Simulasi Perancangan Firewall Security Port untuk Implementasi Keamanan Sistem Jaringan di PT. Alfian Jaya Abadi

Nur Firman Maulana[1], I Made Suartana[2]

[1,2] Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya)
[1]nur.17051204073@mhs.unesa.ac.id
[2]madesuartana@unesa.ac.id

Abstrak— **Perkembangan teknologi komunikasi dan informasi telah mendorong peningkatan signifikan dalam penggunaan internet global, termasuk di Indonesia. Teknologi informasi menjadi tulang punggung operasi, menjadikan keamanan sistem jaringan sebagai aspek kritis yang memerlukan perhatian serius. Pemilihan dan implementasi firewall yang tepat dapat meningkatkan keamanan jaringan perusahaan dengan mengurangi risiko serangan siber, penggunaan port yang tidak sah, dan kebocoran data. Penelitian ini bertujuan untuk mensimulasikan penerapan firewall security port sebagai strategi keamanan jaringan di PT. Alfian Jaya Abadi. Penelitian ini diharapkan dapat memberikan kontribusi positif kepada PT. Alfian Jaya Abadi, yang didasarkan pada pemahaman mendalam tentang dinamika keamanan jaringan dan solusi yang tersedia.**

Kata Kunci*— *Firewall, Firewall Port Security, Solusi Keamanan Jaringan

I. PENDAHULUAN

Perkembangan teknologi komunikasi dan informasi menyebabkan jumlah penggunaan internet di dunia semakin berkembang. Meluasnya jaringan internet digunakan untuk berbagai keperluan, mulai dari bisnis atau organisasi, media social, Pendidikan, maupun hiburan. Salah satu negara yang mengalami pertumbuhan penggunaan internet yaitu Indonesia. Menurut laporan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), pada periode 2022-2023, pengguna internet di Indonesia mencapai 215,63 juta orang, meningkat 2,67% dibandingkan periode sebelumnya [1]. Selain itu, penggunaan internet juga memiliki dampak

Dengan penetrasi internet yang terus meningkat, teknologi informasi menjadi tulang punggung operasional perusahaan, keamanan sistem jaringan menjadi aspek kritis yang membutuhkan perhatian serius. PT. Alfian Jaya Abadi, sebagai entitas bisnis yang mengandalkan infrastruktur jaringan untuk menjalankan operasionalnya, dihadapkan pada tantangan keamanan yang semakin kompleks. Serangan siber, termasuk ancaman melalui port-port jaringan, merupakan risiko yang tidak dapat diabaikan.

Firewall telah lama menjadi solusi utama untuk melindungi sistem jaringan dari ancaman yang berasal dari internet. Dengan penerapan teknologi *firewall* yang terfokus pada pengamanan port-port tertentu, perusahaan dapat meningkatkan tingkat keamanan jaringannya. Pemilihan dan penerapan firewall yang tepat menjadi langkah strategis dalam mengurangi risiko terhadap serangan siber, penggunaan port-port yang tidak sah, dan kebocoran data yang dapat merugikan operasional perusahaan. Berdasarkan penelitian sebelumnya yang dilakukan oleh Oloyede A.O., Yekini N.A., Akinwole A.K., dan Ojo O. (2021), dijelaskan bahwa jaringan komputer sensitif terhadap berbagai faktor. Ada berbagai jenis tenaga penjualan online, seperti pengecer online, pedagang kaki lima, atau karyawan bisnis tidak terampil yang berpotensi menjadi jutawan. Perselisihan tidak selalu berasal dari pihak eksternal, namun bisa juga disebabkan oleh pengelolaan informasi internal yang tidak memadai, serta kesalahan prosedur dan kebijakan. Selain itu, risiko keamanan baru mungkin timbul dari teknik serangan yang berkembang, seperti ransomware, dan kerentanan yang baru ditemukan dalam sistem peretasan wildcard dan kata sandi yang ada. Penggunaan firewall sangat disarankan sebagai cara untuk menghilangkan ancaman internet dan serangan[2].

