Analisis Serangan *Denial Of Service* (DOS) Pada Jaringan Privat Seluler 5G *Stand Alone* Berbasis *Open* Seluler

Analysis Of Denial Of Service (DOS) Attack On Private Mobile Network 5G Stand Alone Based On Open Cellular

1st Alfin Bakti Maulana
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
alfinbakti@student.telkomuniversity.ac.id

2nd Sofia Naning Hertiana
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
sofiananing@telkomuniversity.ac.id

3rd Fardan
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
fardan@telkomuniversity.ac.id

Abstrak —5G merupakan teknologi seluler generasi terbaru untuk meningkatkan layanan dari generasi sebelumnya serta memberikan banyak kemampuan baru didalam sistemnya. Seiring perkembangan teknologi, terdapat program open source yang menyediakan service 5G core network. Dengan adanya program open source memungkinkan pengembang, peneliti, ataupun industry untuk membuat jaringan 5G sendiri atau bisa dikatakan privat seluler. Namun dalam pembangunan privat seluler perlu mempertimbangkan aspek fungsional dan non fungsionalnya. Pada tugas akhir ini, penulis melakukan simulasi dan pengujian terhadap aspek non-fungsional yakni keamanan framework open source 5G core. Pengujian dilakukan dengan menggunakan serangan Denial of Service (DoS) pada program free5GC. Serangan yang dimaksud adalah dengan cara membanjiri jaringan menggunakan trafik yang tinggi. Dengan demikian dapat mengukur pengaruh serangan terhadap faktor availability dari keamanan jaringan. Berdasarkan hasil pengujian, jaringan yang dibangun ketika mendapatkan serangan DoS berdampak terhadap performansi jaringan. Server Free5GC mengalami peningkatan penggunaan CPU sebesar 43.59 % saat percobaan oleh dua penyerang dari keadaan normal akibat beban yang berlebihan. Sehingga menyebabkan throughput yang dialirkan oleh free5GC menurun 51.1 % dari throughput simulasi. Sedangkan serangan DoS pada komponen arsitektur virtualisasi jaringan 5G membuat fungsi AMF Free5GC macet. Dengan demikian pengguna mendapatkan penolakan layanan dari core service.

Kata kunci — Denial of Service, free5GC, Privat seluler.

Abstract—5G is the latest generation of cellular technology to improve services from the previous generation and provide many new capabilities in its system. Along with the development of technology, there are open source programs that provide 5G core network services. The existence of an open source program allows developers, researchers, or industry to create their own 5G networks or it can be said to be private cellular. However, in mobile private development, it is necessary to consider its functional and non-functional aspects. In this final project, the author simulates and tests the non-functional aspects, namely the security of the 5G core open source framework. Testing was performed using Denial of Service (DoS) attacks on the free5GC program. The attack in question is by flooding the network using high traffic. Thus it can measure the effect of attacks on the availability factor of network security. Based on the test results, the network built when getting a DoS attack has an impact on network performance. The Free5GC server experienced a 68.83% increase in CPU resources during an

attempted TCP SYN flood attack due to excessive load. Thus causing network performance parameters that refer to the quality of service (QoS) including throughput, packet loss, delay and jitter flowed by free5GC to decrease. Meanwhile, DoS attacks on components of the 5G network virtualization architecture have made the AMF Free5GC function stuck. Thus the user gets a denial of service from the core service.

Keywords— Denial of Service, free5GC, Privat seluler.

I. PENDAHULUAN

Evolusi teknologi telekomunikasi khususnya seluler memberikan dampak yang besar bagi kehidupan manusia. Proses komunikasi dapat dilakukan dengan mudah, cepat, dan dapat dilakukan dimana saja. 5G merupakan teknologi seluler generasi terbaru untuk meningkatkan layanan dari generasi sebelumnya serta memberikan banyak kemampuan baru didalam sistemnya. Penerapan 5G memperkenalkan serangkaian teknologi baru seperti softwarisasi fungsi jaringan yang diaktifkan software define Network (SDN), Network Function virtualization (NFV), Mobile Edge Computing (MEC), dan Network slicing (NS) [1]. kini ada beberapa developer yang mengembangkan software open source sehingga mempermudah untuk mempelajari infrastruktur komunikasi seluler serta diterapkan dalam jaringan privat seluler. beberapa framework 5g core service yang terkenal antara lain Free5GC, OpenAirInterce, dan Open5GS.

Pembangunan jaringan privat seluler perlu mempertimbangkan keamanan arsitektur yang dibangun. maka dari itu diperlukan informasi mengenai kehandalan keamanan dari platform core network yang ada mengingat kerahasiaan data serta ketersediaan layanan merupakan aspek utama dari sebuah operator penyedia jasa atau service provider (SP). Penelitian yang berjudul "Experimental Security Analysis for Fake eNodeB Attack on LTE Network" 2020 [2]. Berfokus pada analisa terhadap fake eNodeB yang digunakan untuk melakukan serangan IMSI catche dan DoS menggunakan OpenAirInterface (OAI) sebagai framework core network. Namun implementasi dari penelitian tersebut menggunakan standarisasi 4G LTE. berbeda dengan free5gc yang menerapkan infrastruktur baru yakni 5G Stand Alone (5G SA) berdasarkan rilis 15 3rd Generation Partnership Project (3GPP) [3]. Mengenai masalah keamanan 5G, beberapa sumber mempelajari terdapat kerentanan terhadap replay pada jaringan 5G. penelitian yang dilakukan oleh European Union Agency for Cybersecurity (ENISA, 2019), melaporkan bahwa memungkinkan pelaku kejahatan untuk melakukan serangan dengan DoS [4]. DoS adalah serangan keamanan terhadap ketersediaan layanan dengan menghabiskan sumber daya jaringan sehingga pengguna tidak mendapatkan akses [5].

