GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)

Implementasi Keamanan Jaringan Komputer Menggunakan Fortigate Sebagai Firewall pada Lab Komputer IAIN Bengkulu

Implementation of Computer Network Security Using Fortigate as a Firewall at the Computer Lab of IAIN Bengkulu

Dhanu Prima Jaya[1)]; Hari Aspriyono[2)]; Eko Suryana [2)]
[1,2)] ***Department of Informatics, Faculty of Computer Science, Universitas Dehasen Bengkulu***
Email: [2)] hari.aspriyono@gmail.com

How to Cite :
Jaya, D. P., Aspriyono, H., Suryana, E. (2021). *Implementation of Computer Network Security Using Fortigate as a Firewall at the Computer Lab of IAIN Bengkulu*. Gatotkaca Journal, 2(1) page: 31-38. DOI: **https://doi.org/10.37638/gatotkaca.2.1.31-38**

ARTICLE HISTORY
Submited [29 Desember 2021]
Received [29 Desember 2021]
Revised [30 Desember 2021]
Accepted [31 December 2021]

KEYWORDS
Fortigate, Firewall, Flooding, Port scanningInformation

ABSTRAK
Penelitian ini bertujuan untuk mengamankan jaringan dengan menggunakan Fortigate sebagai Firewall pada komputer server di lab komputer Kampus IAIN Bengkulu sehingga dapat mengetahui adanya serangan, menangkal serangan, dan memblokir IP dari si penyerang yang ditujukan kepada komputer server. Metode penelitian yang digunakan yaitu NDLC (Network Development Life Cycle) metode ini bertujuan untuk menganalisa, menerapkan dan memonitoring dari metode penelitian tersebut. Menerapkan Fortigate sebagai Firewall untuk mengamankan komputer server jika terjadi serangan ICMP Flooding dan Port scanning yang ditujukan pada komputer server sehingga dapat teridentifikasi apabila serangan terjadi dan dapat menghindari terjadinya hang pada komputer server..

ABSTRACT
This study aims to secure the network by using Fortigate as Firewall on the server computer at computer lab of IAIN Bengkulu so that it can detect attacks, counter attack, and block the attacker's IP address to the server computer. The research method used is NDLC (Network Development Life Cycle). This method aims to analyze, implement and monitor the research method. Implementing Fortigate as a Firewall to secure the server computer in the event of ICMP Flooding attack and Port scanning aimed at the server computer so that it can be identified when an attack occurs and can avoid hangs on the server computer.

PENDAHULUAN

Dengan pesatnya perkembangan teknologi saat ini membuat teknologi berperan penting dalam kehidupan kita saat ini. Seiring dengan perkembangan teknologi informasi saat ini yang selalu berubah-ubah, menjadikan keamanan informasi sangatlah penting. Banyak terjadi serangan yang sering dilakukan oleh orang yang tidak bertanggung jawab pada suatu sekolah, perusahaan, maupun instansi negara. Lemahnya sistem keamanan jaringan membuat orang yang tidak bertanggung jawab dapat mengakses informasi dari web maupun dari komputer server. Jalur komunikasi jaringan yang kurang baik dapat menyebabkan suatu hal yang buruk, seperti yang terjadi pada server UPT Puskom IAIN Bengkulu yang diretas oleh orang yang tidak dikenal. Maka untuk mengatasi serangan tersebut dibutukan kemanan pada jaringan komputer, salah saatunya dengan menggunakan Fortigate sebagai Firewall.

UPT Puskom IAIN Bengkulu adalah unit pelaksana teknis dalam pengelolaan dan pengembangan sistem informasi manajemen serta pengembangan teknologi institut yang berada di bawah Rektor. UPT Puskom sendiri mempunyai tugas mengelolah dan mengembangkan sistem informasi manajemen, pengembangan dan pemeliharaan jaringan dan aplikasi, pengelolaan basisdata dan kerja sama jaringan antar unit.

Komputer server pada UPT Puskom di kampus IAIN sendiri sudah beberapa kali di serang oleh orang yang tidak dikenal, salah satu serangannya yaitu serangan DOS (Denial Of Service) UDF Flooding dengan membanjiri komputer server dengan data yang besar sehinngga komputer server menjadi hang, maka untuk mencegah serangan yang dituju ke kompurter Server UPT Puskom IAIN salah satunya dibutukan sistem keamanan jaringan menggunakan Fortigate sebagai Firewall.

