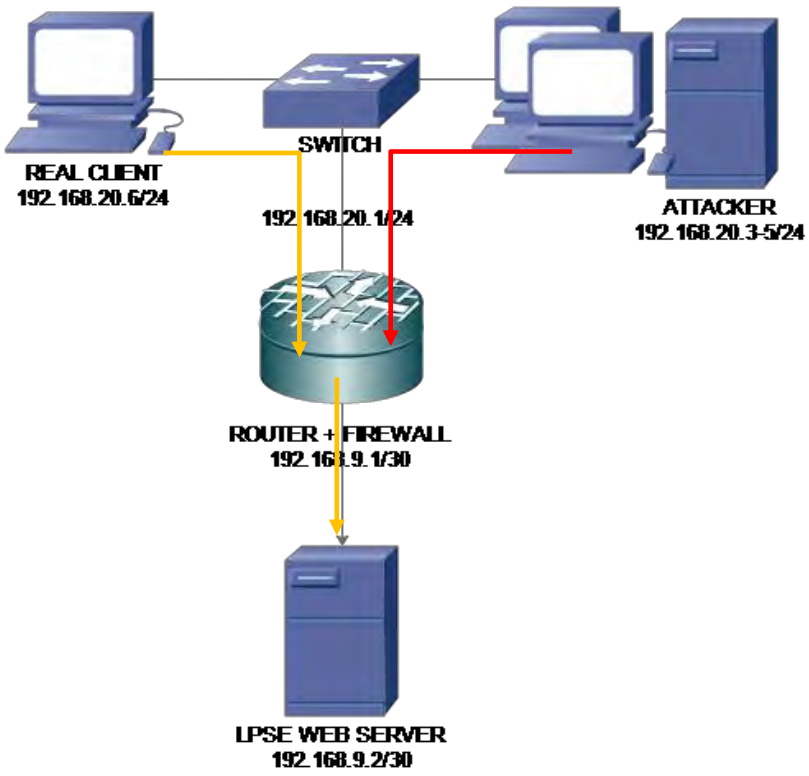
3.5.4. Server LPSE

Pada topologi ini digunakan 2 (dua) server LPSE dengan spesifikasi hardware dan software yang hampir sama, dimana semua proses pada server utama diduplikasikan pada server cadangan, sehingga jika server utama mengalami kegagalan maka server cadangan akan mengambil alih fungsi server utama dengan tepat waktu.

3.6. Rancangan Skenario Uji Coba

3.6.1. Rancangan Skenario Uji Coba Serangan DDoS Pada Topologi Pertama (Existing).

Arsitektur skenario uji coba serangan DDoS pada topologi jaringan existing dapat dilihat pada gambar 3.6 berikut :



Gambar 3.6 Rancangan Skenario Uji Coba Mitigasi Serangan DDos Pada Topologi Pertama (Topologi Existing)

Rancangan Skenario ini menggunakan infrastruktur Existing Jaringan LPSE. Pada skenario ini dilakukan simulasi serangan DDoS dari Sisi Attacker server dan client yang mengirimkan paket-paket DDoS jenis UDP dan Http Flood secara terus menerus ke alamat IP server LPSE, aktivitas tersebut dilakukan guna membanjiri jaringan LPSE dan bertujuan untuk membuat klien yang sah/real client tidak dapat mengakses web server LPSE. Selanjutnya sembari serangan berlangsung, real client akan melakukan pengukuran kinerja dan fungsionalitas dari web server LPSE, aplikasi SPSE dan perangkat-perangkat yang terdapat dalam jaringan.

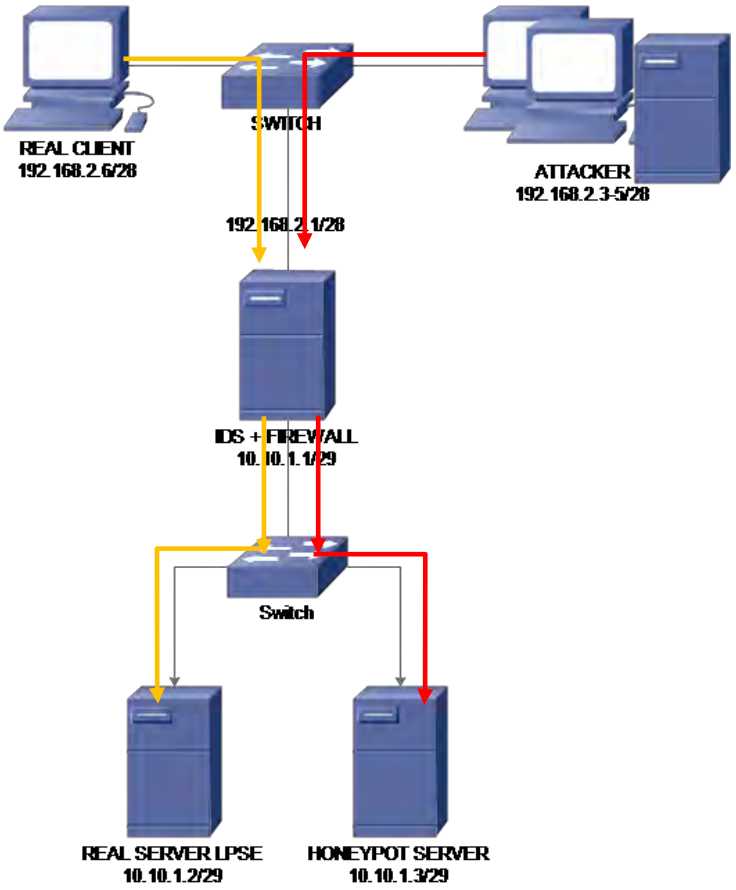
Selanjutnya Firewall Mikrotik akan menganalisa dan mendeteksi traffic yang melalui jaringan LPSE. Jika dikenali atau merupakan paket DDoS yang sesuai dengan rule pada firewall mikrotik, paket DDoS tersebut akan di blok. Sementara jika paket-paket pada traffic jaringan LPSE tidak dikenali dan atau dianggap merupakan paket-paket sah maka akan diteruskan ke Server LPSE.

3.6.2. Rancangan Skenario Uji Coba Dan Mitigasi Serangan DDoS Pada Topologi Kedua.

Pada skenario ini beberapa perangkat yang berfungsi sebagai attacker/penyerang akan melakukan serangan DDoS secara bersamaan dan terus menerus mengirimkan paket-paket DDoS jenis UDP dan Http Flood ke alamat IP server LPSE dalam kurun waktu tertentu guna membanjiri jaringan LPSE yang bertujuan untuk membuat klien yang sah/real client tidak dapat mengakses web server LPSE. Topologi ini merupakan penyempurnaan dari topologi existing dimana beban traffic DDoS menumpuk pada firewall dan dapat mengakibatkan firewall crash dan koneksi menjadi tidak stabil. Oleh karena itu digunakan IDS untuk menganalisa dan mendeteksi traffic yang melalui jaringan LPSE, kika paket dikenali atau merupakan paket DDoS maka IDS akan mengintegrasi hasil analisa ke firewall untuk mengarahkan paket DDoS tersebut ke Honeypot Server, sehingga beban traffic tidak berada pada firewall dan Server LPSE. Sementara jika paket-paket pada traffic jaringan LPSE tidak dikenali dan atau dianggap merupakan paket-paket sah atau traffic normal maka akan diteruskan ke Real Server LPSE.

Skenario ini merupakan penyempurnaan dari rancangan topologi kedua atau yang menggunakan honeypot, dimana jika IDS tidak mengenali paket DDoS masih terdapat resiko serangan dapat secara langsung mengarah ke Server LPSE. Pada rancangan skenario ini telah dipersiapkan Load balancer dan 2 Unit server LPSE sebagai langkah antisipasi jika serangan DoS dan DDoS tidak dapat dikenali oleh IDS.

Rancangan skenario uji coba DDoS dengan metode mitigasi menggunakan IDS, Firewall Server Based dan Honeypot dapat dilihat pada gambar 3.16 berikut :

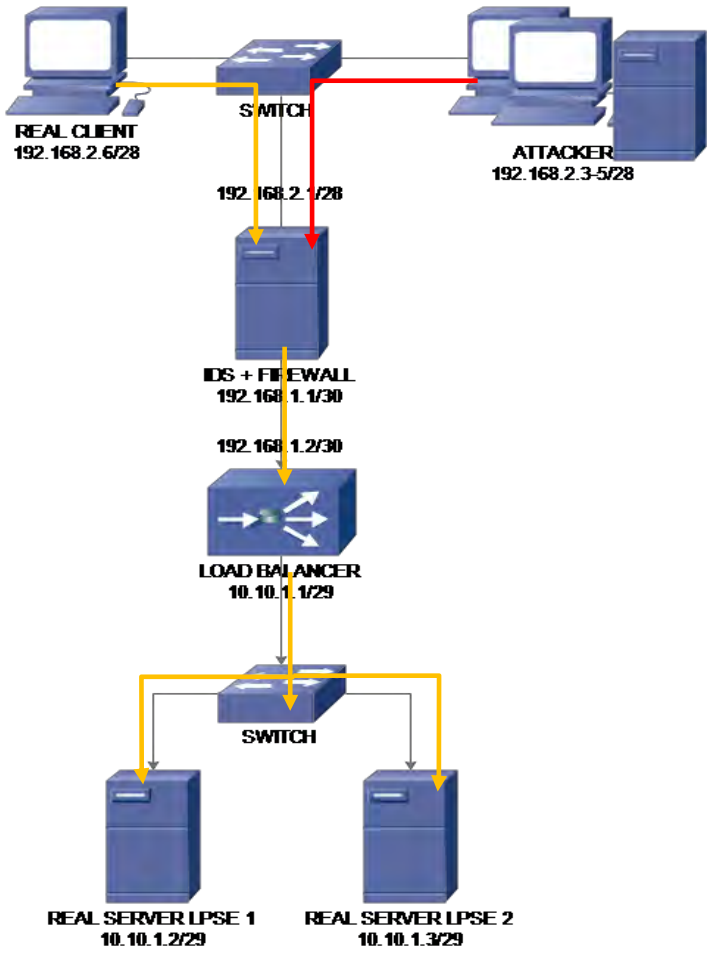


Gambar 3.7 Rancangan Skenario Uji Coba Mitigasi serangan DDoS Pada Topologi Kedua

3.6.3. Rancangan Skenario Uji Coba Dan Mitigasi Serangan DDoS Pada Topologi Ketiga

Pada Skenario ini beberapa perangkat yang berfungsi sebagai penyerang akan melakukan serangan DDoS secara bersamaan dan terus menerus mengirimkan paket-paket DDoS jenis UDP dan Http Flood ke alamat IP server LPSE dalam kurun waktu tertentu guna membanjiri jaringan LPSE. Seraangan ini bertujuan untuk membuat klien yang sah/real client tidak dapat mengakses web server LPSE. Selanjutnya IDS akan menganalisa dan mendeteksi traffic yang melalui jaringan LPSE, Jika paket dikenali IDS maka analisa akan dintegrasi ke firewall untuk memblok paket DoS dan DDoS tersebut. Jika paket-paket pada traffic jaringan LPSE tidak dikenali dan atau merupakan paket-paket sah maka akan diteruskan ke Real Server LPSE.

Jika paket-paket pada traffic jaringan LPSE tidak dikenali oleh IDS namun merupakan paket-paket DDoS, maka firewall tetap akan meneruskan paket-paket tersebut ke Load Balancer. Selanjutnya Load balancer akan mengatur beban traffic dan meneruskan paket tersebut ke Real Server LPSE 1 dan 2 sesuai beban server-server yang dapat di terima dan diproses secara bergiliran. Jika real server 1 kelebihan beban maka akses akan dialihkan ke real server 2, sembari menunggu real server 1 menyelesaikan beban proses sebelumnya. Jika serangan DDoS berhasil masuk sampai pada real server LPSE maka layanan LPSE tetap dapat diakses oleh klien yang sah/real client melalui server LPSE cadangan. Skenario serangan DDoS dengan metode Mitigasi menggunakan IDS, Firewall Server Based dan Load Balancer dapat dilihat pada gambar 3.17 berikut :



Gambar 3.8 Rancangan Skenario Uji Coba Mitigasi Serangan DDoS Pada Topologi Ketiga

BAB IV
PELAKSANAAN, HASIL DAN PEMBAHASAN

4.1. Implementasi Rancangan Skenario Uji Coba dan Metode Mitigasi.

Dalam pelaksanaan ketiga rancangan skenario uji coba dan metode mitigasi pada penelitian ini, peneliti memanfaatkan perangkat keras dan jaringan yang merupakan aset LPSE Pemerintah Daerah Kabupaten Luwu Timur, dimana pada saat uji coba dilakukan, perangkat-perangkat tersebut tidak sedang beroperasi atau tidak digunakan karena merupakan perangkat cadangan. Jika terjadi gangguan ataupun kerusakan pada perangkat utama, maka perangkat-perangkat tersebut akan dimanfaatkan sewaktu-waktu.

Pada ketiga skenario uji coba ini dilakukan simulasi serangan DDoS jenis UDP Flood dan Http Flood. Selain itu dilakukan pengukuran kinerja web server dan perangkat-perangkat yang terdapat pada pada ketiga rancangan topologi jaringan dan metode mitigasinya di infrastruktur jaringan LPSE.

4.1.1. Perangkat Lunak (Software) yang digunakan.

Terdapat beberapa aplikasi pendukung yang akan digunakan dalam penelitian ini, aplikasi-aplikasi yang digunakan dalam proses uji coba antara lain adalah :

1. Suricata (Stable) version 2.0.1 adalah aplikasi IDS yang digunakan untuk mendeteksi serangan DoS dan DDoS.
2. Iptables Version 1.6.0 aplikasi yang berfungsi sebagai firewall digunakan untuk memfilter paket ddos dan memblacklist sumber IP.
3. GNU Compiler Collection (GCC) adalah aplikasi yang digunakan untuk mengcompile dan menjalankan script serangan DoS UDP Flood. GCC Versi 5.3
4. Perl adalah aplikasi yang digunakan untuk mengcompile dan menjalankan script slowloris yaitu serangan DoS jenis HTTP Flood. Versi 5.0
5. LOIC adalah aplikasi yang digunakan untuk mengenerate dan mengirimkan paket-paket DDoS jenis UDP Flood dan Http Flood Versi 1.0.4.0 (attacker Client)

6. Httperf dan Autobench adalah aplikasi yang digunakan untuk mendapatkan performa dari web server seperti (reply rate, packet loss rate, response time). Httperf Versi 0.9.0 dan Autobench v2.1.2
7. Putty adalah aplikasi digunakan meremote device server dan client untuk keperluan konfigurasi dan pengamatan. Putty Versi 0.63
8. Sysstat adalah aplikasi yang digunakan untuk menghitung penggunaan CPUdan Memory dalam rentang waktu tertentu.
   Sysstat Versi 11.2.0
9. Winbox adalah aplikasi yang digunakan untuk mengakses, meremote dan mengkonfigurasi Mikrotik Router.
   Winbox Versi 5.5.18
10. Apache Web Server adalah aplikasi yang digunakan untuk menjalankan web server. Apache Versi 2.4
11. Aplikasi SPSE adalah aplikasi yang digunakan untuk melakukan tender project secara online. SPSE Versi 3.6 dan 4.0

4.1.2. Perangkat Keras (Hardware) yang digunakan.

Sementara untuk kebutuhan perangkat keras dalam pelaksanaan implementasi rancangan skenario dan uji coba dan metode mitigasi, berikut ini adalah perangkat keras yang dipergunakan :

1. Firewall-IDS Server (1 Unit)
   Spesifikasi :
   - Prosesor : Intel Xeon 2.6 GHz
   - Memori : 4GB DDR3 1333 Hz
   - Harddisk : 300 GB SATA
   - LAN Card : 100/1000 Mbps LAN Card
   - Sistem Operasi : Debian

Gambar 4.1 Firewall-IDS Server

2. Honeypot Server (1 Unit)

   Spesifikasi :

   ◦ Prosesor : Intel Xeon 2.6 GHz

   ◦ Memori : 2 GB DDR3 1333 Hz

   ◦ Harddisk : 300 GB SATA

   ◦ LAN Card : 100/1000 Mbps

   ◦ Sistem Operasi Honeypot : Ubuntu 10

Gambar 4.2 Honeypot Server

3. LPSE Web Server (1 Unit)

   Spesifikasi :

   ◦ Prosesor : Intel Xeon 2.6 GHz

   ◦ Memori : 2 GB DDR3 1333 Hz

   ◦ Harddisk : 300 GB SATA

   ◦ LAN Card : 100/1000 Mbps

   ◦ Sistem Operasi : Centos 6.5

Gambar 4.3 LPSE Web Server

4. Load Balancer

   Spesifikasi :

   ◦ Distributes Traffic Across Multiple Servers

   ◦ Real Server Support: 10

   ◦ Maximum Throughput: 950 Mbps

   ◦ SSL Offloading/Acceleration : 500 TPS

   ◦ Ethernet: 2 x Gigabit

   ◦ 1U Mini Rackmount Chassis

Gambar 4.4 Load Balancer

5. Attacker Client (2 Unit)

   Spesifikasi :

   ◦ Prosesor : Intel Core i3 2.93 GHz

   ◦ Memori : 2 GB DDR3 1333 Hz

   ◦ Harddisk : 250 GB SATA

   ◦ LAN Card : 100 Mbps LAN Card

   ◦ Sistem Operasi : Windows 7

Gambar 4.5 Attacker Clients

6. Attacker Server (1 Unit)

   Spesifikasi :

   ◦ Prosesor : Intel Xeon 2.6 GHz

   ◦ Memori : 2 GB DDR3 1333 Hz

   ◦ Harddisk : 300 GB SATA

   ◦ LAN Card : 100/1000 Mbps

   ◦ Sistem Operasi : Proxmox

Gambar 4.6 Attacker Server

7. Real Client (1 Unit)

   Spesifikasi :

   ◦ Prosesor : Intel Core i5 2.3 GHz

   ◦ Memori : 4 GB DDR3 1333 Hz

   ◦ Harddisk : 250 GB SATA

   ◦ LAN Card : 100/1000 Mbps LAN Card

   ◦ Sistem Operasi : Windows 8 dan Ubuntu

Gambar 4.7 Real Client

8. Switch Unmanageable (2 Unit)

   Spesifikasi 8 Port 100 Mbps

Gambar 4.8 Switch

9. Router Mikrotik RB1200 (1 Unit)

   Spesifikasi

   ◦ Architecture PPC

   ◦ CPU PPC460GT 1000MHz

   ◦ Main Storage/NAND 64MB

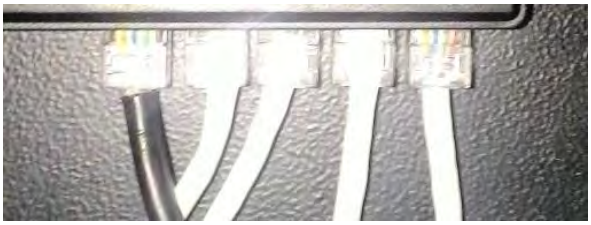
   ◦ RAM 512MB

   ◦ LAN Ports 10 Gigabit Yes

   ◦ Switch Chip 1

Gambar 4.9 Mikrotik RB1200

10. Kabel Lan Cat 5 10/100 Mbps



Gambar 4.10 Kabel LAN Cat 5

Perangkat yang digunakan dalam penelitian ini adalah perangkat yang terdapat didalam infrastruktur LPSE. Sehingga membutuhkan proses otorisasi untuk melakukan uji coba. Dalam proses pengujian ini peneliti bekerja sama dengan Pihak LPSE Kab. Luwu Timur, peneliti memberikan informasi dan pemahaman tentang prosedur penelitian. Seluruh proses pengujian yang dilakukan terhadap perangkat infrastruktur LPSE berada dibawah pengawasan pihak LPSE Kab. Luwu Timur.

4.1.3. Parameter Pengukuran Kinerja Web Server

Dalam sistem komunikasi web Server terdiri dari web server, sejumlah klien, dan jaringan yang menghubungkan klien ke server. Protokol yang digunakan untuk berkomunikasi antara klien dan server adalah protokol HTTP[19]. Untuk

mengukur kinerja web server maka perlu untuk menjalankan tool pada PC client yang menghasilkan beban traffic pada web server[20]. Tool yang digunakan mengukur kinerja web server adalah adalah aplikasi Httperf dan Autobench. pengukuran kinerja dilakukan sebelum dan dalam kondisi serangan DDoS berlangsung, beberapa parameter kinerja web server yang diukur antara lain :

- Request Rate adalah jumlah request yang dapat di respon dan direply oleh web server, semakin tinggi nilai request yang dapat direspon oleh web server maka semakin baik.
- Response Time adalah waktu yang dibutuhkan oleh web server untuk merespon dan memproses permintaan client terhadap web server, semakin cepat response time semakin baik.
- Erorr Request adalah jumlah request yang diirimkan ke web server namun tidak dapat diproses dan direspon oleh web server, semakin sedikit jumlah error pada request semakin baik.

Parameter input Tool Httperf dan Autobench:

- Target Port = 80
- IP address Target Host = 192.168.9.2, 10.10.1.2, 192.168.1.3
- Minimum Request Rate = 50
- Penambahan Request Rate = 50
- Maximum Request Rate = 500
- Numm Conns = 500
- Timeout = 5 Second

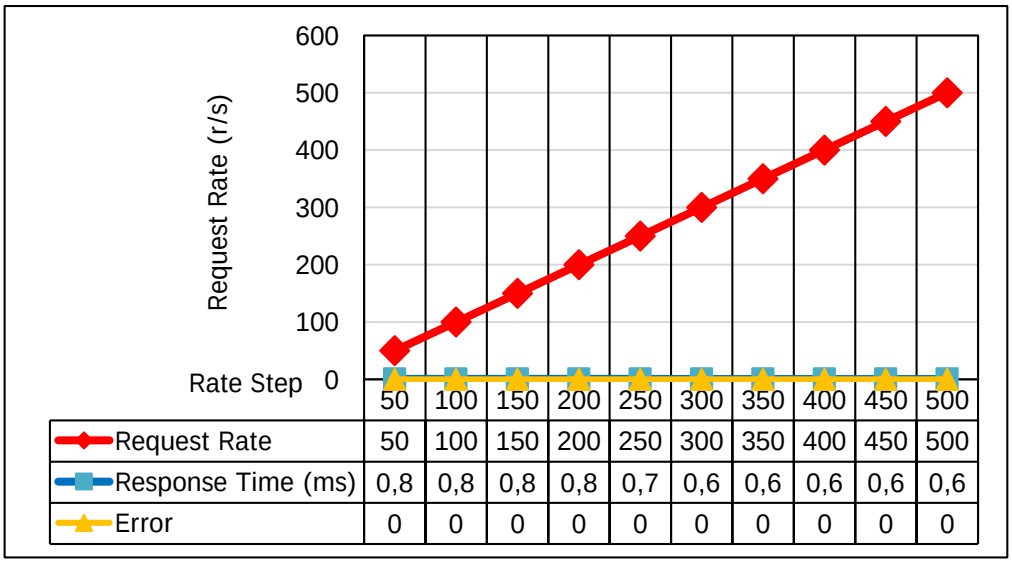
Selain itu Parameter Kinerja Perangkat LPSE seperti Firewall dan Honeypot Server dan Server LPSE, juga akan diukur sebelum dan dalam kondisi serangan DDoS berlangsung. Pengukuran dilakukan dengan menggunakan aplikasi Sysstat dengan objek :

- Penggunaan CPU
- Penggunaan Memory

Parameter input Tool Sysstat (1 Minute) dimana aplikasi Sysstat akan menyimpan log penggunaan CPU dan Memory setiap 1 menit.

4.2. Hasil Uji Coba Performansi Pada Topologi Pertama (Existing).

Uji coba ini menggunakan topologi dan perangkat sesuai dengan kondisi jaringan existing infrastruktur LPSE Kab. Luwu Timur, baik dari sisi konfigurasi, aplikasi, sistem operasi, perangkat dan topologi jaringan sesuai dengan gambar 3.5 pada Bab III. Sebelum simulasi serangan DDoS dijalankan pada infrastruktur jaringan LPSE existing ini, maka terlebih dahulu dilakukan pengambilan data pada kondisi jaringan sebelum serangan, untuk nantinya dibandingkan dengan kondisi ketika serangan DDoS jenis UDP dan Http Flood berlangsung.



