JURNAL CAHAYA MANDALIKA

P-ISSN: 2828-495X
E-ISSN: 2721-4796

OPTIMALISASI KEAMANAN FIREWALL PADA INFRASTRUKTUR JARINGAN SMK IDN BOGOR

Mesra Betty Yel[1], Dadang Iskandar Mulyana[2], Joe Renaldy F[3], Muhammad Dzaky Nurfaishal[4], Muhamad Hasbi Toharudin B[5]

Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta

Email: optime.mby@gmail.com[1], mahvin2012@gmail.com[2], joerenaldyf13@gmail.com[3], dzakymuh22@gmail.com[4], muhammadhasbi1611@gmail.com[5]

Kata Kunci:
LAN, Firewall, Peretasan Sosial

ABSTRAK

SMK IDN Bogor yang berdiri sejak tahun 2016 dikenal sebagai salah satu dari banyaknya sekolah yang terjun di dunia akademik, agama dan juga berfokus pada IT, sebagai mana visinya "Jagoan IT Pinter Ngaji". Mengingat banyaknya aktivitas IT baik dari sisi pembelajaran maupun secara administratif pendataan perkantoran (Tata Usaha), tentunya penerapan Firewall pada jaringan merupakan salah satu hal krusial yang diperlukan guna memfasilitasi keamanan dan keaslian data dari para guru dan siswa. Tujuan dari dibuatnya laporan KKP ini tidak lain adalah untuk membantu melakukan optimalisasi konfigurasi Firewall, baik di perangkat Firewall maupun PC/ Laptop beserta strategi penyuluhan sebagai tindakan preventive untuk menghindari peretasan secara fisik/ social engineering di SMK IDN Bogor. Seperti yang sudah sama-sama diketahui, bahwa permasalahan kemanan siber merupakan hal yang tidak bisa dianggap remeh. Oleh karena itu, demi keberlangsungan dan kelancaran aktivitas Pendidikan sekolah diperlukan Optimalisasi/Standarisasi terhadap seluruh segmen atau bagian yang menggunakan jaringan di lingkungan SMK IDN Bogor.

Keywords :
LAN, Firewall, Social Engineering

ABSTRACT

IDN Bogor Vocational High School, which was established in 2016, is known as one of the many schools that are involved in the academic, religious and IT-focused world, as its vision is "Wonder of IT Smart of Praying". Given the large number of IT activities both in terms of learning and administratively office data collection (Administration), of course the application of a Firewall on the network is one of the crucial things needed to facilitate the security and authenticity of data from teachers and students. The purpose of preparing this KKP report is none other than to help optimize Firewall configurations, both on Firewall devices and PCs/Laptops along with counseling strategies as preventive measures to avoid physical/social engineering hacking at SMK IDN Bogor. As we all know, cybersecurity issues cannot be taken lightly. Therefore, for the sake of the continuity and smooth running of school education activities, Optimization/Standardization of all segments or parts that use the network within SMK IDN Bogor is required.

PENDAHULUAN

Kebutuhan internet saat ini sudah sangat menjadi bagian dari masyarakat Indonesia. Dalam perkembangan teknologi saat ini, internet menjadi sarana penting dalam suatu pencarian informasi seperti ilmu pengetahuan, dunia hiburan, hingga menjadi salah satu faktor penting dalam dunia Pendidikan (Hapsari & Pamungkas, 2019). Oleh karena itu, Indonesia merupakan salah satu dari banyak nya negara yang memiliki sosial media aktif terbanyak mencapai 191 juta pada januari 2022 mengutip data dari website dataindonesia.id. Namun, apabila merujuk ke hal yang berkaitan dengan permasalahan pembobolan akun, phising (Pencurian Data), ataupun Man in the middle (peretasan dengan cara membobol internet internal) tidak dapat dipungkiri Indonesia masih jadi yang terbawah dalam hal pengamanan data bersifat pribadi ataupun semacam nya, berdasarkan data yang diambil dari website databooks.katadata.co.id bahwa Indonesia berada di peringkat 3 terendah diantara negara G20 dalam hal pengamanan Siber.

Peretasan yang terjadi tidak hanya terjadi secara daring/ online namun juga secara fisik dan tentunya tidak akan memandang bulu dalam mencari target, begitupun dengan dunia Pendidikan saat ini (Sulaiman, 2021). Salah satu kasus yang pernah terjadi di dunia Pendidikan adalah peretasan data – data para siswa ataupun Guru yang selanjutnya di jual secara bebas di dark web. Oleh karena itu, keamanan siber yang ada di setiap lembaga pemerintahan maupun swasta diharuskan memiliki keamanan tingkat tinggi ataupun sesuai dengan standard yang sudah di tentukan. Dengan masih ada nya masalah yang berhubungan dengan keamanan siber, maka diperlukan ada nya standarisasi di setiap perangkat jaringan khusus nya di perangkat firewall yang notabene berfungsi sebagai pertahanan pertama di infrastruktur jaringan dari kejahatan siber.

Laporan KKP ini kami buat dengan maksud sebagai persyaratan dalam menuntaskan studi S1. Adapun tujuan dari dibuatkan laporan ini untuk menjawab beberapa masalah, diatanra lain bagaimana cara membuat Lingkup jaringan internet yang dimiliki oleh SMK IDN Bogor bisa semakin aman dibanding sebelumnya.

TINJAUAN PUSTAKA

1. Local Area Network

LAN adalah suatu jaringan komputer yang cakupan wilayahnya hanya mencakup wilayah lokal saja atau terbatas. Contoh yang termasuk jaringan LAN adalah jaringan komputer di perkantoran, sekolah, cafe, rumah pribadi, dan lain sebagainya. Sederhananya, LAN adalah sebuah sistem komunikasi komputer yang jaraknya dibatasi tidak lebih dari beberapa kilometer dan menggunakan koneksi high-speed antara 2 hingga 100 Mbps (Widiatmoko Herbimo, 2021).

Pada LAN, setiap komputer dapat mengakses sumber daya yang ada di LAN sesuai dengan akses yang diberikan yang sudah diatur sebelumnya. LAN memungkinkan kita untuk sharing data atau menggunakan satu printer bersamaan dalam satu (Alfurqon & Assegaff, 2018).

2. Firewall

Firewall adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya. Firewall umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah firewall menjadi istilah generik yang merujuk pada sistem yang

mengatur komunikasi antar dua jaringan yang berbeda (Diskominfo Kota Bogor) (Hikmaturokhman et al., 2015).

Sehingga, tugas utama dari adanya firewall sendiri adalah untuk melakukan monitoring dan mengontrol semua akses masuk atau keluar koneksi jaringan berdasarkan aturan keamanan yang telah ditetapkan.

3. Access-list/ Access Rules

ACL merupakan daftar access control yang berisi perizinan serta data kemana user akan diberikan izin. Jika data telah memiliki izin, maka hanya dapat diakses oleh beberapa user yang telah diberikan akses saja dan tentunya sudah dikontrol oleh access control tersebut. Dalam hal ini, diperlukan administrator untuk mengamankan informasi dan mengatur hak atas informasi apa saja yang boleh diakses dan kapan informasi tersebut dapat diakses. Secara sederhana ACL merupakan sebuah standar keamanan (Jaelani, 2021).

Cara kerja ACL sendiri adalah selalu membaca setiap list dengan cara sequential atau berurut dari atas ke bawah. Ketika ada paket data ACL akan membaca dan membandingkan setiap list yang sudah dibuat. Jika menemukan kondisi yang sesuai, paket akan mengikuti aturan yang sudah ada dalam Access List. Namun jika paket tidak menemukan kondisi yang sesuai maka paket tidak bisa mendapatkan akses (Sari et al., 2020).

Penggunaan paling umum dan paling mudah untuk dimengerti adalah melakukan penyaringan paket yang tidak diinginkan saat Anda melakukan implementasi kebijakan keamanan, seperti mengatur Access Control List untuk membuat keputusan yang sangat spesifik mengenai pola lalu lintas sehingga hanya host tertentu saja yang dapat mengakses sumber daya tersebut, sedangkan yang lainnya ditolak (Roza et al., 2020).