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)

LANDASAN TEORI

Implementasi

"*Implementation as to carry out, acoumplish, fulfill, produce, complete*" maksudnya yakni "membawa, menyelesaikan, mengisi, menghasilkan, melengkapi" Jadi secara etimologis implementasi itu dapat dimaksudkan sebagai suatu aktifitas yang bertalian dengan penyelesaian suatu pekerjaan dengan penggunaan sarana (alat) untuk memperoleh hasil [1].

Ada beberapa faktor yang menentukan berhasil atau tidaknya suatu proses implementasi yaitu [2] :

1. Kualitas kebijakan itu sendiri
2. Kecukupan input kebijakan (terutama anggaran)
3. Ketepatan instrumen yang dipakai untuk mencapai tujuan kebijakan (pelayanan, subsidi, hibah, dan lainnya)
4. Kapasitas implementor (struktur organisasi, dukungan SDM, koordinasi, pengawasan, dan sebagainya)
5. Karakteristik dan dukungan kelompok sasaran (apakah kelompok sasaran adalah individu atau kelompok, laki-laki atau perempuan, terdidik atau tidak)
6. Kondisi lingkungan geografi, sosial, ekonomi, dan politik dimana implementasi tersebut dilakukan.

Implementasi pada hakikatnya juga merupakan upaya pemahaman apa yang seharusnya terjadi setelah program dilaksanakan. Dalam tataran praktis, implementasi adalah proses pelaksanaan keputusan dasar. Proses tersebut terdiri atas beberapa tahapan yakni:

1. Tahapan pengesahan peraturan perundangan.
2. Pelaksanaan keputusan oleh instansi pelaksana.
3. Kesediaan kelompok sasaran untuk menjalankan keputusan.
4. Dampak nyata keputusan baik yang dikehendaki maupun tidak.
5. Dampak keputusan sebagaimana yang diharapkan instansi pelaksana.
6. Upaya perbaikan atas kebijakan atau peraturan perundangan.

Proses persiapan implementasi setidaknya menyangkut beberapa hal penting yakni:

1. Penyiapan sumber daya, unit dan metode.
2. Penerjemahan kebijakan menjadi rencana dan arahan yang dapat diterima dan dijalankan.
3. Penyediaan layanan, pembayaran dan hal lain secara rutin.

Implementasi mengacu pada tindakan untuk mencapai tujuan-tujuan yang telah ditetapkan dalam suatu keputusan. Tindakan ini berusaha untuk mengubah keputusan-keputusan tersebut menjadi pola-pola operasional serta berusaha mencapai perubahan-perubahan besar atau kecil sebagaimana yang telah diputuskan sebelumnya. Implementasi pada hakikatnya juga merupakan upaya pemahaman apa yang seharusnya terjadi setelah program dilaksanakan [3].

Beradasarkan pengertian diatas dapat di simpulakan bahwa implentasi adalah suatu proses untuk menilai, mengevaluasi dan mengukur apakah suatu peraturan atau kebijakan dapat berjalan dengan baik atau tidak, dengan begitu maka akan di nilai apakah harus ada evaluasi atau tidak terhadap program tersebut.

Keamanan

Keamanan atau *security* secara umum dapat diartikan sebagai kemampuan mempertahankan diri dalam menghadapi ancaman yang nyata [4].

Sistem keamanan jaringan adalah proses untuk mengidentifikasi dan mencegah pengguna yang tidak sah dari suatu jaringan komputer. Tujuannya tentu saja untuk mengantisipasi resiko ancaman berupa perusakan bagian fisik komputer maupun pencurian data seseorang [5].

Jaringan Komputer

Jaringan komputer adalah kumpulan komputer dan alat-alat yang saling dihubungkan bersama menggunakan media komunikasi tertentu [6]. Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Informasi dan data memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer secara bersama-sama menggunakan hardware/software yang terhubung dengan jaringan [7]

Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi bertukar data [8]. Jaringan komputer didefinisikan sebagai sekumpulan komputer

e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)

yang terhubung satu dengan yang lainnya menggunakan media tertentu sehingga memungkinkan diantara komputer tersebut untuk berinteraksi, bertukar data, dan berbagi peralatan bersama [9].