Rate Step	50	100	150	200	250	300	350	400	450	500
Request Rate	50	100	150	200	250	300	350	400	450	500
Response Time (ms)	0,8	0,8	0,8	0,8	0,7	0,6	0,6	0,6	0,6	0,6
Error	0	0	0	0	0	0	0	0	0	0

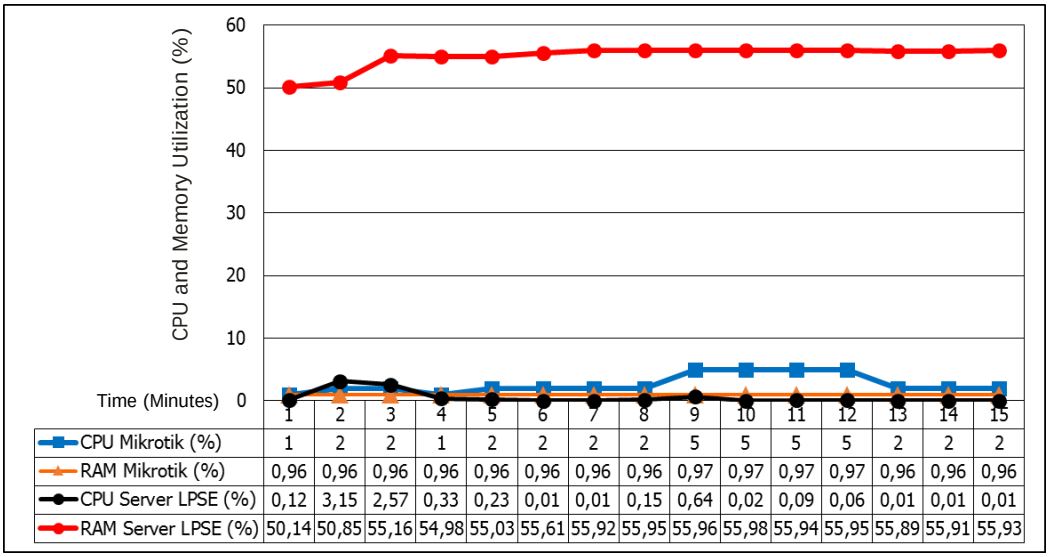
Gambar 4.11 Chart Data Performansi Web Server LPSE Kondisi Sebelum Serangan DDoS

Pada gambar 4.11 dapat dilihat dalam kondisi normal, request rate terhadap web server LPSE adalah sesuai dengan request rate yang telah ditentukan yaitu dari 50 sampai dengan 500 request/s dengan penambahan 50 request setiap rate, sementara response times Web Server LPSE terhadap request sangat kecil dan tidak terdapat error. Pengukuran kinerja performansi web server LPSE menggunakan aplikasi Httperf dengan parameter sebagai berikut :

Parameter Tool Httperf :

- Target Port = 80

- Target Host = IP address 192.168.9.2
- Minimum Request Rate = 50
- Penambahan Request Rate = 50
- Maximum Request Rate = 500
- Numm Conns = 500
- Timeout = 5 Second



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CPU Mikrotik (%)	1	2	2	1	2	2	2	2	5	5	5	5	2	2	2
RAM Mikrotik (%)	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,97	0,97	0,97	0,97	0,96	0,96	0,96
CPU Server LPSE (%)	0,12	3,15	2,57	0,33	0,23	0,01	0,01	0,15	0,64	0,02	0,09	0,06	0,01	0,01	0,01
RAM Server LPSE (%)	50,14	50,85	55,16	54,98	55,03	55,61	55,92	55,95	55,96	55,98	55,94	55,95	55,89	55,91	55,93

Gambar 4.12 Chart Data Log Penggunaan CPU dan Memory Kondisi Sebelum Serangan DDoS

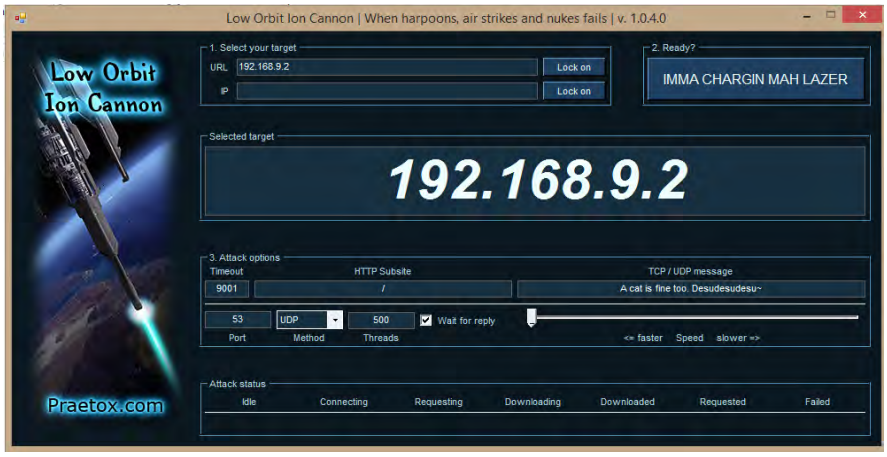
Pada gambar chart 4.12 dapat dilihat dalam kondisi normal, penggunaan CPU dan RAM Mikrotik tidak terlalu tinggi begitupun dengan CPU Server LPSE, namun demikian dalam kondisi normal penggunaan RAM Server LPSE justru rata-rata lebih dari 50% hal tersebut disebabkan oleh aplikasi-aplikasi pendukung yang berjalan sejak sistem operasi mulai, aplikasi-aplikasi tersebut antara lain, Apache, Java dan Aplikasi SPSE v3 dan v4.

4.2.1. Hasil Uji Coba Performansi dan Fungsionalitas Pada Topologi Existing dengan kondisi Serangan DDoS Jenis UDP Flood Berlangsung.

Dalam ujicoba serangan DDoS-UDP Flood pada topologi jaringan existing LPSE ini, dua unit client dan 1 unit server bertindak sebagai attacker/penyerang,

attacker client menggunakan aplikasi LOIC v.1.0.4.0 dikombinakasikan dengan script UDP DDoS yang dicompile dengan aplikasi GNU Compiler Collection yang dijalankan pada server attacker dengan sistem operasi Linux proxmox, parameter-parameter serangan sebagai berikut :

- Parameter Serangan UDP FLood Loic pada PC client:
  - Target IP address = 192.168.9.2
  - Port = 53
  - Type Serangan = UDP Flood
  - Threads = 500



Gambar 4.13 Parameter Serangan UDP FLood dengan Aplikasi LOIC

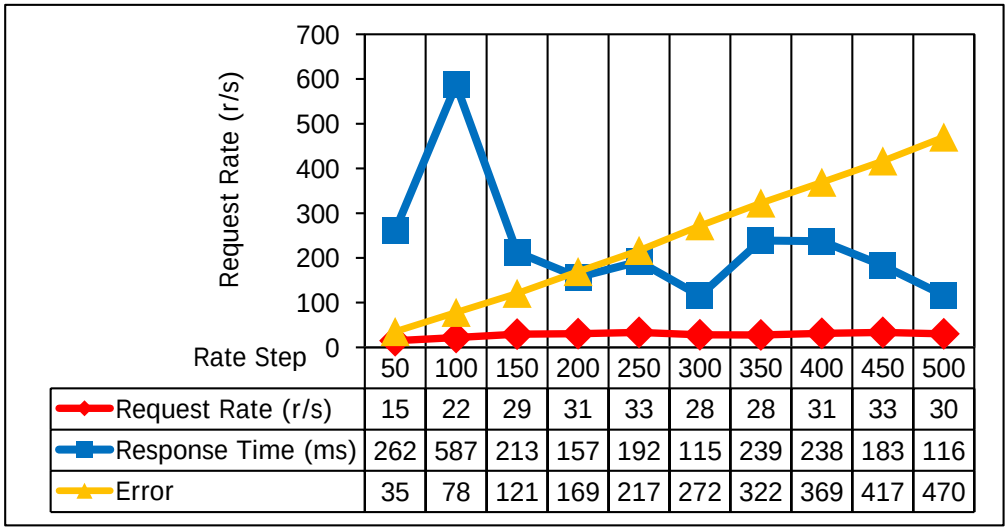
- Parameter Script UDP DDoS pada Attacker Server:
  - IP address = 192.168.9.2
  - Port = 53
  - Type Serangan = UDP Flood
  - Spoffed IP = 9999999999999999

```
root@kominfo:/home/THESIS# ./udp 192.168.9.2 53 9999999999999999
```

Gambar 4.14 Parameter Script Serangan UDP Flood pada Attacker Server

Hasilnya pada gambar Chart 4.15 dibawah ini, berdasarkan data yang diambil dari aplikasi Httperf pada real client, terjadi penurunan performansi yang signifikan pada web server LPSE yaitu request rate yang lebih kecil dari request real, dimana

pada 500 request ke web server LPSE hanya terdapat 30 request yang dapat direspon, response times terhadap request memakan waktu lebih lama dan terdapat sejumlah erorr dari request real yang direspon. Dibandingkan dengan kondisi sebelum serangan, hasil ini tentu jauh berbeda dibandingkan dengan kondisi sebelumnya dimana pada 500 request rate hanya 30 request yang dapat diproses web server LPSE, response times yang jauh lebih lama yaitu mencapai 587 ms dibandingkan dengan kondisi normal yang hanya memakan waktu maximal 0,8 ms, pada kondisi sebelum serangan tidak terdapat erorr, namun selama serangan DDoS jenis UDP Flood berlangsung, pada 500 request ke web server LPSE terdapat 470 error.

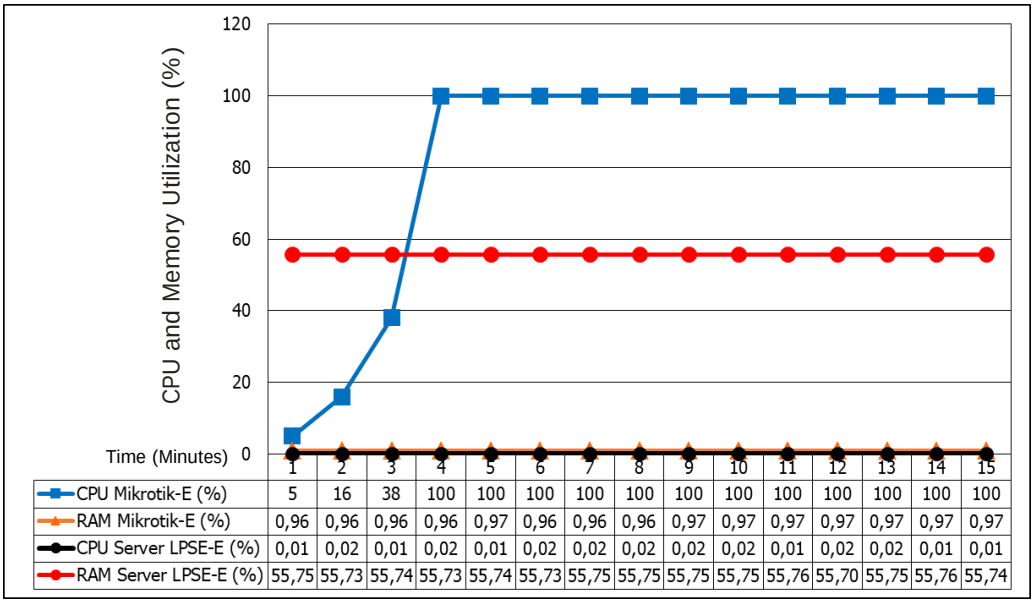


Rate Step	50	100	150	200	250	300	350	400	450	500
Request Rate (r/s)	15	22	29	31	33	28	28	31	33	30
Response Time (ms)	262	587	213	157	192	115	239	238	183	116
Error	35	78	121	169	217	272	322	369	417	470

Gambar 4.15 Chart Data Performansi Web Server LPSE Kondisi Serangan DDoS UDP Flood Berlangsung

Sementara data log penggunaan CPU dan Memory pada gambar 4.16, menunjukkan perangkat-perangkat yang terdapat pada infrastruktur LPSE mengalami peningkatan penggunaan CPU, dimana pada Mikrotik router dan firewall penggunaan CPU sangat tinggi yaitu dari kondisi sebelum serangan hanya maximum 5% menjadi 100%, hal tersebut menyebabkan koneksi ke Mikrotik terputus pada saat ujicoba serangan DDoS berlangsung. Namun demikian CPU dan Ram server LPSE serta Ram Mikrotik tidak mengalami peningkatan penggunaan yang signifikan. Dalam ujicoba simulasi serangan DDoS jenis UDP Flood ini,

pengguna yang sah/real client tidak dapat mengakses dan menggunakan aplikasi SPSE pada web server LPSE dengan normal.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CPU Mikrotik-E (%)	5	16	38	100	100	100	100	100	100	100	100	100	100	100	100
RAM Mikrotik-E (%)	0,96	0,96	0,96	0,96	0,97	0,96	0,96	0,96	0,97	0,97	0,97	0,97	0,97	0,97	0,97
CPU Server LPSE-E (%)	0,01	0,02	0,01	0,02	0,01	0,02	0,02	0,02	0,02	0,02	0,01	0,02	0,02	0,01	0,01
RAM Server LPSE-E (%)	55,75	55,73	55,74	55,73	55,74	55,73	55,75	55,75	55,75	55,75	55,76	55,70	55,75	55,76	55,74

Gambar 4.16 Chart Data log penggunaan CPU dan Memory Kondisi Serangan DDoS Jenis UDP Flood Berlangsung

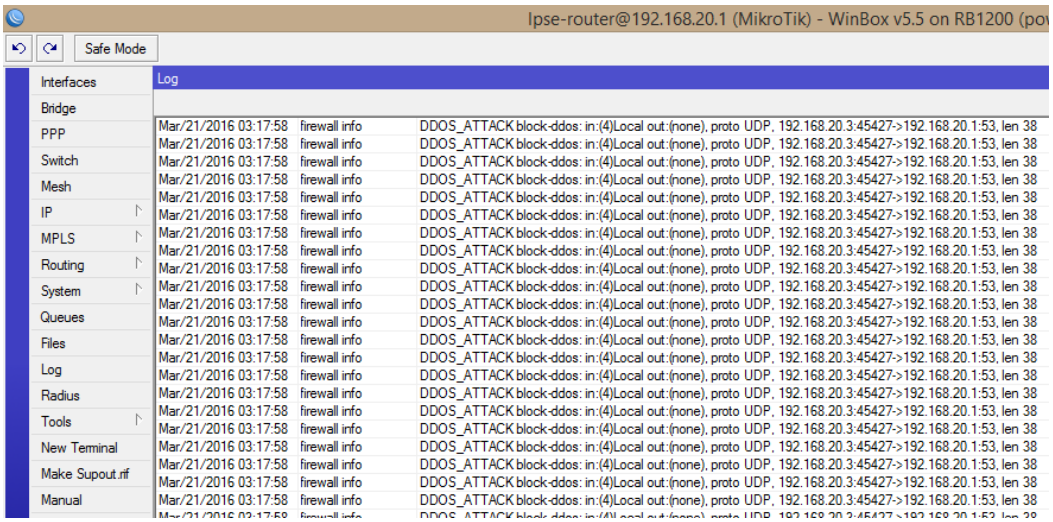
Data hasil uji coba ini diambil dari masing-masing log perangkat seperti Mikrotik dan Server LPSE serta hasil Ujicoba Aplikasi Httperf yang dilakukan pada real client, dimana hasil yang didapatkan diatas menggambarkan bahwa Mikrotik yang berfungsi sebagai router dan firewall tidak dapat mengatasi serangan DDoS jenis UDP Flood. Untuk itu peneliti melakukan pemeriksaan konfigurasi firewall pada Mikrotik tersebut. Hasil Pemeriksaan menunjukkan bahwa mikrotik yang juga berfungsi sebagai firewall telah dikonfigurasi untuk mengenali dan menangani serangan DDoS jenis UDP Flood seperti yang terlihat pada gambar-gambar berikut.

Pada gambar 4.17 Source Sript Firewall mitigasi DDoS pada mikrotik yang aktif seperti dibawah ini, dapat dilihat bahwa Mikrotik telah di set untuk mengidentifikasi, memfilter, memblok dan memblacklist ip addres serangan DDoS dengan jenis serangan UDP Flood.

```
/ip firewall filter
add action=jump chain=forward comment=jump_to_block_ddos disabled=no \
    jump-target=block-ddos protocol=udp
add action=jump chain=input comment=jump_to_block_ddos disabled=no \
    jump-target=block-ddos protocol=udp
add action=return chain=block-ddos disabled=no limit=16,32
add action=log chain=block-ddos disabled=no log-prefix=DDOS_ATTACK
add action=drop chain=block-ddos disabled=no limit=16,32
add action=jump chain=input comment=jump_to_block_ddos disabled=yes \
    jump-target=block-ddos protocol=udp
add action=add-src-to-address-list address-list=black_list \
    address-list-timeout=1d chain=input comment=\
    "Add ddos to adress list -input" connection-limit=10,32 disabled=no \
    protocol=tcp
add action=log chain=input comment="Log ddos" connection-limit=3,32 disabled=\
    yes log-prefix="FILTER, DDOS DROPPED:" protocol=tcp src-address-list=\
    black_list
add action=tarpit chain=input comment="Tarpit ddos" connection-limit=3,32 \
    disabled=no protocol=tcp src-address-list=black_list
add action=drop chain=input comment=ICMP disabled=no protocol=icmp
```

Gambar 4.17 Source Script Firewall, Mitigasi DDoS pada Mikrotik

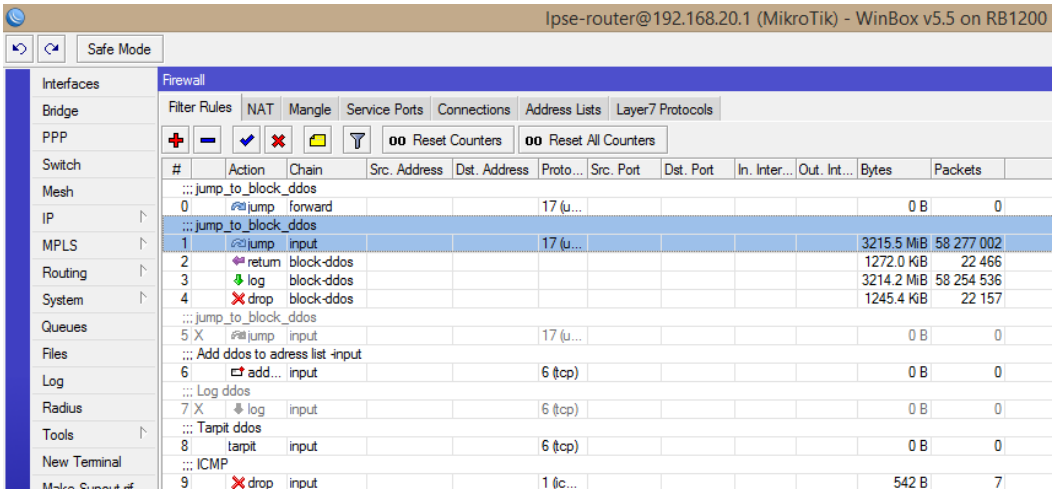
Sedangkan Pada Gambar 4.18 dibawah ini dapat dilihat bahwa firewall mikrotik berhasil mengidentifikasi serangan DDoS yang telah dilakukan.



Gambar 4.18 Data Log Serangan DDoS UDP Flood yang berhasil Di identifikasi oleh Mikrotik

Namun demikian pada proses filtering dan blocking terhadap paket-paket yang di identifikasi sebagai paket DDoS oleh mikrotik, hanya sebagian kecil paket yang dapat di drop/block dimana dari 58.254.536 paket yang teridentifikasi sebagai

serangan DDoS hanya 22.157 paket yang dapat di drop, sesuai data log firewall mikrotik terlampir pada gambar 4.8 dibawah ini.



Gambar 4.19 Data Paket DDoS UDP Flood yang berhasil di Identifikasi Dan di Blok Oleh Mikrotik.

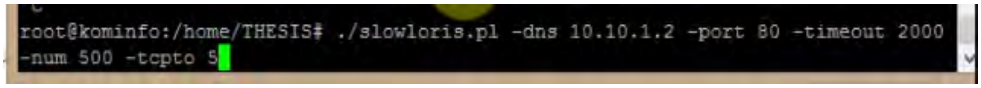
4.2.2. Hasil Uji Coba Performansi dan Fungsionalitas, Kondisi Serangan DDoS Jenis Http Flood Berlangsung.