Dalam penelitian ini bertujuan untuk melakukan simulasi penerapan firewall security port sebagai strategi keamanan sistem jaringan di PT. Alfian Jaya Abadi. Dengan mengidentifikasi potensi risiko keamanan yang dihadapi perusahaan, penelitian ini akan memberikan rekomendasi untuk meningkatkan keefektifan keamanan sistem jaringan melalui penggunaan firewall yang dioptimalkan secara spesifik pada port-port yang rentan terhadap serangan. Diharapkan penelitian ini dapat memberikan dampak positif bagi PT. Upaya Alfian Jaya Abadi dalam menjaga integritas jaringan dan memastikan prosedur operasional yang aman melalui pemahaman dinamika keamanan jaringan dan solusi yang tersedia.

II. KAJIAN PUSTAKA

A. Network Security:

Keamanan jaringan adalah seperangkat aturan, prosedur, dan praktik yang digunakan untuk mencegah akses tidak sah, modifikasi, atau eksploitasi jaringan komputer dan data yang

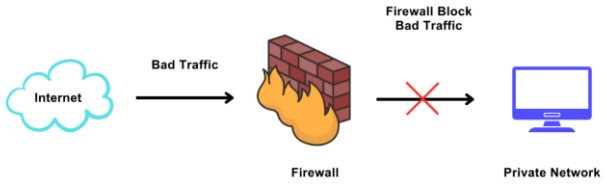
dapat diakses melalui jaringan tersebut [3] [5]. Hal ini menghasilkan otorisasi akses data yang dikendalikan oleh administrator jaringan [5]. Setiap jaringan komputer, baik publik maupun pribadi, yang digunakan untuk transaksi bisnis sehari-hari dan komunikasi antar individu, lembaga pemerintah, dan bisnis dilindungi oleh keamanan jaringan. Menjaga integritas jaringan melibatkan pembatasan akses ke data dalam jaringan, yang diawasi oleh administrator jaringan [6].

B. *Port Security :*

Mekanisme yang digunakan dalam switch untuk mengurangi jumlah host yang dapat terhubung ke port tertentu dan mengidentifikasi host tertentu yang dapat terhubung ke port keamanan firewall switch disebut port security [7]. Ide dasar di balik konfigurasi keamanan port adalah mendaftarkan alamat MAC perangkat apa pun yang dapat terhubung ke switch. Sebaliknya, tugas petugas keamanan pelabuhan adalah membuat paket host atau memblok host yang alamat MAC-nya tidak sesuai dengan konfigurasi keamanan port [8].

C. *Firewall :*

Sistem keamanan jaringan yang berfungsi sebagai pertahanan utama dalam melindungi jaringan komputer dari serangan dan akses yang tidak diizinkan. Dengan mengontrol lalu lintas data yang masuk dan keluar dari jaringan, firewall memastikan bahwa hanya lalu lintas yang sesuai dengan aturan keamanan yang diizinkan untuk melewati batas jaringan. Proses ini melibatkan filtrasi paket data, verifikasi identitas pengguna atau perangkat, dan penerapan aturan keamanan yang telah ditetapkan oleh administrator jaringan.

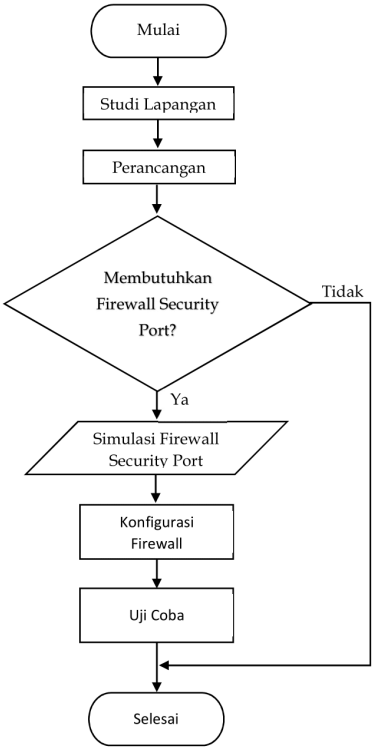


Gbr 1. Firewall [9]

Gbr 1 merupakan gambaran dari firewall dimana terdapat beberapa jenis firewall termasuk firewall berbasis jaringan yang mengontrol lalu lintas di antara jaringan internal dan eksternal, firewall berbasis host yang melindungi perangkat individu, dan firewall berbasis aplikasi yang memonitor lalu lintas pada tingkat aplikasi tertentu. Manfaat utama dari penggunaan firewall termasuk peningkatan keamanan jaringan, kontrol akses yang lebih baik, dan kemampuan untuk memantau aktivitas jaringan secara efektif. Dengan adopsi firewall yang tepat, organisasi dan individu dapat meningkatkan tingkat keamanan jaringan mereka dan melindungi data sensitif dari ancaman cyber yang berpotensi merusak[10[.