Berdasarkan permasalahan tersebut, dengan adanya framework open source 5G core network yang menduplikasi arsitektur 5G Stand Alone. Diharapkan bisa diimplementasikan menjadi privat seluler yang memiliki beberapa kelebihan serta dapat mengevaluasi performansi keamanan jaringan. Penelitian dilakukan dengan mendeploy 5G core network menggunakan framework free5gc dan simulator UERANSIM untuk Radio Akses Network (RAN) dan UE. Deployment jaringan 5G privat tersebut guna mendapatkan analisa terhadap serangan DoS khususnya pada free5gc. Diharapkan dari hasil analisis tersebut dapat menjadi referensi pemilihan framework 5G core services.

II. KAJIAN TEORI

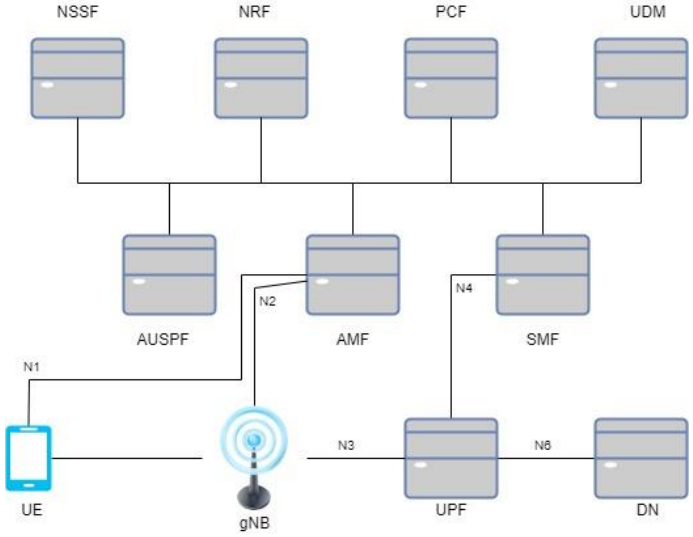
A. Private Cellular Network

Privat seluler adalah Jaringan seluler pribadi atau disebut sebagai jaringan non-publik oleh 3GPP. Privat seluler mirip halnya seperti WLAN konvensional atau WI-FI, tetapi menggunakan teknologi, spektrum dan arsitektur seluler untuk mendukung penggunaan yang lebih canggih dan mampu menjangkau area yang lebih luas [6]. Perbedaan antara jaringan privat dan publik terletak pada kepemilikan lisensi atau akses prioritas ke spektrum nirkabel.

B. Jaringan Seluler 5G

5G merupakan jaringan telekomunikasi seluler terbaru pengembangan dari generasi sebelumnya. Berbeda dari pengembangan generasi sebelumnya yang berfokus terutama pada peningkatan bandwidth dan kecepatan pengguna. Namun 5G memiliki pendekatan baru pada infrastruktur jaringan untuk menyediakan layanan secara global. Tentunya juga berpengaruh terhadap performa jaringan yang lebih diandalkan. 3 keunggulan 5G yakni Enhanced Mobile

Broadband (eMBB), Ultra-Reliable and Low Latency Communications (URLLC), massive Machine Type Communications (mMTC)Layanan ini memiliki tujuan untuk mengakomodasi tipe layanan mesin to mesin serta perkembangan internet of things (IoT) yans semakin massif digunakan.



GAMBAR 1
ARSITEKTUR 5G

5G System Architecture (5GS), terdiri dari 5G New Radio Access (5GNR) dan 5G core network (5GC). Arsitektur 5G SA terdiri dari beberapa NF seperti tampak pada Gambar 2.2 diatas. Fungsi dari masing – masing NF tersebut antara lain:

1. Access and Mobility Management (AMF):
   Bertanggung jawab atas segala pensinyalan, perlindungan keamanan, manajemen registrasi, manajemen koneksi, manajemen mobilitas dan merupakan titik akhir untuk komunikasi control plane.
2. Session Management function (SMF):
   Fungi dari SMF antara lain menangani manajemen sesi (pembentukan sesi, modifikasi, release), alokasi & manajemen alamat IP UE, fungsi DHCP, penghentian pensinyalan NAS terkait dengan session manajemen, manajemen data DL, konfigurasi routing traffic untuk UPF.
3. User plane function (UPF)
   UPF tersambung langsung ke NG-RAN melalui GPRS Tunnelling Protocol (GTP)-U, yaitu, channel GTP untuk lalu lintas UP. Fungsi ini menerima permintaan koneksi dari NG-RAN dan membuat channel GTP untuk setiap UE
4. Network Repository function (NRF) berfungsi untuk manajemen pencarian layanan, memelihara profil NF dan instance NF yang tersedia.
5. Unified Data Management (UDM): pembuatan credential Otentikasi dan Kunci (AKA), penanganan identifikasi pengguna, otorisasi akses, manajemen pelanggan
6. Authentication Server Function (AUSF) sebagai server autentikasi.
7. Policy Control Function (PCF) menyediakan aturan kebijakan untuk fungsi CP, mengakses informasi berlangganan untuk keputusan kebijakan di UDR.
8. Network Slice Selection Function (NSSF) memilih instance Network Slice untuk melayani UE, menentukan NSSAI yang diijinkan, menentukan AMF yang akan digunakan untuk melayani UE.