Dalam ujicoba serangan DDoS Http Flood pada topologi jaringan existing ini, 2 unit PC client dan 1 unit server bertindak sebagai attacker/penyerang. Attacker client yang menggunakan aplikasi LOIC v.1.0.4.0 dikombinasikan dengan aplikasi DDoS Http Flood Slowloris dijalankan pada Attacker Server dengan parameter-parameter serangan sebagai berikut :

- Parameter Http Flood aplikasi Loic pada PC Client :
  - Target IP address = 192.168.9.2
  - Port = 80
  - Type Serangan = UDP Flood
  - Threads = 500
  - Timeout = 2000

Gambar 4.20 Parameter Serangan Http Flood dengan Aplikasi LOIC

- Parameter Aplikasi DDoS Http Flood Slowloris :
  - IP address = 192.168.9.2
  - Port = 53
  - Type Serangan = Http Flood
  - Timeout = 2000
  - Num = 500
  - Tcpto = 5

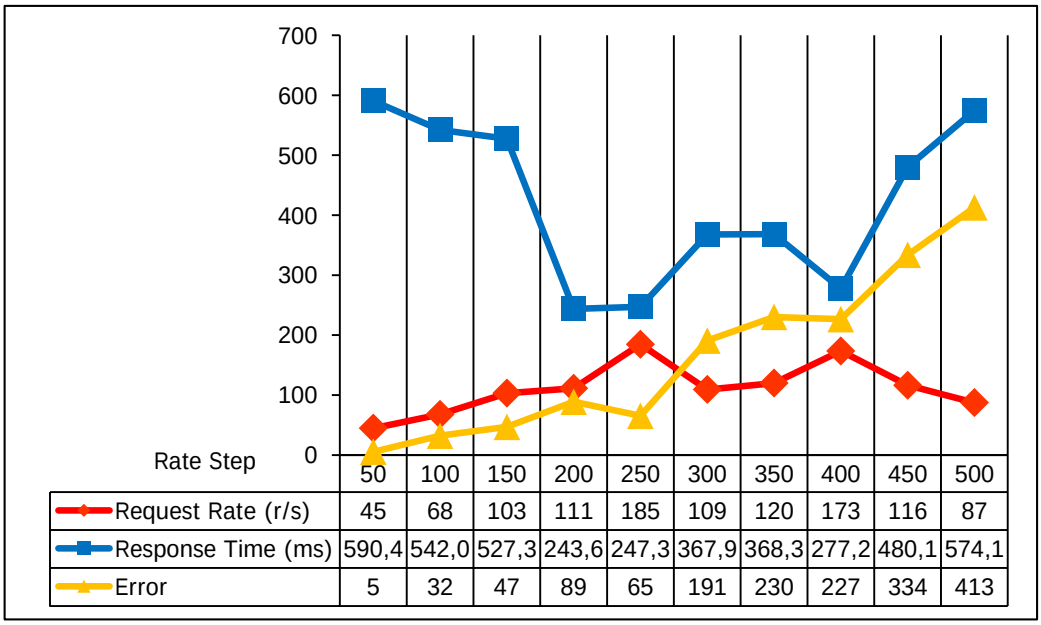


Gambar 4.21 Parameter Serangan Http Flood dengan Aplikasi Slowloris

Hasilnya pada gambar Chart 4.22 dibawah ini, berdasarkan data yang diambil dari aplikasi Httperf pada real client, terjadi penurunan performansi web server LPSE yaitu request rate yang lebih kecil dari request real, dimana pada 500 request ke web server LPSE hanya 87 request yang dapat direspon, response times terhadap request memakan waktu lebih lama dan terdapat sejumlah erorr, jika dibandingkan dengan kondisi sebelum serangan hasil ini tentu jauh berbeda, dimana pada 500 Request tetap 500 request yang dapat diproses, response time yang jauh lebih lama yaitu maximum 590 ms dibandingkan dengan kondisi normal hanya memakan waktu 0,8 ms, sedangkan erorr adalah 0 pada kondisi normal setelah UDP flood berlangsung pada 500 request ke Web server LPSE terdapat 413 error. Pada saat uji coba dilakukan real client/pengguna yang sah tetap dapat mengakses web LPSE

dengan waktu yang lebih lama. Pengukuran performansi web server dilakukan pada saat serangan DDoS Http Flood berlangsung, menggunakan aplikasi Httperf dengan parameter sebagai berikut:

- Target Port = 80
- Target Host = IP address 192.168.9.2
- Minimum Request Rate = 50
- Penambahan Request Rate = 50
- Maximum Request Rate = 500
- Numm Conns = 500
- Timeout = 5 Second

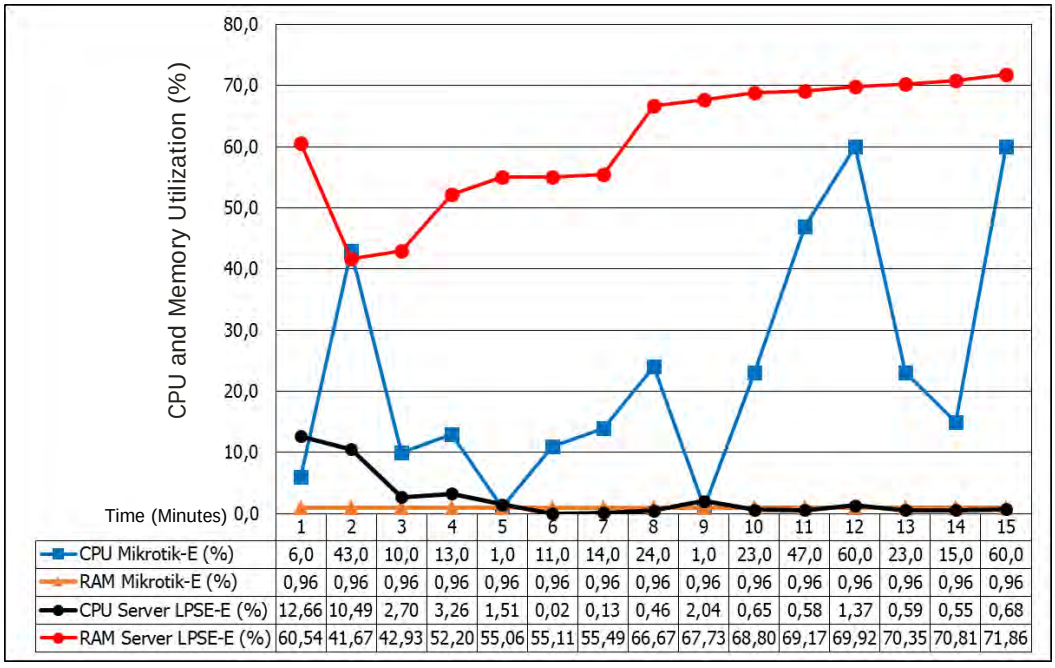


Rate Step	50	100	150	200	250	300	350	400	450	500
Request Rate (r/s)	45	68	103	111	185	109	120	173	116	87
Response Time (ms)	590,4	542,0	527,3	243,6	247,3	367,9	368,3	277,2	480,1	574,1
Error	5	32	47	89	65	191	230	227	334	413

Gambar 4.22 Chart Data Performansi Web Server LPSE, Kondisi Serangan DDoS Http Flood Berlangsung

Sementara Data penggunaan CPU dan Memory pada perangkat-perangkat yang terdapat pada infrastruktur LPSE pun mengalami penurunan fungsionalitas, dimana terjadi penggunaan CPU yang cukup tinggi pada router Mikrotik dari kondisi normal maximal 5% menjadi maximal 60%, penggunaan Ram Mikrotik tidak mengalami peningkatan maximal 0,97 %, penggunaan CPU Server LPSE dari kondisi normal maximum 2,57 % meningkat menjadi maximal 12,66 %,

penggunaan Ram server LPSE dari kondisi normal maximum 55,98 % meningkat menjadi maximal 71,86 %, seperti pada gambar chart 4.13 dibawah ini.



Time (Minutes)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CPU Mikrotik-E (%)	6,0	43,0	10,0	13,0	1,0	11,0	14,0	24,0	1,0	23,0	47,0	60,0	23,0	15,0	60,0
RAM Mikrotik-E (%)	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96
CPU Server LPSE-E (%)	12,66	10,49	2,70	3,26	1,51	0,02	0,13	0,46	2,04	0,65	0,58	1,37	0,59	0,55	0,68
RAM Server LPSE-E (%)	60,54	41,67	42,93	52,20	55,06	55,11	55,49	66,67	67,73	68,80	69,17	69,92	70,35	70,81	71,86

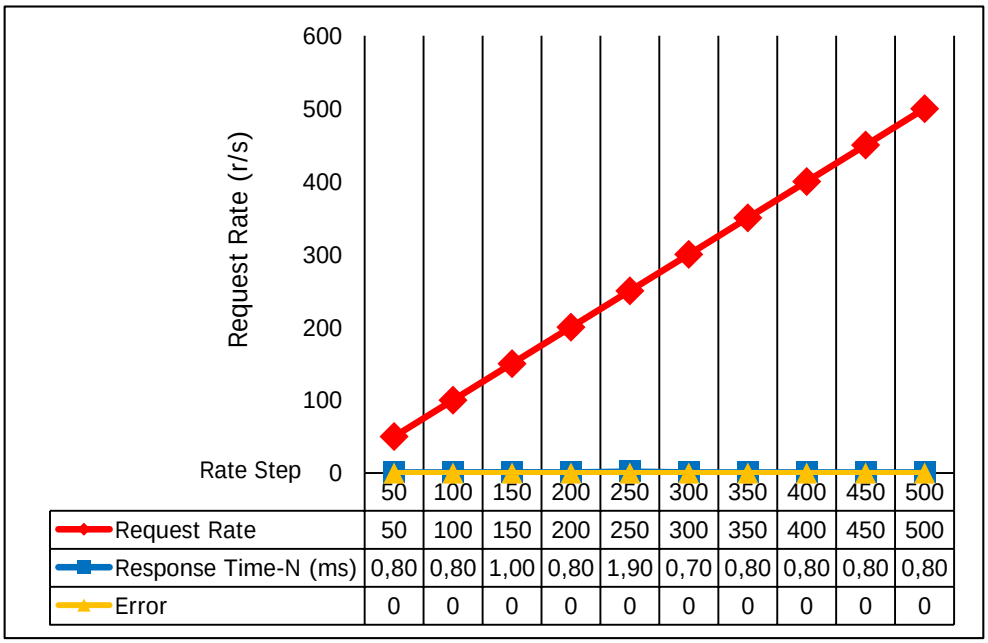
Gambar 4.23 Chart Data Penggunaan CPU dan Memory Kondisi Serangan DDoS Http Flood Berlangsung

4.3. Hasil Uji Coba Performansi Pada Topologi Jaringan Menggunakan IDS, Firewall dan Honeypot

Dalam uji coba ini simulasi serangan DDoS dilakukan pada topologi jaringan sesuai dengan gambar 3.6 pada Bab III. Sebelum simulasi serangan DDoS dijalankan, maka terlebih dahulu dilakukan pengambilan data performansi web server LPSE dan perangkat-perangkat yang terdapat pada jaringan, untuk nantinya dibandingkan dengan kondisi ketika serangan DDoS jenis UDP dan Http Flood berlangsung. Uji coba serangan DDoS jenis UDP Flood dan Http Flood dengan topologi jaringan menggunakan Intrusion Detection System, Firewall server based dan Honeypot server, dimana pada ujicoba ini, topologi jaringan berubah signifikan jika dibandingkan dengan topologi existing LPSE, dengan skenario Serangan DDoS di identifikasi oleh IDS dan Firewall mengalihkan Paket yang dideteksi sebagai paket-paket DDoS ke Honeypot agar paket-paket tersebut tidak sampai pada Web server LPSE dan mengganggu kinerjanya.

4.3.1. Hasil Uji Coba Performansi dan Fungsionalitas Sebelum Serangan DDoS.

Sebelum simulasi serangan DDoS dijalankan, pada infrastruktur jaringan LPSE dengan topologi yang menggunakan Intrusion Detection System, Firewall server based dan Honeypot ini, maka terlebih dahulu uji coba performansi dan fungsionalitas dilakukan untuk pengambilan data pada kondisi jaringan sebelum serangan. Dimana nantinya data ini dibandingkan dengan kondisi ketika serangan DDoS berlangsung, hal ini penting dilakukan karena topologi jaringan yang berubah signifikan.



Rate Step	50	100	150	200	250	300	350	400	450	500
Request Rate	50	100	150	200	250	300	350	400	450	500
Response Time-N (ms)	0,80	0,80	1,00	0,80	1,90	0,70	0,80	0,80	0,80	0,80
Error	0	0	0	0	0	0	0	0	0	0

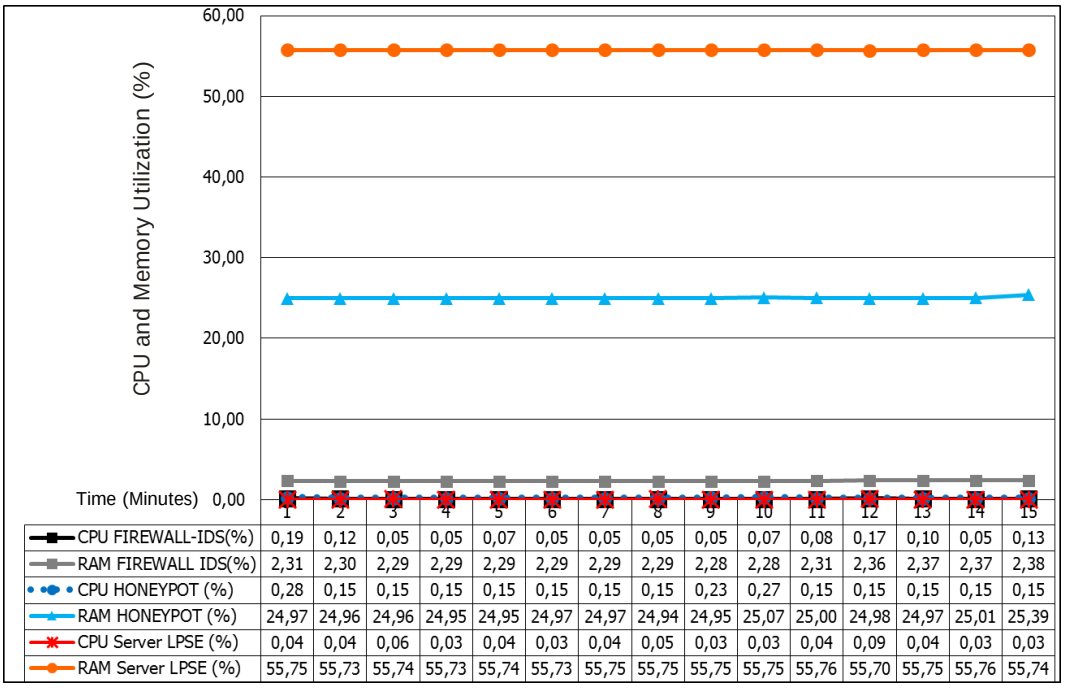
Gambar 4.24 Chart Data Performansi Web Server LPSE Kondisi Jaringan Sebelum Serangan

Pada gambar 4.24 dapat dilihat dalam kondisi normal, request rate terhadap web server LPSE adalah sesuai dengan request rate yang telah ditentukan yaitu dari 50 sampai dengan 500 request/s dengan penambahan 50 request setiap rate, sementara response times terhadap request Web Server LPSE masih tergolong kecil dan tidak terdapat error. Meski demikian jika dibandingkan dengan response times pada topologi jaringan existing terdapat perbedaan sangat kecil, pada 250 request terhadap web server LPSE dimana pada topologi existing response times hanya

memakan waktu 0,8 ms sedangkan dengan pada topologi IDS, Firewall dan Honeypot meningkat menjadi 1,90 ms. Pengukuran performansi web server LPSE menggunakan aplikasi Httperf dengan parameter sebagai berikut :

- Target Port = 80
- Target Host = 10.10.1.2
- Minimum Request Rate = 50
- Penambahan Request Rate = 50
- Maximum Request Rate = 500
- Num Conns = 500
- Timeout = 5 Second

Pada gambar chart 4.25 dibawah ini dapat dilihat dalam kondisi sebelum serangan topologi ini, penggunaan CPU pada masing-masing perangkat seperti pada Server Firewall, Honeypot dan LPSE tidak terlalu besar, namun demikian dalam kondisi normal penggunaan RAM Server LPSE justru rata-rata lebih dari 50% hal tersebut disebabkan oleh aplikasi-aplikasi pendukung SPSE yang berjalan sejak sistem operasi mulai, aplikasi-aplikasi tersebut yaitu antara lain, Apache, Java dan Aplikasi SPSE sendiri, penggunaan RAM Server Honeypot juga rata-rata lebih dari 20% hal tersebut disebabkan oleh aplikasi yang berjalan sejak sistem operasi mulai seperti Apache web server, sedangkan RAM Server IDS-Firewall dalam kondisi normal hanya menggunakan RAM yang kecil yaitu rata-rata diatas 2% meskipun terdapat aplikasi IDS –Suricata yang sedang berjalan. Secara umum hasil ujicoba fungsionalitas ini pada perangkat-perangkat dengan topologi ini dapat dikategorikan normal.



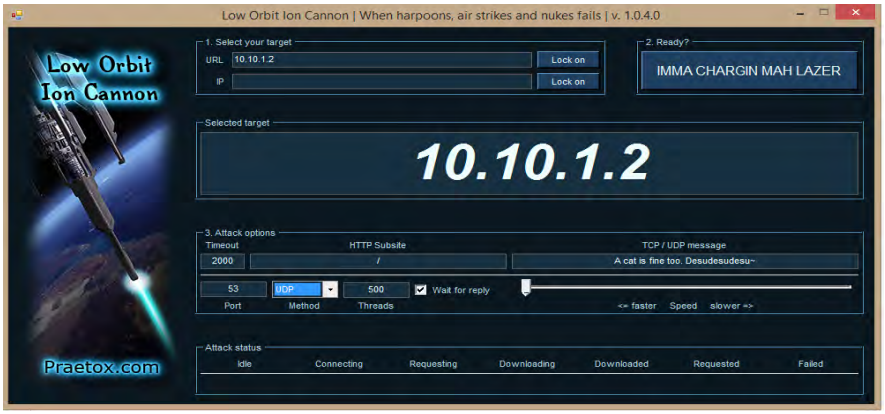
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CPU FIREWALL-IDS(%)	0,19	0,12	0,05	0,05	0,07	0,05	0,05	0,05	0,05	0,07	0,08	0,17	0,10	0,05	0,13
RAM FIREWALL IDS(%)	2,31	2,30	2,29	2,29	2,29	2,29	2,29	2,29	2,28	2,28	2,31	2,36	2,37	2,37	2,38
CPU HONEYPOT (%)	0,28	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,23	0,27	0,15	0,15	0,15	0,15	0,15
RAM HONEYPOT (%)	24,97	24,96	24,96	24,95	24,95	24,97	24,97	24,94	24,95	25,07	25,00	24,98	24,97	25,01	25,39
CPU Server LPSE (%)	0,04	0,04	0,06	0,03	0,04	0,03	0,04	0,05	0,03	0,03	0,04	0,09	0,04	0,03	0,03
RAM Server LPSE (%)	55,75	55,73	55,74	55,73	55,74	55,73	55,75	55,75	55,75	55,75	55,76	55,70	55,75	55,76	55,74

Gambar 4.25 Chart Data Penggunaan CPU dan Memory Kondisi Sebelum Serangan DDoS

4.3.2. Hasil Uji Coba Performansi, kondisi Serangan DDoS Jenis UDP Flood Berlangsung

Dalam uji coba serangan DDoS UDP Flood pada topologi jaringan ini, 2 unit client dan 1 unit server bertindak sebagai attacker/penyerang, dimana 2 client yang menggunakan tools DDoS aplikasi LOIC v.1.0.4.0 dikombinakasikan dengan script UDP DDoS yang dicompile dengan aplikasi GNU Compiler Collection dan dijalankan pada Attacker server, dengan parameter-parameter serangan sebagai berikut :

- Parameter Loic pada Attacker PC client :
  - Target IP address = 10.10.1.2
  - Port = 53
  - Type Serangan = UDP Flood
  - Threads = 500
  - Timeout = 2000



Gambar 4.26 Parameter Serangan DDoS UDP Flood dengan Aplikasi LOIC

- Parameter Script DDoS - UDP Flood yang dicompile dengan aplikasi GNU Compiler Colection :
  - IP address = 10.10.1.2
  - Port = 53
  - Type Serangan = UDP Flood
  - Spoffed IP = 9999999999999999

```
root@kominfo:/home/THESIS# ./udp 10.10.1.2  53 9999999999999999
```

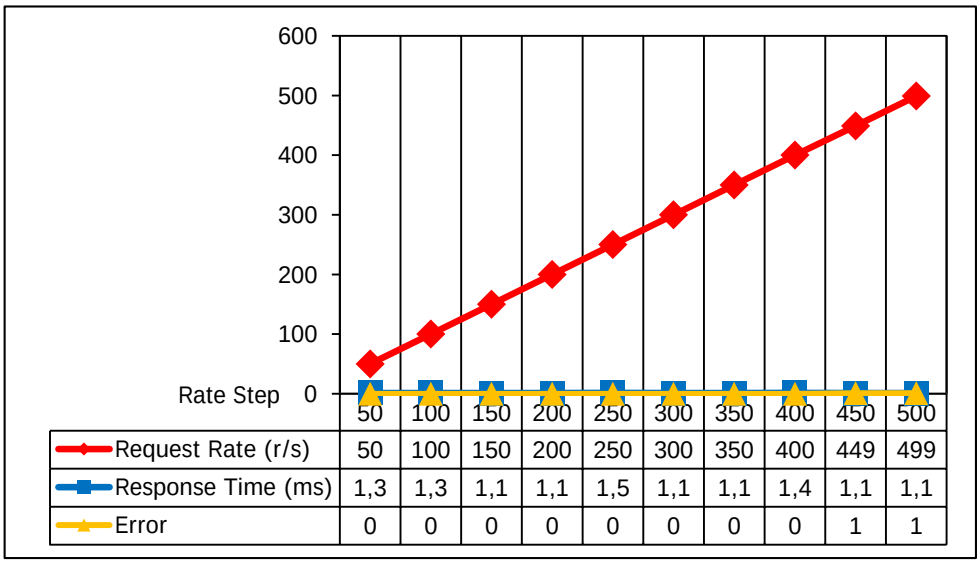
Gambar 4.27 Parameter Serangan dengan Script DDoS UDP Flood pada Attacker Server

Hasilnya pada gambar Chart 4.18 dibawah ini, berdasarkan data yang diambil dari aplikasi Httperf pada real client ke web server LPSE. Pada 500 request ke web server LPSE terdapat 499 request yang dapat direspon, response times terhadap request yang memakan waktu cukup kecil yaitu rata-rata hanya lebih 1 ms dan terdapat 1 erorr, hasil ini tergolong baik dalam kondisi infrastruktur jaringan LPSE yang mengalami serangan DDoS jenis UDP Flood. Data performansi web server diambil menggunakan aplikasi Httperf, pada saat serangan DDoS Jenis UDP Flood berlangsung dengan parameter sebagai berikut :

Parameter Tool Httperf :

- Target Port = 80
- Target Host = 10.10.1.2
- Minimum Request Rate = 50

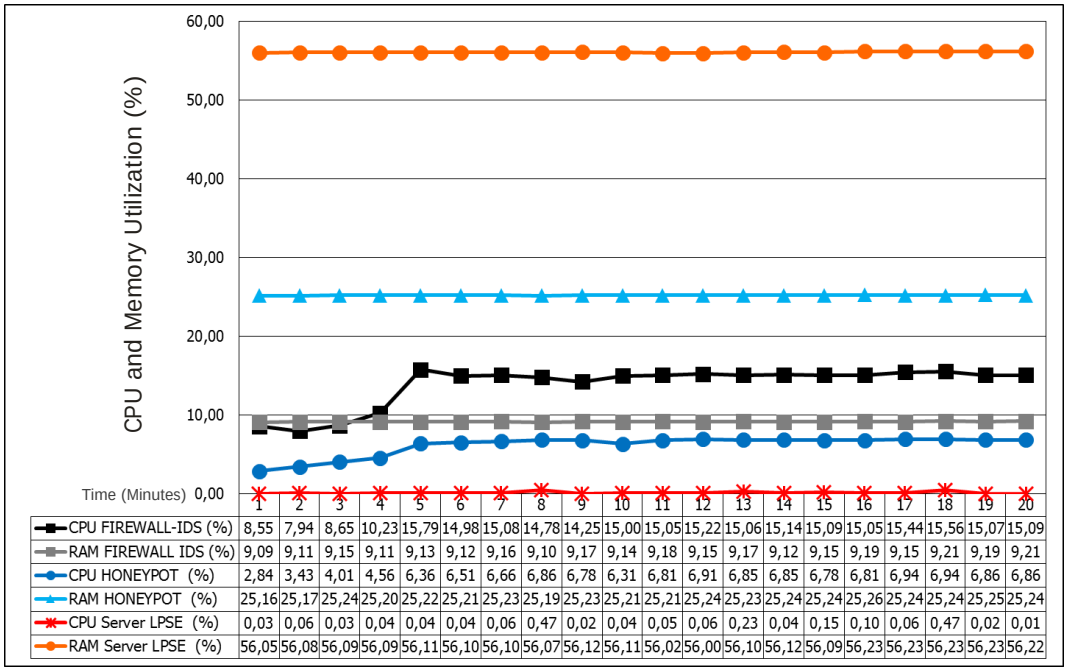
- Penambahan Request Rate = 50
- Maximum Request Rate = 500
- Numm Conns = 500
- Timeout = 5 Second



Rate Step	50	100	150	200	250	300	350	400	450	500
Request Rate (r/s)	50	100	150	200	250	300	350	400	449	499
Response Time (ms)	1,3	1,3	1,1	1,1	1,5	1,1	1,1	1,4	1,1	1,1
Error	0	0	0	0	0	0	0	0	1	1

Gambar 4.28 Chart Data Performansi Web Server LPSE Kondisi Serangan DDoS UDP Flood Berlangsung

Sementara data penggunaan CPU dan Memory dapat dilihat pada gambar 4.19 dibawah ini, dimana perangkat-perangkat yang terdapat pada infrastruktur LPSE mengalami peningkatan penggunaan CPU dan Memory. Jika dibandingkan dengan kondisi sebelum serangan, penggunaan CPU pada Server Firewall-IDS adalah hanya maximal 0,19% dan setelah serangan berlangsung menjadi maximal 15,56 %, penggunaan Ram Server Firewall IDS dari maximal 2,38 % menjadi maximal 15,79 %, penggunaan CPU Server Honeypot dari maximal 0,28 % menjadi Maximal 6,86 %, penggunaan RAM Server Honeypot 25,39 % menjadi 25,24 %, penggunaan CPU Server LPSE dari maximal 0,09 % menjadi 0,47 % , penggunaan RAM server LPSE dari maximal 55,76 % menjadi 56,22 %. Dalam ujicoba simulasi serangan DDoS-UDP Flood ini, pengguna yang sah/real client dapat mengakses dan menggunakan aplikasi SPSE pada web server LPSE dengan normal.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
CPU FIREWALL-IDS (%)	8,55	7,94	8,65	10,23	15,79	14,98	15,08	14,78	14,25	15,00	15,05	15,22	15,06	15,14	15,09	15,05	15,44	15,56	15,07	15,09
RAM FIREWALL IDS (%)	9,09	9,11	9,15	9,11	9,13	9,12	9,16	9,10	9,17	9,14	9,18	9,15	9,17	9,12	9,15	9,19	9,15	9,21	9,19	9,21
CPU HONEYPOT (%)	2,84	3,43	4,01	4,56	6,36	6,51	6,66	6,86	6,78	6,31	6,81	6,91	6,85	6,85	6,78	6,81	6,94	6,94	6,86	6,86
RAM HONEYPOT (%)	25,16	25,17	25,24	25,20	25,22	25,21	25,23	25,19	25,23	25,21	25,21	25,24	25,23	25,24	25,24	25,26	25,24	25,24	25,25	25,24
CPU Server LPSE (%)	0,03	0,06	0,03	0,04	0,04	0,04	0,06	0,47	0,02	0,04	0,05	0,06	0,23	0,04	0,15	0,10	0,06	0,47	0,02	0,01
RAM Server LPSE (%)	56,05	56,08	56,09	56,09	56,11	56,10	56,10	56,07	56,12	56,11	56,02	56,00	56,10	56,12	56,09	56,23	56,23	56,23	56,23	56,22

Gambar 4.29 Chart Data Penggunaan CPU dan Memory Kondisi Serangan DDoS UDP Flood Berlangsung

Hasil yang didapatkan pada ujicoba ini dapat dikategorikan baik dan sesuai dengan hasil yang diharapkan, dimana Intrusion Detection System (IDS) dan Firewall Server Based berfungsi sebagaimana mestinya untuk medeteksi dan mengarahkan paket-paket yang dikategorikan sebagai serangan DDoS dan Honeypot server sebagai pengalihan paket-paket DDoS.