Access list juga dapat digunakan pada situasi lain, dimana tidak harus meliputi penolakan paket, seperti mengontrol network yang akan atau tidak dinyatakan sebagai protokol dynamic routing dengan mengkonfigurasikan access list dengan cara yang sama seperti sebelumnya dimana penerapannya dilakukan ke protocol routing bukan ke interface. Selain itu, kita juga dapat menggunakan ACL ini untuk mengkategorikan paket atau antrian atau layanan QOS serta mengontrol tipe lalu lintas data nama yang akan mengaktifkan link ISDN (Chaidir, 2018).

Statement ACL pada dasarnya merupakan paket filter, dimana paket akan dibandingkan, dikategorikan serta dilakukan tindakan terhadap paket yang dikirimkan. List daftar yang telah dibuat kemudian diterapkan kepada lalu lintas inbound maupun outbond pada interface dimanapun. Dengan menerapkan ACL, akan membuat router mampu menganalisa setiap paket arah spesifik yang melalui interface tersebut serta mengambil tindakan yang sesuai (Kautsar, 2013).

4. TCP/ IP

TCP/IP merupakan standar komunikasi data dalam proses tukar menukar data dari satu komputer ke komputer lain dalam sebuah jaringan. TCP/IP merupakan protocol yang paling banyak digunakan saat ini (Anshori, 2019).

Untuk perkembangan TCP/IP sendiri dilakukan oleh beberapa badan seperti Internet Society (ISOC), Internet Architecture Board (IAB), dan Internet Engineering Task Force (IETF). Macam-macam protokol yang berjalan di atas TCP/IP, skema pengalamatan, dan konsep TCP/IP didefinisikan dalam dokumen yang disebut sebagai Request for Comment (RFC) yang dirilis oleh IETF. TCP/IP mengimplementasikan arsitektur berlapis yang terdiri dari empat lapis yang

dapat dipetakan terhadap model referensi OSI. OSI merupakan arsitektur komunikasi yang terdiri dari 7 layer.

5. Social Engineering/ Rekayasa Sosial

Social engineering adalah tindakan memanipulasi seseorang dengan memanfaatkan kesalahan mereka untuk memberikan data atau informasi yang bersifat rahasia (Hastuti et al., 2021). Dalam menjalankan aksinya, pelaku kejahatan human hacking biasanya menyamar sebagai pihak yang berwenang, sehingga korban mau memberikan data berharganya kepada pelaku.

Serangan seperti ini bisa saja terjadi secara online, tatap muka, ataupun dalam bentuk interaksi lainnya. Salah satu contohnya adalah kasus penipuan yang memanfaatkan informasi yang bagikan seseorang melalui media sosialnya (Mauhibatillah, 2022).

6. Peretas/ Hacker

Hacker adalah seorang yang ahli dalam bidang komputer jaringan atau keterampilan lain untuk mengatasi masalah teknis (Suharmanto et al., 2018). Dalam bahasa Indonesia, arti hacker adalah peretas. Hacker menggunakan keterampilan teknis untuk mengeksploitasi pertahanan keamanan siber.

Peretasan mengacu pada aktivitas yang berupaya mengakses secara ilegal perangkat digital, seperti komputer, ponsel cerdas, tablet, dan bahkan seluruh jaringan (Raharjo, 2021). Tujuan hacker adalah seringkali untuk mendapatkan akses tidak sah ke komputer, jaringan, sistem komputasi, perangkat seluler, atau sistem. Hal ini justru akan menimbulkan kerugian bagi pengguna dan termasuk dalam tindakan kejahatan siber.

METODE

Data Penelitian

Data penelitian merupakan keterangan atau bahan yang bisa dijadikan sebagai dasar kajian dalam suatu penelitian. Berdasarkan penelitian yang dilakukan, peneliti memilih untuk menggunakan klasifikasi berdasarkan Sumber yang terbagi menjadi dua jenis data, yaitu:

1. Data internal

Jenis data ini adalah data yang didapatkan dari dalam tempat penelitian, dalam hal ini didalam sekolah SMK IDN Bogor kita melakukan pendataan mengenai seberapa seringnya para siswa dan guru mengakses jaringan internet beserta dengan situs – situs yang sering dibuka, dengan adanya pengumpulan data ini diharapkan bisa membuat mudah proses implementasi yang digunakan kedepannya.

2. Data Eksternal

Jenis data yang didapatkan dari luar ruang lingkup tempat penelitian dilakukan ini digunakan peneliti sebagai pembanding dengan data internal yang sudah dikumpulkan sebelumnya untuk mencapai kesesuaian konfigurasi sesuai dengan standar yang ada didunia saat ini. Peneliti melakukan pencarian data mengenai situs – situs yang dinilai tidak sesuai dengan lingkungan para siswa yang notabene masih berada dijenjang SMP dan SMK, serta penyesuaian mengenai alur data trafik yang digunakan dilingkungan SMK IDN Bogor.

Penerapan Metodologi

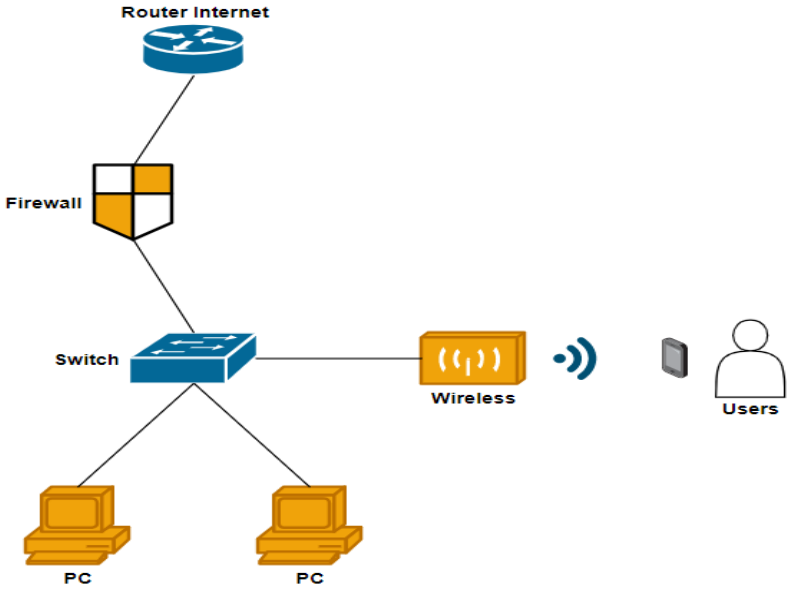
Dalam tahap ini peneliti menggunakan metode yang bernama Network Development Life Cycle (NDLC), merupakan suatu pendekatan proses dalam komunikasi data yang menggunakan siklus yang tiada awal dan akhirnya dalam membangun sebuah jaringan provider, mencakup

sejumlah tahap yaitu analisis, desain, simulasi prototype, implementasi, monitoring dan manajemen.

HASIL DAN PEMBAHASAN

1. Alat Penelitian

Alat Penelitian yang digunakan di lingkup jaringan RS Siloam terdiri dari Router, Firewall, Switch, Access Point, dan juga endpoint (PC, Laptop, Dll.)