C. Softwarisasi 5G Cellular Network

Keterbukaan dan fleksibilitas menjadi referensi desain dari 5GC. Fungsionalitas control dan user plane core service telah dipisah menjadi beberapa fungsi jaringan [7]. Untuk mengelola integrasi dari kumpulan teknologi semacam itu dan mengendalikan infrastruktur yang beragam serta mengatur layanan dan fungsi jaringan bukanlah hal

yang mudah. Sistem 5G mengandalkan perangkat lunak dimana mengadopsi dari konsep software defined network (SDN) dan Network Function Virtualisasition (NFV). SDN memanfaatkan perangkat lunak untuk memisahkan control plane dengan data plane sehingga tidak lagi menggunakan operasi dari perangkat keras. Sdangkan NFV adalah konsep untuk membuat network function yang dapat diimplementasikan seluruhnya kedalam bentuk software defined yang berjalan pada perangkat keras berstandar industri[7]

D. Denial of Service DoS

Denial of Service (DoS) adalah serangan terhadap ketersediaan jaringan. serangan DoS dapat menghabiskan sumber daya jaringan oleh musuh. Terbentuknya serangan DoS juga bisa lebih dari satu musuh yang terdistribusi yang disebut Distributed Denial of Service (DDoS). Kedua serangan tersebut tergolong serangan aktif yang dapat diterapkan pada layer yang berbeda. Dengan penggunaan jaringan nirkabel 5G yang massif, serangan DoS dan DDoS menjadi ancaman yang serius bagi operator [8].

E. Free5GC

Free5gc merupakan platform proyek core network jaringan seluler generasi 5 (5G) [9]. Dikembangkan menggunakan bahasa pemrograman Go serta dapat dijalankan didalam mesin host linux. free5gc mampu mendukung semua fungsi jaringan inti 5G. meliputi pengelolaan akses, mobilitas, dan sesi pengguna (AMF dan SMF), pengelolaan akses, mobilitas, dan sesi pengguna (AMF dan SMF), melakukan Otentikasi UE dalam jaringan.

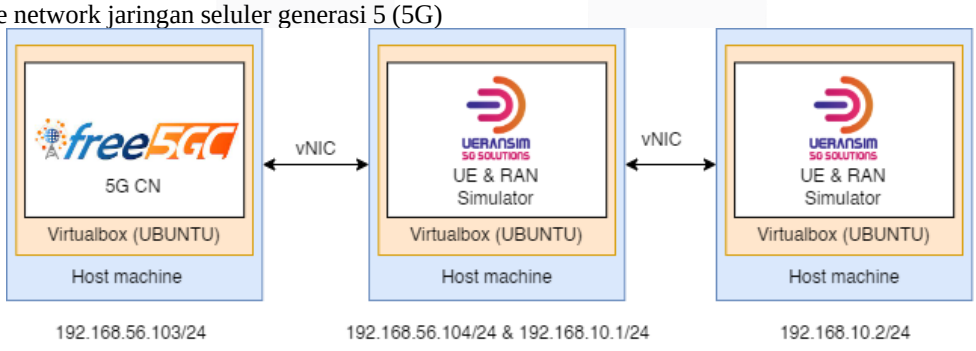
F. Ueransim

UERANSIM merupakan simulator open source 5G UE dan 5G RAN (gNB) [10]. Secara sederhana UERANSIM dapat menggantikan ponsel 5G secara virtual dengan fungsi mekanisme yang sama. Komunikasi yang dapat dikontrol oleh UERANSIM antara lain Control Interface yaitu komunikasi antra RAN dan AMF, User Interface yaitu komunikasi antara RAN dan UPF, Radio Interface yaitu komunikasi antara UE dan RAN.

III. METODE

A. Desain Simulasi

Gambar 2 dibawah merupakan model dari sistem yang akan unuk dilakukan pengujian.



GAMBAR 2
TOPOLOGI DESAIN SIMULASI

Proses pnliatian ini mensimulasikan jaringan 5G dengan core service mengunakan platform open source. Mengimplementasikan free5GC daam sebua virtual mesin sbagai host server sedangkan UERANSIM sebagai gNB dan UE diimplementasikan dalam virtual mesin lainya. Fokus pada penelitaian ini yaitu pada performansi server virtual dengan layana 5G core core service ketika mendapati serangan DoS. Pengujian Serangan DoS dalam penelitian ini dibagi menjadi dua yakni pertama attacker menggunakan metode SYN flood dengan alamat ip UPF server. Kedua menggnakan 5Greplay untuk mengenerate paket komunikasi kontrol kedalam layanan freee5GC

B. Perangkat Keras

Menurut rekomendasi dari free5gc *recommended environment* [11]. spesifikasi perangkat yang layak digunakan untuk simulasi berdasarkan minimum dan rekomendasinya adalah sebagai berikut

TABLE 1
MINIMUM SPESIFIKASI PERANGKAT KERAS

Spesifikasi	Keterangan
Prosesor	Intel i5
RAM	4GB
HDD	160 GB
Ethernet	1GB

Berdasarkan kebutuhan minimal dan rekomendasi perangkat, maka dalam tugas akhir ini menggunakan spesifikasi sebagai berikut mengacu pada kebutuhan minimum dikarenakan keterbatasan environment yang tersedia.