Pada gambar 4.20, dari log sampel Aplikasi Intrusion Detection System (IDS) Suricata dibawah ini, menunjukan bahwa paket-paket yang dikategorikan sebagai paket DDoS dengan jenis UDP Flood dapat diidentifikasi dengan baik oleh aplikasi IDS Suricata, kemudian di integrasi ke Firewall lalu paket-paket tersebut dialihkan ke Honeypot Server. Sedangkan penggunaan CPU dan RAM server honeypot saat menerima paket-paket DDoS sendiri masih dalam rentang yang normal.

```
03/27/2016-04:52:06.652663  [**] [1:2014702:8] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port
Opcode 8 through 15 set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] {UDP} 192.168.2.3:55498 -> 10.10.1.2:53

03/27/2016-04:52:06.652663  [**] [1:2014703:8] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port
Reserved Bit Set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{UDP} 192.168.2.3:55498 -> 10.10.1.2:53

03/27/2016-04:56:06.006085  [**] [1:2014702:8] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port
Opcode 8 through 15 set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] {UDP} 192.168.2.2:63191 -> 10.10.1.2:53

03/27/2016-04:56:06.006085  [**] [1:2014703:8] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port
Reserved Bit Set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{UDP} 192.168.2.2:63191 -> 10.10.1.2:53

03/24/2016-00:33:49.244711  [**] [1:2014701:11] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port
Opcode 6 or 7 set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{UDP} 192.168.2.5:58336 -> 10.10.1.2:53

03/27/2016-04:58:39.985618  [**] [1:2014701:11] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port
Opcode 6 or 7 set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{UDP} 192.168.2.5:40446 -> 10.10.1.2:53
```

Gambar 4.30 Data Log IDS-Suricata Mendeteksi Sumber IP dan Jenis Serangan DDoS Jenis UDP Flood.

```
03/27/2016-04:52:06.652663  [**] [1:2014702:8] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port
Opcode 8 through 15 set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] {UDP} 192.168.2.3:55498 -> 10.10.1.2:53

03/27/2016-04:53:00.660150  [**] [1:2014702:8] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port
Opcode 8 through 15 set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] {UDP} 192.168.2.3:55516 -> 10.10.1.3:53

03/27/2016-04:56:06.006085  [**] [1:2014702:8] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port
Opcode 8 through 15 set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] {UDP} 192.168.2.2:63191 -> 10.10.1.2:53

03/27/2016-04:57:00.000127  [**] [1:2014702:8] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port
Opcode 8 through 15 set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] {UDP} 192.168.2.2:63429 -> 10.10.1.3:53

03/24/2016-00:33:49.244711  [**] [1:2014701:11] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS port
Opcode 6 or 7 set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1]
{UDP} 192.168.2.5:58336 -> 10.10.1.2:53

03/24/2016-00:34:18.470111  [**] [1:2100366:8] GPL ICMP_INFO PING *NIX [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 10.10.1.1:8 -> 10.10.1.2:0

03/24/2016-00:36:42.943080  [**] [1:2100366:8] GPL ICMP_INFO PING *NIX [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 192.168.2.5:8 -> 10.10.1.3:0
```

Gambar 4.31 Data Log IDS- Suricata mengintegrasi alert Ke Firewall untuk mengarahkan paket UDP Flood ke Honeypot Server

Meskipun IDS-Suricata dan Firewall memeriksa seluruh paket yang melalui jaringan LPSE, mendeteksi paket-paket DDoS dan mengintegrasi ke Firewall kemudian dialihkan ke Honeypot, real client/pengguna yang sah tetap dapat mengakses dan menggunakan Aplikasi Web SPSE dengan normal pada saat serangan DDoS Berlangsung. Paket-paket yang bersumber dari pengguna yang sah tidak dideteksi sebagai paket DDoS Oleh Suricata. Hal ini dapat dilihat pada Gambar 4.32 dibawah ini, log Suricata yang menampilkan request dari real

client/pengguna yang sah ke halaman Web Server LPSE, yang kemudian Direspon oleh Server LPSE sesuai dengan request kepada pengguna yang sah.


```
{"timestamp":"2016-03-27T04:50:57.782274-
0400","flow_id":52616976,"event_type":"http","src_ip":"192.168.2.6","src_port":53546,"dest_ip":"10.10.1.2",
"dest_port":80,"proto":"TCP","tx_id":0,"http":{"hostname":"10.10.1.2","url":"\/eproc4lat\/","http_user_agen
t":"Mozilla\/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/50.0.2661.49
Safari/537.36","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\/1.1","status":200,"le
ngth":709}}

{"timestamp":"2016-03-27T04:50:57.712758-
0400","flow_id":52616672,"in_iface":"eth0","event_type":"fileinfo","src_ip":"10.10.1.2","src_port":80,"dest
_ip":"192.168.2.6","dest_port":53545,"proto":"TCP","http":{"hostname":"10.10.1.2","url":"\/","http_user_age
nt":"Mozilla\/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/50.0.2661.49
Safari\/537.36","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\/1.1","status":302,"r
edirect":"http:\/\/10.10.1.2\/eproc4lat\/","length":237},"app_proto":"http","fileinfo":{"filename":"\/","st
ate":"CLOSED","stored":false,"size":286,"tx_id":0}}
```


Gambar 4.32 Data Log IDS,Suricata mendeteksi aktivitas traffic antara real Client dengan Server LPSE sebagai traffic yang sah/normal

4.3.3. Hasil Uji Coba Performansi dan Fungsionalitas dengan kondisi Serangan DDoS Jenis Http Flood Berlangsung.

Dalam ujicoba serangan DDoS jenis Http Flood pada Topologi ini, 2 unit client dan 1 unit server bertindak sebagai attacker/penyerang. Attacker client menggunakan aplikasi LOIC v.1.0.4.0 dikombinasikan dengan script DDoS Http Flood Slowloris yang dijalankan pada Attacker server, dengan parameter-parameter serangan sebagai berikut :

- Parameter Loic :
  - Target IP address = 10.10.1.2
  - Port = 80
  - Type Serangan = Http Flood
  - Threads = 500
  - Timeout = 2000

Gambar 4.33 Parameter Serangan Http Flood dengan Aplikasi LOIC

- Parameter serangan DDoS Http Flood dengan aplikasi Slowloris :
  - IP address = 10.10.1.2
  - Port = 80
  - Type Serangan = Http Flood
  - Timeout = 2000
  - Num = 500
  - Tcpto = 5

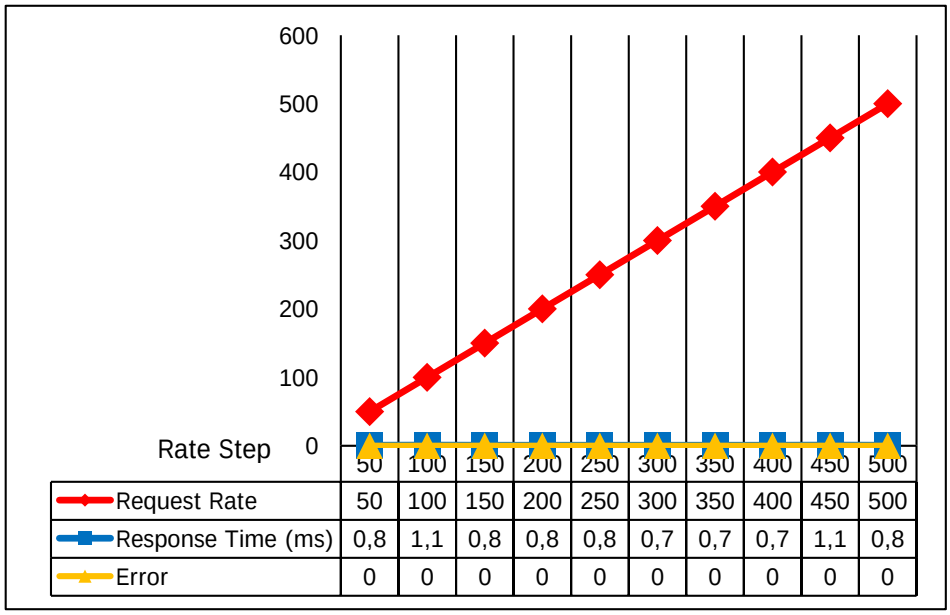
```
root@kominfo:/home/THESIS# ./slowloris.pl -dns 10.10.1.2 -port 80 -timeout 2000 -num 500 -tcpto 5
```

Gambar 4.34 Parameter Serangan DDoS Http Flood dengan Slowloris

Hasilnya pada gambar Chart 4.35 dibawah ini, berdasarkan data yang diambil dari aplikasi Httperf pada real client ke web server LPSE, menunjukkan pada 500 request ke web server LPSE terdapat 500 request yang dapat direspon, response times terhadap request yang memakan waktu cukup kecil, yaitu rata-rata hanya 1 ms dan maximal 1,1 ms, tidak terdapat erorr dari request yang direspon, hasil ini tergolong baik dalam kondisi infrastruktur jaringan LPSE yang mengalami serangan DDoS jenis Http Flood. Pengukuran performansi web server LPSE menggunakan aplikasi Httperf dengan parameter sebagai berikut :

- Target Port = 80
- Target Host = 10.10.1.2/Server LPSE
- Minimum Request Rate = 50
- Penambahan Request Rate = 50

- Maximum Request Rate = 500
- Numm Conns = 500
- Timeout = 5 Second



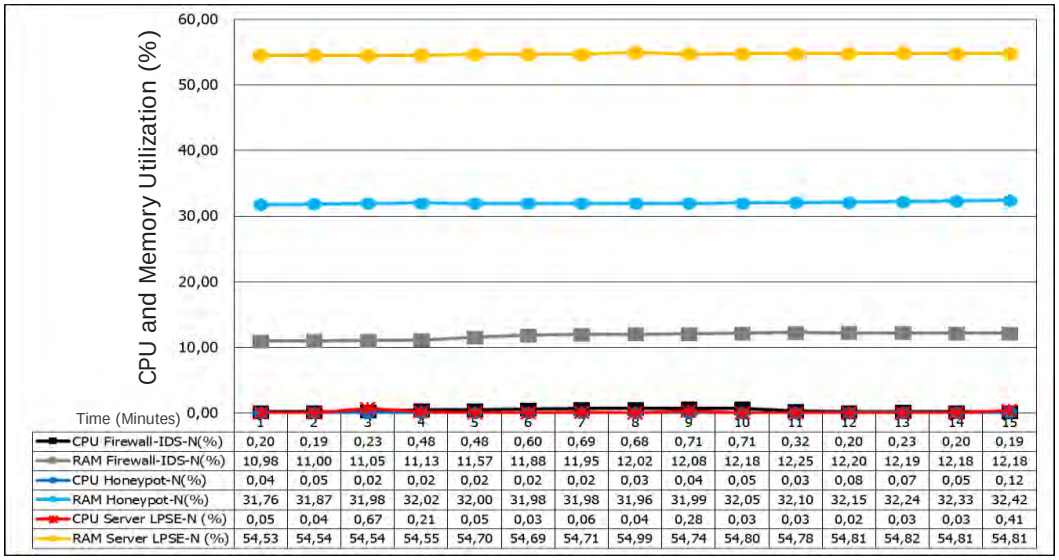
Rate Step	50	100	150	200	250	300	350	400	450	500
Request Rate	50	100	150	200	250	300	350	400	450	500
Response Time (ms)	0,8	1,1	0,8	0,8	0,8	0,7	0,7	0,7	1,1	0,8
Error	0	0	0	0	0	0	0	0	0	0

Gambar 4.35 Chart Data Performansi Web Server LPSE Kondisi Serangan DDoS-Http Flood Berlangsung

Sementara Data uji fungsionalitas perangkat-perangkat yang terdapat pada infrastruktur LPSE dapat dilihat pada gambar chart 4.26, yang menunjukkan perangkat-perangkat pada jaringan mengalami penurunan fungsionalitas yang kecil atau tidak signifikan. Jika dibandingkan dengan kondisi sebelum serangan, penggunaan CPU pada Server Firewall-IDS adalah maximal 0,19 % dan setelah serangan DDoS-Http Flood berlangsung menjadi maximal 0,71 %, penggunaan Ram Server Firewall IDS dari maximal 2,38 % menjadi Maximal 12,25 %, penggunaan CPU Server Honeypot dari maximal 0,28 % menjadi Maximal 0,12 %, penggunaan RAM Server Honeypot 25,39 % menjadi 32,42 %, penggunaan CPU Server LPSE dari maximal 0,09 % menjadi 0,41 % , penggunaan RAM server LPSE dari maximal 55,76 % menjadi 54,99 %.

Dalam ujicoba simulasi serangan DDoS-UDP Flood ini, pengguna yang sah/real client dapat mengakses dan menggunakan aplikasi SPSE pada web server LPSE dengan normal. Hasil yang didapatkan pada uji coba ini dapat dikategorikan baik

dan sesuai dengan hasil yang diharapkan, dimana IDS-Suricata dan firewall berfungsi sebagaimana mestinya untuk memitigasi paket-paket yang dikategorikan sebagai DDoS jenis Http Flood, dan honeypot sebagai pengalihan paket-paket DDoS.



Time (Minutes)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CPU Firewall-IDS-N(%)	0,20	0,19	0,23	0,48	0,48	0,60	0,69	0,68	0,71	0,71	0,32	0,20	0,23	0,20	0,19
RAM Firewall-IDS-N(%)	10,98	11,00	11,05	11,13	11,57	11,88	11,95	12,02	12,08	12,18	12,25	12,20	12,19	12,18	12,18
CPU Honeypot-N(%)	0,04	0,05	0,02	0,02	0,02	0,02	0,02	0,03	0,04	0,05	0,03	0,08	0,07	0,05	0,12
RAM Honeypot-N(%)	31,76	31,87	31,98	32,02	32,00	31,98	31,98	31,96	31,99	32,05	32,10	32,15	32,24	32,33	32,42
CPU Server LPSE-N (%)	0,05	0,04	0,67	0,21	0,05	0,03	0,06	0,04	0,28	0,03	0,03	0,02	0,03	0,03	0,41
RAM Server LPSE-N (%)	54,53	54,54	54,54	54,55	54,70	54,69	54,71	54,99	54,74	54,80	54,78	54,81	54,82	54,81	54,81

Gambar 4.36 Chart Data CPU dan Memory Utilization Kondisi Serangan DDoS-Http Flood Berlangsung

Pada gambar 4.37 dari log sampel IDS –Suricata dibawah ini menunjukan bahwa paket-paket yang dicurigai sebagai paket DDoS Http-Flood dapat diidentifikasi dengan baik oleh IDS, kemudian di integrasi ke firewall lalu paket-paket tersebut dialihkan ke honeypot. Sedangkan penggunaan CPU dan RAM server honeypot saat menerima paket-paket DDoS masih dalam rentang yang normal.

```
03/28/2016-02:55:28.652080  [**] [1:2210036:2] SURICATA STREAM FIN2
invalid ack [**] [Classification: Generic Protocol Command Decode]
[Priority: 3] {TCP} 192.168.2.2:51410 -> 10.10.1.3:80

03/28/2016-02:55:28.652080  [**] [1:2210045:2] SURICATA STREAM Packet with
invalid ack [**] [Classification: Generic Protocol Command Decode]
[Priority: 3] {TCP} 192.168.2.2:51410 -> 10.10.1.3:80

03/28/2016-02:55:28.652211  [**] [1:2210036:2] SURICATA STREAM FIN2
invalid ack [**] [Classification: Generic Protocol Command Decode]
[Priority: 3] {TCP} 192.168.2.2:51410 -> 10.10.1.3:80


03/28/2016-03:02:22.173989  [**] [1:2210007:2] SURICATA STREAM 3way
handshake SYNACK with wrong ack [**] [Classification: Generic Protocol
Command Decode] [Priority: 3] {TCP} 10.10.1.3:80 -> 192.168.2.5:1024

03/28/2016-03:12:31.337416  [**] [1:2210045:2] SURICATA STREAM Packet with
invalid ack [**] [Classification: Generic Protocol Command Decode]
[Priority: 3] {TCP} 192.168.2.3:62828 -> 10.10.1.3:80

03/28/2016-03:12:31.338562  [**] [1:2210036:2] SURICATA STREAM FIN2
invalid ack [**] [Classification: Generic Protocol Command Decode]
[Priority: 3] {TCP} 192.168.2.3:62833 -> 10.10.1.3:80
```

Gambar 4.37 Data Log IDS-Suricata Mendeteksi Sumber IP dan Jenis Serangan DDoS Http Flood.

Meskipun IDS-Suricata dan Firewall memeriksa seluruh paket yang melalui jaringan LPSE dan memfilter paket-paket DDoS, real client/pengguna yang sah tetap dapat mengakses dan menggunakan Aplikasi Web SPSE dengan normal pada saat serangan DDoS Http Flood berlangsung, dan paket-paket yang bersumber dari pengguna yang sah tidak dideteksi sebagai paket DDoS Http FLood oleh IDS Suricata. Hal ini dapat dilihat pada Gambar 4,28 yang menunjukkan log Suricata menampilkan request dari real client/pengguna yang sah ke halaman Web Server LPSE, yang kemudian direspon oleh web server LPSE sesuai dengan request kepada Pengguna Yang Sah.


```
{"timestamp":"2016-03-28T02:43:30.675359-
0400","flow_id":140255651371296,"in_iface":"eth0","event_type":"http","src_ip":"192.168.2.6","src_port":526
72,"dest_ip":"10.10.1.2","dest_port":80,"proto":"TCP","tx_id":0,"http":{"hostname":"10.10.1.2","url":"\/epr
oc4lat\/lelang\/1999\/jadwal","http_user_agent":"Mozilla\/5.0 (Windows NT 6.3; Win64; x64)
AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/50.0.2661.49
Safari\/537.36","http_content_type":"text\/html","http_refer":"http:\/\/10.10.1.2\/eproc4lat\/lelang","http
_method":"GET","protocol":"HTTP\/1.1","status":200,"length":1463}}

{"timestamp":"2016-03-28T02:43:30.689890-
0400","flow_id":140255651371296,"in_iface":"eth0","event_type":"fileinfo","src_ip":"10.10.1.2","src_port":8
0,"dest_ip":"192.168.2.6","dest_port":52672,"proto":"TCP","http":{"hostname":"10.10.1.2","url":"\/eproc4lat
\/lelang\/1999\/jadwal","http_user_agent":"Mozilla\/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit\/537.36
(KHTML, like Gecko) Chrome\/50.0.2661.49
Safari\/537.36","http_content_type":"text\/html","http_refer":"http:\/\/10.10.1.2\/eproc4lat\/lelang","http
_method":"GET","protocol":"HTTP\/1.1","status":200,"length":1463},"app_proto":"http","fileinfo":{"filename"
:"\/eproc4lat\/lelang\/1999\/jadwal","state":"CLOSED","stored":false,"size":6779,"tx_id":0}}
```

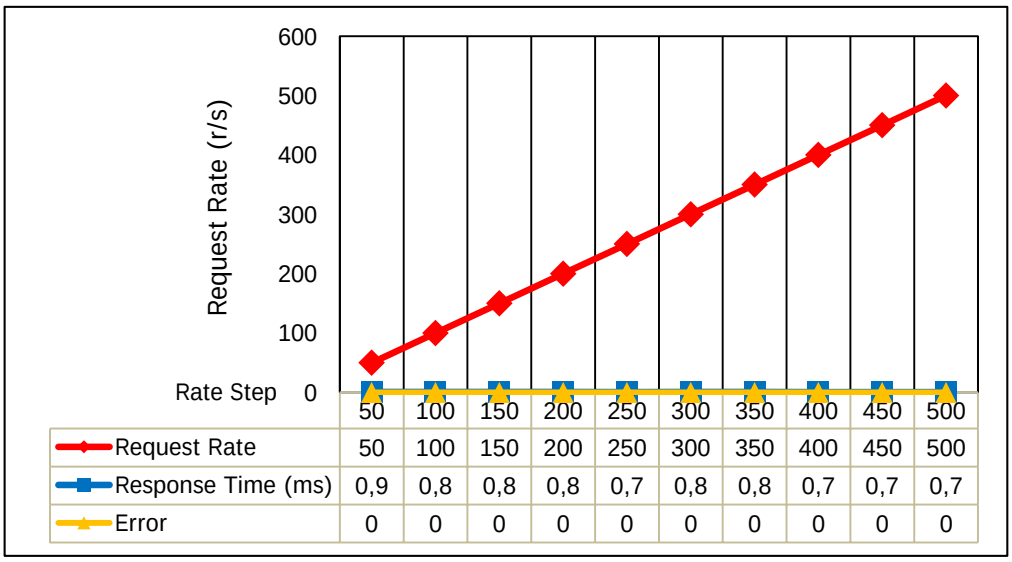

Gambar 4.38 Data Log IDS-Suricata mendeteksi aktivitas traffic antara real Client dengan Server LPSE sebagai traffic yang sah/normal

4.4. Hasil Uji Coba Performansi Pada Topologi Jaringan Menggunakan IDS, Firewall dan Load Balancer

Dalam uji coba ini serangan DDoS dilakukan pada topologi jaringan sesuai dengan gambar 3.7 pada Bab III. Sebelum simulasi serangan DDoS dijalankan pada topologi jaringan ini, maka terlebih dahulu dilakukan pengambilan data kondisi sebelum serangan, untuk nantinya dibandingkan dengan kondisi ketika serangan DDoS jenis UDP dan Http Flood berlangsung. Uji coba serangan DDoS jenis UDP Flood dan Http Flood dengan topologi jaringan menggunakan Intrusion Detection System, Firewall Server Based dan Load Balancer, dimana pada ujicoba ini topologi jaringan berubah signifikan dibandingkan dengan topologi existing LPSE, dan topologi dengan menggunakan IDS dan Honeypot.

4.4.1. Hasil Uji Coba Fungsionalitas dan Performansi Kondisi Sebelum Serangan.

Sebelum simulasi serangan DDoS dijalankan pada infrastruktur jaringan LPSE yang ketiga, atau pada topologi yang menggunakan Intrusion Detection System, Firewall Server Based dan Load Balancer, maka terlebih dahulu dilakukan uji coba performansi dan fungsionalitas pada perangkat-perangkat pada infrastruktur LPSE, untuk pengambilan data pada kondisi sebelum serangan, dimana nantinya data tersebut akan dibandingkan dengan data pada kondisi ketika serangan DDoS jenis UDP dan Http Flood berlangsung, hal ini penting dilakukan karena topologi jaringan yang berubah.



