IMPLEMENTASI NETWORK ACCESS CONTROL PADA JARINGAN SERVER INSTITUT TEKNOLOGI TELKOM SURABAYA

Tugas Akhir

diajukan untuk memenuhi salah satu syarat

memperoleh gelar sarjana

dari Program Studi Teknologi Informasi

Fakultas Informatika

Universitas Telkom

1202200033

MOCHAMAD NUR FIRMANSYACH

Program Studi Sarjana Teknologi Informasi (Kampus Surabaya)

Fakultas Informatika

Universitas Telkom

Surabaya

2024

LEMBAR PENGESAHAN

IMPLEMENTASI NETWORK ACCESS CONTROL PADA JARINGAN SERVER INSTITUT TEKNOLOGI TELKOM SURABAYA

IMPLEMENTATION OF NETWORK ACCESS CONTROL ON THE SERVER NETWORK OF THE TELKOM INSTITUTE OF TECHNOLOGY SURABAYA

NIM :1202200033
MOCHAMAD NUR FIRMANSYACH

Tugas akhir ini telah diterima dan disahkan untuk memenuhi sebagian syarat memperoleh gelar pada Program Studi Sarjana Teknologi Informasi (Kampus Surabaya)
Fakultas Informatika
Universitas Telkom

Surabaya, 12 Juni 2024
Menyetujui

Pembimbing I,	Pembimbing II,
Oktavia Ayu Permata, S.T, M.T.	Rizky Fenaldo Maulana S.Kom., M.Kom.
NIP. 19900006	NIP. 20970031

Ketua Program Studi
Sarjana Teknologi Informasi

Bernadus Anggo Seno Aji, S.Kom., M.Kom.
NIP. 23929009

LEMBAR PERNYATAAN

Dengan ini saya, Mochamad Nur Firmansyach, menyatakan sesungguhnya bahwa Tugas Akhir saya dengan judul Implementasi Network Access Control Pada Jaringan Server Institut Teknologi Telkom Surabaya beserta dengan seluruh isinya adalah merupakan hasil karya sendiri, dan saya tidak melakukan penjiplakan yang tidak sesuai dengan etika keilmuan yang belaku dalam masyarakat keilmuan. Saya siap menanggung resiko/sanksi yang diberikan jika di kemudian hari ditemukan pelanggaran terhadap etika keilmuan dalam buku TA atau jika ada klaim dari pihak lain terhadap keaslian karya,

Surabaya, 12 Juni 2024

Yang Menyatakan

Mochamad Nur Firmansyach

IMPLEMENTASI NETWORK ACCESS CONTROL PADA JARINGAN SERVER INSTITUT TEKNOLOGI TELKOM SURABAYA

IMPLEMENTATION OF NETWORK ACCESS CONTROL ON THE SERVER NETWORK OF THE TELKOM INSTITUTE OF TECHNOLOGY SURABAYA

Mochamad Nur Firmansyach[1], Oktavia Ayu Permata, S.T, M.T.[2], Rizky Fenaldo Maulana S.Kom., M.Kom.[3],

[1,2,3]Prodi S1 Teknologi Informasi, Fakultas Informatika, Universitas Telkom, Surabaya
[1]mnfirman@students.telkomuniversity.ac.id, [2]oktapermata@telkomuniversity.ac.id,
[3]rizkyfenaldo@telkomuniversity.ac.id

Abstrak

Pada lingkungan pendidikan seperti halnya kampus tempat dimana mahasiswa menuntut ilmu serta melakukan penelitian tentunya disediakan sebuah fasilitas berupa jaringan dan komputer untuk mempermudah dalam melakukan kegiatan tersebut. Tidak dapat dipungkiri banyak aktifitas pada jaringan *Local Area Network* (LAN) dan publik yang terpantau oleh sistem keamanan. Pada Fakultas Teknologi Informasi dan Bisnis (FTIB) tentunya suatu saat akan terjadi sebuah serangan menuju server yang bisa berasal dari manapun yang dapat mempengaruhi performa pada server FTIB.

Untuk mencegah hal tersebut dibutuhkan sebuah sistem *Network Access Control* (NAC) yang disertai dengan *firewall* dan *Intrusion Detection System* (IDS) dalam mengantisipasi serangan menuju server FTIB yang dapat mempengaruhi kinerja server. Sistem NAC ini menggunakan platform milik FortiGate untuk mengontrol lalu lintas jaringan serta melakukan pemeriksaan identitas dan penetapan kebijakan akses. Dalam penerapan NAC dilakukan secara simulasi berdasarkan topologi yang ada pada FTIB.

Dalam pengujian sistem NAC autentikasi yang diterapkan pada jaringan lokal dapat membatasi *user* tertentu agar dapat terhubung. Hasil pengujian untuk *firewall* dengan adanya *rules policy* tidak semua *user* dapat mengakses port tertentu dan untuk IDS menghasilkan nilai akurasi 41% untuk jaringan publik dan 99% untuk jaringan lokal. Meskipun terdapat perbedaan persentase, FortiGate berhasil melakukan *clear-session* serangan sehingga performa server FTIB tetap stabil.

Kata kunci : *network access control, firewall,* IDS, jaringan komputer

Abstract

In educational environment like a campus where students study and conduct research, facilities like networks and computers are provided to make it easier to support these activities. It will normal when many activities on local area networks (LAN) and public are monitored by security systems. In Faculty of Information Technology and Business (FTIB) absolutely someday there will be an attack to server which could come from anywhere and can affected the performance of the FTIB server.

Result of NAC system applied to prevent this, Network Access Control (NAC) system is needed which is accompanied by firewall and Intrusion Detection System (IDS) in anticipating attacks to FTIB server which affect server performance. This NAC system uses FortiGate to control network traffic, perform identity checks and establish access policies. This research use simulation with based topology in FTIB.

Result for authentication system to the local network, it can restrict certain users to connect. Results for firewalls with policy rules, not all users can access certain ports and for IDS, gain accuracy values of 43% for public networks and 94% for local networks. Even theres a difference in percentage, FortiGate succeeded in clearing the attack so FTIB server performance remained stable.

Keywords: network access control, firewall, IDS, computer network

1. Pendahuluan

Latar Belakang

Keamanan jaringan merupakan salah satu aspek penting dalam teknologi, baik dalam industry bisnis, Pendidikan, dan beberapa aspek serupa lainnya. Keamanan jaringan berperan utama dalam mencegah serta mengatasi terjadinya serangan yang dilakukan oleh *attacker*. Pada lingkungan kampus terutama pada Fakultas Teknologi Informasi dan Bisnis (FTIB) yang terdapat banyak mahasiswa dan mahasiswi yang memiliki

keberagaman pengetahuan tentunya merupakan salah satu faktor dapat terjadinya suatu serangan yang ditujukan pada server. Keberadaan server FTIB yang masih baru telah digunakan oleh sebagian mahasiswa dan mahasiswi untuk penelitian sehingga ketersediaan Server FTIB sangatlah penting. Dengan penggunaanya yang masih minim dalam satu tahun belakangan tentunya keamanan jaringan masih belum ada dan diterapkan pada lalu lintas server FTIB.

Berdasarkan sumber dari Badan Siber dan Sandi Negara yang dituangkan dalam sebuah dokumen yaitu lanskap keamanan siber Indonesia tahun 2023[1]. Dalam dokumen tersebut diprediksi adanya beberapa serangan siber salah satunya adalah serangan *Denial of Service* (DoS) atau *Distributed Denial of Service* (DDoS). Dengan adanya serangan tersebut tentunya akan sangat berpengaruh terhadap performa pada server FTIB.

Sebuah sistem *Network Access Control* berfungsi dalam memberikan akses control menuju server dan memberikan aturan/*policy* terkait pengguna sebagai bentuk preventif akan adanya suatu serangan menuju server. Penerapan sistem NAC beserta *firewall* dan IDS pada lalu lintas menuju server FTIB dapat mengecilkan kemungkinan serangan menuju server FTIB secara langsung.