TABLE 2
REKOMENDASI SPESIFIKASI PERANGKAT KERAS

Spesifikasi	keterangan
Prosesor	AMD A8
RAM	8 GB
HDD	160 GB
Ethernet	1 GB

C. Perangkat Lunak

Selain perangkat keras, tentu juga membutuhkan perangkat lunak untuk menunjang implementasi jaringan privat seluler 5G. berikut perangkat lunak yang diperlukan berdasarkan Free5gc dan Ueransim *system requirement*.

- Sistem operasi Ubuntu 18.04 LTS
- gcc 7.3.0
- Go 1.14.4 linux/amd64
- kernel version 5.0.0-23-generic
- VirtualBox

IV. HASIL DAN PEMBAHASAN

A. **Pengujian Fungsionalitas Sistem**

Pengujian dilakukan untuk memastikan semua komponen yang dibutuhkan berjalan sesuai dengan yang diharapkan serta dapat mengukur performansi jaringan 5G yang dibangun. Simulasi dilakukan pada 3 host mesin virtual masing - masing menggunakan system operasi ubuntu 18.04 untuk host Free5gc dan 20.0 untuk UERANSIM .Kesimpulan dari hasil pengujian fungsionalitas core free5GC ditunjukan pada tabel 4 dibawah.

TABLE 3
UJI FUNGSIONAL KOMPONEN VIRTUAL JARINGAN

NO	Fungsi Virtual Jaringan	Keterangan
1	AMF	Server Started
2	SMF	Server Started
3	UPF	Server Started
4	AUSF	Server Started
5	NSSF	Server Started
6	UDR	Server Started
7	NRF	Server Started
8	PCF	Server Started
9	UDM	Server Started

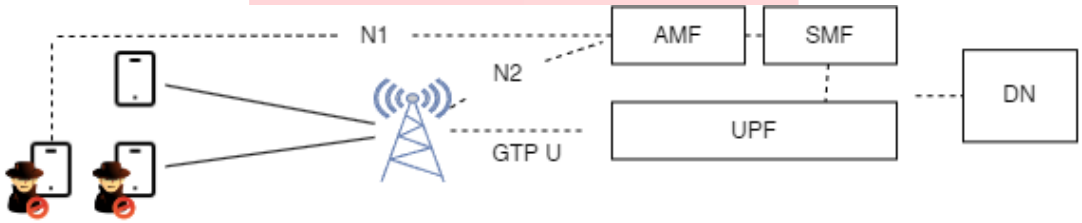
Setelah pengujian fungsional simulasi core network didapatkan hasil semua komponen fungsi jaringan virtual berjalan dengan baik. Selanjutnya dilakukan pengujian koneksi gNB dan UE dengan core network. Prosedur komunikasi kontrol antara UE, gNB dan Core didapatkan hasil pada tabel 5 dibawah.

TABLE 2 UJI FUNGSIONAL UE SIGNALLING

No	Prosedur Pesan Signalling	Hasil
1	Registrasi UE	Sukses
2	Permintaan otentikasi dan Balasan Otentikasi	Sukses
3	Identitas UE detail	Sukses
4	*Transport NAS message* UL dan DL	Sukses
5	Pengecekan keamanan	Sukses
6	*Session management* PDU *Request* dan respon	Sukses

Prosedur koneksi antara UE, gNb dan Core yang mengimplementasikan infrastruktur 5G stand alone mendapatkanhasil UE berhasil tersambung dengan layanan core . dengan demikian dapat disimpulakna bahwa sistem simulasi jaringan 5G berjalan dengan baik.

B. Pengujian Serangan Denial of Service

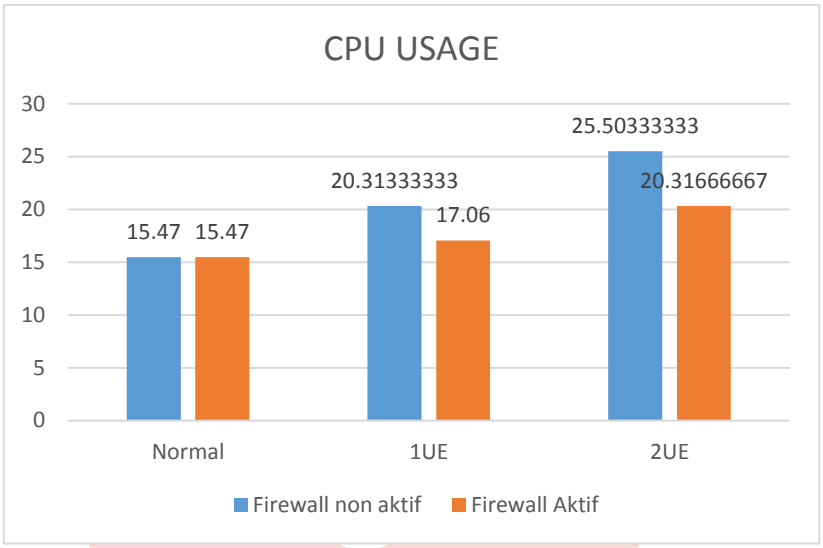


GAMBAR 3 SKEMA DOS ATTACK SIMULASI JARINGAN 5G

Gambar 3 diatas merupakan sketsa skema pengujian denial of service pada jaringan 5G. Serangan berasal dari UE yang merupakan client pada sistem jaringan dengan tujuan server core network melalui channel GTP antara RAN dan UPF