Dari pengertian diatas, dapat disimpulkan bahwa jaringan komputer adalah sekumpulan komputer dan peralatannya yang saling berhubungan dengan menggunakan media komunikasi tertentu sehingga antara komputer satu dengan yang lainya dapat berbagi data dan sumber daya yang dimiliki.

Fortinet

*Fortine*t adalah penyedia peralatan keamanan jaringan dan pemimpin pasar dalam manajemen ancaman terpadu (UTM) kelas dunia. Produk dan layanan yang diberikan luas dan beragam. Fortigate menyediakan perlindungan terpadu dan kinerja tinggi terhadap ancaman keamanan yang dinamis sementara menyederhanakan infrastruktur keamanan TI.

Fortinet menawarkan perpaduan yang kuat antara perlindungan ASIC-*accelerated*, respon terhadap multi-ancaman terpadu, dan update yang terus menerus serta intelijen ancaman yang mendalam. Dengan menggunakan teknologi inovatif untuk analisis jaringan, keamanan dan konten, sistem Fortinet mengintegrasikan fitur terluas dalam teknologi keamanan, termasuk pencegahan *firewall*, VPN, antivirus, pengendalian aplikasi, web filtering, antispam, *wireless controller*, dan WAN *accelerator*, yang semuanya dapat digunakan secara individual untuk melengkapi solusi yang sudah ada atau dikombinasikan untuk solusi manajemen ancaman yang komprehensif. Perusahaan juga dapat melengkapi solusi dengan manajemen array, analisis, e-mail, database dan end-point security [10].

Berikut beberapa keunggulan yang didapatkan jika menggunakan *Fortinet*, yaitu :

Fleksibilitas Manajemen

Perangkat Manajemen Fortinet memiliki fleksibilitas yang tinggi dalam hal manajemen dengan berbagai perangkat dari vendor yang berbeda-beda. Dengan adanya perangkat ini, kita tidak perlu melakukan pembaruan satu persatu pada masing-masing perangkat untuk menyesuaikan dengan perangkat keamanan. Namun, kita hanya perlu melakukan setting pertama kali pada perangkat keamanan tersebut. *Fortinet* menjamin keamanan jaringan secara menyeluruh sebagai *gateway*, router *firewall*, VPN, antivirus dan lain sebagainya. Dan yang menarik, kita tetap bisa memantau atau monitoring perangkat ini via internet browser.

UTM *Fortinet*

Keunggulan berikutnya adalah adanya fitur UTM (*Unified Threat Management*) yang merupakan fasilitas khusus untuk menangani masalah jaringan yang ada. Dalam hal ini, Fortinet memiliki beberapa fitur seperti *firewall*, *intrusion prevention system* (IPS), *web filtering*, antivirus sekaligus routing dalam satu paket hardware yang super lengkap. Ketika perangkat ini digunakan, maka semuanya akan langsung berjalan sekaligus, tidak perlu berhadapan dengan berbagai hal yang rumit, sebab kecanggihan dari produk ini.

***Virtual domain* (VDOMs)**

Virtual domain yang ditawarkan oleh Fortinet ini adalah salah satu fitur yang memberi akses menuju beragam perusahaan dengan administrator yang berbeda, namun tetap dengan unit fisik yang sama. Tujuannya agar masing-masing dapat menjaga konfigurasi yang spesifik, tanpa memberikan dampak berlebihan antara satu dengan yang lain.

FortiASIC

Lewat fasilitas *FortiASIC*, *Fortinet* bisa mendeteksi dan meminimalisir secara *real time*, ancaman yang terintegrasi. Tak hanya ancaman minor, *Fortinet* sanggup mengatasi ancaman dalam skala yang lebih kompleks tanpa menurunkan kinerja jaringan. Hal ini tentu sangat bermanfaat untuk meminimalisir ancaman dan gangguan pada perusahaan.