Gambar 1 Jenis – jenis perangkat

Spesifikasi perangkat yang dimiliki oleh tim IT SMK IDN saat ini adalah sebagai berikut.
:

Tabel 1 Tipe dan Jenis Perangkat

No	Perangkat Keras	Spesifikasi	Keterangan
1	Router Mikrotik RB750Gr3	- Processor Baru (MediaTek 2 Core 4 threads – 880Mhz) - RAM 256MB - Slot USB - Slot MicroSD	
2	Router Mikrotik sebagai Firewall RB941-2^{nD}	- Processor 650Mhz - 4 port Fast Ethernet - Build-in Wireless 2.4Ghz (802.11b/g/n) - Antenna internal Dual-Chain 2 x 1.5dbi	

3	Switch HPE	- Managed Switch - 24 x 10/100/1000Mbps Ethernet Ports - 2 x SFP Gigabit Ports - Unit Utama	
4	Wireless Unifi AP AC LR	Networking Interface: (1) 10/100/1000 Ethernet Ports Antennas: (1) Dual-Band Antenna, Tri-Polarity, 3 dBi Max TX Power: 2.4GHz: 24 dBm – 5GHz: 22 dBm Buttons: Reset Wifi Standards: 802.11 a/b/g/n/ac	

2. Implementasi Dan Pengujian

Implementasi yang kami lakukan meliputi beberapa skema karena tidak hanya menggunakan satu perangkat/ system untuk membuat optimalisasi semakin baik. Oleh karena itu, yang pertama adalah tahap untuk menentukan alur dari traffic yang melewati proses pemfilteran menggunakan firewall.

a. Desain

Desain merupakan tahap penelitian untuk mendapatkan cara yang paling efektif dan efisien mengimplementasikan sistem dengan bantuan data yang didapatkan dalam tahap analisis. Berikut ini rincian desain yang dilakukan dalam penelitian ini:

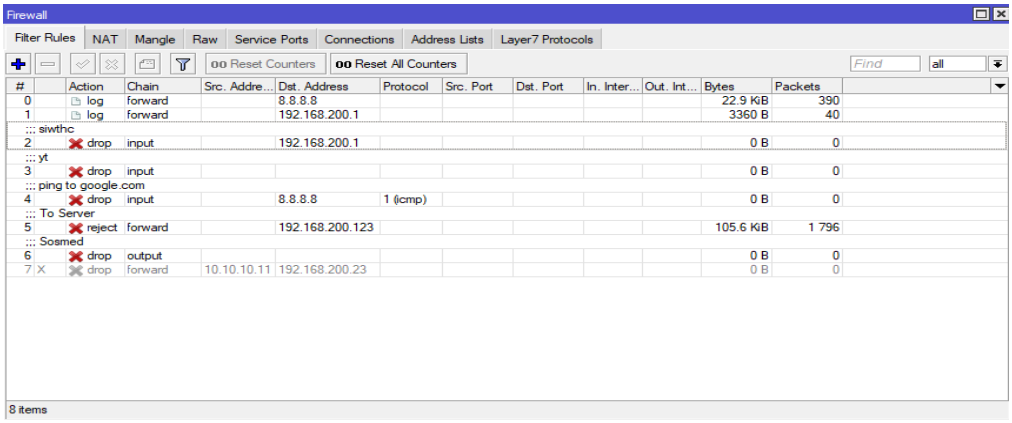
b. Metode Pengaplikasian

Guna mencapai tujuan optimalisasi yang dilakukan di lingkungan IT SMK IDN, berikut kami jelaskan mengenai apa saja cara yang digunakan :

1) Analisa konfigurasi Firewall yang dimiliki saat ini di SMK IDN, selanjutnya melakukan pengetesan apakah rules tersebut sudah berjalan sebagaimana mestinya atau masih memerlukan “tuning”/ perubahan untuk bisa lebih memaksimalkan rules yang ada (termasuk pengecekan Rules untuk Wireless Access Point).
2) Melakukan pengecekan di beberapa laptop/ PC yang ada di SMK IDN sebagai sample untuk melihat apakah sudah dipakaikan password. Jika belum, maka disarankan untuk menambahkan password juga pengecekan apakah firewall yang digunakan di Laptop tersebut sudah dalam kondisi menyala atau belum.
3) Melakukan penyuluhan terkait pentingnya menyimpan data pribadi untuk bisa mencapai perlindungan yang sempurna dari hacker/ peretas termasuk tidak asal menggunakan flashdisk orang lain dan juga tidak asal membuka link yang dikirimkan kepada user lewat media sosial dll.

c. Hasil Analisa Perangkat Firewall lama

Berikut adalah capture yang didapatkan dari perangkat firewall yang dimiliki oleh tim IT SMK IDN.



Gambar 2 Rules Firewall lama

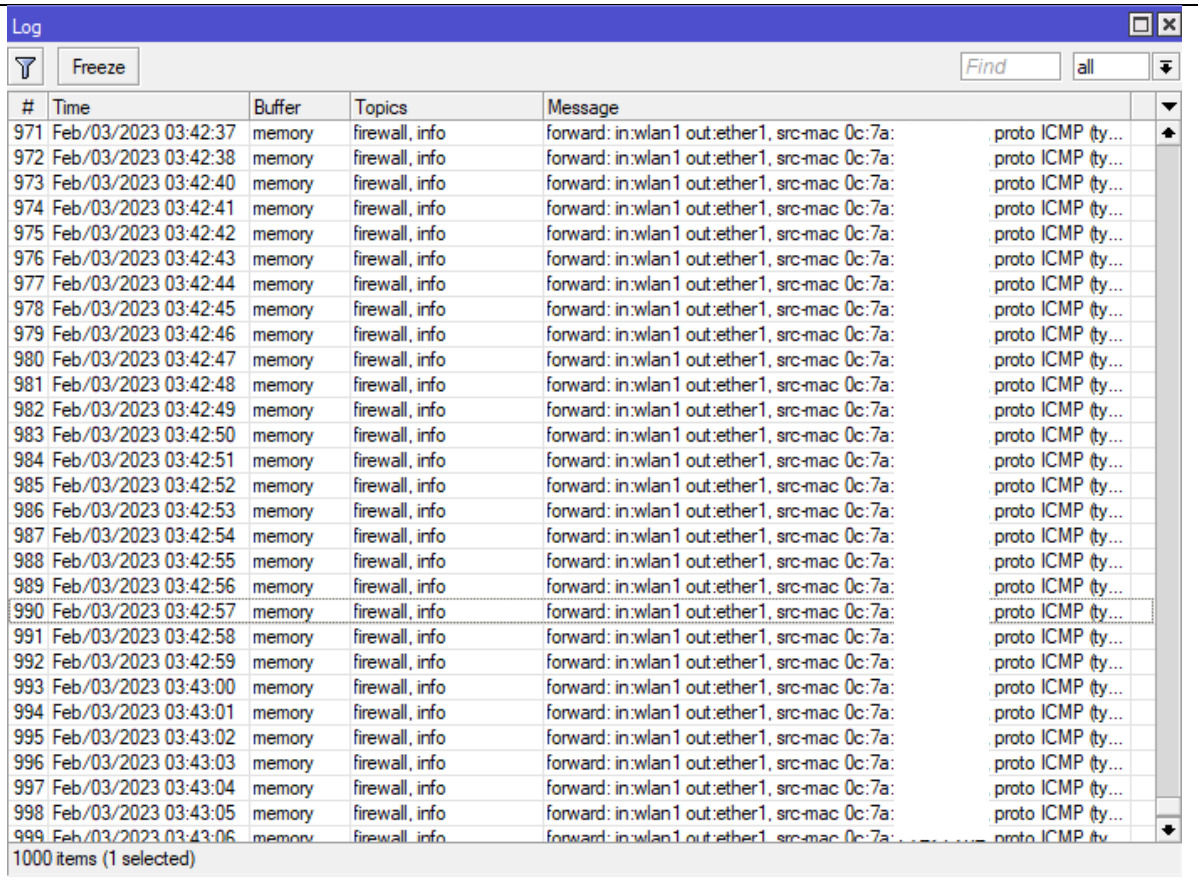
Terlihat ada beberapa Rules yang digunakan untuk mengamankan jaringan internal saat ini, untuk penjelasan detailnya adalah sebagai berikut:

Tabel 2 Hasil Analisa Firewall Rules

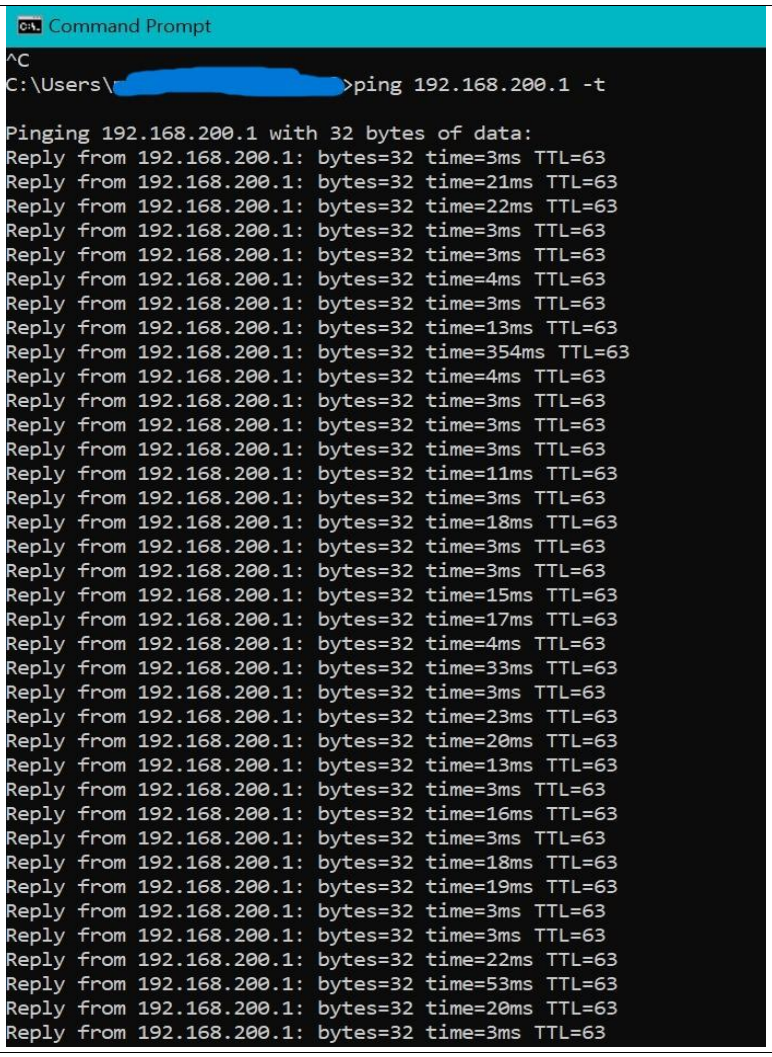
No.	Hasil Analisa Rules Firewall
1	0 log forward 8.8.8.8 10.5 KiB 180 1 log forward 192.168.200.1 2268 B 27
	Rules nol dan pertama memiliki tujuan untuk melakukan logging/ pendataan terhadap IP Address yang terdata dilist tersebut, dimana sering ditemui bahwa ip tersebut adalah salah satu DNS Google.com yang merupakan salah satu web browser terpopuler saat ini.
2	;;; siwthc 2 drop input 192.168.200.1 0 B 0
	Rules kedua jika dilihat dari deskripsi yang ada merupakan sebuah rules yang digunakan untuk melakukan blocking menuju IP Address Switch (*tertulis siwthc*).
3	;;; yt 3 drop input 0 B 0
	Rules ketiga memiliki tujuan untuk memblokir akses dari user menuju ke laman YouTube (*berdasarkan deskripsi yang ada dilist tersebut*).
4	;;; ping to google.com 4 drop input 8.8.8.8 1 (icmp) 0 B 0
	Rules keempat bertujuan untuk memblokir akses ping menuju ke DNS yang dimiliki Google.com
5	;;; To Server 5 reject forward 192.168.200.123 105.6 KiB 1 796
	Rules kelima bertujuan untuk me-reject/ blocking packet yang berasal dari manapun menuju ke IP Server tersebut.
6	;;; Sosmed 6 drop output 0 B 0
	Rules keenam digunakan untuk memblokir akses dari user menuju laman sosial media tertentu.
7	7 X drop forward 10.10.10.11 192.168.200.23 0 B 0

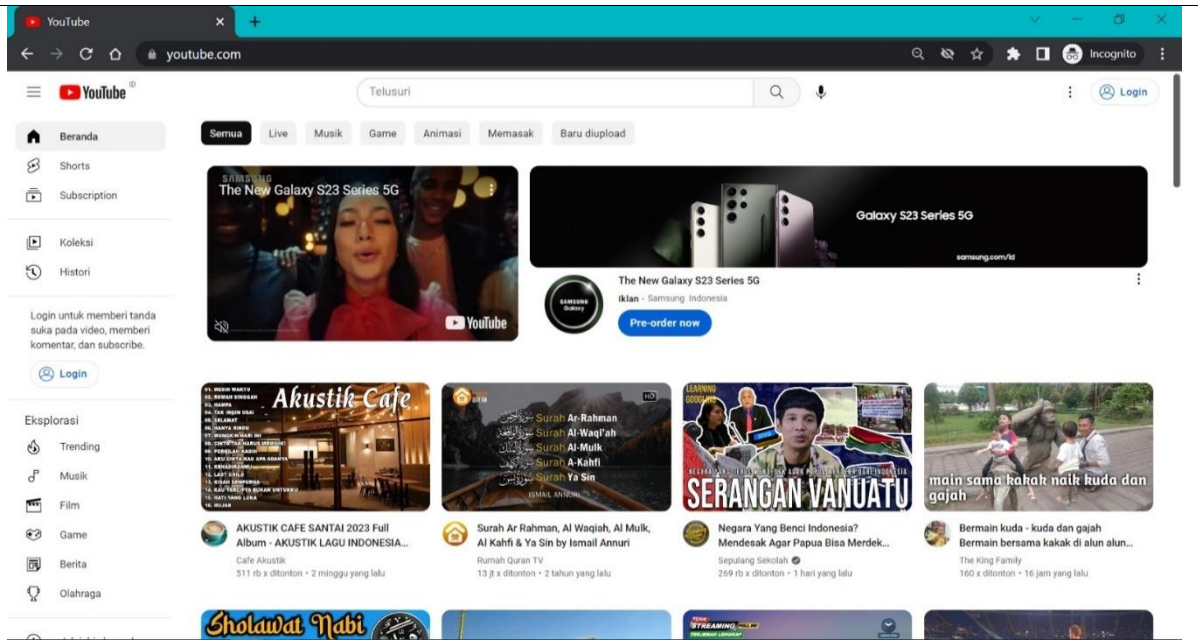
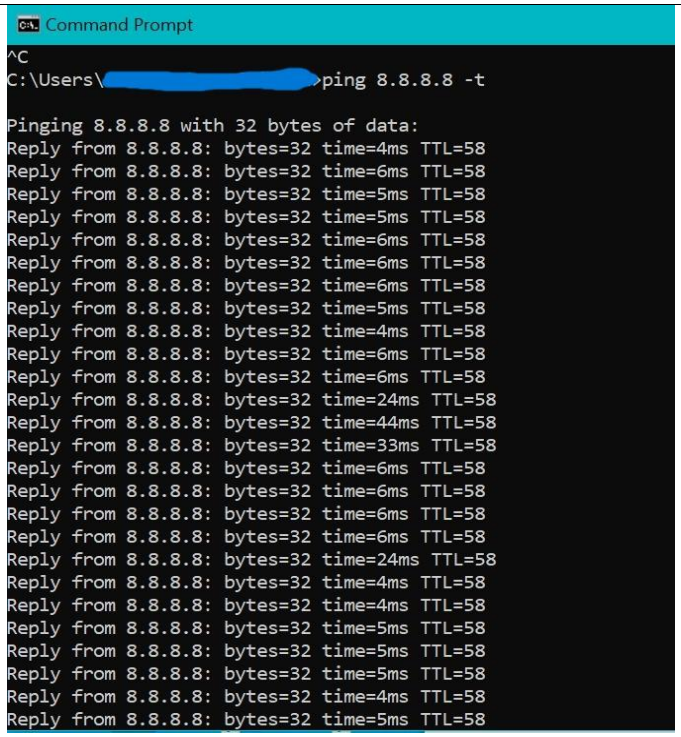
	Rules ketujuh merupakan rules yang digunakan untuk memblokir user saat mengakses salah satu IP yang ada di lingkungan jaringan SMK IDN namun kondisi nya disable/ nonaktif.