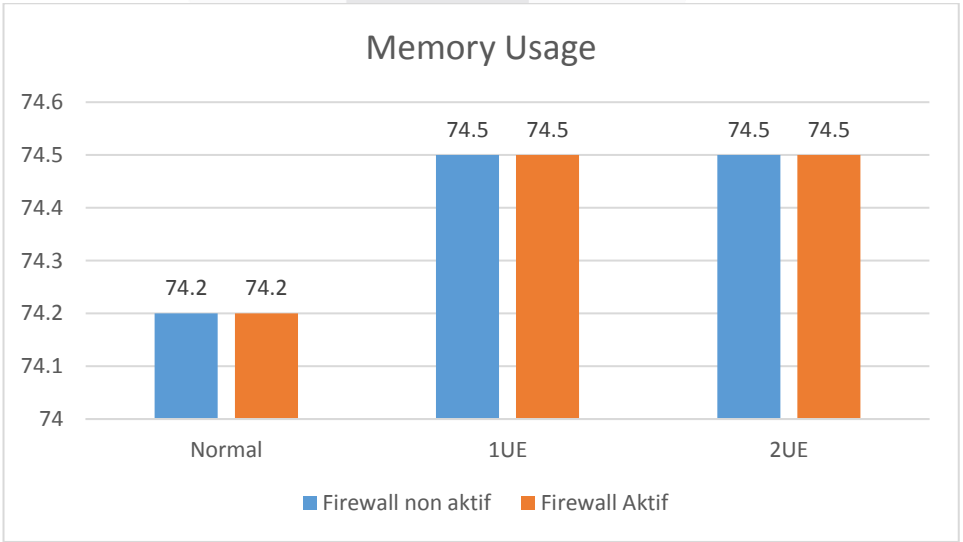
1. TCP SYN FLOOD

Pengujian keamanan pada jaringan dilakukan dengan tools hping3. Hping3 terinstall pada UE dan mengirimkan sinyal SYN secara cepat dan terus menerus dengan harapan dapat melumpuhkan sumber daya korban. Adapun parameter yang diuji yakni CPU usage, memori usage dan throughput yang diambil dari 30 sampel pengukuran dari servis yang dibangun oleh free5gc. Berikut hasil pengukuran yang didapat.



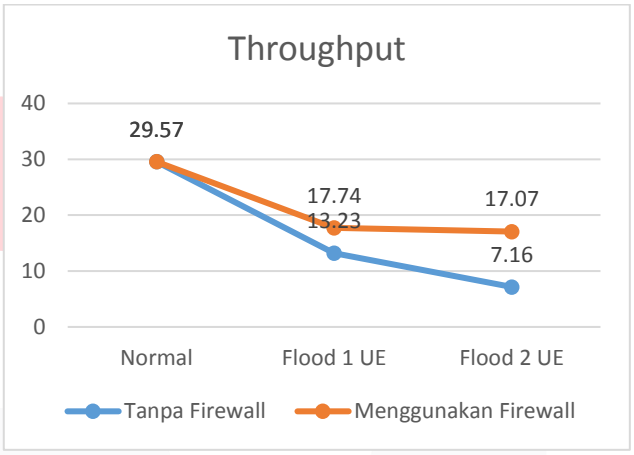
GAMBAR 4
GRAFIK PERBANDINGAN CPU USAGE

Gambar 4 diatas menunjukkan hasil perbandingan penggunaan CPU saat mendapatkan serangan TCP SYN Flood. Resource yang dihabiskan CPU rata - rata sebesar 15.47 %. Semakin sedikit sumber daya CPU yang terpakai semakin baik performansinya. Artinya akan ada banyak proses yang mampu ditampung oleh CPU. Terlihat terjadi penurunan performansi CPU ditinjau dari peningkatan sumber daya yang terpakai pada saat menerima serangan SYN sebesar 20.3 % dengan flooder berjumlah satu UE dan 25.5 % ketika flooder bertambah menjadi dua. Peningkatan ini disebabkan karena CPU bekerja untuk memproses paket SYN. Menyebabkan server berusaha memproses semua paket SYN yang berdampak pada penggunaan CPU. Namun ketika terdapat firewall yang memfilter paket masuk ke server berdasarkan set aturan yang dibuat, firewall membatasi dan menjatuhkan paket SYN sehingga penggunaan CPU tidak sebesar pada saat tanpa menggunakan firewall. Terlihat pada grafik diatas penggunaan CPU sebesar 17.06 % dan 20.3% masing - masing saat terserang oleh 1 UE dan 2 UE.



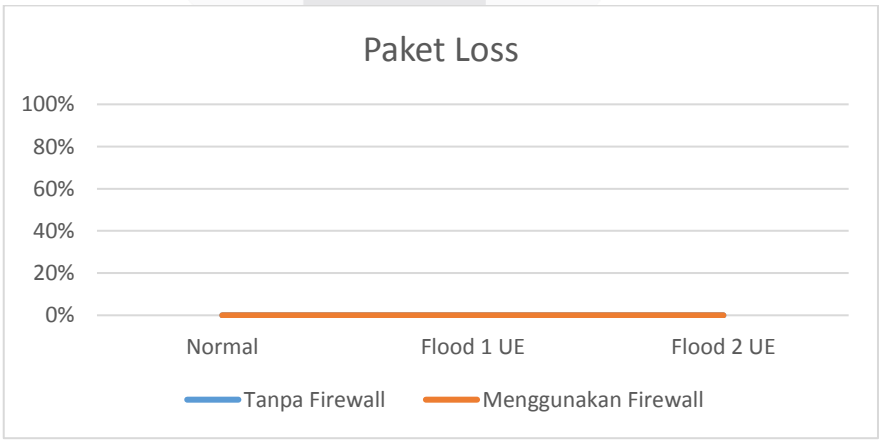
GAMBAR 5
GRAFIK PERBANDINGAN MEMORY USAGE