Fortiguard

FortiGuard yaitu jasa *support* dalam menyediakan layanan beragam *update* yang berkelanjutan, untuk menjamin keamanan jaringan komputer. Fasilitas ini mempunyai database jutaan situs yang kemudian dikategorikan dalam beberapa kelompok, dan diperlakukan secara berbeda. Biasanya, staf yang bertugas di unit kendali teknis memiliki wewenang penuh atas monitoring maupun pemblokiran situs-situs tersebut. *FortiGuard* juga dapat dipergunakan untuk mengontrol pemakaian bandwidth internet, untuk mengatur pemakaian akses internet di luar keperluan kantor, atau disesuaikan dengan kebijakan perusahaan dan terutama untuk mencegah terjadinya kebocoran informasi penting.

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)

Fortigate

Fortigate adalah sebuah sistem keamanan yang dikeluarkan oleh perusahaan *Fortinet*. *Fortigate* sebagai perangkat yang menjamin keamanan jaringan secara keseluruhan sekaligus berfungsi sebagai *gateway* dan router bagi jaringan LAN sehingga tak dibutuhkan lagi *router* ataupun perangkat tambahan *load balancing* bila ada lebih dari satu koneksi WAN [11]. Sistem Fortigate memungkinkan untuk mendeteksi secara real time ancaman yang terintegrasi, bahkan dalam skala kompleks, tanpa menurunkan kinerja jaringan, sementara serangkaian proses manajemen, analisa, database dan solusi perlindungan endpoint bekerja meningkatkan penyebaran fleksibilitas dan memberikan dampak yang nyata dalam mengurangi biaya operasional manajemen keamanan jaringan.

Firewall

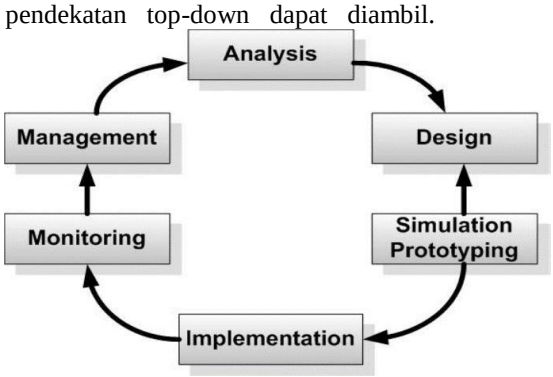
Firewall yaitu suatu kombinasi antara *Hardware* (perangkat keras) dan *Software* (perangkat lunak) yang fungsinya menjadi pemisah diantara jaringan komputer menjadi dua atau lebih untuk menjaga keamanan data. Pengertian lain dari *Firewall* adalah suatu sistem kemanan pada jaringan komputer yang dipakai untuk melindungi komputer dari beberapa serangan dari komputer luar.

Firewall merupakan sebuah sistem yang didesain untuk mencegah akses yang tidak sah ke atau dari jaringan pribadi (*Private Network*). Implementasi *Firewall* pada perangkat keras (*Hardware*) dan perangkat lunak (*Software*) atau kombinasi antara keduanya. Penggunaan dari *Firewall* adalah membatasi atau menjadi pengontrol kepada siapa saja yang memiliki akses ke jaringan pribadi dari jaringan luar. *Firewall* mengacu kepada sistem pengatur komunikasi antara dua jenis jaringan yang tidak sama[12].

METODE PENELITIAN

Metode Analisis

Untuk penelitian Keamanan jaringan menggunakan *Fortigate* sebagai Firewall pada lab komputer penulis mengggunakan Metode Penelitian *Network Development Life Cycle* (NDLC). *Network Development Life Cycle* (NDLC) merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan aplikasi, dan analisis pendistribusian data. Jika pengimplementasian teknologi jaringan dilaksanakan dengan efektif, maka akan memberikan sistem informasi yang akan memenuhi tujuan bisnis strategis, kemudian pendekatan top-down dapat diambil.



Gambar 1. Metode NDLC

Metode Pengumpulan Data

Metode kepustakaan

Metode ini adalah metode pengumpulan data dimana penulis mencari dan membaca serta mempelajari buku dan jurnal dari sumber tertulis yang relevan dengan materi pembahasan laporan yang dapat dijadikan sebagai bahan referensi dalam masalah yang diangkat yaitu implementasi keamanan jaringan menggunakan *Fortigate* sebagai Firewall pada lab komputer.