III. METODE PENELITIAN

Dalam penelitian ini dirancang mekanisme keamanan pada dengan menerapkan firewall yang disimulasikan dengan Packet Tracer. Simulasi bertujuan untuk menguji rancangan security yang akan diterapkan pada studi kasus penelitian.



Gbr 2. Flowchart Penelitian

Pada Gbr 2 merupakan flowchart penelitian ini dimana proses dimulai dengan tahap persiapan di mana penelitian diawali dengan studi lapangan. Tahap ini mencakup pengumpulan data dan informasi terkait kondisi jaringan dan potensi ancaman keamanan di PT. Alfian Jaya Abadi. Selanjutnya, dilakukan perancangan untuk menentukan kebutuhan dan spesifikasi firewall security port yang sesuai. Setelah perancangan, peneliti mengevaluasi apakah jaringan memerlukan firewall security port. Jika tidak diperlukan, proses berakhir. Namun, jika diperlukan, langkah berikutnya adalah melakukan simulasi firewall security port untuk memastikan desain yang direncanakan dapat memenuhi kebutuhan keamanan.

A. *Subjek Penelitian*

Subjek penelitian disini menjelaskan bahwa fokus yang nantinya dikaji dari penelitian, dalam hal ini adalah Sistem Keamanan Jaringan PT. Alfian Jaya Abadi. Sesuai dengan judul tersebut maka subjek dalam penelitian ini adalah PT. Alfian Jaya Abadi.

B. *Alat Pendukung Penelitian*

Dalam membangun sebuah sistem maka dibutuhkanlah peralatan yang mendukung terdiri dari perangkat keras *(hardware)* dan perangkan lunak *(software)*. Perangkat yang digunakan dalam penlitian antara lain dijabarkan sebagai berikut: *Perangkat Keras (Hardware)* Komputer Yang memiliki spesifikasi:

- *Intel Core i*5
- 4GB *RAM (Random Access Memory)*
- SSD 250GB
- `NVIDIA Geforce 930MX

Perangkat Lunak (Software) Agar sistem yang dibangun dapat berjalan baik dan benar maka diperlukan beberapa perangkat lunak yang membantu dalam pengerjaan sistem. Perangkat yang digunakan antara lain sebagai berikut:

- *Operating System Windows 11*
- *Browser Internet : Google Chrome*
- *Network Simulator : Cisco Packet Tracer*

C. Tempat dan Waktu Penelitian

Penelitian dilakukan pada lokasi di mana peneliti mengumpulkan informasi yang diperlukan untuk penelitian. Dalam hal ini, peneliti melakukan penelitian di berbagai lokasi yang fleksibel, termasuk di sepenggunar rumah dan kantor PT. Alfian Jaya Abadi. Waktu pelaksanaan penelitian meliputi rentang waktu yang dimulai dari awal hingga akhir penelitian. Proses ini melibatkan beberapa tahapan, seperti menentukan topik penelitian, mengajukan judul, menyusun proposal, seminar proposal, revisi proposal, pelaksanaan penelitian, dan akhir penelitian. Dalam hal ini, pelaksanaan penelitian dimulai sejak awal tahun 2024.

D. Perancangan Simulasi Penelitian

Dari analisa permasalahan jaringan diatas penulis membuat solusi untuk permasalahan jaringan di PT. Alfian Jaya Abadi yaitu sebagai berikut:

1) Melakukan subnetting atau pengalamatan sesuai kebutuhan jaringan yang akan diterapkan untuk berapa pengguna client Server agar terstruktur rapi dalam pengalamatannya.
2) Menerapkan sistem firewall untuk keamanan pada jaringan PT. Alfian Jaya Abadi.
3) Melakukan Perancangan desain perubahan Server untuk meminimalisir biaya pembelian perangkat keras Server.