Gambar 5 diatas menunjukan hasil perbandingan penggunaan memori saat layanan 5G core mendapat serangan DoS. Pada saat menjalankan Free5GC resource memori terpakai sebesar 74.2 % saat pengamatan. Semakin banyak ruang memori yang tersedia semakin baik performansinya. Terlihat penurun performansi ditinjau dari peningkatan sumber daya yang terpakai pada saat menerima serangan DoS. Terlihat selisih peningkatan penggunaan sumber daya memori menjadi 74.5 pada saat terjadi serangan DoS oleh satu dan dua flooder. Hal tersebut disebabkan oleh serangan SYN flood dianggap oleh server ingin membangun koneksi, kemudian server merespon dengan mengirim sinyal SYN-ACK, dan mengalokasikan memori untuk menunggu respon balasan ACK. Namun tidak terjadi perubahan yang signifikan dikarenakan besar paket data yang tidak begitu besar berkisar 50 byte.



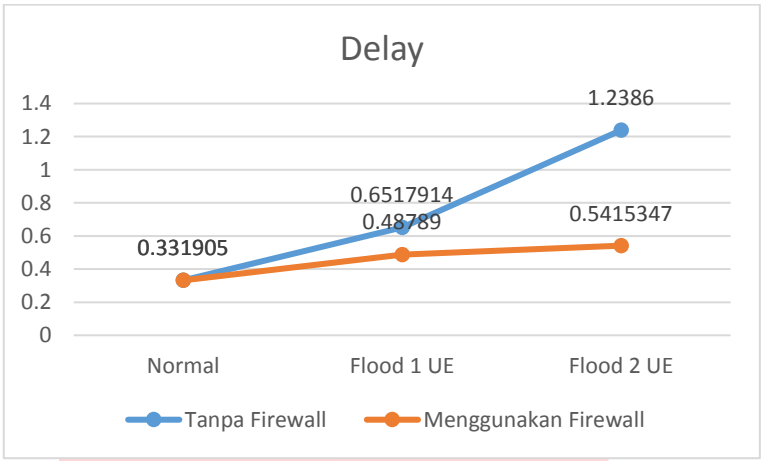
GAMBAR 6
GRAFIK PERBANDINGAN NETWORK THROUGHPUT

Gambar 6 diatas menunjukan hasil perbandingan performa jaringan. pada parameter throughput terlihat bahwa terjadi penurunan kualitas yang berawal dari 29,57 Mbps menjadi 13,23 Mbps dan 7 ,16 Mbps masing - masing saat jaringan dibanjiri oleh satu dan 2 flooder namun pada saat jaringan dilengkapi firewall throughput dapat bertahan pada kisaran 17 Mbps saat terjadi serangan SYN flood.



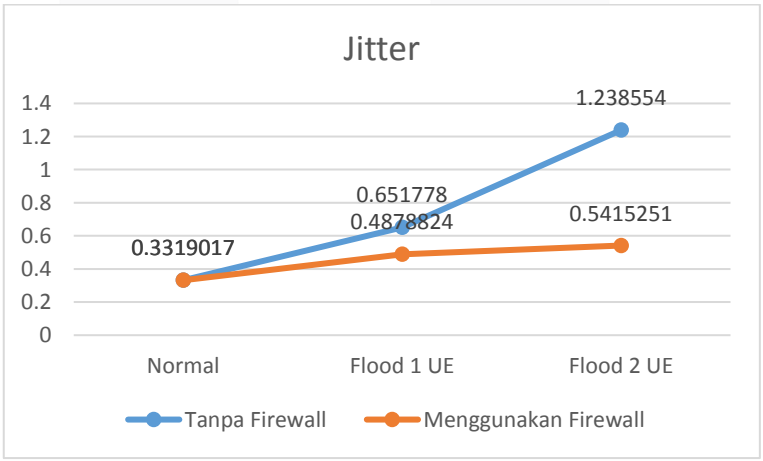
GAMBAR 7
GRAFIK DELAY

Pada gambar 7 menunjukan parameter selanjutnya yakni paket loss dari hasil pengukuran mendapatkan nilai 0%. Hal ini dikarenakan lingkungan jaringan yang dibuat berdasarkan simulasi dan transmisi paket berupa TCP yang memiliki kemampuan untuk meminimalisir kerusakan dalam transmisi.



GAMBAR 8
GRAFIK DELAY

Selanjutnya untuk parameter delay juga mengalami penurunan kualitas pada setiap skenario pengujian terlihat pada gambar 10. Delay pada saat kondisi jaringan normal sebesar 0.3 ms meningkat 0.6 ms dan 1.2 ms masing - masing pada saat kondisi jaringan menerima banjir serangan paket SYN. Sedangkan penggunaan firewall cukup meredam peningkatan delay tidak sebesar pada saat tanpa menggunakan firewall**.**