Metode Studi Labolatorium

Metode ini adalah suatu metode yang dimana penulis melakukan simulasi serangan terhadap komputer server untuk mengetahui apakah sistem keamanan jaringan baru dapat berjalan dengan baik.

Metode Observasi

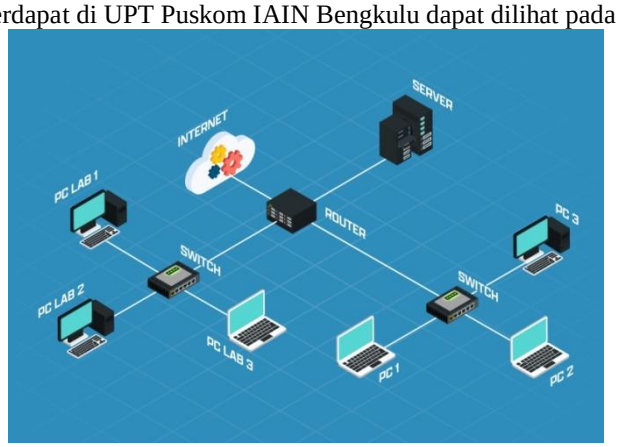
adalah metode pengumpulan data dimana penulis mengumpulkan data dengan pengamatan langsung pada objek yang diteliti yakni implementasi keamanan jaringan menggunakan Fortigate pada lab komputer IAIN Bengkulu.

GATOT KACA JOURNAL
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

Metode perancangan sistem

Analisa Sistem Aktual

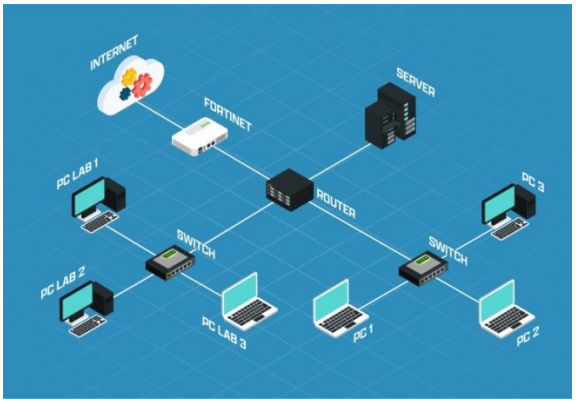
Seperti yang telah diuraikan dalam latar belakang, masalah yang terjadi di kampus IAIN Bengkulu yaitu terjadinya serangan DOS *(Denial Of Service*) ICMP *Flooding* dengan membanjiri komputer server dengan data yang besar sehingga komputer server menjadi hang, maka untuk mencegah serangan yang dituju ke kompurter Server UPT Puskom IAIN salah satunya dibutukan sistem keamanan jaringan menggunakan *Fortigate* sebagai *Firewall*. Adapun topologi jaringan yang terdapat di UPT Puskom IAIN Bengkulu dapat dilihat pada gambar dibawah ini.



Gambar 2. Skema alur jaringan

Rancangan Sistem Baru

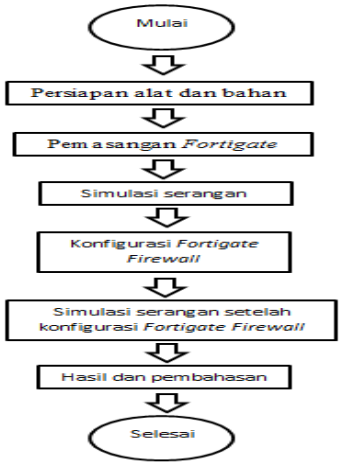
Untuk mengatasi permasalahan yang di hadapi, maka diperlukan topologi jaringan baru pada UPT Puskom IAIN Bengkulu dimana Fortigate bertindak sebagai firewall untuk mencegah serangan yang di tujukan pada komputer server berikut ini :



Gambar 3. Skema alur jaringan baru

Perancangan Rencana Kerja

Perancangan rencana kerja tidak terlepas dari blok diagram yang merupakan suatu pernyataan gambar ringkas, yaitu mulai dari menyiapkan peralatan yang diperlukan , instalasi sampai dengan mendapatkan hasil dan kesimpulan dari keamanan jaringan menggunakan Fortigate pada komputer server di gedung UPT Puskom kampus IAIN Bengkulu. Adapun rencana dapat dilihat pada gambar berikut.