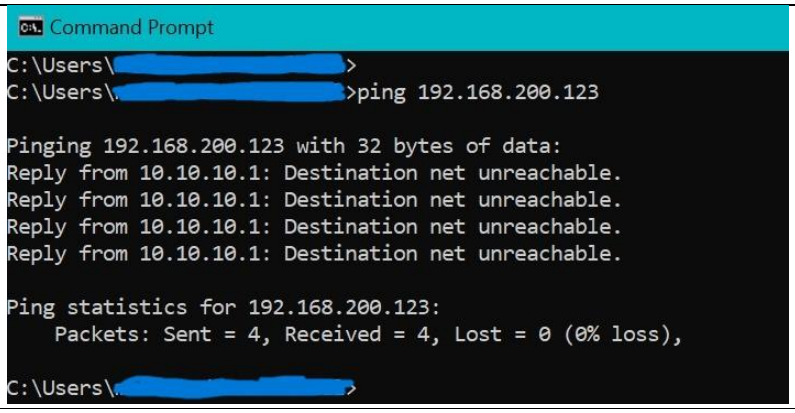
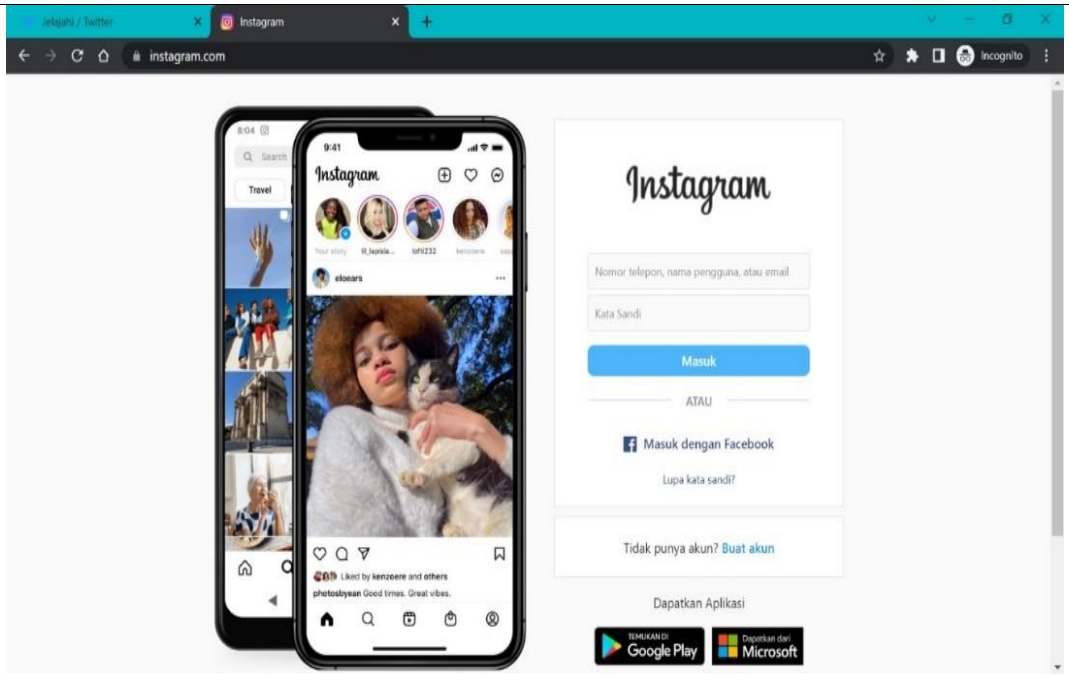
Tabel 3 Masalah yang Ditemukan

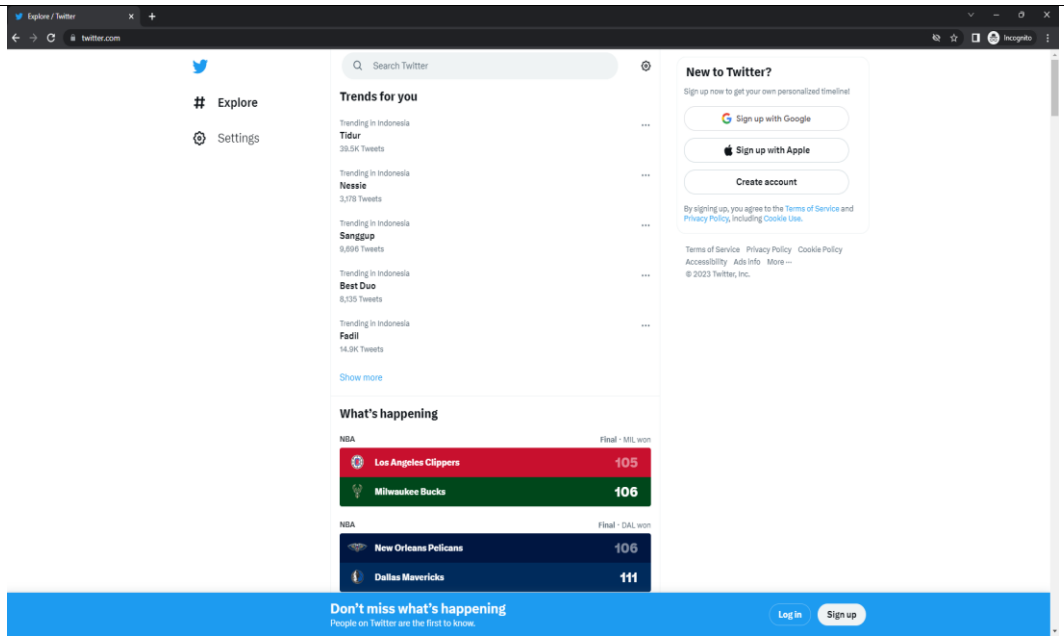
No.	Masalah yang ditemukan
1	 Dengan adanya filter rules yang menggunakan action Log, bukan tidak mungkin bisa membuat memori internal yang dimiliki router firewall itu sendiri bisa cepat full dan bisa berpengaruh terhadap kinerja firewall itu sendiri, diatas merupakan salah satu sebab dari diaktifkannya fungsi action Log. Fungsi dari action Log itu sendiri biasa digunakan untuk mendata paket data yang ada di setiap traffic jaringan tertentu yang dipilih. Namun biasanya tidak disarankan untuk menggunakannya kearah DNS Google.com maupun IP perangkat yang ada di jaringan internal.

#	Time	Buffer	Topics	Message
971	Feb/03/2023 03:42:37	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
972	Feb/03/2023 03:42:38	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
973	Feb/03/2023 03:42:40	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
974	Feb/03/2023 03:42:41	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
975	Feb/03/2023 03:42:42	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
976	Feb/03/2023 03:42:43	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
977	Feb/03/2023 03:42:44	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
978	Feb/03/2023 03:42:45	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
979	Feb/03/2023 03:42:46	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
980	Feb/03/2023 03:42:47	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
981	Feb/03/2023 03:42:48	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
982	Feb/03/2023 03:42:49	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
983	Feb/03/2023 03:42:50	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
984	Feb/03/2023 03:42:51	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
985	Feb/03/2023 03:42:52	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
986	Feb/03/2023 03:42:53	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
987	Feb/03/2023 03:42:54	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
988	Feb/03/2023 03:42:55	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
989	Feb/03/2023 03:42:56	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
990	Feb/03/2023 03:42:57	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
991	Feb/03/2023 03:42:58	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
992	Feb/03/2023 03:42:59	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
993	Feb/03/2023 03:43:00	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
994	Feb/03/2023 03:43:01	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
995	Feb/03/2023 03:43:02	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
996	Feb/03/2023 03:43:03	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
997	Feb/03/2023 03:43:04	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
998	Feb/03/2023 03:43:05	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...
999	Feb/03/2023 03:43:06	memory	firewall, info	forward: in:wlan1 out:ether1, src-mac 0c:7a: proto ICMP (ty...