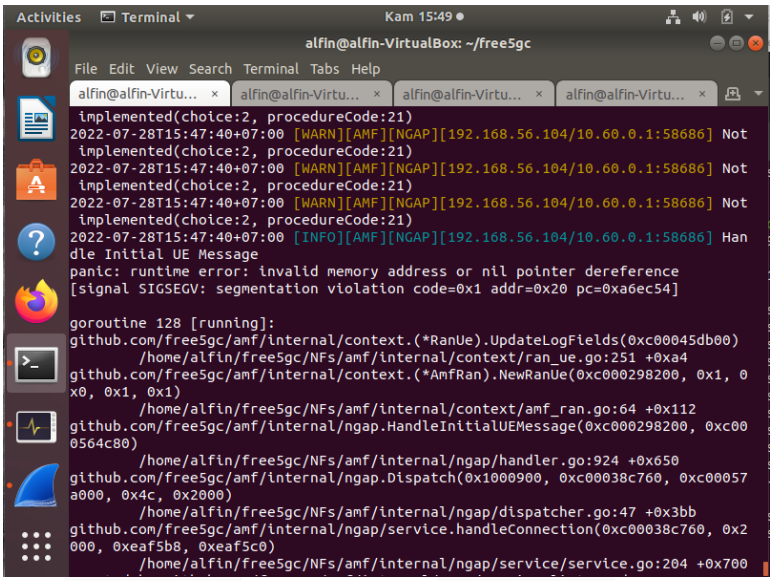


GAMBAR 9
GRAFIK DELAY

Gambar 9 Parameter terakhir yaitu jitter juga mengalami peningkatan saat jaringan normal ukuran jitter sebesar 0,33 ms meningkat menjadi 0,65 ms dan 1.23 ms masing - masing saat kondisi menerima serangan banjir SYN dari 1 UE dan 2 UE. Sedangkan pada saat jaringan dilengkapi oleh firewall, peningkatan jitter tidak terlalu signifikan menjadi 0,48 ms dan 0,54 ms pada setiap skenario.

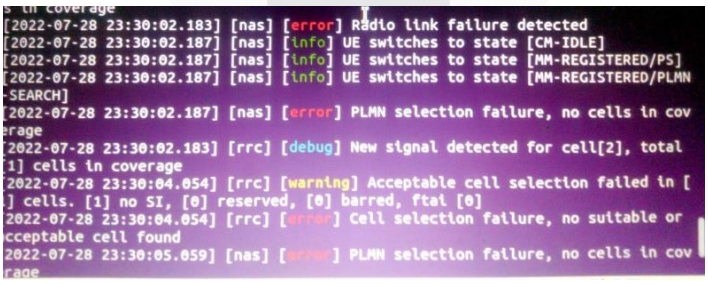
2. Hight Packet Injection From UE

5Greplay melakukan proses serangan dengan menganalisa file pcap yang berisi trafik lengkap sesi antara UE dan core kemudian disuntikkan ke target layanan core. 5Greplay terdapat parameter nb-copies yang berfungsi menduplikasi paket yang akan disuntikkan kedalam jaringan. Dalam pengujian ini dilakukan percobaan sebanyak mungkin untuk memperagakan DoS hingga terjadi kemacetan pada AMF. Hasil Pengujian dari serangan terhadap simulasi jaringan privat seluler 5G berbasis layanan core free5gc sebagai berikut.



GAMBAR 10
FREE5GC *ERROR*

Pada Gambar 10 menunjukan hasil pengujian. Free5gc AMF rusak ketika menerima paket dari 5GReplay. Hal tersebut dikarenakan permintaan registrasi dengan jumlah UE yang cukup tinggi menyebabkan AMF macet dan tidak bisa merespon soket SCTP lagi. Ketika AMF crash maka menyebabkan gNB tidak mendapat sambungan dari core sehingga layanan dari free5gc terhenti

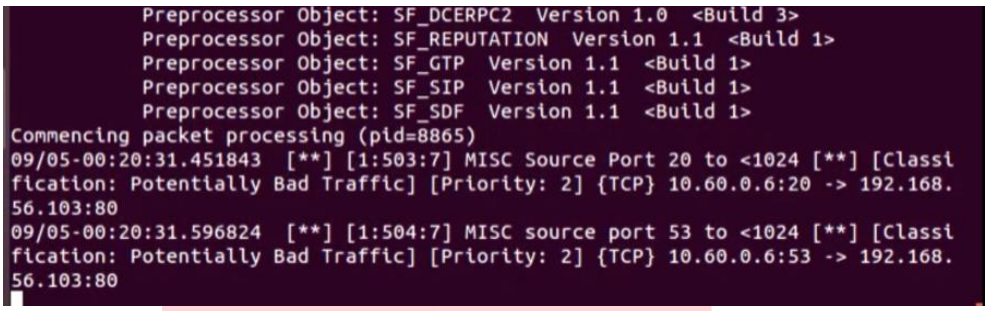


GAMBAR 11
RESPON UE

Gambar 11 menunjukan dampak terhadap UE simulator menerima notifikasi eror pada radio link (gNB) sehingga menyebabkan UE tidak dapat terkoneksi dengan PLMN free5gc.

3. Pengujian Serangan DoS Dengan Keamanan Network Intrusion Detection System SNORT

Berdasarkan pengujian keamanan sebelumnya, untuk menangani suatu tindakan penetrasi kedalam jaringan maka diperlukan suatu mekanisme untuk pendeteksian. Dengan demikian administrator dapat menentukan tindakan selanjutnya untuk mengamankan jaringan. Hasil yang diperoleh ketika menggunakan NIDS berbasis snort ditunjukan pada gambar dibawah.