Rate Step	50	100	150	200	250	300	350	400	450	500
Request Rate	50	100	150	200	250	300	350	400	450	500
Response Time (ms)	0,9	0,8	0,8	0,8	0,7	0,8	0,8	0,7	0,7	0,7
Error	0	0	0	0	0	0	0	0	0	0

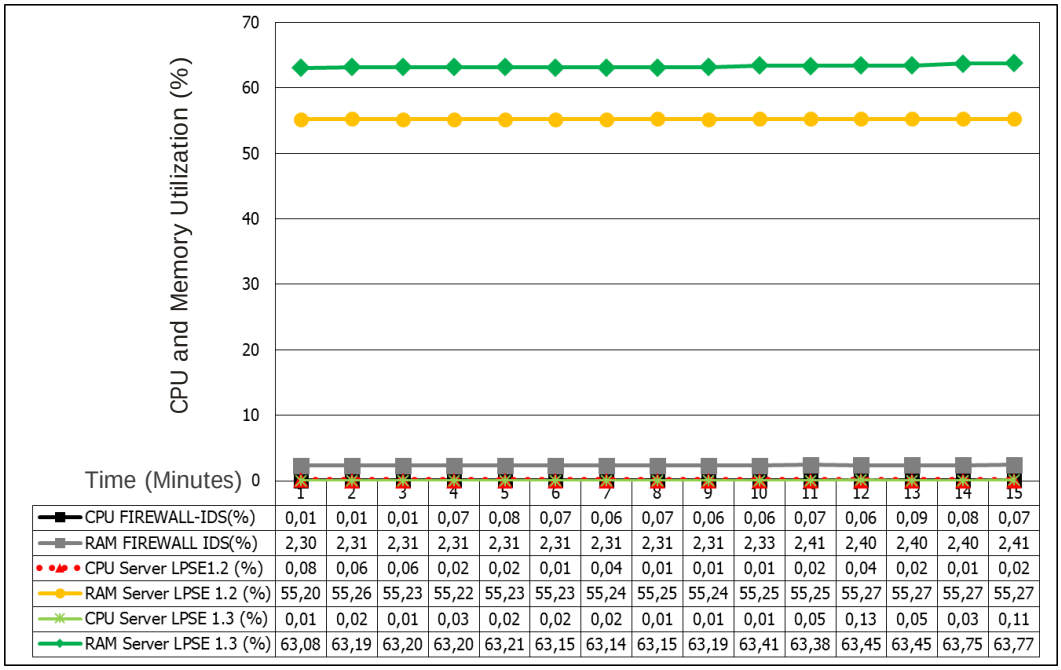
Gambar 4.39 Chart Data Performansi Web Server LPSE Kondisi Sebelum Serangan DDoS

Pada gambar chart 4.39 dapat dilihat pada kondisi sebelum serangan, request rate terhadap web server LPSE adalah sesuai dengan request rate yang telah ditentukan yaitu dari 50 sampai dengan 500 request/s dengan penambahan 50 request setiap rate, sementara response times terhadap request masih tergolong kecil dan tidak terdapat error. Meski demikian jika dibandingkan dengan response times pada topologi jaringan existing terdapat perbedaan sangat kecil pada 50 request terhadap web server LPSE pada topologi existing hanya memakan waktu 0,8 ms sedangkan dengan skenario topologi IDS, Firewall dan Honeypot meningkat menjadi 0,9 ms.

Pengukuran performansi web server LPSE menggunakan aplikasi Httperf dengan parameter sebagai berikut :

Parameter Tool Httperf :

- Target Port = 80
- Target Host = 192.168.9.3
- Minimum Request Rate = 50
- Penambahan Request Rate = 50
- Maximum Request Rate = 500
- Numm Conns = 500
- Timeout = 5 Second



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CPU FIREWALL-IDS(%)	0,01	0,01	0,01	0,07	0,08	0,07	0,06	0,07	0,06	0,06	0,07	0,06	0,09	0,08	0,07
RAM FIREWALL IDS(%)	2,30	2,31	2,31	2,31	2,31	2,31	2,31	2,31	2,31	2,33	2,41	2,40	2,40	2,40	2,41
CPU Server LPSE1.2 (%)	0,08	0,06	0,06	0,02	0,02	0,01	0,04	0,01	0,01	0,01	0,02	0,04	0,02	0,01	0,02
RAM Server LPSE 1.2 (%)	55,20	55,26	55,23	55,22	55,23	55,23	55,24	55,25	55,24	55,25	55,25	55,27	55,27	55,27	55,27
CPU Server LPSE 1.3 (%)	0,01	0,02	0,01	0,03	0,02	0,02	0,02	0,01	0,01	0,01	0,05	0,13	0,05	0,03	0,11
RAM Server LPSE 1.3 (%)	63,08	63,19	63,20	63,20	63,21	63,15	63,14	63,15	63,19	63,41	63,38	63,45	63,45	63,75	63,77

Gambar 4.40 Chart Data Log Penggunaan CPU dan Memory Kondisi Sebelum serangan DDoS

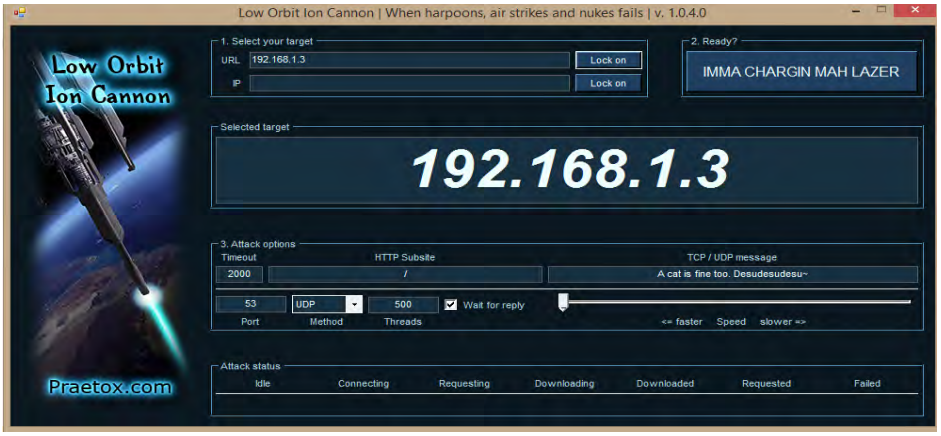
Pada gambar chart 4.40 diatas dapat dilihat dalam kondisi sebelum serangan pada topologi ini, penggunaan CPU pada masing-masing perangkat seperti pada Server Firewall, Load Balancer dan Server LPSE tergolong kecil, namun demikian dalam kondisi normal atau sebelum serangan penggunaan RAM Server LPSE justru rata-rata lebih dari 50% hal tersebut disebabkan oleh aplikasi-aplikasi pendukung SPSE yang berjalan sejak sistem operasi mulai, aplikasi-aplikasi tersebut yaitu antara lain,

Apache, Java dan Aplikasi SPSE sendiri, sedangkan RAM Server IDS-Firewall dalam kondisi normal hanya menggunakan RAM yang kecil yaitu rata-rata diatas 2% meskipun terdapat aplikasi IDS –Suricata yang sedang berjalan.

4.4.2. Hasil Uji Coba Performansi dan Fungsionalitas dengan kondisi Jaringan Serangan DDoS Jenis UDP Flood

Dalam ujicoba serangan DDoS-UDP Flood pada topologi jaringan ini, 2 unit client dan 1 unit server bertindak sebagai attacker/penyerang. Dua PC client menggunakan tools DDoS aplikasi LOIC v.1.0.4.0 dikombinakasikan dengan script UDP DDoS yang dicompile dengan aplikasi GNU Compiler Collection dan dijalankan pada Attacker server, dengan parameter-parameter serangan sebagai berikut :

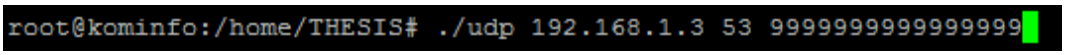
- Parameter Loic pada PC Client:
  - Target IP address = 192.168.1.3
  - Port = 53
  - Type Serangan = UDP Flood
  - Threads = 500
  - Timeout = 2000



Gambar 4.41 Parameter Serangan DDoS UDP Flood dengan Aplikasi LOIC

- Parameter Script DDoS - UDP Flood yang dicompile dengan aplikasi GCC:
  - IP address = 192.168.1.3

- Port = 53
- Type Serangan = UDP Flood
- Spoffed IP = 9999999999999999

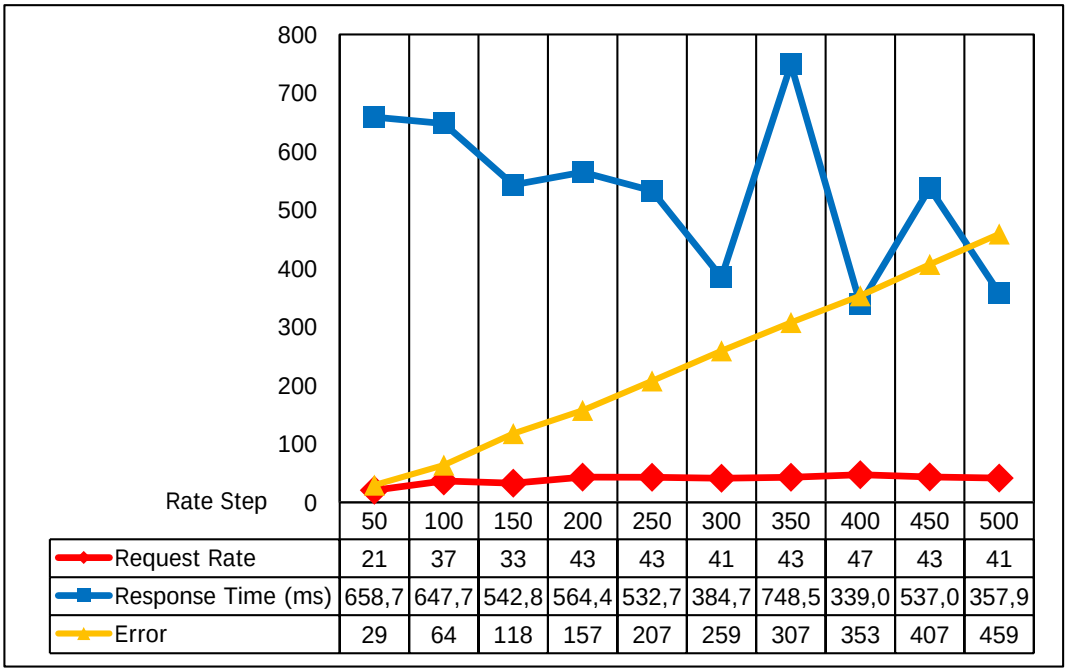


Gambar 4.42 Parameter Serangan dengan Script UDP DDoS Pada Attacker Server

Hasilnya pada gambar Chart 4.43 dibawah ini, menunjukkan data yang diambil dari aplikasi Httperf pada real client ke web server LPSE, pada 500 request ke web server LPSE, hanya terdapat 41 request yang dapat direspon, response times terhadap request memakan waktu jauh lebih lama dari kondisi sebelum serangan yaitu minimal 339 ms dan maximal 658,7 ms.

Terdapat sejumlah erorr request pada setiap request rate, seperti pada 500 request rate ke web server LPSE terdapat erorr sejumlah 459. hasil ini tergolong kurang baik pada kondisi infrastruktur jaringan LPSE yang sedang mengalami serangan DDoS jenis UDP Flood. Pengukuran performansi web server LPSE menggunakan aplikasi Httperf pada saat serangan DDoS jenis UDP Flood berlangsung, dengan parameter-parameter sebagai berikut :

- Target Port = 80
- Target Host = 192.168.1.3
- Minimum Request Rate = 50
- Penambahan Request Rate = 50
- Maximum Request Rate = 500
- Num Conns = 500
- Timeout = 5 Second

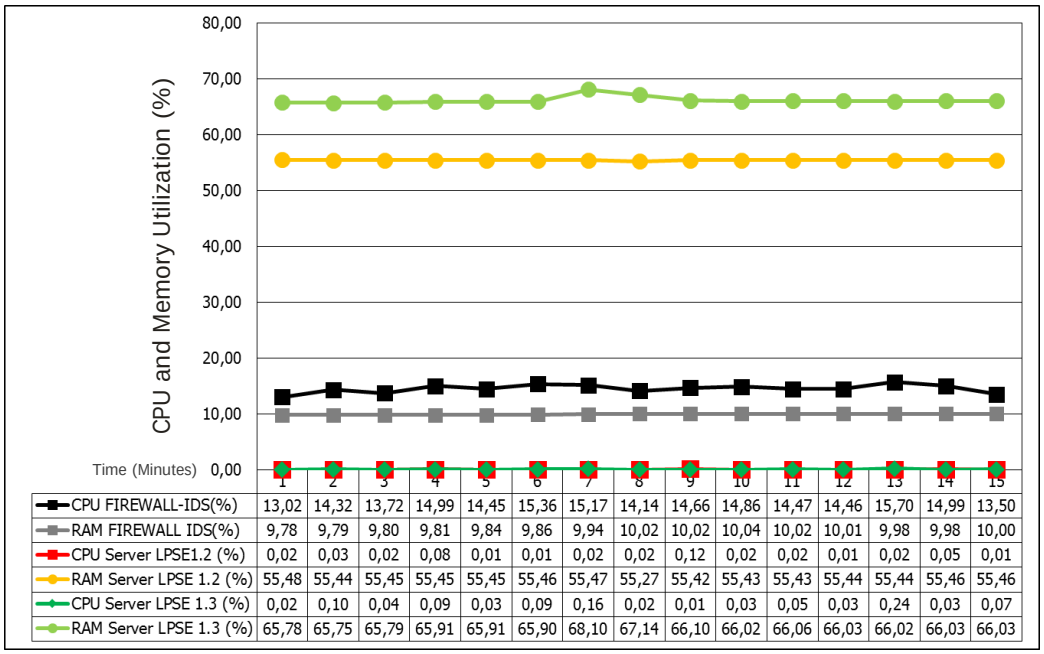


Rate Step	50	100	150	200	250	300	350	400	450	500
Request Rate	21	37	33	43	43	41	43	47	43	41
Response Time (ms)	658,7	647,7	542,8	564,4	532,7	384,7	748,5	339,0	537,0	357,9
Error	29	64	118	157	207	259	307	353	407	459

Gambar 4.43 Chart Data Performansi Web Server LPSE Kondisi Serangan DDoS UDP Flood Berlangsung

Sementara data penggunaan CPU dan Memory perangkat-perangkat yang terdapat pada infrastruktur LPSE dapat dilihat pada gambar chart 4.34 dibawah ini, yang menunjukkan penurunan performansi yang cukup signifikan jika dibandingkan dengan kondisi sebelum serangan, penggunaan CPU pada Server Firewall-IDS adalah max 0,19% dan setelah serangan DDoS-UDP Flood berlangsung menjadi maximal 15,70 %, penggunaan Ram Server Firewall IDS dari maximal 2,38 % menjadi Maximal 10,04, penggunaan CPU Server LPSE 1 tidak mengalami peningkatan yaitu maximal 0,08 %, penggunaan RAM Server LPSE 1 tidak mengalami peningkatan signifikan yaitu rata-rata diatas 55% penggunaan CPU Server LPSE 2 yaitu rata-rata 0,07 %, penggunaan RAM server LPSE 2 rata-rata 66,17%.

Dalam ujicoba simulasi serangan DDoS-UDP Flood ini, pengguna yang sah/real client dapat mengakses dan menggunakan aplikasi SPSE pada web server LPSE dengan waktu yang lebih lama.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CPU FIREWALL-IDS(%)	13,02	14,32	13,72	14,99	14,45	15,36	15,17	14,14	14,66	14,86	14,47	14,46	15,70	14,99	13,50
RAM FIREWALL IDS(%)	9,78	9,79	9,80	9,81	9,84	9,86	9,94	10,02	10,02	10,04	10,02	10,01	9,98	9,98	10,00
CPU Server LPSE1.2 (%)	0,02	0,03	0,02	0,08	0,01	0,01	0,02	0,02	0,12	0,02	0,02	0,01	0,02	0,05	0,01
RAM Server LPSE 1.2 (%)	55,48	55,44	55,45	55,45	55,45	55,46	55,47	55,27	55,42	55,43	55,43	55,44	55,44	55,46	55,46
CPU Server LPSE 1.3 (%)	0,02	0,10	0,04	0,09	0,03	0,09	0,16	0,02	0,01	0,03	0,05	0,03	0,24	0,03	0,07
RAM Server LPSE 1.3 (%)	65,78	65,75	65,79	65,91	65,91	65,90	68,10	67,14	66,10	66,02	66,06	66,03	66,02	66,03	66,03

Gambar 4.44 Chart Data Log Penggunaan CPU dan Memory Kondisi Serangan DDoS UDP Flood Berlangsung

Hasil yang diperoleh pada uji coba ini dapat dikategorikan kurang baik, dimana pada gambar 4.45 dibawah ini, dapat dilihat IDS Suricata mengenali paket-paket yang dikategorikan sebagai DDoS namun firewall tidak bekerja maximal.

```
04/26/2016-03:26:52.580375  [**] [1:2014701:11] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS
port Opcode 6 or 7 set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] {UDP} 192.168.2.5:35941 -> 192.168.1.3:53

04/26/2016-03:27:00.793091  [**] [1:2014702:8] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS
port Opcode 8 through 15 set - Likely Kazy [**] [Classification: Potential Corporate Privacy
Violation] [Priority: 1] {UDP} 192.168.2.3:51915 -> 192.168.1.3:53

04/26/2016-03:31:00.000025  [**] [1:2014702:8] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS
port Opcode 8 through 15 set - Likely Kazy [**] [Classification: Potential Corporate Privacy
Violation] [Priority: 1] {UDP} 192.168.2.4:54227 -> 192.168.1.3:53

04/26/2016-03:31:00.000025  [**] [1:2014703:8] ET DNS Non-DNS or Non-Compliant DNS traffic on DNS
port Reserved Bit Set - Likely Kazy [**] [Classification: Potential Corporate Privacy Violation]
[Priority: 1] {UDP} 192.168.2.4:54227 -> 192.168.1.3:53
```

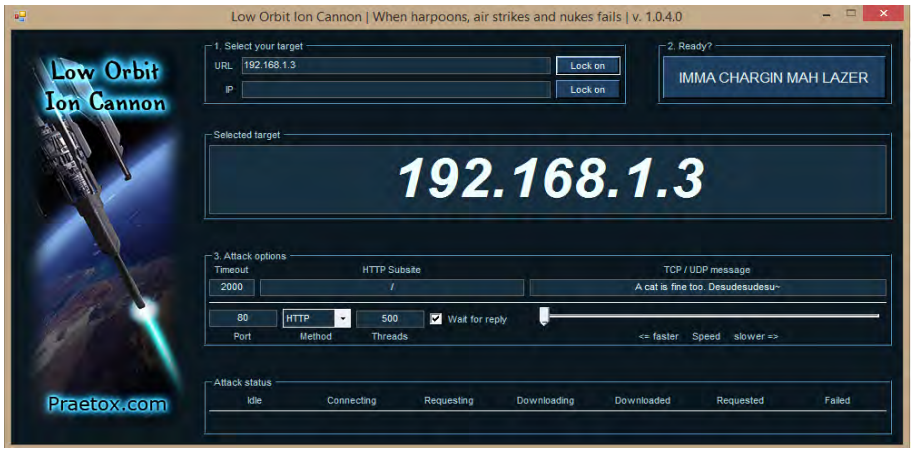
Gambar 4.45 Data Log IDS-Suricata Mendeteksi Sumber IP dan Jenis Serangan DDoS UDP Flood.

Meskipun IDS-Suricata dan Firewall IPTables memeriksa dan dapat mengenali paket-paket DDoS namun pada kenyataannya Firewall Iptables tidak dapat memitigasi paket-paket DDoS UDP Flood dengan baik hal tersebut dapat dilihat pada performansi Web Server LPSE selama serangan DDoS UDP Flood berlangsung.

4.4.3. Hasil Uji Coba Performansi Kondisi Sebelum Serangan DDoS Jenis Http Flood.

Dalam ujicoba serangan DDoS-Http Flood pada topologi jaringan ini, 2 unit client dan 1 unit server bertindak sebagai attacker/penyerang. 2 client attacker menggunakan tools DDoS aplikasi LOIC v.1.0.4.0 dikombinakasikan dengan aplikasi DDoS Http Flood slowloris yang dijalankan pada Attacker server, dengan parameter-parameter serangan sebagai berikut :

- Parameter Loic :
  - Target IP address = 192.168.1.3
  - Port = 80
  - Type Serangan = Http Flood
  - Threads = 500
  - Timeout = 2000



Gambar 4.46 Parameter Serangan DDoS Http Flood dengan Aplikasi LOIC

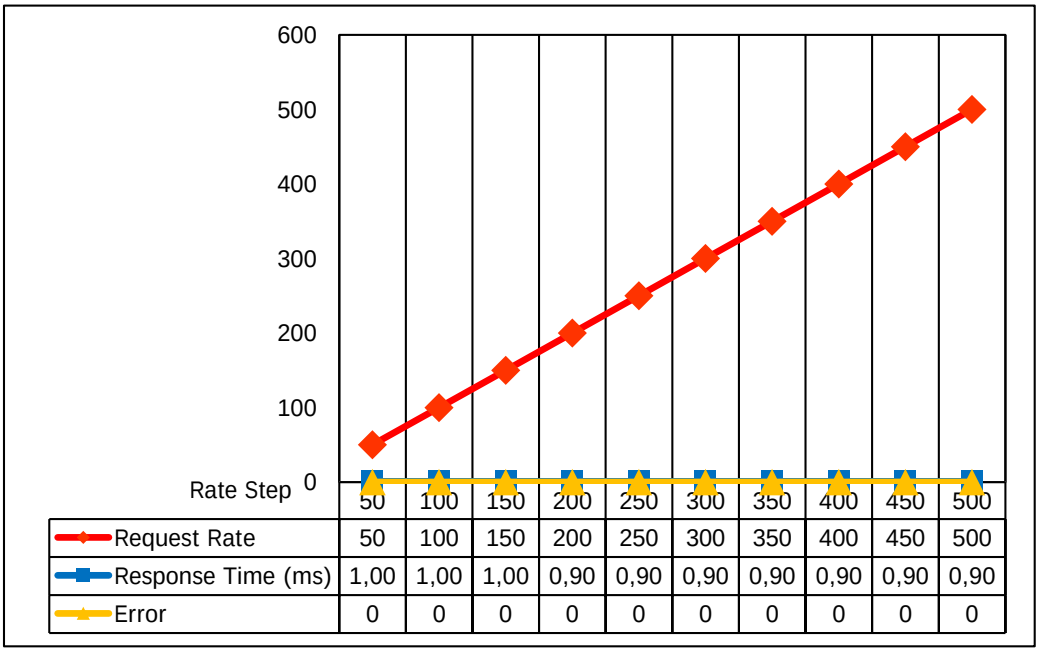
- Parameter Script DDoS Http Flood Slowloris :
  - IP address = 192.168.1.3
  - Port = 80
  - Type Serangan = Http Flood
  - Timeout = 2000
  - Num = 500
  - Tcpto = 5

```
root@kominfo:/home/THESIS# ./slowloris.pl -dns 192.168.1.3 -port 80 -timeout 2000 -num 500 -tcpto 5
```