2	
	Rules kedua yang dimiliki oleh tim IT SMK IDN Bogor jika dilihat dari action dan tujuannya ingin untuk membatasi akses dari berbagai source menuju ke IP Switch, tapi yang terjadi secara aktual saat ini user masih bisa mencoba akses test ping menuju ke IP yang dituju. Sebagai tambahan info juga dari tim IT yang memiliki IP tersebut ternyata dimiliki Router Internet, oleh sebab itu akan kami lakukan perubahan juga untuk deskripsi yang ada.	

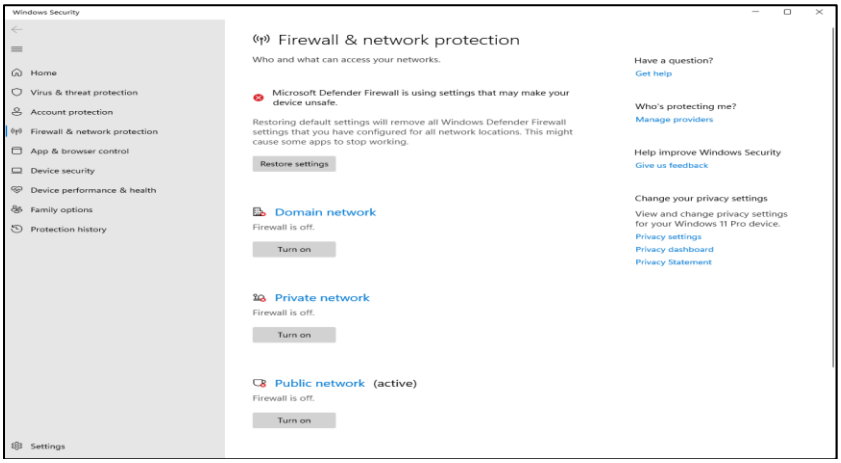
3	
	Rules kali ini mengharuskan user agar tidak bisa mengakses laman YouTube untuk beberapa alasan, diantaranya agar bandwith yang dimiliki oleh pihak SMK tidak sering full load karena digunakan streaming dan agar para siswa tidak sering membuka video – video yang kurang baik untuk ditonton. Namun untuk kondisi rules yang ada saat ini, masih belum cukup untuk bisa memblokir laman YouTube sesuai dengan gambar yang kami ambil.	
4		

	Rules keempat berisi pemblokiran ping protokol ICMP dari semua segment jaringan menuju ke IP DNS Google.com, namun masih tembus untuk ping nya tersebut. Dan juga ada request tambahan agar bagaimana caranya reply ping RTO nantinya digantikan dengan reply "Destination host unreachable" sebagai custom reply.
5	
	Pada rules nomor 5 terdapat pemblokiran yang berasal dari semua segment IP menuju IP Server yang dimiliki oleh tim IT SMK IDN. Tapi faktanya, setelah beberapa kali digunakan IP PC Server diperlukan agar bisa di ping dari semua segment yang ada untuk berbagai keperluan salah satunya memastikan koneksi menuju ke server dalam keadaan baik.
6	

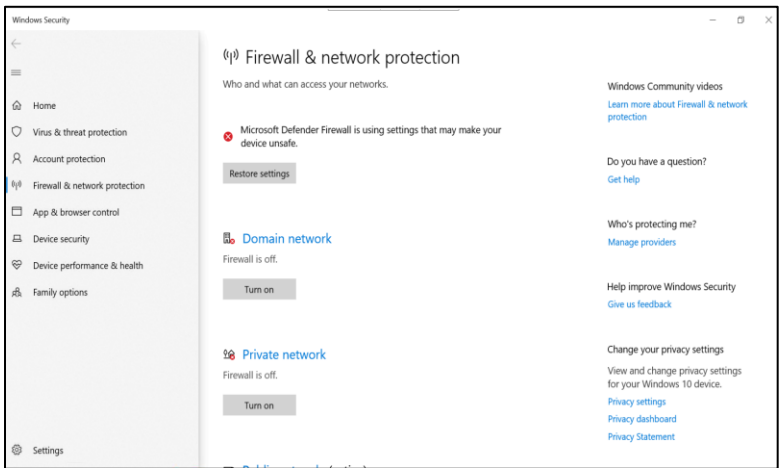
	
	Pada list aktif rules terakhir saat ini yaitu dengan deskripsi "Sosmed" sepertinya masih belum berjalan dengan baik, karena saat kami lakukan testing terhadap Sosmed yang dilist agar di bloking masih bisa terbuka dengan normal seperti gambar diatas.
7	
	Untuk Rules nomor 7 kami sarankan untuk menghapus sekalian rules yang memang sudah tidak terpakai, disamping agar bisa meringankan beban memori juga bisa membuat rapih rules yang dimiliki saat ini.

d. Hasil Analisis perangkat User/ Client

Selanjutnya adalah gambar yang menunjukan beberapa laptop yang tidak mengaktifkan firewall yang ada di masing – masing perangkat nya.



Gambar 3 Pengecekan Firewall Laptop user1



Gambar 4 Pengecekan Firewall Laptop user2

3. Hasil Akhir Pengujian

Dari hasil yang dilakukan terhadap perangkat yang dimaksud, terbagi menjadi dua bagian diantaranya hasil akhir di perangkat firewall dan hasil akhir perangkat user. Berikut dibawah ini merupakan penjelasan detail mengenai hasil akhir yang sudah dilakukan:

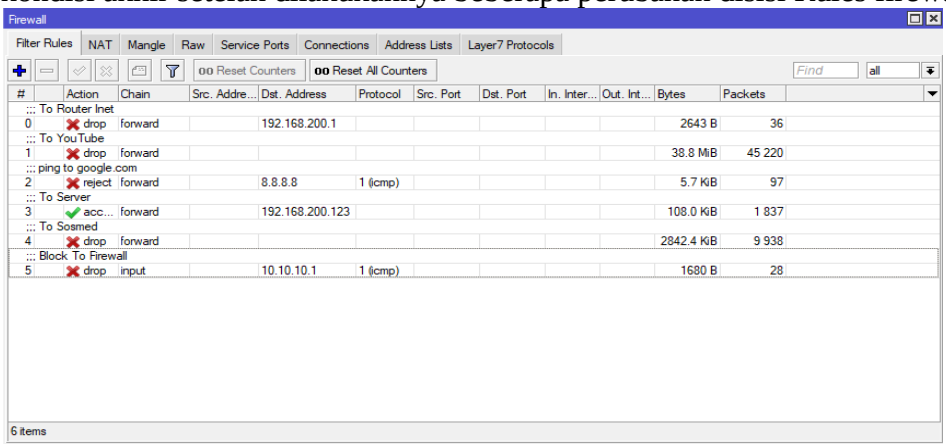
a. Perubahan/ Optimalisasi yang dilakukan

Setelah melakukan Analisa berdasarkan data yang didapat di sub-bab sebelumnya, berikut dibawah ini merupakan hasil dari perubahan/ optimaliasi yang dilakukan terhadap perangkat yang dimaksud, juga terbagi menjadi dua bagian diantaranya analisa di perangkat firewall dan Analisa fisik perangkat user. Berikut dibawah ini merupakan penjelasan detail mengenai perubahan/ optimalisasi yang sudah dilakukan:

Berikut adalah beberapa perubahan dan penyesuaian yang dilakukan untuk semakin membuat optimal firewall yang dimiliki oleh tim IT SMK IDN disertai dengan hasil yang sudah kami lakukan perubahan.