Topik dan Batasannya

Pada penelitian ini masalah yang didapati adalah bagaimana memberikan keamanan pada lalu lintas serta keoptimalan *resource* pada server FTIB dengan pengujian berupa serangan DDoS. Dalam penerapan sistem NAC beserta *firewall* dan IDS apakah telah sesuai dengan kebutuhan dalam meningkatkan keamanan pada lalu lintas server FTIB.

Batasan dalam penelitian ini adalah sebagai berikut :

1. Implementasi sistem *Network Access Control* (NAC) dengan platform yang digunakan ialah FortiGate.
2. Implementasi dan uji coba dilakukan secara simulasi berdasarkan topologi nyata pada FTIB.
3. Sistem hanya dapat mendeteksi perangkat yang terhubung.

Tujuan

Pada penelitian ini memiliki tujuan sebagai upaya preventif dalam mengatasi serangan dengan mengidentifikasi pengaruh server terhadap serangan yang terjadi setelah diterapkannya sistem NAC dan pengujian terhadap aturan/*policy* yang diterapkan berdasarkan jaringan yang digunakan. Evaluasi teliti dilakukan dengan membandingkan pengaruh digunakannya sistem NAC dan tidak digunakannya sistem NAC pada lalu lintas server. Parameter yang digunakan untuk mendapatkan hasil evaluasi tersebut adalah jumlah serangan terkirim, jumlah serangan terdeteksi, dan *resource* server berupa kinerja CPU.

Tabel 1. Keterkaitan antara tujuan, pengujian dan kesimpulan

No	Tujuan	Pengujian	Kesimpulan
1	Pengujian NAC	Pengguna dalam mengakses jaringan yang ada pada topologi server FTIB.	Keberhasilan penerapan NAC.
2	Pengujian IDS	Total serangan yang terkirim, total serangan yang terdeteksi serta status CPU.	Keberhasilan dalam meminimalisir serangan.
3	Pengujian *Firewall*	Pengguna mengakses protokol pada port tertentu.	Keberhasilan dalam penerapan *rules.*

Organisasi Tulisan

Pada penelitian ini akan menjelaskan tentang studi terkait terhadap penelitian yang berkaitan dengan topik tugas akhir yang dipilih. Sistem yang dibangun berupa simulasi berdasarkan topologi nyata yang berada pada server FTIB. Evaluasi berisi mengenai hasil dari analisis pengujian berdasarkan sistem yang dibangun. Kesimpulan akan menjelaskan rangkuman secara garis besar pengujian pada penelitian ini.

2. Studi Terkait

Pada bagian penelitian ini terdapat beberapa penelitian yang telah dilakukan sebelumnya serta dasar teori mengenai topik *Network Acces Control* (NAC) yang dijadikan sebagai referensi peneliti.

Pada penelitian [2] menggunakan platform milik Genian dalam melakukan monitoring dan kontrol pada perangkat yang terhubung. Hasil yang didapati dari penelitian ini yaitu *rules* yang telah diterapkan berhasil termonitoring pada bagian log.

Penelitian [3] menggunakan platform milik ForeScout dengan menggunakan protokol SNMP dan LDAP. Hasil dari penelitian ini yaitu log pada jumlah pengguna yang 100% berhasil terhubung ke jaringan setelah menginstall *antivirus*.

Penelitian [4] menggunakan platform milik PacketFence dengan berfokus pada *remote management* oleh pengguna. Hasil dari penelitian yaitu log pada user yang berhasil terhubung ke jaringan yang dapat melakukan aktifitas *remote* menggunakan protokol ssh.

Penelitian [5] menggunakan platform milik Cisco ISE dengan berfokus pada penerapan IDS dan IPS. Hasil dari penelitian ini yaitu penggunaan NAC tidak cukup dalam meningkatkan keamanan jaringan melainkan harus diiringi dengan penggunaan IDS dan IPS dalam meningkatkan keamanan jaringan.

Penelitian [6] menggunakan platform milik Cisco ISE dengan berfokus pada penerapan RADIUS server serta protokol AAA. Hasil dari penelitian ini yaitu perangkat yang telah terdaftar dapat terhubung secara langsung ke jaringan dengan mudah. Sedangkan, perangkat yang tidak terdaftar akan langsung ditolak dalam upaya terhubung ke jaringan.

Network Access Control

Network Access Control (NAC) adalah sebuah solusi dalam keamanan jaringan komputer yang menggunakan beberapa protokol dalam memberikan akses dalam jaringan kepada pengguna [7]. Dalam penerapan NAC dilakukan berdasarkan *policy* atau kebijakan yang dimiliki perusahaan. NAC juga memiliki fungsi sebagai *firewall*, IDS, dan perangkat *anti-virus.*

FortiGate

FortiGate adalah perangkat keamanan jaringan yang dimiliki oleh perusahaan Fortinet. Sedangkan, Fortinet sendiri adalah perusahaan yang bergerak pada industri jaringan dan telah dikenal dibanyak negara. FortiGate memiliki fitur keamanan jaringan yang sehingga tidak memerlukan perangkat keamanan jaringan tambahan [8].

Firewall

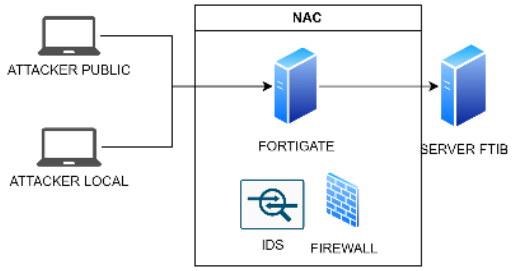
Firewall adalah sistem keamanan jaringan yang berfungsi dalam melakukan filter paket data dari luar (*outbound*) ataupun dari dalam (*inbound*) pada satu jaringan [9].

Intrusion Detection System

Intrusion Detection System (IDS) merupakan sebuah proses monitoring terhadap aktifitas yang tidak wajar atau tidak sesuai dengan *policy* yang diterapkan serta mendeteksi kemungkinan terjadinya serangan [5]. Dalam melakukan deteksi terhadap serangan metode yang dipilih adalah *Anomaly-based* karena metode ini akan memberikan alert apabila terdapat lalu lintas yang tidak wajar atau tidak sesuai *threshold* yang ditentukan sehingga dianggap sebuah anomali [10]. Dalam penerapan *threshold* apabila tidak dikonfigurasi dengan benar maka sistem tidak akan berjalan sesuai [11].

3. Sistem yang Dibangun

Pada penelitian ini sistem yang dibuat dapat dilihat pada gambar1, sistem NAC sendiri akan melakukan autentikasi dalam pemberian akses ke jaringan lokal dengan cara pembuatan *captive portal* yang akan membedakan hak akses pada jaringan lokal dan jaringan publik, agar dapat terhubung maka *user* harus terdaftar pada FortiGate. Sedangkan, Dalam pengujian IDS dilakukan serangan dari *attacker public* dan *attacker local* serangan yang dilakukan adalah DDoS berupa ICMP *flood* untuk menguji ketangguhan FortiGate dalam meredam serangan menuju *server* FTIB. Dalam pengujian *firewall* dilakukan dengan akses pada port tertentu sesuai dengan *rules inbound* dan *outbound*. Pada serangan yang terdeteksi akan tercatat sebagai anomali pada *log* yang terdapat pada FortiGate.