Gambar 4.47 Parameter Serangan DDoS Http Flood dengan Aplikasi Slowloris

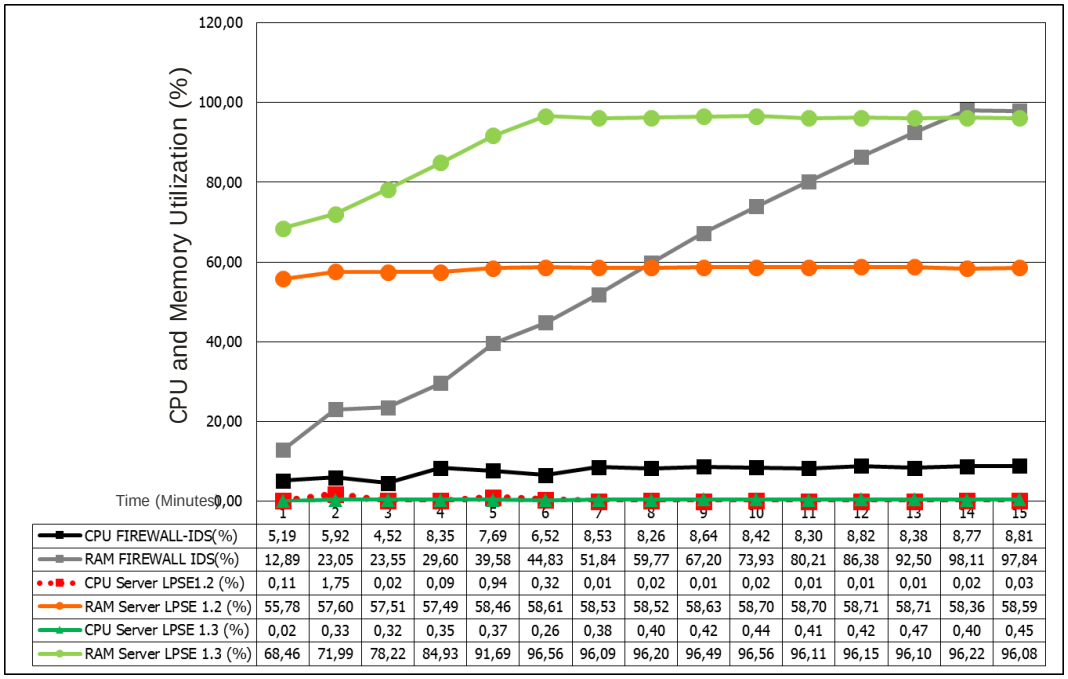
Hasilnya pada gambar Chart 4.38 dibawah ini, menununjukkan request ke web server LPSE sesuai dengan request rate yang telah ditentukan, response time Web Server LPSE terhadap request rata-rata 0,93 ms, dan tidak terdapat erorr pada request. Hasil ini tergolong baik dalam kondisi infrastruktur jaringan LPSE yang sedang mengalami serangan DDoS Jenis Http Flood. Pengukuran performansi web server LPSE menggunakan aplikasi Httperf pada saat serangan DDoS jenis Http Flood berlangsung, dengan parameter-parameter sebagai berikut :

- Target Port = 80
- Target Host = 192.168.1.3
- Minimum Request Rate = 50
- Penambahan Request Rate = 50
- Maximum Request Rate = 500
- Num Conns = 500
- Timeout = 5 Second



Rate Step	50	100	150	200	250	300	350	400	450	500
Request Rate	50	100	150	200	250	300	350	400	450	500
Response Time (ms)	1,00	1,00	1,00	0,90	0,90	0,90	0,90	0,90	0,90	0,90
Error	0	0	0	0	0	0	0	0	0	0

Gambar 4.48 Chart Data Performansi Web Server LPSE Kondisi Serangan DDoS Http Flood Berlangsung



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CPU FIREWALL-IDS(%)	5,19	5,92	4,52	8,35	7,69	6,52	8,53	8,26	8,64	8,42	8,30	8,82	8,38	8,77	8,81
RAM FIREWALL IDS(%)	12,89	23,05	23,55	29,60	39,58	44,83	51,84	59,77	67,20	73,93	80,21	86,38	92,50	98,11	97,84
CPU Server LPSE1.2 (%)	0,11	1,75	0,02	0,09	0,94	0,32	0,01	0,02	0,01	0,02	0,01	0,01	0,01	0,02	0,03
RAM Server LPSE 1.2 (%)	55,78	57,60	57,51	57,49	58,46	58,61	58,53	58,52	58,63	58,70	58,70	58,71	58,71	58,36	58,59
CPU Server LPSE 1.3 (%)	0,02	0,33	0,32	0,35	0,37	0,26	0,38	0,40	0,42	0,44	0,41	0,42	0,47	0,40	0,45
RAM Server LPSE 1.3 (%)	68,46	71,99	78,22	84,93	91,69	96,56	96,09	96,20	96,49	96,56	96,11	96,15	96,10	96,22	96,08

Gambar 4.49 Chart Data Penggunaan CPU dan Memory Kondisi Serangan DDoS Http Flood Berlangsung

Data penggunaan CPU dan Memory perangkat-perangkat yang terdapat pada infrastruktur LPSE dapat dilihat pada gambar chart 4.40, yang menunjukkan peningkatan penggunaan khususnya RAM, penggunaan RAM Server Firewall IDS mencapai 97,84 %, penggunaan RAM Server LPSE 2 mencapai 96,56 %, Sementara penggunaan CPU Server Firewall-IDS pun mengalami peningkatan dari kondisi sebelum serangan dari maximal 2,41% menjadi 8,82%, meski demikian penggunaan CPU pada Server LPSE 1 dan 2 tidak mengalami peningkatan yang signifikan, Dalam ujicoba simulasi serangan DDoS jenis Http Flood ini, pengguna yang sah/real client dapat mengakses dan menggunakan aplikasi SPSE pada web server LPSE dengan dengan normal.

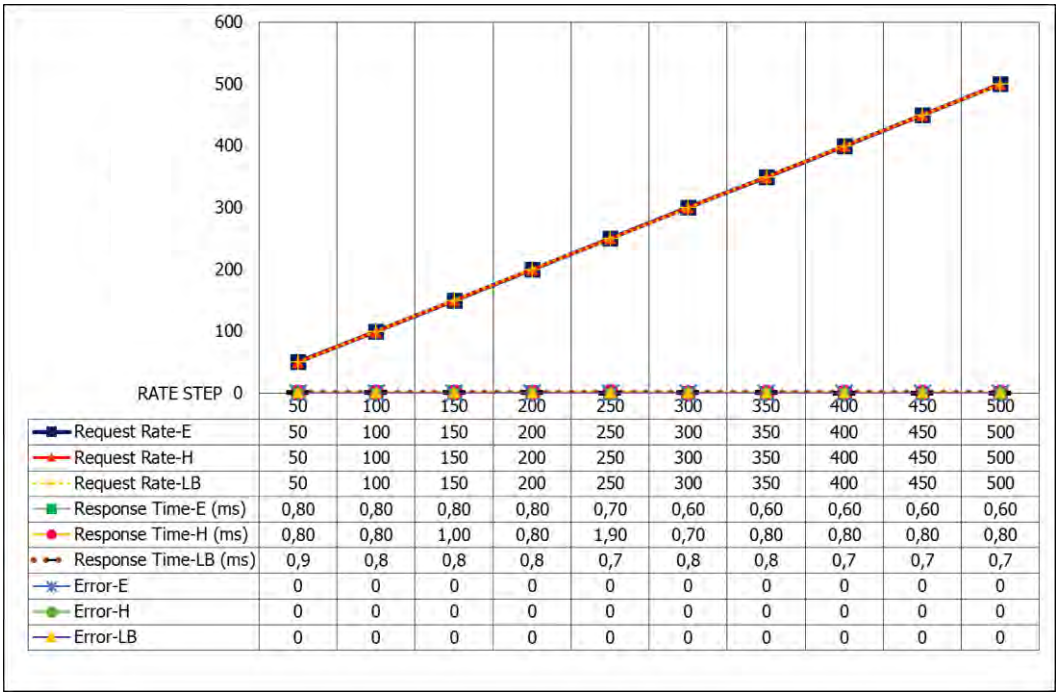
Hasil yang diperoleh pada uji coba ini dapat dikategorikan cukup baik, dimana IDS Suricata dapat mengenali paket-paket yang merupakan paket DDoS Http Flood, seperti pada gambar 4.40 dari log sampel IDS –Suricata dibawah ini menunjukan bahwa paket-paket yang dicurigai sebagai paket DDoS Http-Flood dapat diidentifikasi oleh IDS Suricata kemudian di integrasi ke firewall untuk di blok.

```
04/26/2016-04:25:02.194723  [**] [1:2012708:2] ET WEB_SERVER HTTP 414 Request URI Too Large [**]
[Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.1.3:80 -> 192.168.2.4:49185

04/26/2016-04:26:56.260728 [**] [1:2012708:2] ET WEB_SERVER HTTP 414 Request URI Too Large [**]
[Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.1.3:80 -> 192.168.2.3:49193

04/26/2016-04:27:08.266507  [**] [1:2100366:8] GPL ICMP_INFO PING *NIX [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 192.168.2.5:8 -> 192.168.1.3:0
```

Gambar 4.50 Data Log IDS Suricata Mendeteksi IP Sumber dan Jenis Serangan Http Flood

4.5. Hasil Perbandingan Performansi Web Server pada Tiga topologi Jaringan, kondisi serangan DDoS UDP Flood berlangsung.

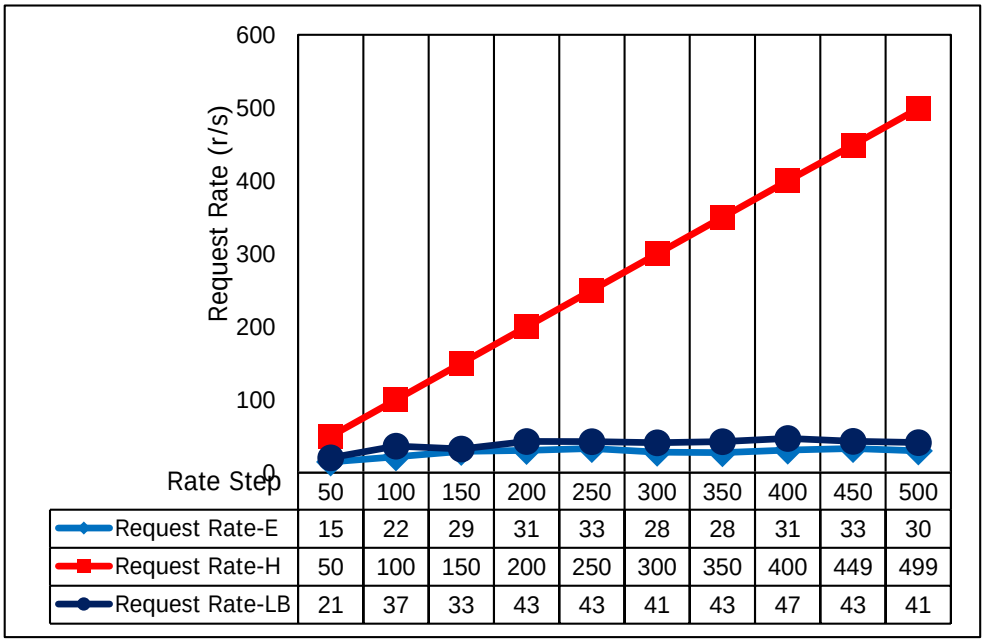
Sebelum dilakukan uji coba serangan DDoS, pengukuran Performansi Web Server LPSE dilakukan dengan menggunakan aplikasi Httperf. Dimana nantinya data tersebut akan dibandingkan dengan data setelah serangan DDoS berlangsung pada ke tiga topologi jaringan yang berbeda. Pada Gambar Chart 4.42 dibawah ini terlihat gambaran performansi Web Server LPSE kondisi sebelum serangan DDoS berlangsung.



RATE STEP	50	100	150	200	250	300	350	400	450	500
Request Rate-E	50	100	150	200	250	300	350	400	450	500
Request Rate-H	50	100	150	200	250	300	350	400	450	500
Request Rate-LB	50	100	150	200	250	300	350	400	450	500
Response Time-E (ms)	0,80	0,80	0,80	0,80	0,70	0,60	0,60	0,60	0,60	0,60
Response Time-H (ms)	0,80	0,80	1,00	0,80	1,90	0,70	0,80	0,80	0,80	0,80
Response Time-LB (ms)	0,9	0,8	0,8	0,8	0,7	0,8	0,8	0,7	0,7	0,7
Error-E	0	0	0	0	0	0	0	0	0	0
Error-H	0	0	0	0	0	0	0	0	0	0
Error-LB	0	0	0	0	0	0	0	0	0	0

Gambar 4.51 Chart Data Performansi Web Server LPSE pada tiga Topologi, Kondisi Sebelum Serangan (E=Existing Network, H=With Honeypott, LB=With Load Balancer)

Pada gambar chart 4.51 diatas terlihat Request Rate Web Server LPSE sesuai dengan nilai request yang ditentukan pada tiga topologi yang berbeda, selanjutnya Reponse times Web Server LPSE pada topologi Existing memiliki waktu lebih sedikit dengan rata-rata 0,69 ms dan mencapai 0,80 ms, pada topologi kedua atau topologi dengan menggunakan Firewall Server Based, IDS dan Honeypot server memiliki Response Time 0,92% dan mencapai 1,90% dan pada topologi ketiga atau topologi dengan menggunakan Firewall Server Based, IDS dan Load Balancer memiliki Response Time 0,77% dan mencapai 0,80%, sedangkan Error Request tidak terdapat pada ketiga topologi tersebut.

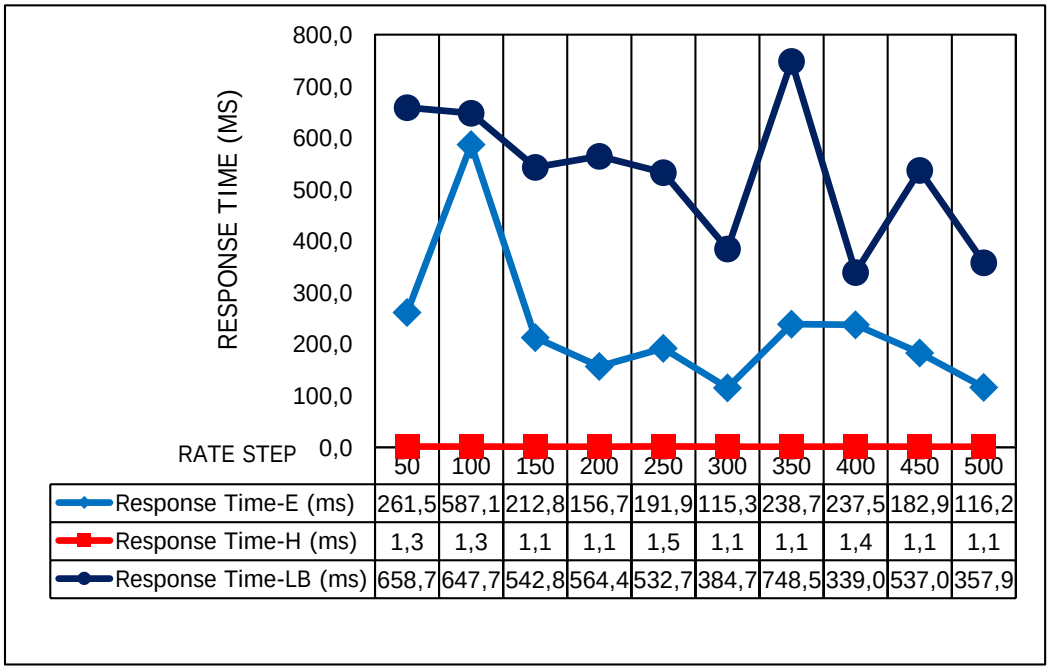


Rate Step	50	100	150	200	250	300	350	400	450	500
Request Rate-E	15	22	29	31	33	28	28	31	33	30
Request Rate-H	50	100	150	200	250	300	350	400	449	499
Request Rate-LB	21	37	33	43	43	41	43	47	43	41

Gambar 4.52 Chart Data Request Rate Web Server LPSE pada Tiga Topologi, Kondisi Serangan DDoS UDP Flood Berlangsung (E=Existing Network, H=With Honeypot, LB=With Load Balancer)

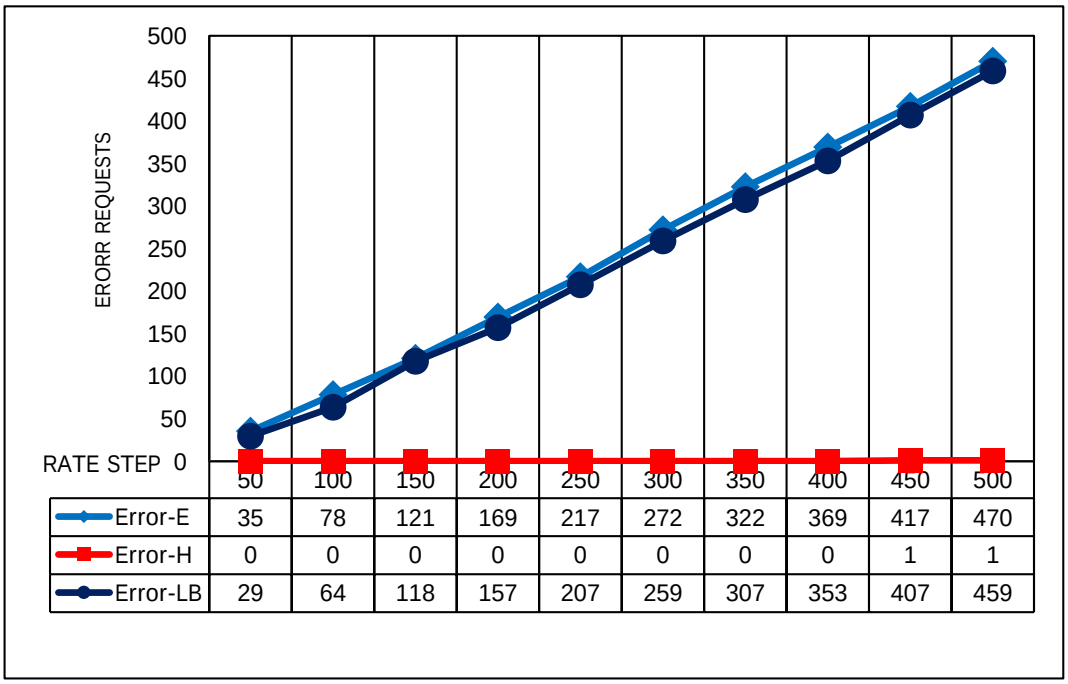
Pada gambar chart 4.52 terlihat pada topologi jaringan yang kedua atau yang menggunakan Honeypot LPSE Web server memiliki request rate yang paling tinggi atau hampir sesuai dengan request rate yang telah ditentukan, pada kondisi serangan DDoS UDP Flood berlangsung, sedangkan pada Topologi jaringan Existing dan Topologi ke tiga atau topologi yang menggunakan Load Balancer memiliki request rate yang lebih rendah dari jumlah request rate yang telah ditentukan, meski

demikian request rate pada Topologi yang ke tiga memiliki request rate yang lebih tinggi dibandingkan dengan topologi jaringan existing.



Gambar 4.53 Chart Response Time Web Server LPSE pada ke 3 Topologi (E=Existing Network, H=With Honeypot, LB=With Load Balancer) Kondisi Serangan DDOs UDP Flood Berlangsung

Pada gambar chart 4.53, terlihat pada topologi jaringan yang kedua atau yang menggunakan Honeypot, Web Server LPSE memiliki Response Time yang memakan waktu paling sedikit dengan kondisi serangan DDoS UDP Flood berlangsung, sedangkan pada topologi jaringan Existing dan Topologi ke tiga atau topologi yang menggunakan Load Balancer, Web Server LPSE memiliki response times memakan waktu yang lebih lama. Namun demikian response times pada topologi jaringan Existing memiliki Response time yang lebih baik dibandingkan dengan topologi Jaringan dengan menggunakan Load Balancer pada kondisi serangan DDoS jenis UDP flood berlangsung pada infrastruktur LPSE.

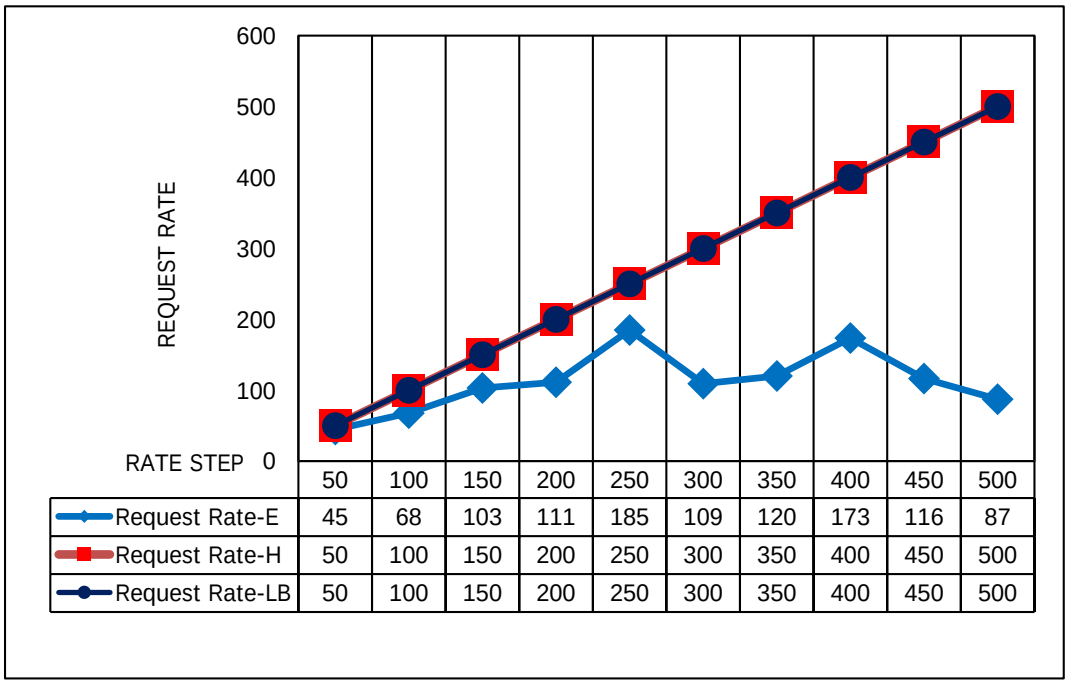


Gambar 4.54 Chart Data Error Requests Web Server LPSE pada Tiga Topologi Kondisi Serangan DDoS UDP Flood Berlangsung (E=Existing Network, H=With Honeypot, LB=With Load Balancer)

Pada gambar chart 4.54 diatas, terlihat pada topologi jaringan yang kedua atau yang menggunakan Honeypot, Web Server LPSE memiliki Erorr requests yang paling sedikit, yaitu pada 450 dan 500 request hanya terdapat erorr masing-masing 1 dalam kondisi serangan DDoS UDP Flood berlangsung, sedangkan pada topologi jaringan Existing dan topologi ke tiga atau topologi yang menggunakan Load Balancer, Web Server LPSE memiliki erorr requests yang lebih tinggi, yaitu pada setiap request rate terdapat erorr, seperti pada 500 request rate ke Web Server LPSE pada topologi jaringan Existing terdapat 470 erorr sedangkan pada topologi yang menggunakan Load Balancer terdapat 459 erorr. Jumlah erorr request pada topologi jaringan Existing lebih tinggi dibandingkan dengan topologi jaringan yang menggunakan Load Balancer.

4.6. Hasil Perbandingan Performansi Web Server pada Tiga topologi Jaringan, kondisi serangan DDoS Http Flood berlangsung.

Pada gambar chart 4.55 dibawah ini, terlihat pada topologi jaringan yang kedua atau yang menggunakan Honeypot dan topologi yang ke tiga dengan menggunakan Load Balancer, LPSE web server memiliki request rate yang paling tinggi atau sesuai dengan request rate real dengan kondisi serangan DDoS Http Flood berlangsung, sedangkan pada Topologi jaringan Existing, Web Server LPSE memiliki request rate yang lebih rendah dari jumlah request rate yang telah ditentukan, sebagai contoh pada 500 request rate hanya 87 request yang dapat di proses dalam kondisi serangan DDoS jenis Http Flood berlangsung.