Gambar 4. Rancangan Kerja Sistem

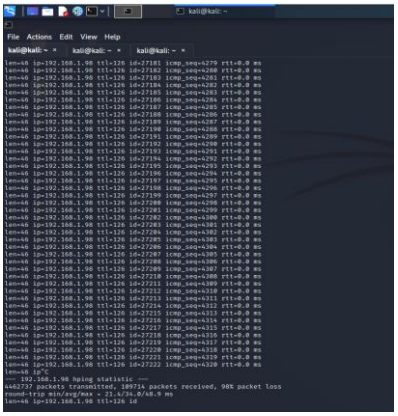
GATOT KACA JOURNAL
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

HASIL DAN PEMBAHASAN

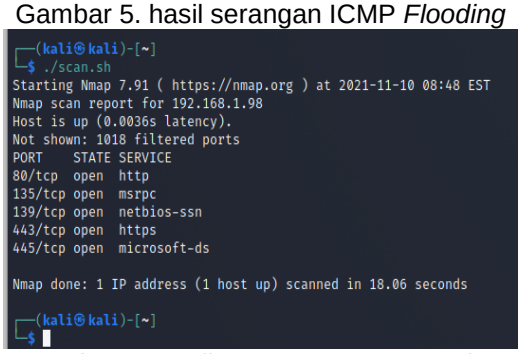
Simulasi serangan ICMP *Flooding* dan *Port Scanning*

Untuk menegtahui Fortigate berhasil atau tidak mengamankan komputer server dari serangan, maka dibutuhkan simulasi serangan yang di tuju ke komputer server dengan serangan ICMP *Flooding* dan *port scanning*. Berikut langkah-langkah serangan ke komputer server :

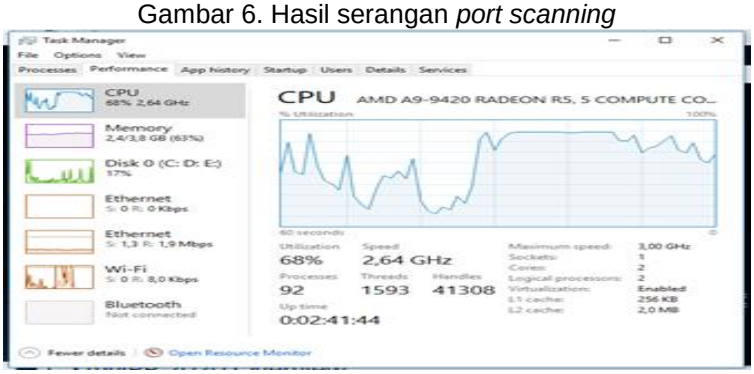
a. Masuk ke linux yang telah di instal lewat *virtualbox* pada komputer *attacker* untuk melakukan simulasi serangan.
b. Kemudian masuk ke *terminal emulator* untuk melakukan perintah serangan yang dituju ke ip komputer server.
c. Kemudian masukan perintah serangan ICMP *Flooding* dan *port scanning* pada terminal *emulator*.
d. Kemudian kita lihat hasil serangan ICMP Flooding dan port scanning dan CPU komputer server yang telah di serang