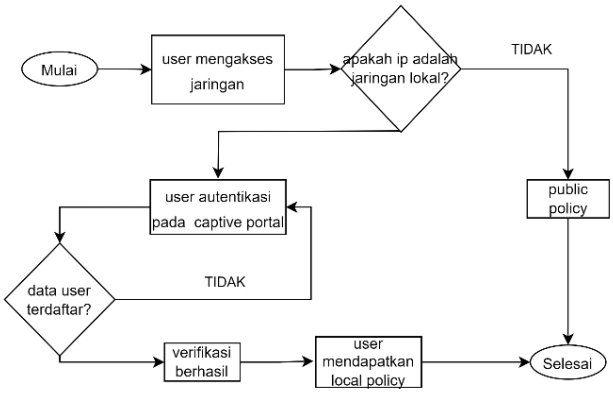


Gambar 1. Desain sistem

Sistem yang dibangun sesuai dengan topologi nyata yang berada pada lalu lintas jaringan server FTIB dapat dilihat pada gambar 1 (lampiran). FortiGate yang sudah terkonfigurasi akan berfungsi dalam memberikan *captive portal* dalam mengautentikasi *user* yang hendak terhubung, memberikan *rules firewall*, dan memantau lalu lintas menuju server melalui log. Dalam penentuan *threshold* terutama pada ICMP *flood* digunakan sebesar 250 paket per detik [11]. Sehingga, apabila dalam pemantauan ditemukan paket yang melebihi jumlah *threshold* yang ditentukan maka akan langsung dilakukan *clear session* dalam penyesuaian *threshold* sendiri mengacu pada lalu lintas pada jaringan FTIB yang memiliki rentang sedang. Penelitian ini dilakukan secara simulasi dengan

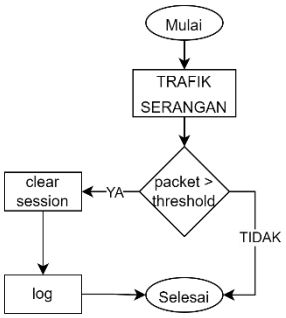
menggunakan EVE-NG agar dapat memudahkan dalam memberi gambaran terkait sistem yang dibangun. Dalam perancangan sistem jaringan lokal dibangun secara *Virtual Local Area Network* (VLAN) pada jaringan lokal dibangun menggunakan VLAN10 dan jaringan server menggunakan VLAN20. Penggunaan VLAN ini untuk memudahkan dalam pemberian alamat IP serta pembagian hak akses pada Fortigate.

Alur sistem dalam melakukan pengujian NAC beserta pemberian *rules firewall* dapat dilihat pada gambar 2 ketika *user* melakukan percobaan *login* pada *captive portal* yang dibuat ketika terhubung pada jaringan lokal dan *session* yang diberikan bersifat *keepalive* yang berarti akan tetap terhubung kecuali *user* yang melakukan *logout*. Pada upaya *login* tersebut *user* wajib telah terdaftar agar dapat terhubung ke jaringan lokal. Alur sistem dalam pemberian *rules firewall user* mencoba mengakses suatu port maka akan melewati FortiGate yang apabila alamat ip milik *user* yang melakukan request berada pada jaringan local maka rules firewall akan menyesuaikan yaitu local policy. Sedangkan, apabila tidak maka akan langsung disesuaikan menjadi public policy.



Gambar 2. Diagram alir pengujian NAC

Alur sistem dalam pengujian IDS dapat dilihat pada gambar 3 dimana ketika terdapat sebuah traffik serangan menuju server maka akan melewati FortiGate dahulu yang tentunya akan diperiksa apakah paket yang masuk diatas *threshold* yang ditentukan apabila benar maka paket tersebut akan langsung dilakukan *clear session* sehingga tidak terkirim menuju server melainkan dibatalkan oleh FortiGate. Dalam skenario serangan dilakukan dengan menggunakan HPING3 untuk mengirimkan paket sebesar 100 paket perdetik dengan mode *faster* pada protokol ICMP dan dilakukan pada beberapa durasi waktu yaitu 5 menit, 10 menit, dan 20 menit. Sehingga, pada upaya serangan tersebut akan terdeteksi sebagai serangan ICMP *flood*.

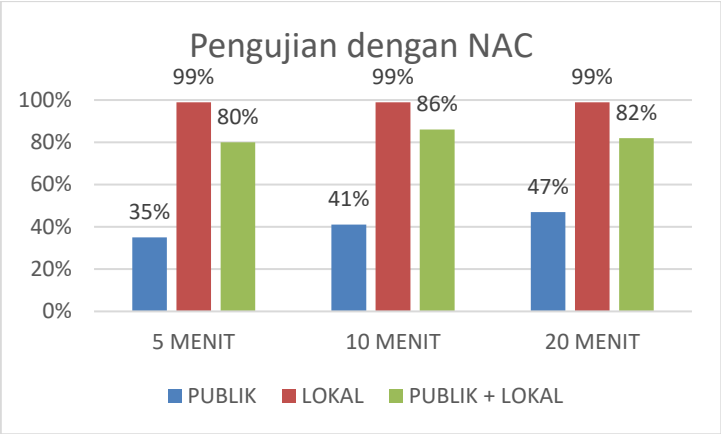


Gambar 3. Diagram alir pengujian IDS

4. Evaluasi

4.1 Hasil Pengujian

Pada penelitian ini dilakukan perbandingan dengan penggunaan NAC dan tanpa NAC untuk pengujian berupa serangan *Denial of Service* (DoS) serta percobaan dalam melakukan akses menuju protokol port FTP, SSH, HTTP, dan MySQL. Data yang diperoleh dapat dilihat pada gambar 4 tentang penggunaan sistem NAC dan pada gambar 3(lampiran) yang tidak menggunakan NAC yaitu perbedaan pada nilai persentase berdasarkan periode waktu dan asal serangan berasal. Dalam pengujian *firewall* dapat dilihat pada tabel 2 bahwa terdapat perbedaan dalam akses menuju *port* 3306 milik protokol MySQL.



Gambar 4. Grafik hasil pengujian IDS dengan sistem NAC

Tabel 2. Hasil pengujian *firewall*

Port	Nama	Dengan NAC		Tanpa NAC	
		Publik	Lokal	Publik	Lokal
3306	MySQL	DENY	ACCEPT	ACCEPT	ACCEPT

4.2 Analisis Hasil Pengujian

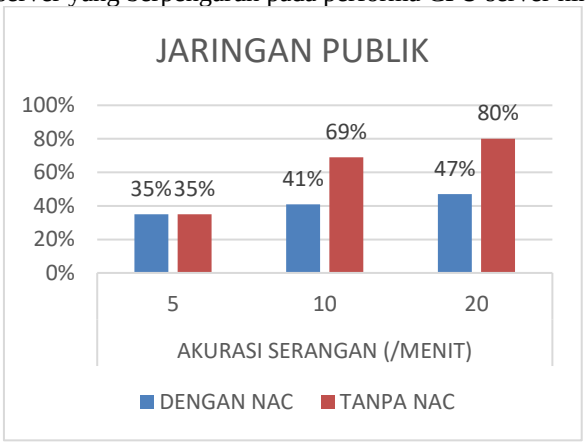
Pada pengujian dalam penelitian ini didapati bahwa terdapat perbedaan data yang diperoleh antara persentase serangan dengan performa pada CPU server.

4.2.1 Hasil pengujian IDS

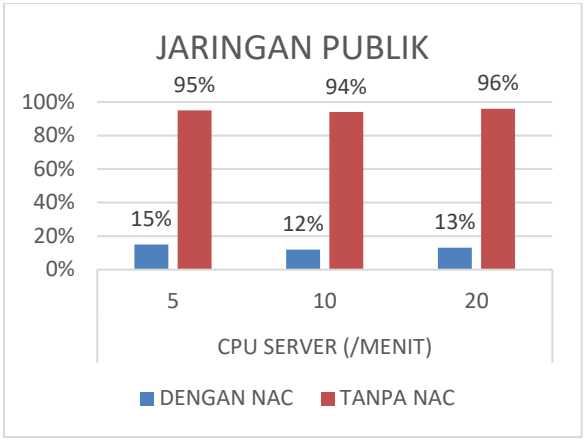
Dari hasil pengujian IDS dilakukan 3 kali skenario serangan yaitu dari *attacker* pada jaringan publik, jaringan lokal, dan kombinasi serangan dari 2 jaringan tersebut.