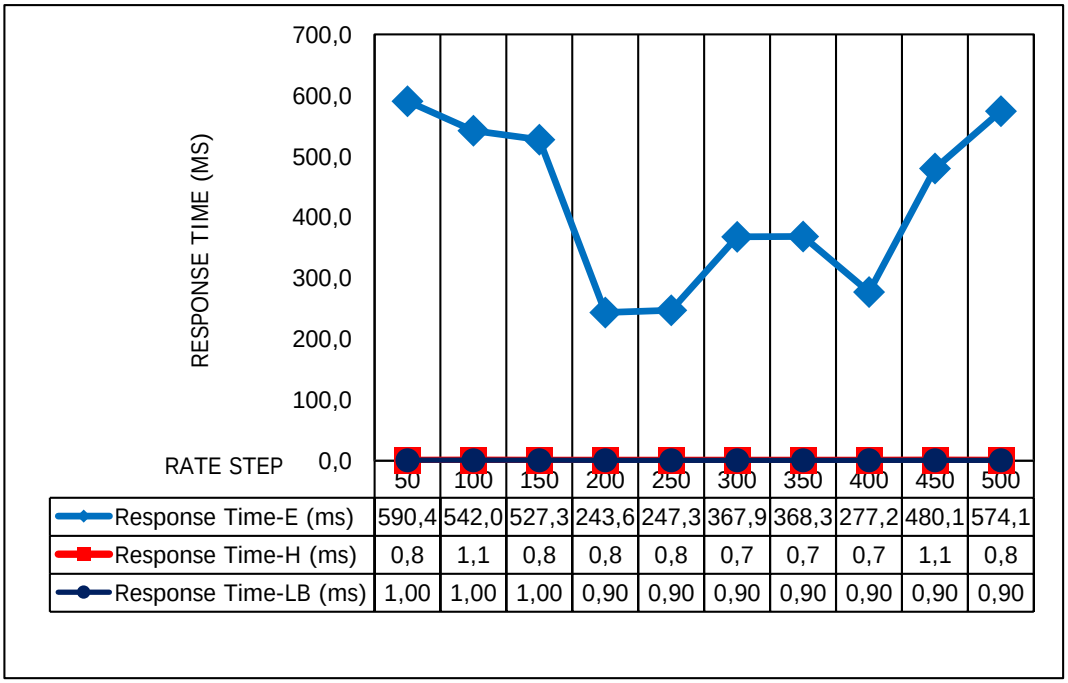


RATE STEP	50	100	150	200	250	300	350	400	450	500
Request Rate-E	45	68	103	111	185	109	120	173	116	87
Request Rate-H	50	100	150	200	250	300	350	400	450	500
Request Rate-LB	50	100	150	200	250	300	350	400	450	500

Gambar 4.55 Chart Request Rate Web Server LPSE pada Tiga Topologi (E=Existing Network, H=With Honeypot, LB=With Load Balancer)

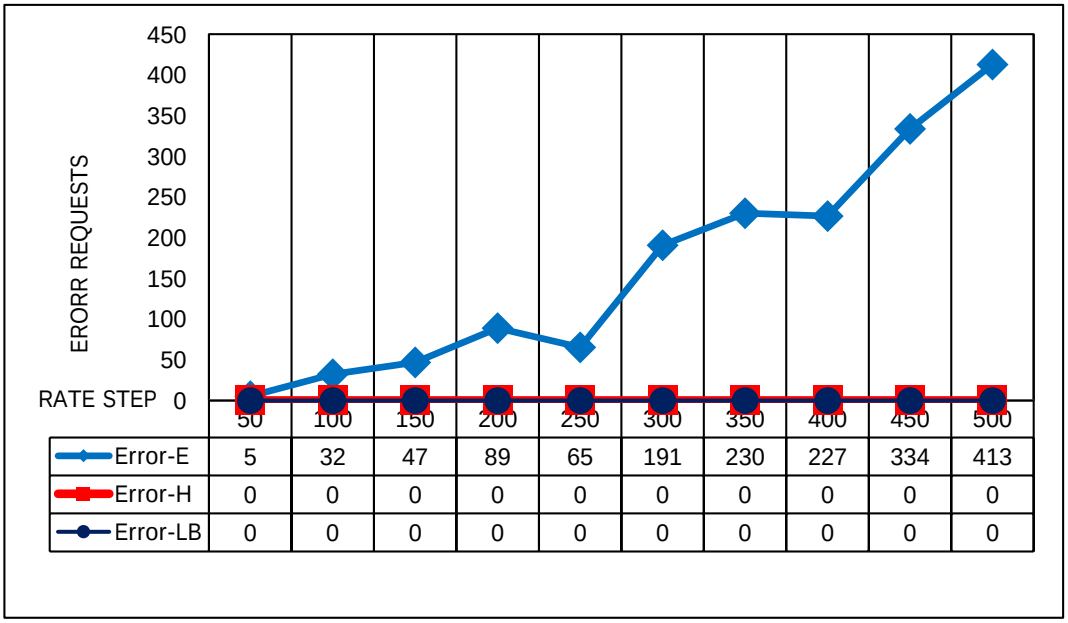
Selanjutnya pada gambar chart 4.56 dibawah ini, terlihat dalam kondisi serangan DDoS Http Flood berlangsung Response Time Web server LPSE, memakan waktu paling sedikit pada topologi jaringan yang menggunakan Honeypot, yaitu rata-rata 0,83 ms dan pada topologi ke tiga atau topologi yang menggunakan Load Balancer

rata-rata 0,93 ms, sedangkan pada Topologi jaringan Existing memiliki response times yang lebih lama yaitu rata-rata 421,8 ms.



RATE STEP	50	100	150	200	250	300	350	400	450	500
Response Time-E (ms)	590,4	542,0	527,3	243,6	247,3	367,9	368,3	277,2	480,1	574,1
Response Time-H (ms)	0,8	1,1	0,8	0,8	0,8	0,7	0,7	0,7	1,1	0,8
Response Time-LB (ms)	1,00	1,00	1,00	0,90	0,90	0,90	0,90	0,90	0,90	0,90

Gambar 4.56 Chart Response Times Web Server LPSE pada Tiga Topologi (E=Existing Network, H=With Honeypot, LB=With Load Balancer) Kondisi Serangan DDOs Http Flood Berlangsung



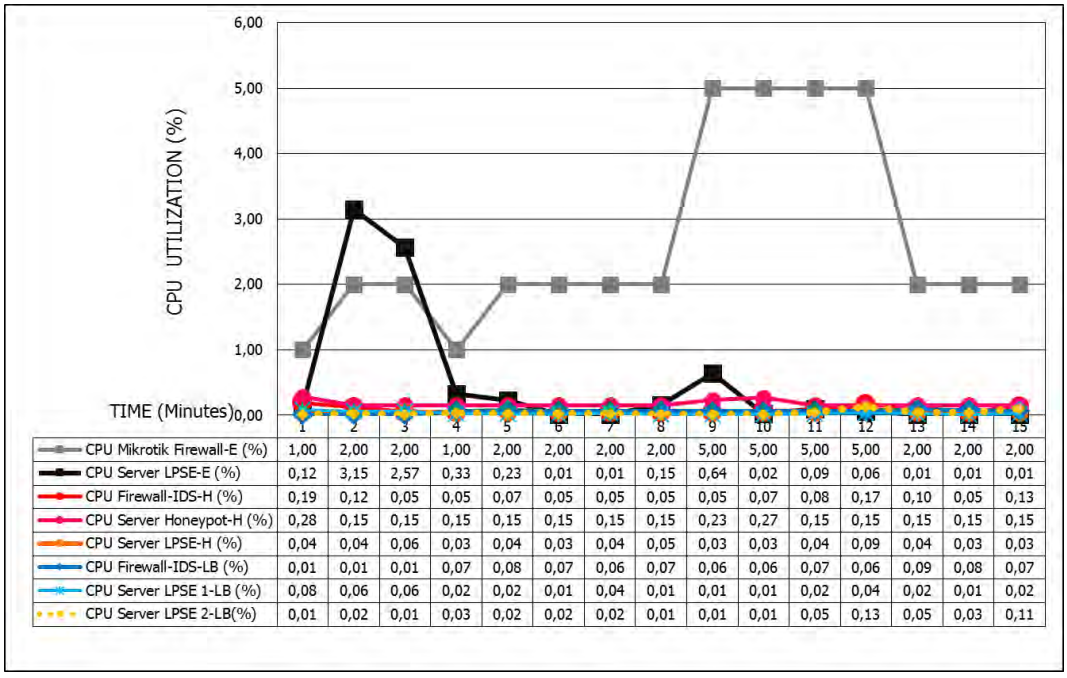
RATE STEP	50	100	150	200	250	300	350	400	450	500
Error-E	5	32	47	89	65	191	230	227	334	413
Error-H	0	0	0	0	0	0	0	0	0	0
Error-LB	0	0	0	0	0	0	0	0	0	0

Gambar 4.57 Chart Error Requests Web Server LPSE pada Tiga Topologi E=Existing Network, H=With Honeypot, LB=With Load Balancer) Kondisi Serangan DDoS Http Flood Berlangsung

Pada gambar chart 4.57 dapat terlihat, pada kondisi jaringan serangan DDoS Http Flood berlangsung, Web Server LPSE tidak memiliki erorr Request pada topologi jaringan yang kedua atau yang menggunakan Honeypot dan topologi ke tiga atau topologi yang menggunakan Load Balancer, sedangkan pada topologi jaringan Existing, Web Server LPSE memiliki Error Requests pada setiap request rate, sebagai contoh pada 500 request rate ke Web Server LPSE terdapat 413 erorr pada topologi jaringan Existing.

4.7. Hasil Perbandingan CPU Utilization Pada Tiga Topologi Jaringan, Kondisi Serangan DDoS UDP Flood berlangsung.

Pada Gambar Chart 4.58 dibawah ini terlihat penggunaan CPU pada masing-masing perangkat di tiga topologi yang berbeda pada kondisi jaringan sebelum serangan DDoS berlangsung.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CPU Mikrotik Firewall-E (%)	1,00	2,00	2,00	1,00	2,00	2,00	2,00	2,00	5,00	5,00	5,00	5,00	2,00	2,00	2,00
CPU Server LPSE-E (%)	0,12	3,15	2,57	0,33	0,23	0,01	0,01	0,15	0,64	0,02	0,09	0,06	0,01	0,01	0,01
CPU Firewall-IDS-H (%)	0,19	0,12	0,05	0,05	0,07	0,05	0,05	0,05	0,05	0,07	0,08	0,17	0,10	0,05	0,13
CPU Server Honeypot-H (%)	0,28	0,15	0,15	0,15	0,15	0,15	0,15	0,15	0,23	0,27	0,15	0,15	0,15	0,15	0,15
CPU Server LPSE-H (%)	0,04	0,04	0,06	0,03	0,04	0,03	0,04	0,05	0,03	0,03	0,04	0,09	0,04	0,03	0,03
CPU Firewall-IDS-LB (%)	0,01	0,01	0,01	0,07	0,08	0,07	0,06	0,07	0,06	0,06	0,07	0,06	0,09	0,08	0,07
CPU Server LPSE 1-LB (%)	0,08	0,06	0,06	0,02	0,02	0,01	0,04	0,01	0,01	0,01	0,02	0,04	0,02	0,01	0,02
CPU Server LPSE 2-LB(%)	0,01	0,02	0,01	0,03	0,02	0,02	0,02	0,01	0,01	0,01	0,05	0,13	0,05	0,03	0,11

Gambar 4.58 Chart Penggunaan CPU perangkat pada Tiga Topologi (E=Existing Network, H=With Honeypot, LB=With Load Balancer) Kondisi Serangan Sebelum Serangan DDoS Berlangsung

Pada Gambar chart 4.58 terlihat pada topologi Existing penggunaan CPU firewall rata-rata 2,67% dan mencapai 5%, sedangkan penggunaan CPU Server LPSE rata-

rata 0,49% dan mencapai 3,15%. Selanjutnya pada topologi kedua yaitu topologi yang menggunakan Firewall Server Based dan Honeypot, penggunaan CPU Server Firewall IDS rata-rata 0,09% dan mencapai 0,19%, penggunaan CPU Server Honeypot rata-rata 0,17% mencapai 0,28%. Selanjutnya CPU Server LPSE tidak mengalami peningkatan penggunaan CPU rata-rata 0,04% dan mencapai 0,09, sedangkan pada topologi ke tiga yaitu pada topologi yang menggunakan IDS, Firewall Server Based dan Load Balancer, menunjukkan penggunaan CPU Firewall IDS rata-rata 0,06% dan mencapai 0,09%, CPU Server LPSE-1 penggunaan CPU rata-rata 0,03% dan mencapai 0,08%, CPU Server LPSE-2 penggunaan CPU rata-rata 0,04% dan mencapai 0,13%.

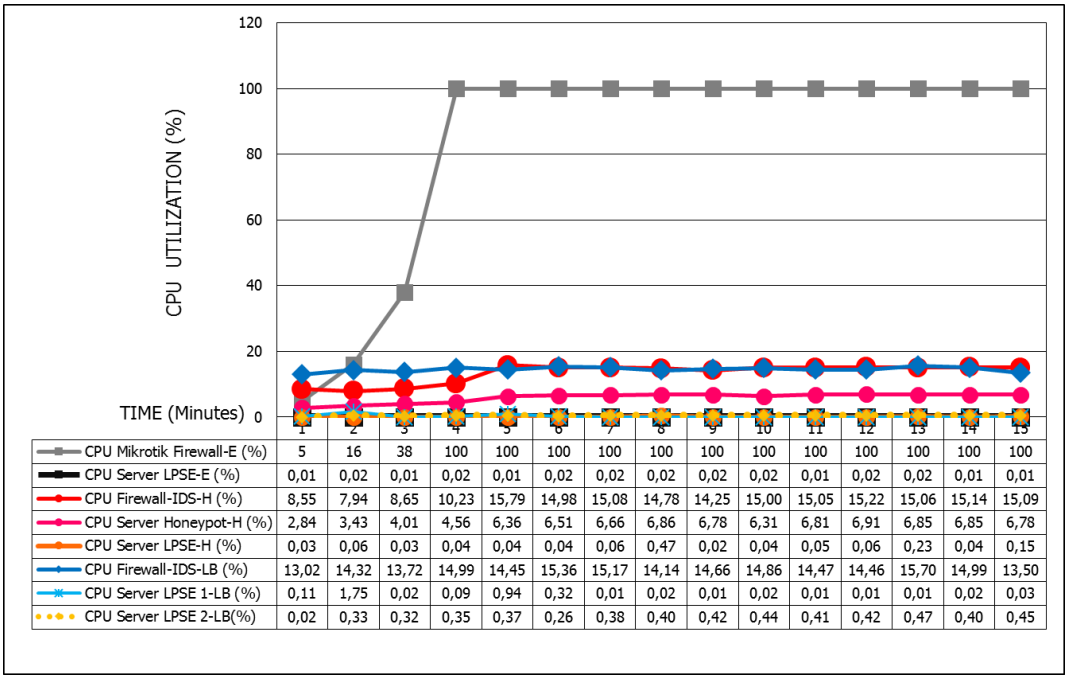
Selanjutnya Terdapat peningkatan penggunaan CPU pada masing-masing perangkat pada ke tiga topologi jaringan selama serangan DDoS UDP Flood berlangsung, Pada gambar Chart 4.50 dibawah ini, terlihat pada topologi Existing terjadi peningkatan penggunaan CPU yang signifikan rata-rata 84% dan mencapai 100% dimana angka ini tergolong sangat tinggi dan melewati ambang batas penggunaan normal CPU, sedangkan penggunaan CPU Server LPSE tidak mengalami peningkatan yaitu rata-rata 0,02%.

Selanjutnya pada topologi kedua yaitu topologi yang menggunakan IDS, Firewall Server Based dan Honeypot, penggunaan CPU Server Firewall rata-rata 13,39% dan mencapai 15,79%, penggunaan CPU Server Honeypot rata-rata 5,90% mencapai 6,91%, sedangkan CPU Server LPSE tidak mengalami peningkatan penggunaan CPU rata-rata 0,09%.

Sedangkan pada topologi ke tiga atau topologi yang menggunakan IDS, Firewall Server Based dan Load Balancer, menunjukkan penggunaan CPU Firewall rata-rata 14,52% dan mencapai 15,70%, CPU Server LPSE-1 tidak mengalami peningkatan penggunaan CPU rata-rata 0,22% dan mencapai 1,75%, CPU Server LPSE-2 tidak mengalami peningkatan penggunaan CPU rata-rata 0,36% dan mencapai 0,47%.

Pada Topologi kedua dan ketiga meskipun terjadi peningkatan penggunaan CPU namun masih dibawah ambang batas normal. Pada setiap topologi tidak terdapat penggunaan CPU yang tinggi pada Server LPSE, hal ini disebabkan oleh Mikrotik

firewall dan Server Firewall yang mengelola dan menerima beban dari lalu lintas paket-paket yang merupakan serangan DDoS UDP Flood.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CPU Mikrotik Firewall-E (%)	5	16	38	100	100	100	100	100	100	100	100	100	100	100	100
CPU Server LPSE-E (%)	0,01	0,02	0,01	0,02	0,01	0,02	0,02	0,02	0,02	0,02	0,01	0,02	0,02	0,01	0,01
CPU Firewall-IDS-H (%)	8,55	7,94	8,65	10,23	15,79	14,98	15,08	14,78	14,25	15,00	15,05	15,22	15,06	15,14	15,09
CPU Server Honeypot-H (%)	2,84	3,43	4,01	4,56	6,36	6,51	6,66	6,86	6,78	6,31	6,81	6,91	6,85	6,85	6,78
CPU Server LPSE-H (%)	0,03	0,06	0,03	0,04	0,04	0,04	0,06	0,47	0,02	0,04	0,05	0,06	0,23	0,04	0,15
CPU Firewall-IDS-LB (%)	13,02	14,32	13,72	14,99	14,45	15,36	15,17	14,14	14,66	14,86	14,47	14,46	15,70	14,99	13,50
CPU Server LPSE 1-LB (%)	0,11	1,75	0,02	0,09	0,94	0,32	0,01	0,02	0,01	0,02	0,01	0,01	0,01	0,02	0,03
CPU Server LPSE 2-LB(%)	0,02	0,33	0,32	0,35	0,37	0,26	0,38	0,40	0,42	0,44	0,41	0,42	0,47	0,40	0,45

Gambar 4.59 Chart Penggunaan CPU perangkat pada tiga Topologi (E=Existing Network, H=With Honeypot, LB=With Load Balancer) Kondisi Serangan DDoS UDP Flood Berlangsung

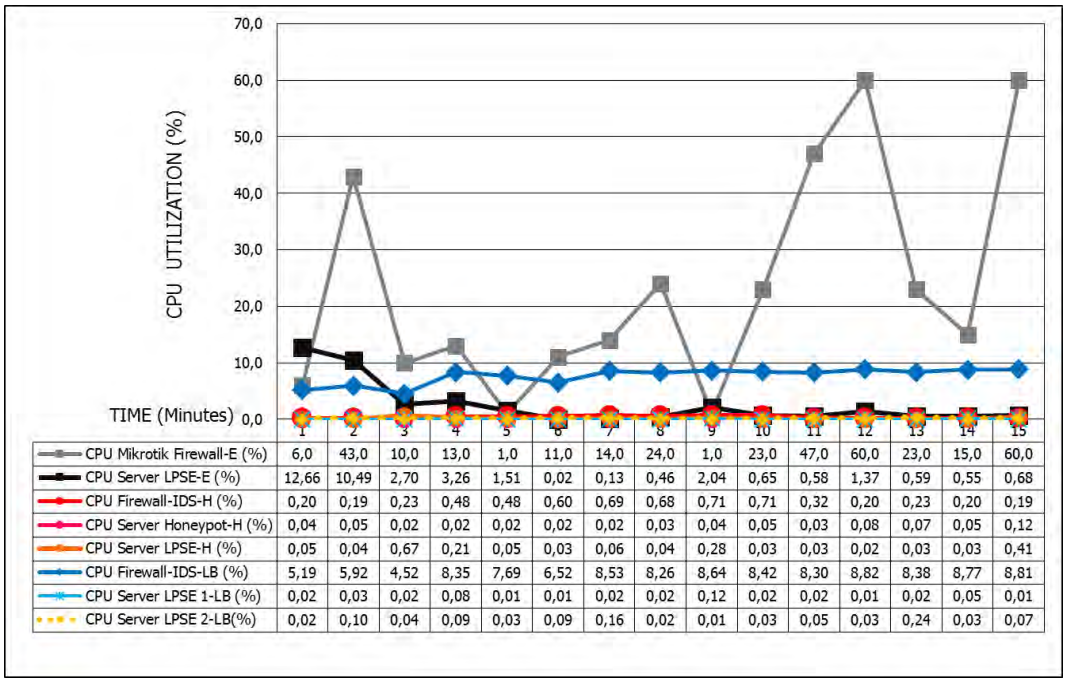
4.8. Hasil Perbandingan CPU Utilization pada Tiga topologi Jaringan, kondisi serangan DDoS Http Flood berlangsung.

Pada gambar Chart 4.60 dibawah ini merupakan data penggunaan CPU pada masing-masing perangkat pada ke tiga topologi jaringan selama serangan DDoS Http Flood berlangsung, pada topologi Existing terjadi peningkatan penggunaan CPU yang random dengan rata-rata 23,40% dan mencapai 60%, dimana angka ini tergolong cukup tinggi namun masih dalam ambang batas normal penggunaan CPU, sedangkan penggunaan CPU Server LPSE juga mengalami peningkatan yaitu rata-rata 2,51% dan mencapai 12,66%.

Selanjutnya pada topologi kedua yaitu topologi yang menggunakan IDS, Firewall Server Based dan Honeypot, penggunaan CPU pada Server Firewall rata-rata 0,41% dan mencapai 0,71%, penggunaan CPU pada Server Honeypot rata-rata 0,04% mencapai 0,12%, penggunaan CPU pada Server LPSE rata-rata 0,13% dan mencapai 0,67%.

Sedangkan pada topologi ke tiga atau topologi yang menggunakan IDS, Firewall Server Based dan Load Balancer penggunaan CPU pada Firewall rata-rata 7,67% dan mencapai 8,82%, penggunaan CPU pada Server LPSE-1 rata-rata 0,03% dan mencapai 0,12%, penggunaan CPU pada Server LPSE-2 CPU rata-rata 0,07% dan mencapai 0,24%.

Pada Topologi Existing dan topologi yang ketiga, meskipun terjadi peningkatan penggunaan CPU firewall namun masih dalam ambang batas normal. Pada topologi kedua dan ketiga dapat dilihat, bahwa tidak terdapat penggunaan CPU yang tinggi pada Server LPSE, hal tersebut karena firewall mengelola dan menerima beban dari lalu lintas paket-paket yang merupakan serangan DDoS Http Flood, namun pada topologi existing penggunaan CPU pada Server LPSE cukup meningkat di awal serangan dikarenakan mikrotik sebagai firewall tidak dapat mendeteksi dan mengelola beban traffic paket-paket DDoS Http Flood sehingga pengunaan CPU firewall meningkat dan sebagian paket-paket Http flood diteruskan ke server LPSE.