Gambar 5. hasil serangan ICMP *Flooding*



Gambar 6. Hasil serangan *port scanning*



Gambar 7. Tampilan CPU yang di serang

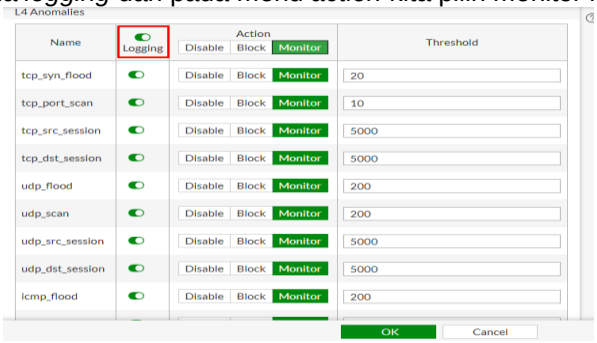
Konfigurasi *Fortigate Firewall*

Untuk mengamankan komputer server yang telah di serang selanjutnya kita konfigurasi *Fortigate Firewall* agar dapat mengantisipasi serangan selanjutnya. Berikut langkah-langkah konfigurasi *Fortigate Firewall* :

a. Pertama kita masuk ke dalam Fortigate terlebih dahulu masukan IP *Fortigate* dengan IP gateway 192.168.1.99 kemudian masuk ke *web browser* untuk login ke dalam *Fortigate*.
b. Kemudian masukkan *username* : admin dan *Password* di kosongkan kemudian klik enter untuk dapat login ke dalam *Fortigate.*

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)

c. Kemudian masuk pada menu *System*, pilih *Feature Fisibility* untuk mengaktifkan DoS *Policy.*
d. kemudian masuk kedalam *Policy & Objects*, pilih menu Ipv4 DoS *Policy* kemudian *create new,* kita dapat memilih untuk mengamankan serangan dari luar atau dari dalam, disini kita buat untuk mengamankan serangan dari luar.
e. kemudian kita *apply* semua *logging* dan pada menu *action* kita pilih monitor kemudian klik Ok.



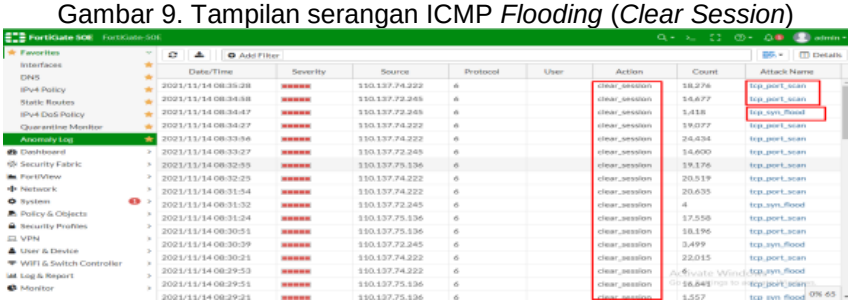
Gambar 8. Tampilan konfogurasi DoS *policy*

Simulasi Serangan ICMP *Flooding* dan *port scanning* setelah konfigurasi *Fortigate*.

Setelah melakukan konfigurasi *Fortigate* pada DoS *Policy* selanjutnya kita melakukan simulasi serangan lagi pada komputer server untuk mengetahui IP dari *attacker* dan melakukan *banned* IP *attaker*.

a. Kemudian kita melakukan serangan yang sama pada komputer server menggunakan linux pada komputer *attacker* sama seperti sebelumnya.
b. Kemudian kita masuk pada menu untuk mengetahui detail serangan yang di tuju ke komputer server seperti Ip *attacker*, tanggal dan waktu serangan, jenis serangan, jumlah serangan ping dan status ip attaker yang terdeteksi.
c. Kemudian kita kembali ke menu DoS *Policy* kemudian kita ubah menu action menjadi block agar saat attacker menyerang lagi Ip *attacker* akan langsung di *block* atau menjadi *Clear session.*

Gambar 9. Tampilan serangan ICMP *Flooding* (*Clear Session*)

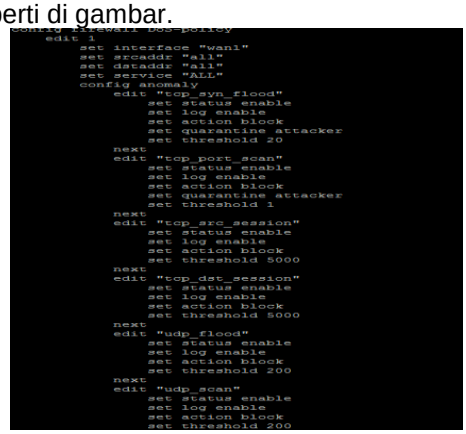


Gambar 10. Tampilan serangan *tcp_port_scan dan tcp_syn_flood* (*Clear Session*)