Pengujian dari jaringan publik

Dari hasil pengujian yang dilakukan pada jaringan publik dapat dilihat terdapat perbedaan nilai persentase dari akurasi serangan pada gambar 6 dan juga performa CPU server pada gambar 7. Dalam penggunaan NAC akurasi serangan yang terdeteksi cenderung dibawah 50% akan tetapi meskipun jumlah terdeteksi dibawah 50% tidak memiliki pengaruh terhadap CPU server yang stabil dibawah 20%. Sedangkan, tanpa penggunaan NAC serangan yang terdeteksi cenderung meningkat hingga 80% yang berarti serangan tersebut berhasil terkirim ke server yang berpengaruh pada performa CPU server hingga diatas 90%.



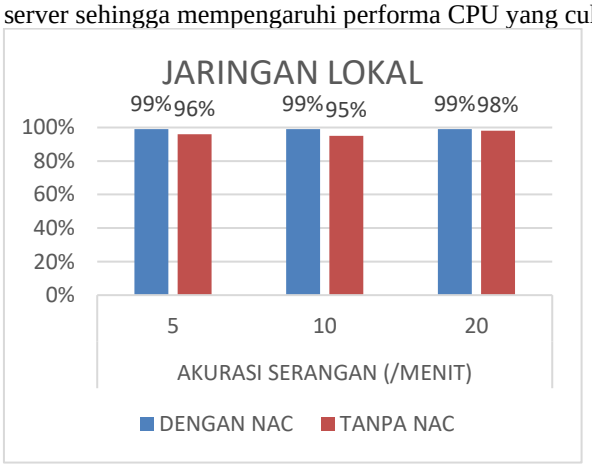
Gambar 6. Grafik hasil pengujian dari jaringan publik



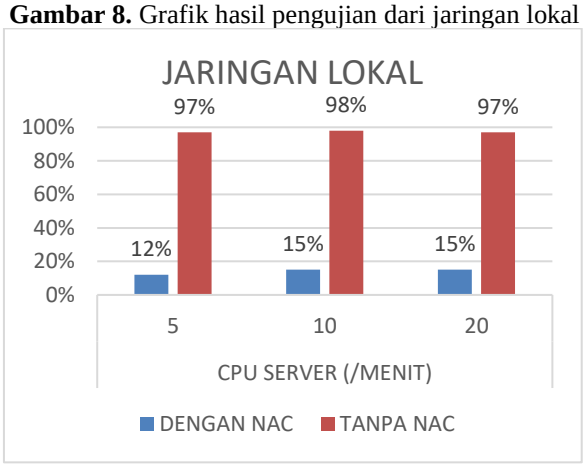
Gambar 7. Grafik hasil performa server

Pengujian dari jaringan lokal

Dari hasil pengujian yang dilakukan pada jaringan lokal dapat dilihat pada bahwa terdapat kemiripan nilai persentase dari akurasi serangan pada gambar 8 akan tetapi pada CPU server terdapat perbedaan pada gambar 9. Pada penggunaan NAC akurasi serangan yang didapat hampir diatas 90% terdeteksi dan juga berhasil ditangani hingga performa CPU server tidak terpengaruh melainkan tetap stabil dibawah 20%. Sedangkan, tanpa penggunaan NAC serangan yang terdeteksi cukup tinggi diatas 90% dengan kata lain serangan secara keseluruhan terkirim menuju server sehingga mempengaruhi performa CPU yang cukup tinggi diatas 90%.



Gambar 8. Grafik hasil pengujian dari jaringan lokal

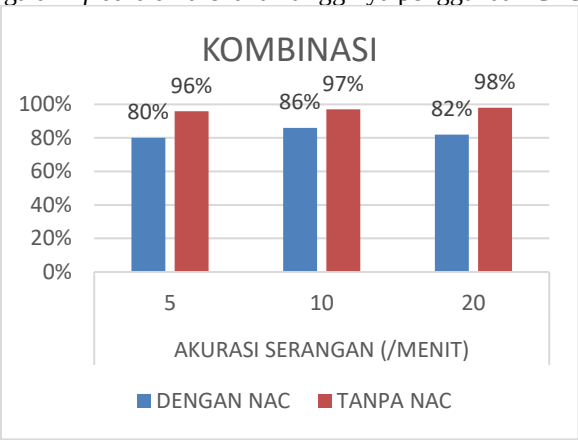


Gambar 9. Grafik hasil performa server

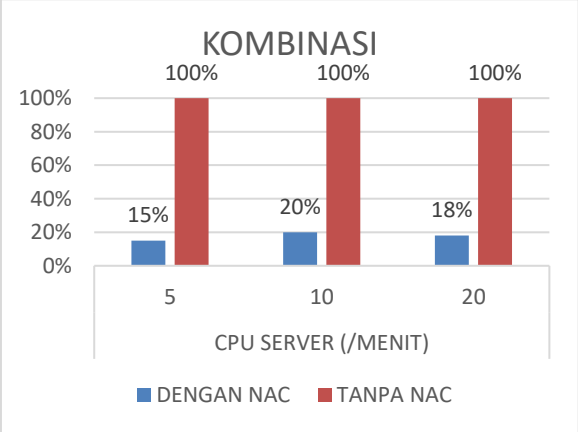
Pengujian dari kombinasi serangan

Dari hasil pengujian yang dilakukan secara kombinasi yaitu *attacker* dari jaringan publik dan jaringan lokal melakukan serangan secara bersamaan dapat dilihat bahwa terdapat perbedaan pada nilai persentase terdeteksinya serangan pada gambar 10 dan pengaruh pada performa CPU server pada gambar 11. Pada penggunaan NAC didapati akurasi terdeteksi serangan diatas 80% dengan tingginya serangan yang terdeteksi NACg berhasil melakukan *clear session* sehingga pengaruh pada performa CPU server tetap stabil dibawah 20%. Sedangkan, pengujian tanpa NAC didapati bahwa nilai akurasi terdeteksi serangan cukup tinggi yang

berarti keseluruhan serangan berhasil terkirim menuju server yang diperkuat juga dengan performa CPU server saat dilakukan pengujian mengalami *freeze* dikarenakan tingginya penggunaan CPU hingga 100%.



Gambar 10. Grafik hasil pengujian dari serangan kombinasi



Gambar 11. Grafik hasil performa server

4.2.2 Hasil pengujian Firewall

Berdasarkan *rules firewall* yang ada pada jaringan FTIB pada tabel 3. Maka hasil dari pengujian dapat dilihat pada tabel 4 hasil dengan diterapkannya *rules firewall* maka jaringan publik tidak memiliki kebebasan akses seperti halnya pada jaringan lokal. *User* pada jaringan lokal tidak dapat mengakses protokol milik MySQL atau database yang berada pada port 3306.

Tabel 3. *Rules firewall* pada jaringan FTIB

Port	Nama	Jaringan	
		Publik	Lokal
20	FTP	ACCEPT	ACCEPT
22	SSH	ACCEPT	ACCEPT
80	HTTP	ACCEPT	ACCEPT
3306	MySQL	DENY	ACCEPT

Tabel 4. Hasil pengujian dengan *firewall*

Port	Nama	Perkiraan		Hasil	
		Publik	Lokal	Publik	Lokal
3306	MySQL	DENY	ACCEPT	DENY	ACCEPT

Sedangkan tanpa diterapkannya *rules firewall* dapat dilihat pada tabel 4 semua user memiliki kebebasan yang sama yang dimana seharusnya *user* pada jaringan publik tidak dapat mengakses database pada server FTIB.

Tabel 5. Hasil pengujian tanpa *firewall*

Port	Nama	Perkiraan		Hasil	
		Publik	Lokal	Publik	Lokal
3306	MySQL	DENY	ACCEPT	ACCEPT	ACCEPT

5. Kesimpulan

Berdasarkan hasil dari penelitian yang dilakukan kesimpulan yang dapat diambil bahwa penggunaan NAC disertai IDS dan *firewall* mendapatkan hasil yang cukup baik dimana nilai akurasi pada jaringan lokal sebesar 99% dan jaringan publik sebesar 41% meskipun terdapat perbedaan nilai akurasi akan tetapi pengaruh pada performa server sangat minim sehingga server tetap stabil. Dengan adanya sistem NAC disertai IDS dan *firewall* dapat meminimalisir terjadinya serangan yang dapat mempengaruhi performa server dan dapat membatasi usaha dalam mengakses protokol tertentu pada server. Adapun, saran untuk penelitian berikutnya yaitu pengujian dalam penggunaan NAC dapat menggunakan metode autentikasi dan verifikasi yang lain.