b. Hasil akhir Perangkat Firewall dan User Laptop

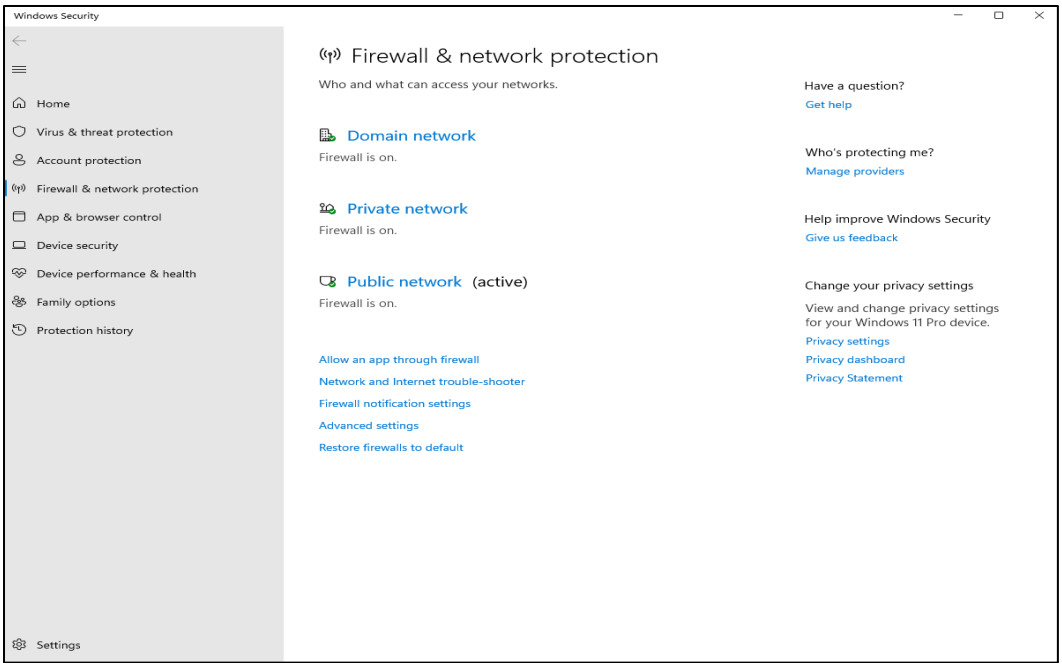
Berikut kondisi akhir setelah dilakukannya beberapa perubahan disisi Rules firewall:



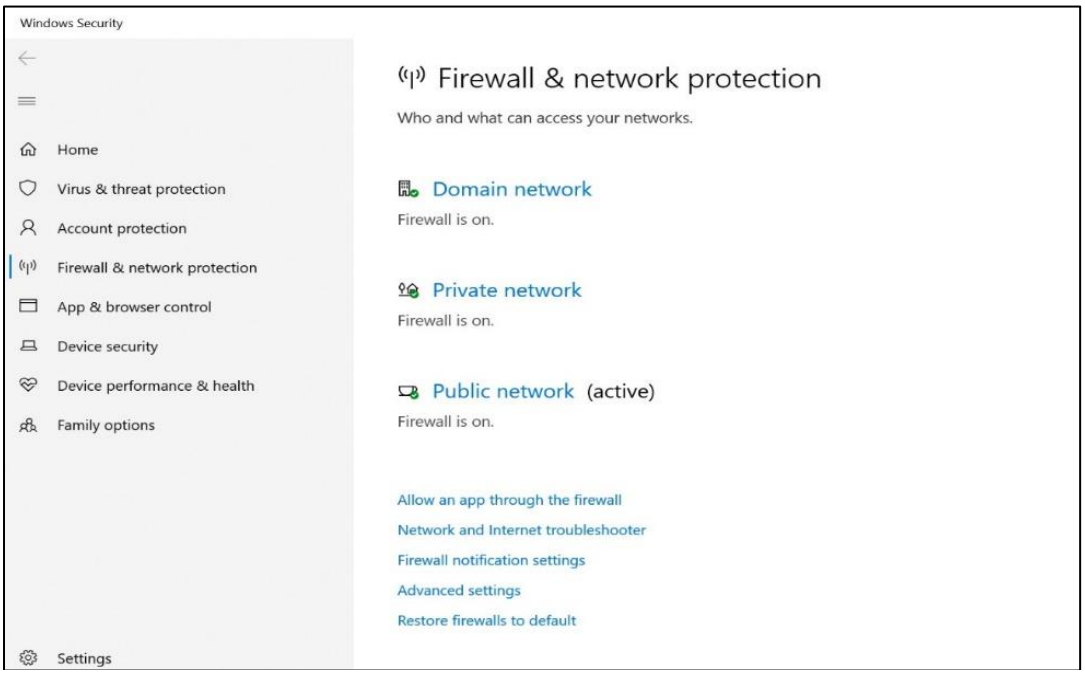
Gambar 5 Hasil akhir Rules Firewall

Selanjutnya untuk beberapa perubahan yang dilakukan di sisi Laptop user adalah sebagai berikut:

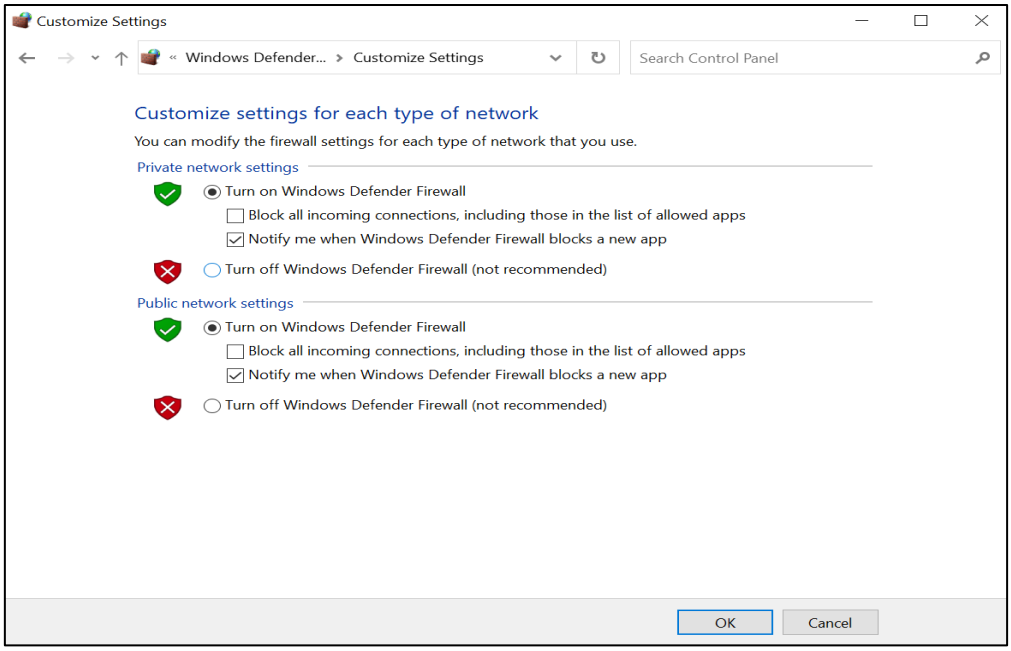
Gambar disisi laptop user



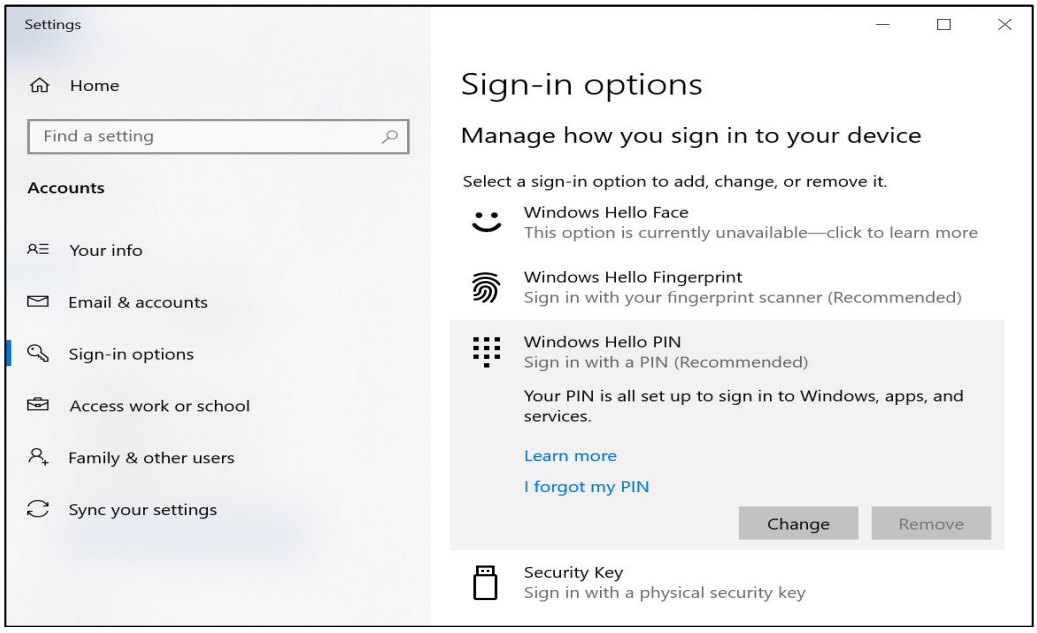
Gambar 6 Penyesuaian Firewall User1 Sesuai Standard



Gambar 7 Penyesuaian Firewall User1 Sesuai Standard



Gambar 8 Penyesuaian Firewall user3 sesuai standard



Gambar 9 Standarisasi pengaturan login

Point terakhir merupakan sebuah penjelasan singkat mengenai apa saja penyuluhan yang kami lakukan guna untuk menekan angka peretasan di Indonesia, diawali dengan betapa pentingnya menjaga keamanan data yang dimiliki setiap orang lalu menjelaskan mengenai sosial engineering yang bisa terjadi kapan saja dimana saja dengan cara yang berbeda – beda tentunya, oleh karena itu harus selalu diingatkan mengenai hal ini mulai dari jangan pernah menggunakan flashdisk orang yg tidak dikenal lalu tidak memposting foto/ video di sosmed yang berkaitan

dengan data privasi kita, yang nantinya apabila dilakukan besar kemungkinan akan menjadi sasaran para peretas untuk melakukan phising/ pencurian data. Begitu juga selalu diingatkan untuk mengaktifkan firewall pada semua kondisi di masing – masing laptop/ pc dan terakhir tidak sembarang membuka Link website yang diberikan orang lain.

Timeline Implementasi / Waktu Pelaksanaan

Tabel 3 Timeline Implementasi

No	Kegiatan	November				Desember			
		1	2	3	4	1	2	3	4
1	Pengumpulan Data dan Analisis Data								
2	Perancangan								
3	Implementasi								
4	Dokumentasi dan Pelaporan								

KESIMPULAN

Berdasarkan hasil penelitian tentang optimalisasi firewall di infrastruktur jaringan SMK IDN Bogor dapat ditarik dalam beberapa kesimpulan bahwa penelitian yang hadir disini terwujud dikarenakan semakin berkembangnya teknologi khususnya Internet yang semakin bebas untuk bisa mengakses apapun dari sumber manapun, oleh karena itu peran Firewall dalam sebuah Infrastruktur jaringan sudah menjadi salah satu yang terpenting mengingat ditambah lagi semakin maraknya peretasan yang terjadi di Indonesia. Maka dengan kekhawatiran akan masalah tersebut terciptalah sebuah ide/ gagasan yang dimana bertujuan untuk bisa membantu lebih optimal lagi perangkat firewall yang dimiliki khususnya di SMK IDN Bogor dengan judul "Optimalisasi Keamanan Firewall Di Infrastruktur Jaringan SMK IDN Bogor". Dari kekhawatiran di atas, peneliti telah berhasil menemukan letak masalah maupun sebuah mekanisme yang memerlukan pengembangan/ optimalisasi yang ada di perangkat firewall dan juga penyuluhan secara langsung dengan para siswa maupun guru mengenai pentingnya menjaga kerahasiaan data sendiri.

DAFTAR PUSTAKA

Alfurqon, D., & Assegaff, S. (2018). Analisis Dan Perancangan Jaringan Local Area Network Pada Laboratorium Smk Negeri 1 Kota Jambi. *Jurnal Manajemen Sistem Informasi*, *3*(3), 1149–1163.

Anshori, I. F. (2019). Implementasi Socket Tcp/Ip Untuk Mengirim Dan Memasukan File Text Kedalam Database. *Jurnal Responsif: Riset Sains Dan Informatika*, *1*(1), 1–5.

Chaidir, I. (2018). Pembatasan Akses Jaringan Internet Pada Clearos Menggunakan Metode Access Control List. *Jurnal Teknik Komputer Amik Bsi*, *4*(1), 212–216.

Hapsari, S. A., & Pamungkas, H. (2019). Pemanfaatan Google Classroom Sebagai Media

Pembelajaran Online Di Universitas Dian Nuswantoro. *Wacana: Jurnal Ilmiah Ilmu Komunikasi*, *18*(2), 225–233.

Hastuti, T., Djuyandi, Y., & Darmawan, W. B. (2021). Deteksi Dini Ancaman Social Engineering Hacker Terhadap Mata Pelajaran Rahasia Di Sekolah Staf Dan Komando Angkatan Udara. *Paradigma Polistaat: Jurnal Ilmu Sosial Dan Ilmu Politik*, *4*(1), 60–81.

Hikmaturokhman, A., Purwanto, A., & Munadi, R. (2015). Analisis Perancangan Dan Implementasi Firewall Dan Traffic Filtering Menggunakan Cisco Router. *Seminar Nasional Informatika (Semnasif)*, *1*(3).

Jaelani, W. L. (2021). Implementasi Replikasi Basis Data Dan Model Discretionary Acces Control Untuk Keamanan Database Studi Kasus Smk Plus Pratama Adi Banjaran. *Scientia Regendi*, *2*(2), 104–115.

Kautsar, M. S. (2013). *Lkp: Perancangan Dan Implementasi Access Control List Dan Vlan Pada Pt. Expert Data Voice Solution*. Stikom Surabaya.

Mauhibatillah, N. (2022). Dramaturgi: Budaya Flexing Berkedok Penipuan Di Media Sosial (Studi Kasus Indra Kenz Dan Doni Salmanan). *Commed: Jurnal Komunikasi Dan Media*, *7*(1), 1–14.

Raharjo, B. (2021). Fintech Teknologi Finansial Perbankan Digital. *Penerbit Yayasan Prima Agus Teknik*, 1–299.

Roza, R., Fauzan, M. N., & Rahayu, W. I. (2020). *Tutorial Sistem Informasi Prediksi Jumlah Pelanggan Menggunakan Metode Regresi Linier Berganda Berbasis Web Menggunakan Framework Codeigniter*. Kreatif.

Sari, I. Y., Muttaqin, M., Jamaludin, J., Simarmata, J., Rahman, M. A., Iskandar, A., Pakpahan, A. F., Abdul Karim, S., Giap, Y. C., & Hazriani, H. (2020). *Keamanan Data Dan Informasi*. Yayasan Kita Menulis.

Suharmanto, A. Y., Lumenta, A. S. M., & Najoan, X. B. N. (2018). Analisa Keamanan Jaringan Wireless Di Universitas Sam Ratulangi. *Jurnal Teknik Informatika*, *13*(3).

Sulaiman, M. (2021). *Tinjauan Fiqh Siyasah Dan Hukum Positif Terhadap Kebebasan Berpikir Dan Berpendapat Dalam Kasus Peretasan Situs Tempo*. Uin Sunan Ampel Surabaya.

Widiatmoko Herbimo, S. T. (2021). *Teknologi Jaringan Berbasis Luas (Wan) Smk/Mak Kelas Xi*. Gramedia Widiasarana Indonesia.