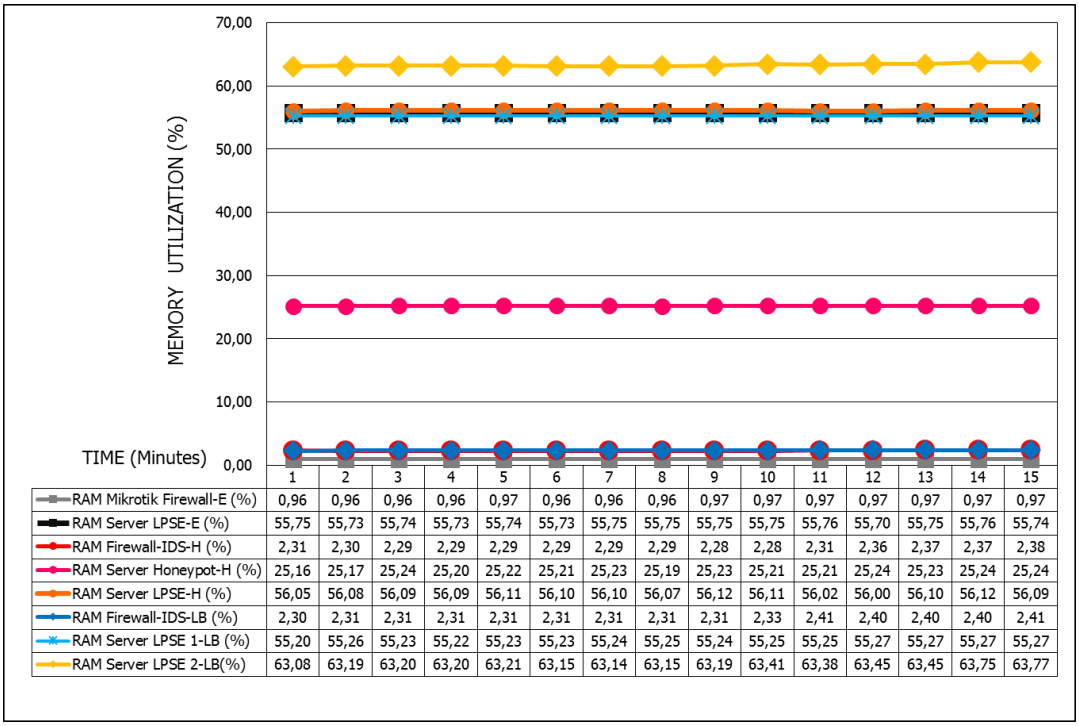


	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CPU Mikrotik Firewall-E (%)	6,0	43,0	10,0	13,0	1,0	11,0	14,0	24,0	1,0	23,0	47,0	60,0	23,0	15,0	60,0
CPU Server LPSE-E (%)	12,66	10,49	2,70	3,26	1,51	0,02	0,13	0,46	2,04	0,65	0,58	1,37	0,59	0,55	0,68
CPU Firewall-IDS-H (%)	0,20	0,19	0,23	0,48	0,48	0,60	0,69	0,68	0,71	0,71	0,32	0,20	0,23	0,20	0,19
CPU Server Honeypot-H (%)	0,04	0,05	0,02	0,02	0,02	0,02	0,02	0,03	0,04	0,05	0,03	0,08	0,07	0,05	0,12
CPU Server LPSE-H (%)	0,05	0,04	0,67	0,21	0,05	0,03	0,06	0,04	0,28	0,03	0,03	0,02	0,03	0,03	0,41
CPU Firewall-IDS-LB (%)	5,19	5,92	4,52	8,35	7,69	6,52	8,53	8,26	8,64	8,42	8,30	8,82	8,38	8,77	8,81
CPU Server LPSE 1-LB (%)	0,02	0,03	0,02	0,08	0,01	0,01	0,02	0,02	0,12	0,02	0,02	0,01	0,02	0,05	0,01
CPU Server LPSE 2-LB(%)	0,02	0,10	0,04	0,09	0,03	0,09	0,16	0,02	0,01	0,03	0,05	0,03	0,24	0,03	0,07

Gambar 4.60 Chart Penggunaan CPU perangkat pada Tiga Topologi (E=Existing Network, H=With Honeypot, LB=With Load Balancer) Kondisi Serangan DDoS Http Flood Berlangsung

4.9. Hasil Perbandingan Memory Utilization Pada Tiga Topologi Jaringan, Kondisi Serangan DDoS UDP Flood Berlangsung.

Pada Gambar Chart 4.61 dibawah ini terlihat data penggunaan Memory pada masing-masing perangkat di tiga topologi yang berbeda, pada kondisi jaringan sebelum serangan DDoS berlangsung.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RAM Mikrotik Firewall-E (%)	0,96	0,96	0,96	0,96	0,97	0,96	0,96	0,96	0,97	0,97	0,97	0,97	0,97	0,97	0,97
RAM Server LPSE-E (%)	55,75	55,73	55,74	55,73	55,74	55,73	55,75	55,75	55,75	55,75	55,76	55,70	55,75	55,76	55,74
RAM Firewall-IDS-H (%)	2,31	2,30	2,29	2,29	2,29	2,29	2,29	2,29	2,28	2,28	2,31	2,36	2,37	2,37	2,38
RAM Server Honeypot-H (%)	25,16	25,17	25,24	25,20	25,22	25,21	25,23	25,19	25,23	25,21	25,21	25,24	25,23	25,24	25,24
RAM Server LPSE-H (%)	56,05	56,08	56,09	56,09	56,11	56,10	56,10	56,07	56,12	56,11	56,02	56,00	56,10	56,12	56,09
RAM Firewall-IDS-LB (%)	2,30	2,31	2,31	2,31	2,31	2,31	2,31	2,31	2,31	2,33	2,41	2,40	2,40	2,40	2,41
RAM Server LPSE 1-LB (%)	55,20	55,26	55,23	55,22	55,23	55,23	55,24	55,25	55,24	55,25	55,25	55,27	55,27	55,27	55,27
RAM Server LPSE 2-LB(%)	63,08	63,19	63,20	63,20	63,21	63,15	63,14	63,15	63,19	63,41	63,38	63,45	63,45	63,75	63,77

Gambar 4.61 Chart Penggunaan Memory perangkat pada Tiga Topologi (E=Existing Network, H=With Honeypot, LB=With Load Balancer) Kondisi Serangan Sebelum Serangan DDoS

Pada topologi Existing penggunaan RAM Mikrotik rata-rata 0,97% sedangkan penggunaan RAM Server LPSE rata-rata 55,74% dan mencapai 55,76%, penggunaan RAM yang cukup tinggi ini disebabkan oleh aplikasi-aplikasi pendukung yang berjalan sejak sistem operasi mulai antara lain, Apache, Java dan Aplikasi SPSE v3 dan v4.

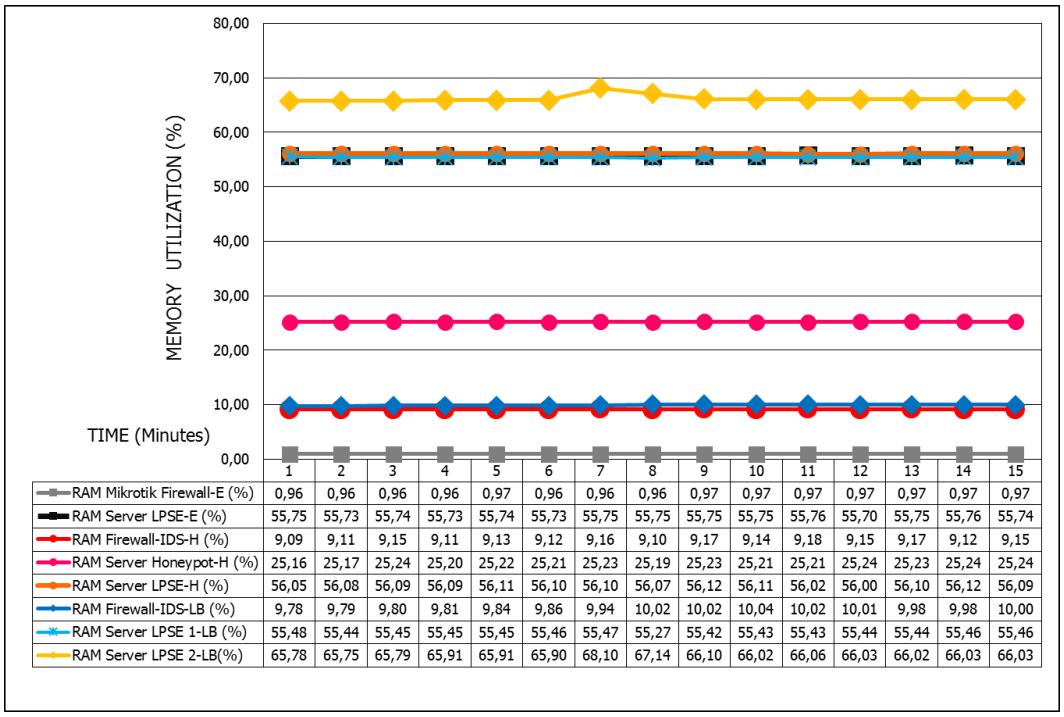
Selanjutnya pada topologi kedua yaitu topologi yang menggunakan Firewall Server Based dan Honeypot, penggunaan RAM Server Firewall rata-rata 2,31% dan mencapai 2,38%, penggunaan ram ini mencakup aplikasi-aplikasi yang yang berjalan sejak sistem operasi mulai yaitu Aplikasi IDS Suricata dan Firewall

IPTables. Penggunaan RAM Server Honeypot rata-rata 25,21% mencapai 25,24%, penggunaan RAM Server LPSE rata-rata 55,74% dan mencapai 55,76%, sedangkan pada topologi ke tiga dengan menggunakan IDS, Firewall Server Based dan Load Balancer menunjukkan penggunaan CPU Firewall rata-rata 2,34% dan mencapai 2,41%, penggunaan CPU pada Server LPSE-1 rata-rata 55,25% dan mencapai 55,27%, penggunaan CPU pada CPU Server LPSE-2 63,31% dan mencapai 63,77%.

Selanjutnya Pada gambar Chart 4.53 dibawah ini, menunjukkan bahwa tidak terjadi peningkatan penggunaan RAM yang signifikan pada perangkat di masing-masing topologi selama serangan DDoS UDP Flood berlangsung.

Pada topologi Existing penggunaan RAM Mikrotik Firewall rata-rata 0,97%, sedangkan penggunaan RAM pada Server LPSE rata-rata 55,74% dan mencapai 55,76 %. Selanjutnya pada topologi kedua yaitu topologi jaringan yang menggunakan IDS, Firewall Server Based dan Honeypot, penggunaan RAM pada Server Firewall rata-rata 9,14% dan mencapai 9,18%, penggunaan RAM pada Server Honeypot rata-rata 25,21% dan mencapai 0,12%, penggunaan RAM Server LPSE rata-rata 56,08% dan mencapai 56,12%.

Pada topologi ke tiga atau topologi yang menggunakan IDS, Firewall Server Based dan Load Balancer penggunaan RAM pada Server Firewall rata-rata 9,93% dan mencapai 10,04%, penggunaan RAM pada Server LPSE-1 rata-rata 55,44% dan mencapai 55,48%, penggunaan RAM Server LPSE-2 rata-rata 66,17% dan mencapai 68,10%. Pada ketiga topologi tidak terjadi peningkatan penggunaan RAM yang signifikan jika dibandingkan dengan kondisi sebelum serangan DDoS UDP Flood berlangsung.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RAM Mikrotik Firewall-E (%)	0,96	0,96	0,96	0,96	0,97	0,96	0,96	0,96	0,97	0,97	0,97	0,97	0,97	0,97	0,97
RAM Server LPSE-E (%)	55,75	55,73	55,74	55,73	55,74	55,73	55,75	55,75	55,75	55,75	55,76	55,70	55,75	55,76	55,74
RAM Firewall-IDS-H (%)	9,09	9,11	9,15	9,11	9,13	9,12	9,16	9,10	9,17	9,14	9,18	9,15	9,17	9,12	9,15
RAM Server Honeypot-H (%)	25,16	25,17	25,24	25,20	25,22	25,21	25,23	25,19	25,23	25,21	25,21	25,24	25,23	25,24	25,24
RAM Server LPSE-H (%)	56,05	56,08	56,09	56,09	56,11	56,10	56,10	56,07	56,12	56,11	56,02	56,00	56,10	56,12	56,09
RAM Firewall-IDS-LB (%)	9,78	9,79	9,80	9,81	9,84	9,86	9,94	10,02	10,02	10,04	10,02	10,01	9,98	9,98	10,00
RAM Server LPSE 1-LB (%)	55,48	55,44	55,45	55,45	55,45	55,46	55,47	55,27	55,42	55,43	55,43	55,44	55,44	55,46	55,46
RAM Server LPSE 2-LB(%)	65,78	65,75	65,79	65,91	65,91	65,90	68,10	67,14	66,10	66,02	66,06	66,03	66,02	66,03	66,03

Gambar 4.62 Chart Penggunaan Memory Perangkat pada Tiga Topologi (E=Existing Network, H=With Honeypot, LB=With Load Balancer) Kondisi Serangan DDoS UDP Flood Berlangsung

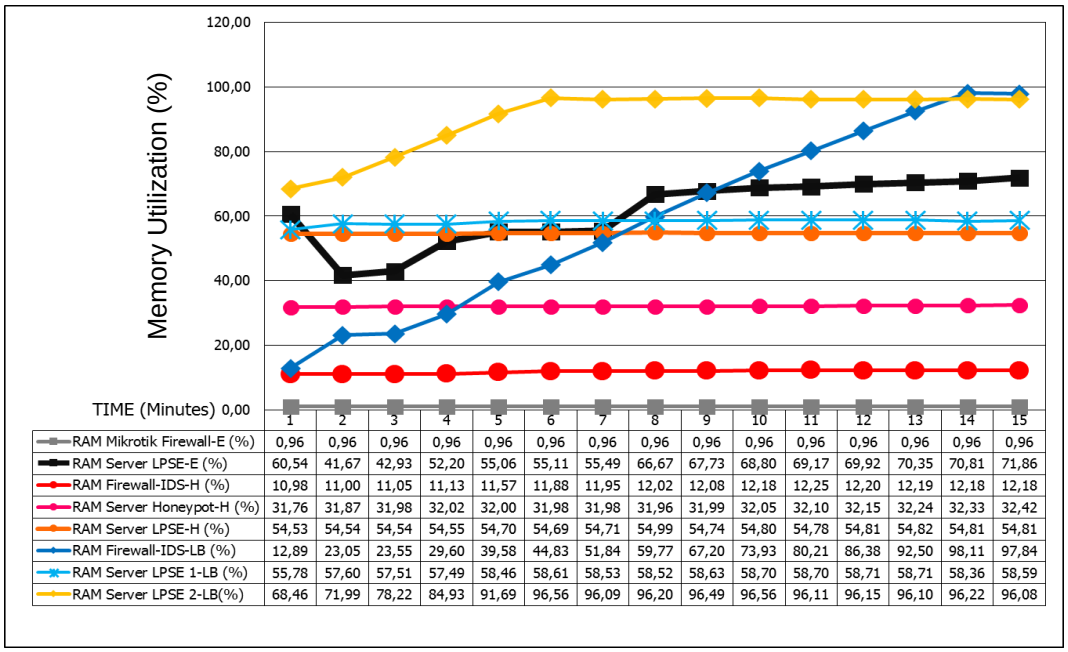
4.10. Hasil Perbandingan Memory Utilization pada tiga topologi Jaringan, kondisi serangan DDoS Http Flood berlangsung.

Pada gambar Chart 4.63 dibawah ini, terlihat peningkatan penggunaan RAM pada perangkat Server LPSE, terjadi topologi Existing dan ketiga selama serangan DDoS Http Flood berlangsung, pada topologi Existing penggunaan RAM pada Mikrotik Firewall rata-rata 0,96%, sedangkan penggunaan RAM pada Server LPSE rata-rata 61,22% dan mencapai 71,86 %.

Selanjutnya pada topologi kedua yaitu topologi jaringan dengan menggunakan IDS, Firewall Server Based dan Honeypot, penggunaan RAM pada Server Firewall rata-rata 11,79% dan mencapai 12,25%, penggunaan RAM pada Server Honeypot rata-rata 32,06% mencapai 32,42%, penggunaan RAM Server LPSE rata-rata 54,72% dan mencapai 54,99%.

Sedangkan pada topologi ke tiga atau topologi yang menggunakan IDS, Firewall Server Based dan Load Balancer, menunjukkan peningkatan penggunaan RAM pada Server Firewall yaitu mencapai 98,11%, penggunaan RAM Server LPSE-1 rata-rata 58,19% dan mencapai 58,71%, penggunaan RAM Server LPSE-

2 rata-rata 90,52% dan mencapai 96,56%. Pada ketiga topologi terjadi peningkatan penggunaan RAM yang signifikan jika dibandingkan dengan kondisi sebelum serangan DDoS Http Flood berlangsung.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RAM Mikrotik Firewall-E (%)	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96	0,96
RAM Server LPSE-E (%)	60,54	41,67	42,93	52,20	55,06	55,11	55,49	66,67	67,73	68,80	69,17	69,92	70,35	70,81	71,86
RAM Firewall-IDS-H (%)	10,98	11,00	11,05	11,13	11,57	11,88	11,95	12,02	12,08	12,18	12,25	12,20	12,19	12,18	12,18
RAM Server Honeypot-H (%)	31,76	31,87	31,98	32,02	32,00	31,98	31,98	31,96	31,99	32,05	32,10	32,15	32,24	32,33	32,42
RAM Server LPSE-H (%)	54,53	54,54	54,54	54,55	54,70	54,69	54,71	54,99	54,74	54,80	54,78	54,81	54,82	54,81	54,81
RAM Firewall-IDS-LB (%)	12,89	23,05	23,55	29,60	39,58	44,83	51,84	59,77	67,20	73,93	80,21	86,38	92,50	98,11	97,84
RAM Server LPSE 1-LB (%)	55,78	57,60	57,51	57,49	58,46	58,61	58,53	58,52	58,63	58,70	58,70	58,71	58,71	58,36	58,59
RAM Server LPSE 2-LB(%)	68,46	71,99	78,22	84,93	91,69	96,56	96,09	96,20	96,49	96,56	96,11	96,15	96,10	96,22	96,08

Gambar 4.63 Chart Penggunaan Memory Perangkat pada ke 3 Topologi (E=Existing Network, H=With Honeypot, LB=With Load Balancer)

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil penelitian diperoleh kesimpulan:

1. Penggunaan integrated firewall seperti Mikrotik yang berfungsi sebagai firewall sekaligus gateway pada jaringan LPSE, sangat beresiko terkena dampak serangan DDoS. Hal ini dikarenakan mikrotik merupakan jembatan yang mengatur koneksi antara dua jaringan, sehingga jika terjadi serangan DDoS maka yang menerima beban serangan adalah firewall tanpa ada pengalihan beban traffic sehingga paket-paket DDoS menumpuk pada firewall dan ketika resource firewall terkuras untuk menerima beban maka otomatis akan menggangu koneksi dari dalam dan luar LPSE. .
2. Infrastruktur dan topologi jaringan Existing LPSE Kab. Luwu Timur rentan terhadap serangan DDoS Jenis UDP dan Http Flood, serangan DDoS jenis ini dapat mengganggu operasional Web Server LPSE.
3. Rancangan Topologi yang menggunakan Intrusion Detection System, Firewall Server Based, dan Honeypot Server, memiliki hasil performansi Web Server LPSE yang paling baik dengan nilai request rate paling tinggi dan memiliki erorr requests dengan jumlah yang paling sedikit pada kondisi serangan DDoS UDP dan Http Flood berlangsung.
4. Dari dua jenis serangan DDoS yang di uji coba yaitu DDoS UDP Flood dan Http Flood, Intrusion Detection System dalam hal ini Suricata dapat mendeteksi jenis serangan dan sumber IP dan traffic Paket DDoS UDP Flood dan Http Flood tersebut.
5. Dari ketiga metode dan topologi jaringan yang diimplementasikan pada penelitian ini, topologi kedua atau topologi yang menggunakan IDS, Firewall Server Based dan Honeypot, memiliki pengukuran kinerja Web

Server LPSE dan mitigasi serangan DDoS jenis UDP dan Http Flood paling baik.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan dengan menggunakan metode yang diusulkan, ada beberapa hal yang perlu diperhatikan untuk penelitian selanjutnya diantaranya yaitu :

1. Jumlah Attacker Server dan client yang perlu ditambahkan untuk mendapatkan serangan yang lebih besar.
2. Peningkatan Resource hardware server honeypot yang lebih besar (CPU dan Memory) untuk pengalihan paket-paket serangan DDoS.
3. Menyediakan backup power untuk perangkat-perangkat yang digunakan sehingga ketika terjadi pemadaman listrik secara tiba-tiba, konfigurasi aplikasi dan perangkat tidak terganggu atau rusak.

DAFTAR PUSTAKA

Republik Indonesia. Undang-Undang No. 11 Tahun 2011 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2008, No. 58. Sekretariat Negara. Jakarta, 2008.

Republik Indonesia. Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2012, No. 189. Sekretariat Negara. Jakarta, 2008.

ID-SIRTII/CC, Pemantauan dan Deteksi Intrusi, Jakarta:Laporan Progress Kegiatan, 2014.

LPSE Kab. Luwu Timur, Laporan Evaluasi LPSE, Luwu Timur, Bidang Administrasi Sistem Informasi, Jl. Soekarno Hatta Kab. Luwu Timur, Sulawesi Selatan, 2014.

Republik Indonesia. Peraturan Kepala Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah Nomor 2 Tahun 2010 tentang Layanan Pengadaan Secara Elektronik. Jl. Epicentrum Tengah Lot 11 B Jakarta Selatan, DKI Jakarta 12940, 2010.

Republik Indonesia. Peraturan Kepala Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah Nomor 1 Tahun 2011 tentang E-Tendering, Jl. Epicentrum Tengah Lot 11 B Jakarta Selatan, DKI Jakarta 12940, 2015.

Lowe, Doug, Networking For Dummies 10th Edition, wiley publishing, 2013.

Cheeswick, W & Bellovin, S., Networks Firewall, Addison Wesley Publishing Company, ISBN 0-201-63357-4, 1994.

Sulaman . S D, “An Analysis and Comparison of The Security Features of Firewalls andIDSs” Department of Electrical Engineering Linkoping University S-581 83, Linkoping, Sweden, 2011.

Zhou, Qian., Comparing Dedicated and Integrated Firewall Performance. Mikkeli: Mikkeli University of Applied Sciences, 2013.

Patrikakis .C, Masikos .M, & Zouraraki .0, Distributed Denial of Service Attacks National Technical University of Athens, The Internet Protocol Journal - Volume 7, Number 4, Cisco System Inc.

Sandeep, Rajneet, A Study of DOS & DDOS - Smurf Attack and Preventive Measures, International Journal of Computer Science and Information Technology Research, ISSN 2348-1196, 2014.

SANS Institute. "Understanding Intrusion Detection Systems", 2001. https://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337.

Davis .B, "Leveraging the Load Balancer to Fight DDoS", SANS Institute. 2009. https://www.sans.org/reading-room/whitepapers/firewalls/leveraging-load-balancer-fight-ddos-33408

Muhammad Zamrudi AH "analisa mekanisme pertahanan DOS dan DDOS (Distributed Denial Of Service) pada virtual machine menggunakan IDS Center" Fakultas Teknik, Universitas Indonesia, 2013

Pratomo, Baskoro Adi "Pengalihan Paket Ke Honeypot Pada Linux Virtual Server Untuk Mengatasi Serangan DDOS" Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember, 2011.

Vordos, Ioannis, Mitigating Distributed Denial Of Service Attacks With Multiprotocol Label Switching—Traffic Engineering (MPLS-TE). Naval Postgraduate School, 2009.

R. Fielding, J. Gettys, J. Mogul, H. Frystyk, and T. Berners-Lee. Hypertext Transfer Protocol – HTTP/1.1. Internet Engineering Task Force, January 1997.

David Mosberger and Tai Jin. httperf: A Tool for Measuring Web Server Performance. In SIGMETRICS First Workshop on Internet Server Performance, ACM, June 1998.

BIODATA PENULIS

Penulis tesis bernama Salman Akbar, anak ketiga dari empat bersaudara, lahir 27 April 1983 di kota Malili Kabupaten Luwu Timur, Propinsi Sulawesi Selatan Indonesia. Penulis dinyatakan lulus dari SMA Negeri 1 Malili pada tahun 2001 dan melanjutkan studi ke S1 Teknik Informatika Institut Sains dan Teknologi Palapa Malang hingga lulus pada tahun 2004. Saat ini penulis tinggal di kota Malili kabupaten Luwu Timur dan beprofesi sebagai ASN pada Dinas Perhubungan, Komunikasi dan Informatika Kab. Luwu Timur. Selain bekerja, penulis juga aktif di organisasi kepemudaan yang bergerak diberbagai bidang seperti bidang teknologi dan informasi, otomotif dan musik di Kabupaten Luwu Timur. Keinginan kuat untuk menimba ilmu dan profesi yang penulis jalani, mengantarkan penulis kembali ke bangku kuliah dengan mengambil studi S2 Bidang keahlian Telematika-CIO, Jurusan Teknik Elektro, Institut Teknologi Sepuluh Nopember pada tahun 2014. Penulis dapat dihubungi melalui email di shallman83[at]gmail.com