Daftar Pustaka

[1] A. Yusuf, "LANSKAP KEAMANAN SIBER INDONESIA 2023," 2023. [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

[2] S. R. Damara, "Analisis dan Implementasi Kontrol Akses Jaringan dan Kebijakan pada PT. Asuransi Jiwa Sinarmas MSIG Tbk Menggunakan Sistem Genian NAC," *J. Ilm. Komputasi*, vol. 19, no. 3, pp. 373–382, 2020, doi: 10.32409/jikstik.19.3.67.

[3] M. Syani, R. M. Tresna, E. A. Firdaus, and F. F. Nugraha, "Penerapan Network Access Control Autentikasi Internal Network Security Protokol 802.1 X," *Nuansa Inform.*, vol. 16, no. 2, pp. 77–86, 2022, doi: 10.25134/nuansa.v16i2.5800.

[4] R. Agyare, C. Adu-Boahene, and S. N. Nikoi, "Secure Remote Network Management and Network Access Control, the Case of University of Education-kumasi Campus," *Int. J. Syst. Eng.*, vol. 6, no. 1, pp. 18–45, 2022, doi: 10.11648/j.ijse.20220601.13.

[5] A. S. Putra and N. Surantha, "Internal threat defense using network access control and Intrusion Prevention System," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 9, pp. 371–375, 2019, doi: 10.14569/ijacsa.2019.0100948.

[6] D. Kus Heryadi and A. Surya Budiman, "Optimasi Keamanan Pada Jaringan Multi-Endpoint Access Menggunakan Network Access Control Berbasis Cisco ISE," *JIKA (Jurnal Inform. Univ. Muhammadiyah Tangerang* , pp. 313–324, 2021.

[7] I. Winarno, "IMPLEMENTASI NETWORK ACCESS CONTROL PADA JARINGAN EEPIS," no. July, 2015.

[8] F. R. Arbie and M. Raharjo, "IMPLEMENTASI KEAMANAN JARINGAN DENGAN METODE SECURITY PROFILES MENGGUNAKAN FORTIGATE PADA KOMISI APARATUR SIPIL NEGARA," *J. Inform. Terpadu*, vol. 7, no. 1, pp. 21–26, 2021, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[9] K. Aziz, S. Zakir, W. Aprison, and L. Efriyanti, "Implementasi Keamanan Jaringan Dengan Metode Firewall Filtering Menggunakan Mikrotik," *J. Simki-Techsain*, vol. 02, no. 01, p. 9, 2018, [Online]. Available: http://simki.unpkediri.ac.id/mahasiswa/file_artikel/2018/49b68be9ba26a905f0a3b0883b428eb4.pdf

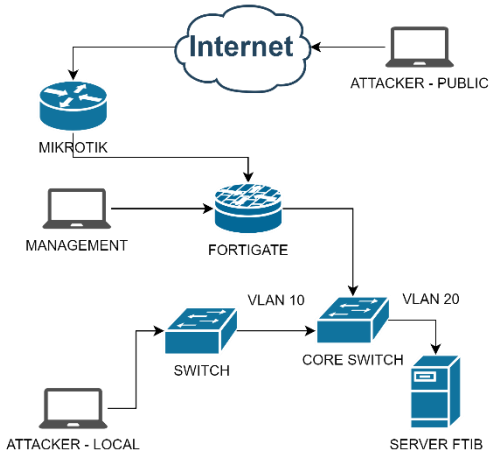
[10] A. S. Fadhlillah, D. N. Bogi, and A. I. Irawan, "ANALISIS PERFORMANSI IDS MENGGUNAKAN METODE DETEKSI ANOMALY- BASED TERHADAP SERANGAN DOS," vol. 6, no. 2, p. 3398, 2019.

[11] M. Pruett, "DoS Protection." Accessed: May 15, 2024. [Online]. Available: https://www.fortinetguru.com/2018/12/dos-protection-3/

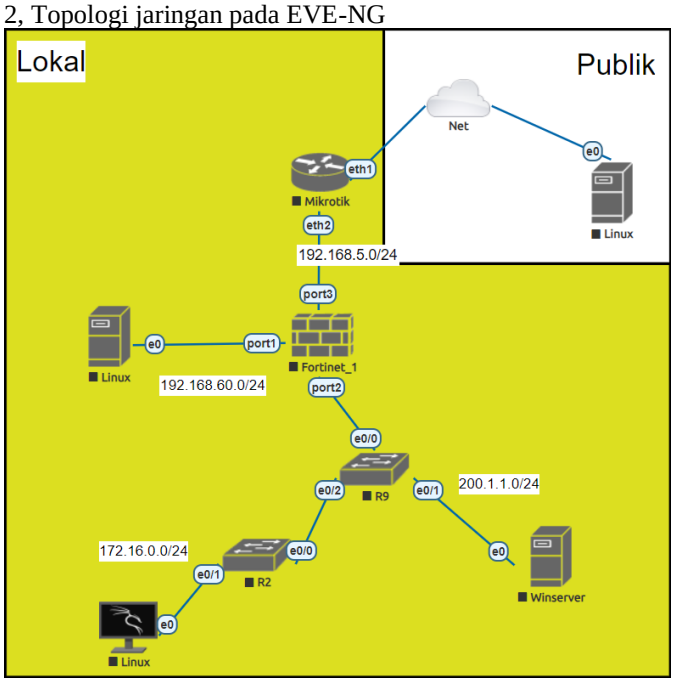
Lampiran

Topologi jaringan :

1. Desain topologi jaringan

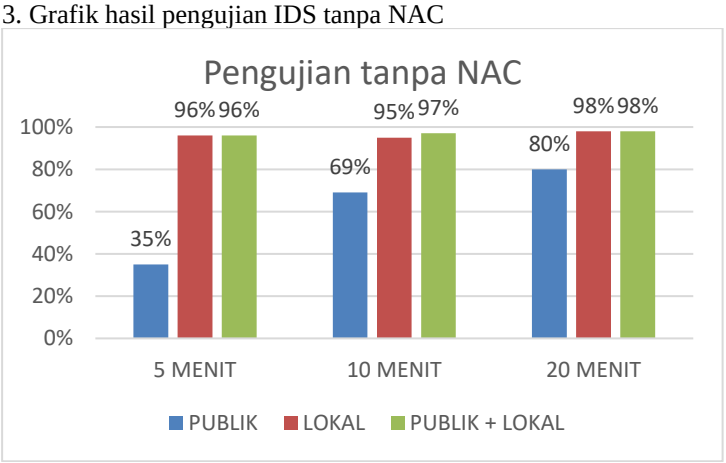


2, Topologi jaringan pada EVE-NG



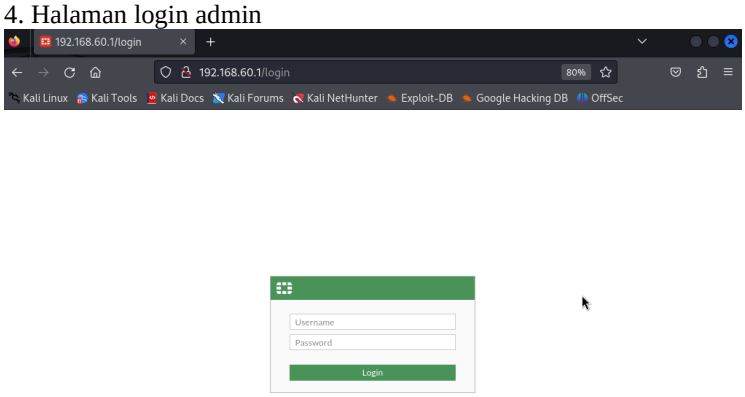
Grafik pengujian :