Penarikan kesimpulan dari analisa hasil penelitian mengacu pada data yang diteliti, yaitu menghasilkan sistem keamanan yang terjamin pada sistem jaringan PT. Alfian Jaya Abadi.

E. Uji Coba

Untuk pengujian jaringan penulis akan menggunakan scenario berikut:

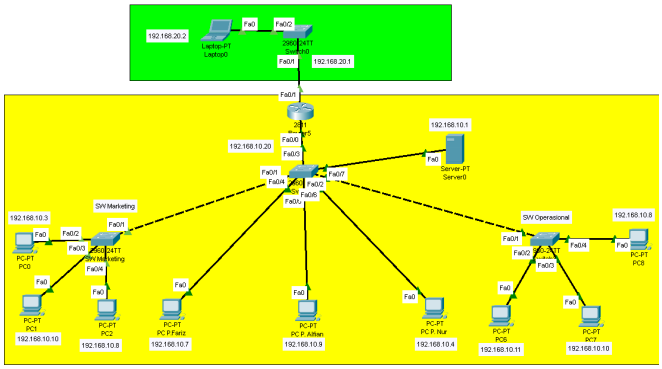
1) Attacker dan PC perusahaan mencoba masuk ke Server FTP perusahaan dan melakukan perintah ping yang dimana sebelum diterapkannya access list maupun firewall.
2) Attacker dan PC perusahaan mencoba masuk ke Server FTP perusahaan dan melakukan ping saat setelah firewall maupun access list diterapkan.
3) Attacker dan PC perusahaan mencoba masuk kedalam Web Server saat setelah firewall port filtering diterapkan.

IV. Hasil dan Pembahasan

Bagian ini membahas terkait dengan hasil penelitian yang telah dilakukan. Bagian ini menjelaskan temuan serta analisa yang telah dilakukan.

A. Topologi Jaringan

Berdasarkan dari hasil analisa dan penelitian penulis terkait kebutuhan akan sumber pemanfaatan jaringan di PT. Alfian Jaya Abadi penulis tidak merubah topologi jaringan sebelumnya karena dianggap sudah memenuhi kebutuhan dan efisien untuk keperluan jaringan tersebut. Topologi jaringan star adalah topologi yang sebelumnya telah digunakan oleh perusahaan PT. Alfian Jaya Abadi.



Gbr 3. Tipologi Jaringan pada PT Alfian Jaya Abadi

Pada Gbr 3, dapat diamati bahwa adanya 9 pc 4 switch 1 router dan 1 Server pada jaringan di PT. Alfian Jaya Abadi, untuk pembagian penulis memberikan 2 area yaitu area kuning dimana pada area tersebut merupakan jaringan local perusahaan, sementara pada jaringan hijau marupakan area untuk client atau customer perusahaan.

B. IP Address

Pengalamatan IP address dilakukan beberapa subneting atau perubahan pengalamatan untuk membatasi client setiap cabang, hal ini dilakukan bertujuan untuk membatasi ip address dan penataan alamat ip address agar terhindar dari kemacetan lalu lintas dalam jaringan.

```
Router#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.11           4   0001.643B.E260  ARPA   FastEthernet0/0
Internet  192.168.10.12           4   0004.9A10.0267  ARPA   FastEthernet0/0
Internet  192.168.10.13           4   000C.8533.1C37  ARPA   FastEthernet0/0
Internet  192.168.10.20           -   00D0.972E.9E01  ARPA   FastEthernet0/0
Internet  192.168.10.21           4   0060.2F15.B607  ARPA   FastEthernet0/0
Internet  192.168.10.22           0   0001.C708.436E  ARPA   FastEthernet0/0
Internet  192.168.10.23           0   000D.BD02.0577  ARPA   FastEthernet0/0
Internet  192.168.10.31           4   00E0.8F58.8A58  ARPA   FastEthernet0/0
Internet  192.168.10.32           4   0009.7C6A.C392  ARPA   FastEthernet0/0
Internet  192.168.10.33           4   00D0.58EB.3BD5  ARPA   FastEthernet0/0
Internet  192.168.20.1            -   00D0.972E.9E02  ARPA   FastEthernet0/1
Internet  192.168.20.2          129   000A.4145.C389  ARPA   FastEthernet0/1
Internet  192.168.20.3           18   0002.1786.B3C3  ARPA   FastEthernet0/1
Router#
```