GAMBAR 12
DETEKSI TRAFIK NIDS SNORT

Pada Gambar 12 menunjukan NIDS memberikan peringatan adanya trafik mencurigakan yang masuk kedalam interface ketika pengamatan pada server dengan serangan DoS SYN flooding. Paket data yang masuk berupa TCP dari sumber ip 10.60.0.6 pada port 80. Hal demikian mengindikasikan bahwa jaringan sedang dalam keadaan diserang oleh pelaku jahat yang mencoba melumpuhkan jaringan dengan serangan DoS. Sedangkan pengamatan saat serangan menggunakan 5greplay paket injection NIDS tidak mendeteksi adanya trafik yang masuk. Namun indikasi trafik yang tidak wajar dapat dilihat melalui log Free5GC.

V. KESIMPULAN

A. Kesimpulan

Dari hasil pengujian dan analisis jaringan simulasi 5G berbasis layanan core free5gc dibawah serangan DoS didapatkan kesimpulan

1. Free5GC memberikan layanan core yang cukup mudah diimplementasikan pada jaringan privat seluler. Namun masih banyak ancaman yang mengintai. Ditinjau dari pengujian informasi mengenai transmisi didalam jaringan dapat terbaca oleh paket sniffer seperti Wireshark. Di sisi lain hal ini membantu administrator untuk mengetahui trafik Jaringannya namun berbeda ketika informasi diketahui oleh aktor jahat.
2. Ketika informasi mengenai transmisi jaringan dapat digali, maka pelaku jahat akan secara leluasa untuk melancarkan berbagai macam bentuk serangan salah satunya DoS attack. Berdasarkan pengujian skenario satu yang melakukan banjir SYN menyebabkan penurunan seluruh performansi server termasuk juga parameter throughput yang dapat dialirkan jaringan. Tidak menutup kemungkinan jika intensitas serangan ditingkatkan akan menyebabkan jaringan lumpuh dan mengakibatkan penolakan layanan
3. Terdapat kelemahan pada arsitektur fungsi jaringan virtual dibangun oleh free5gc ketika mendapatkan serangan pengulangan pesan NAS atau permintaan pesan kontrol

dalam jumlah yang besar menyebabkan fungsi AMF core macet. Mengakibatkan seluruh aktifitas dari jaringan akses terjadi penolakan layanan.

4. Tindakan keamanan berlapis menjadi solusi untuk mengamankan jaringan 5G opensource melibatkan proses monitoring, pendeteksian, peredaman dan penolakan serangan merupakan kunci dari suatu jaringan
5.

B. Saran

1. Dapat menggunakan program 5g core service lain untuk pembanding performansi maupun aspek keamanan mengingat masih banyak proyek open source 5G
2. Disadari pada tugas akhir ini masih menggunakan konsep simulasi. Agar mendapatkan gambaran lebih jelas dapat mendesain sistem jaringan privatyang lebih baik dengan menerapkan Software Defined Radio (SDR), Antena USRP, dan perangkat UE komersil
3. Bentuk serangan dalam tugas akhir ini tergolong masih sederhana, untuk mempelajari ancaman jaringan lebih lanjut dapat menyiapkan skenario penyerangan jaringan yang lebih baik and bervariasi
4. Mendesain bentuk proteksi yang aman bagi jaringan open source dan menganalisa apakah masih bisa untuk dilakukan serangan oleh aktor jahat. Bisa dengan menempatkan arsitektur 5G pada VPS yang ada seperti Microsoft Azure, Idcloudhost, GCP, dan sebagainya.

REFERENSI

[1] Z. Salazar, H. N. Nguyen, W. Mallouli, A. R. Cavalli, dan E. M. Montes De Oca, “5Greplay: A 5G Network Traffic Fuzzer - Application to Attack Injection,” Agu 2021. doi: 10.1145/3465481.3470079.

[2] Fardan, Istikmal, I. Mawaldi, T. Anugraha, I. Ginting, dan N. Karna, “Experimental Security Analysis for Fake eNodeB Attack on LTE Network,” *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2020*, hlm. 140–145, 2020, doi: 10.1109/ISRITI51436.2020.9315427.

[3] Positive Technologies, “5G Standalone Core Security Research,” hlm. 21, 2020.

[4] “ENISA THREAT LANDSCAPE FOR 5G NETWORKS,” 2019, doi: 10.2824/49299.

[5] D. Fang, Y. Qian, dan R. Q. Hu, “Security for 5G Mobile Wireless Networks,” *IEEE Access*, vol. 6, no. AUGUST, hlm. 4850–4874, 2017, doi: 10.1109/ACCESS.2017.2779146.

[6] Harrison J. Son, “7 Deployment Scenarios of Private 5G Networks,” *NETMANIAS*, 2019. https://www.netmanias.com/en/post/blog/14500/5g-edge-kt-sk-telecom/7-deployment-scenarios-of-private-5g-networks

[7] L. Bonati, M. Polese, S. D’Oro, S. Basagni, dan T. Melodia, “Open, Programmable, and Virtualized 5G Networks: State-of-the-Art and the Road Ahead,” *Computer Networks*, vol. 182. Elsevier B.V., Des 09, 2020. doi: 10.1016/j.comnet.2020.107516.

[8] ENISA, *5G NETWORKS Threat assessment for the fifth generation of mobile*, no. November. 2019. doi: 10.2824/49299.

[9] Free5GC.org, “What is free5GC,” 2019. https://www.free5gc.org/ (diakses Mar 27, 2022).

[10] Iria Míguez González, “Virtualized Cellular Networks With Native Cloud Functions,” 2021.

[11] Free5GC, “Environment,” 2021. https://github.com/free5gc/free5gc/wiki/Environment