3. Grafik hasil pengujian IDS tanpa NAC

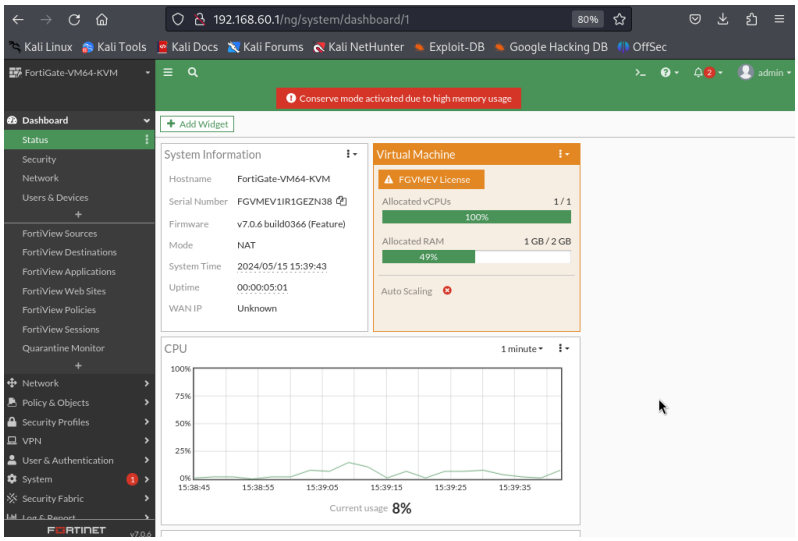


Halaman pada FortiGate :