Banned* Ip *Attacker

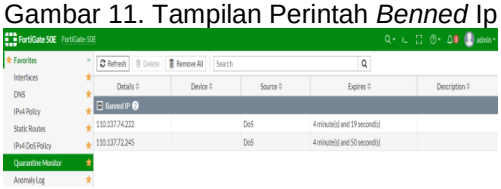
Setelah mengetahui Ip *attacker* yang di tuju ke komputer server selanjutnya kita akan melakukan konfigurasi untuk mem-banned Ip *attacker* agar tidak terjadi serangan lanjutan dari Ip attacker tersebut. Berikut langkah-langkah untuk mem-*banned* Ip :

a. Masuk kedalam CLI untuk melakukan konfigurasinya.
b. Kemudian masukan perintah seperti di gambar.



GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa
e-ISSN : 2775-4561 (Online)
ISSN : 2775-2992(Print)

Gambar 11. Tampilan Perintah *Benned* Ip



Gambar 12. Tampilan Ip yang di *Banned*

KESIMPULAN DAN SARAN

Kesimpulan

Hasil dari simulasi serangan pengujian yang telah dilakukan, dapat di simpulkan serangan ICMP Flooding dan Port scanning sangat berbahaya jika di tuju ke komputer server dapat menyebabkan komputer server hang , dan dengan menggunakan Fortigate sebagai Firewall dapat menjadi salah satu solusi untuk mengatasi serangan ICMP Flooding dan Port scanning untuk mengamankan komputer server dari serangan tersebut

Saran

1. Pengujian Fortigate Firewall ini hanya berfokus pada serangan ICMP Flooding dan Port Scanning saja, karna itu untuk penelitian selanjutnya dapat mengamankan dari serangan yang lainya.
2. Untuk keamanan jaringan dari serangan ICMP Flooding dan Port scanning dapat menggunakan Fotigate sebagai Firewall.

DAFTAR PUSTAKA

Nofriandi, Reza. 2017. “Implementasi Peraturan Walikota Langsa Nomor REG. 800/I/I/227/2016 Tentang Pemberlakuan Absensi Elektronik (E-Disiplin) di Lingkungan Sekretariat Daerah Kota Langsa”. Doctoral dissertation, Universitas Medan Area.

Purwanto dan Sulistyastuti, Analisis Kebijakan dari Formulasi ke Implementasi Kebijakan, Bumi Aksara Jakarta, 1991, Hal. 21

Mulyadi, Deddy. 2015. Studi Kebijakan Publik dan Pelayanan Publik: Konsep dan Aplikasi Proses Kebijakan Publik dan Pelayanan Publik. Cetakan Kesatu. Bandung: Alfabeta CV.

Triwahyuni, D. (2017). Security Pengertian dasar dan Jenisnya. Studi Keamanan Internasional.

Bakti. (2018). Mengetahui Tentang Sistem Keamanan Jaringan Untuk Proteksi Perangkat Anda.

Sofana, I. “Membangun Jaringan Komputer”. Bandung: Informatika Bandung, 2015.

Saputro, B, “Manajemen Penelitian Pengembangan (Research & Development) Bagi Penyusun Tesis dan Disertasi”. Aswaja Pressindo, Yogyakarta, 2017.

Husen, Z., & Surbakti, S. M, “Membangun Server dan Jaringan Komputer dengan Linux Ubuntu”. Syiah Kuala University Press, Aceh, 2020.

Yuliandoko, H, “Jaringan Komputer Wire dan Wireless Beserta Penerapanya”, Deepublish, Yogyakarta, 2018.

MagnaNetwork (2021). Pengertian Fortinet. Diakses pada 15 mei 2021 melalui https://magna-net.com/index.php?page=fortinet

Syseven (2018). Pengertian Fortigate. Diakses pada 15 mei 2021. Melalui https://sysseven.blogspot.com/2018/10/pengertian-dan-pengenalan-fortigate.html

Seputarpengetahuan. (2020, April). Firewall adalah : Pengertian, Fungsi, Manfaat, Jenis, Karakteristik, Cara Kerja.