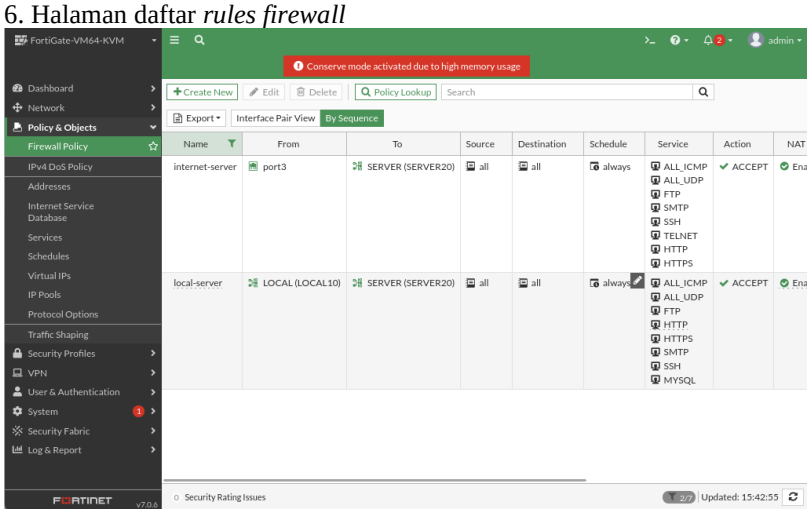
4. Halaman login admin



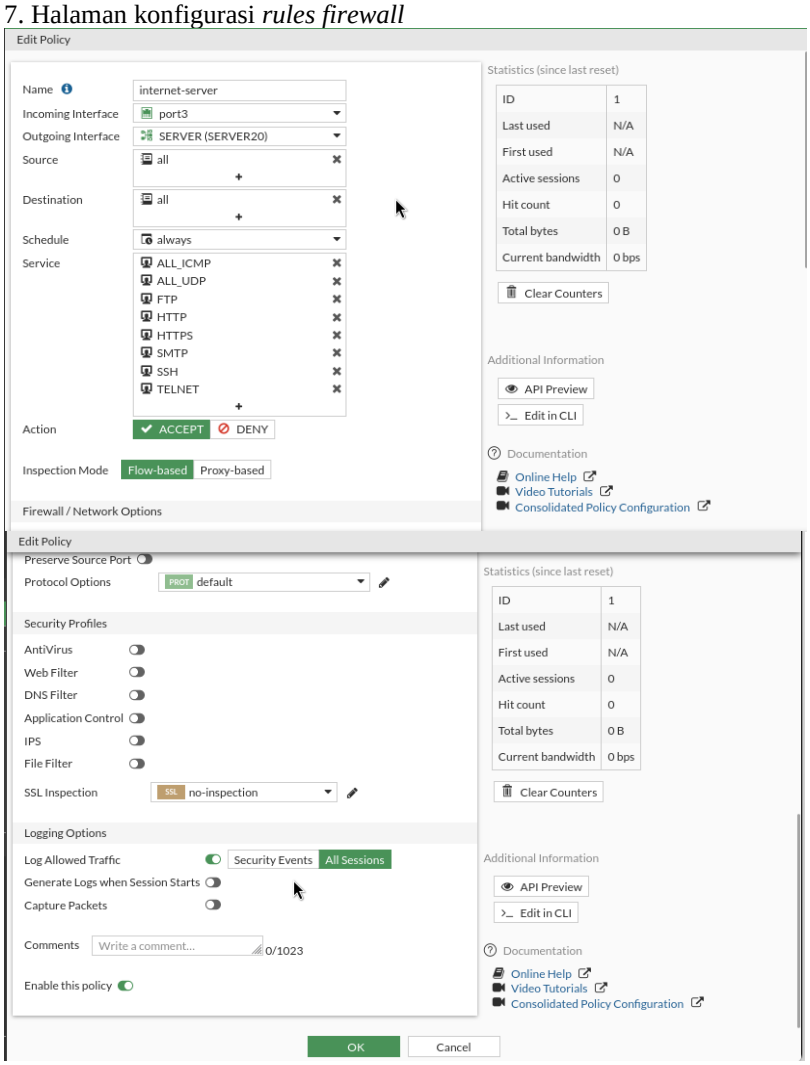
5. Halaman dashboard admin



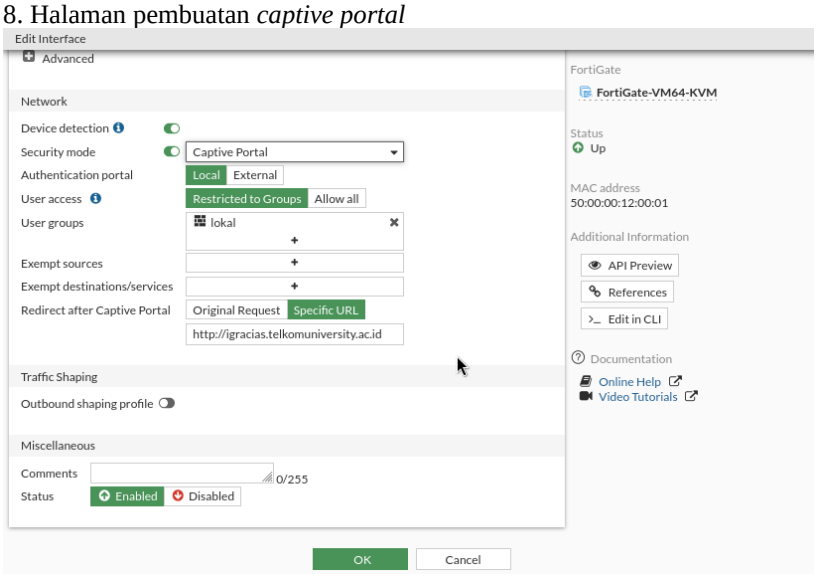
6. Halaman daftar *rules firewall*



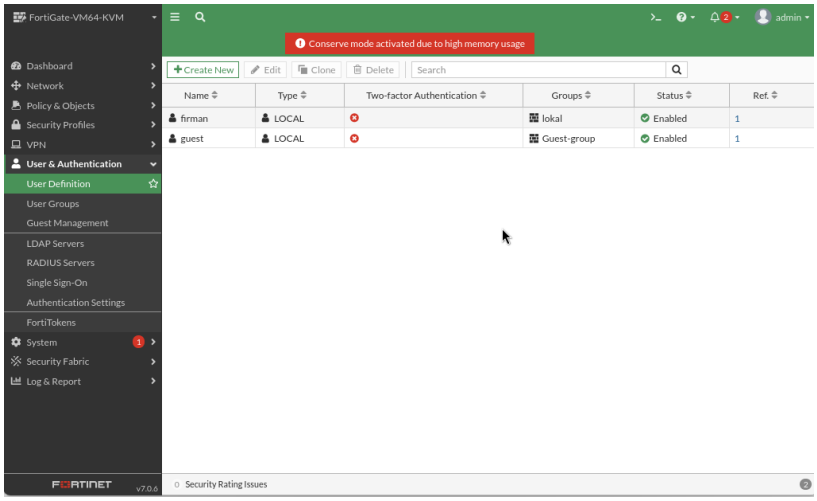
7. Halaman konfigurasi *rules firewall*



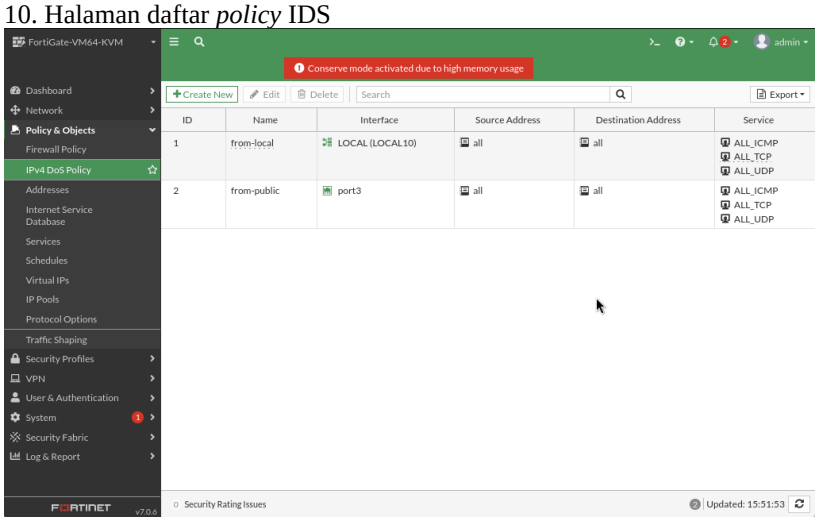
8. Halaman pembuatan *captive portal*



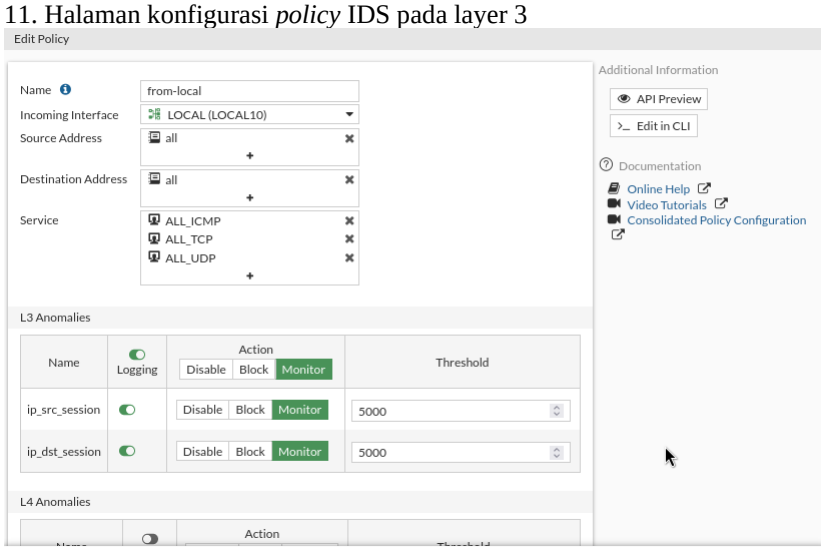
9. Halaman daftar user untuk autentikasi NAC



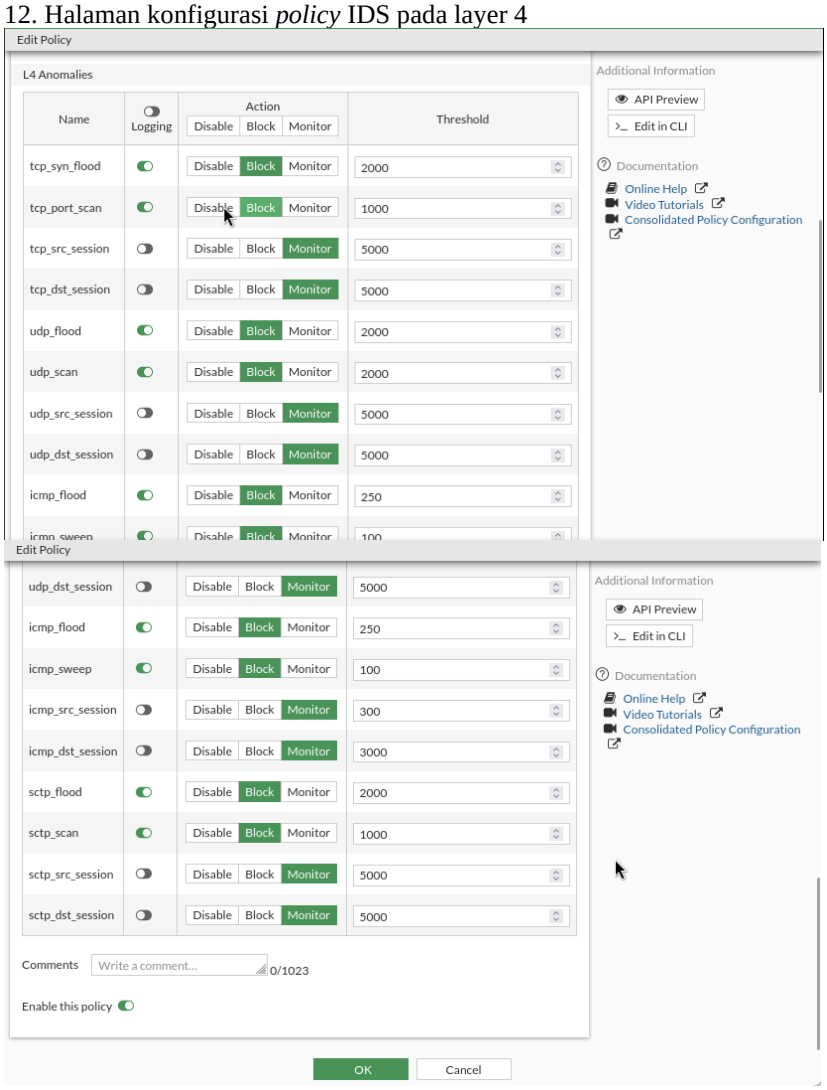
10. Halaman daftar *policy* IDS



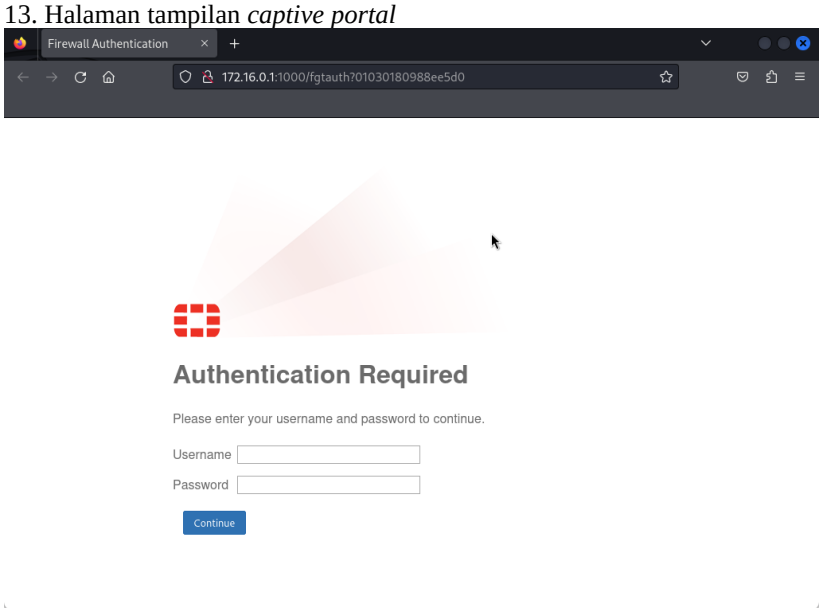
11. Halaman konfigurasi *policy* IDS pada layer 3



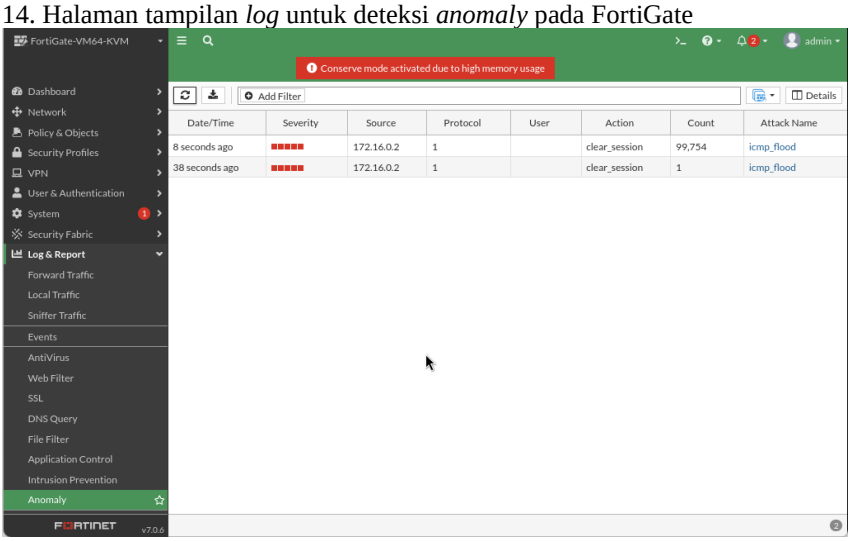
12. Halaman konfigurasi *policy* IDS pada layer 4



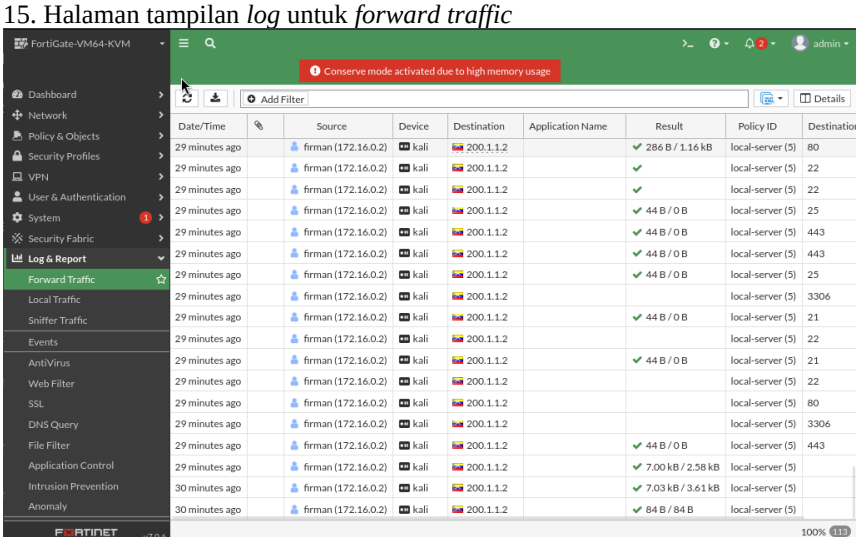
13. Halaman tampilan *captive portal*



14. Halaman tampilan *log* untuk deteksi *anomaly* pada FortiGate



15. Halaman tampilan *log* untuk *forward traffic*



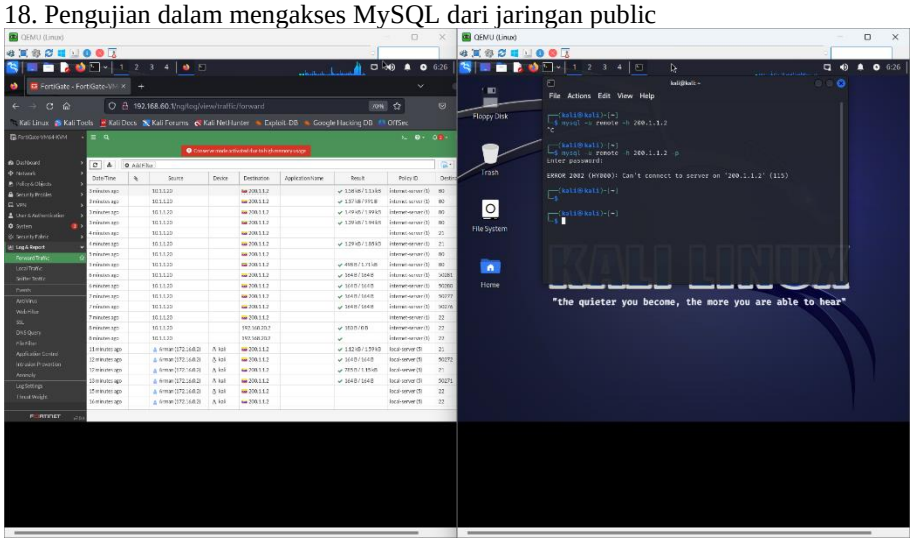
16. Pengambilan data selama durasi 10 menit

2 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,676
3 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,795
3 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,677
4 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,708
4 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,971
5 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,805
5 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,900
6 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,878
6 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,782
7 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,875
7 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,763
8 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,783
8 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,925
9 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,795
9 minutes ago	■■■■■	10.1.1.20	1		clear_session	87,783
10 minutes ago	■■■■■	10.1.1.20	1		clear_session	92,034
10 minutes ago	■■■■■	10.1.1.20	1		clear_session	20,398

Pengujian terhadap firewall :

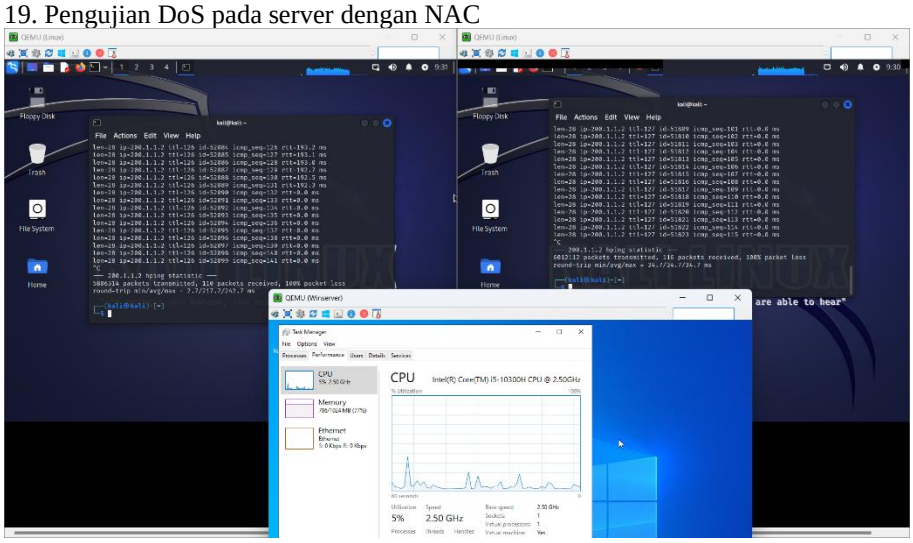
17. Pengujian dalam mengakses MySQL dari jaringan lokal

18. Pengujian dalam mengakses MySQL dari jaringan public



Pengujian terhadap IDS

19. Pengujian DoS pada server dengan NAC



20. Pengujian DoS pada server tanpa NAC