Gbr 4. IP Address pada PT. Alfian Jaya Abadi

Pada Gbr 4, menampilkan IP address dari jaringan PT. Alfian Jaya Abadi dimana untuk ip configuration yang digunakan adalah static sehingga untuk gateway pada semua perangkat yang digunakan perusahaan yaitu 192.168.10.0, sementara untuk gateway 192.168.20.0 merupakan ip address untuk client atau customer yang nantinya diperoleh dari sistem ip configuration dhcp. Untuk perintah membuat dhcp pada router dapat diperhatikan pada gambar di bawah.

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#service dhcp
Router(config)#ip dhcp pool cs
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.20.1
```

Gbr 5. Tampilan CLI pada Router saat Setting DHCP

Pada Gbr 5, untuk memulai setting dhcp melalui cli pada router pengguna diharuskan masuk kedalam configure terminal seperti pada tampilan gambar 4.3 pada baris pertama. Selanjutnya untuk masuk kedalam layanan service dhcp seperti pada baris tiga, untuk penjelasan pada baris empat pengguna akan memberikan nama untuk dhcp pool pada jaringan yang akan digunakan nantinya. Selanjutnya pada baris lima pengguna diharuskan memberikan alamat ip network dan subnet yang digunakan, kemudian pada baris enam merupakan ip gateway yang nantinya akan digunakan untuk setiap tamu yang menggunakan service dhcp, pada baris tujuh merupakan perintah untuk setting ip dns Server, dan untuk baris terakhir pengguna membuat perintah dimana pengguna memberikan range ip yang dapat digunakan oleh client atau tamu yang nantinya menggunakan service dhcp.

C. *Keamanan Jaringan*

1) *Penerapan access list (router)*

Ketika access list diterapkan dalam router ataupun sebuah PC Server dan clientnya, maka access list tersebut berfungsi sebagai filtering terhadap paket yang dikirim oleh client, maka dari itu access list tersebut hanya memperbolehkan beberapa network yang terdaftar saja yang diperbolehkan. Berikut tampilan CLI dan penjelasan untuk perintah konfigurasi access list pada router perusahaan.

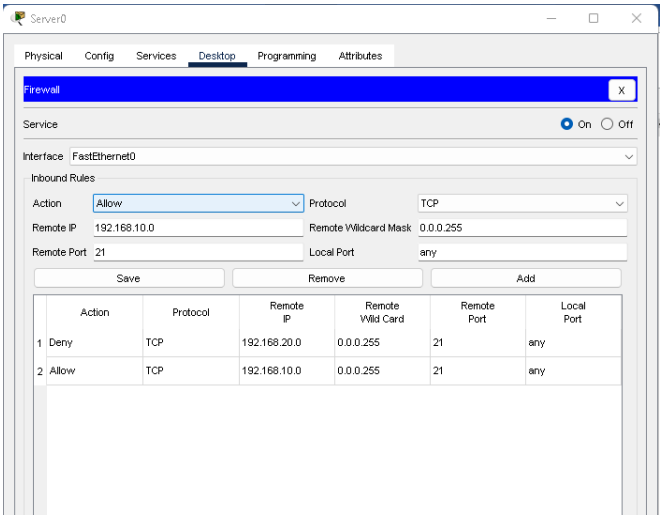
```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 100 deny tcp 192.168.20.0 0.0.0.255 host 192.168.10.1 eq ftp
Router(config)#access-list 100 permit ip any any
Router(config)#int fa0/1
Router(config-if)#ip access-group 100 in
Router(config-if)#
```

Gbr 6. Tampilan CLI untuk Perintah Konfigurasi Access list

Pada Gbr 6, diharuskan untuk masuk kedalam configure terminal sebelum memulai setting access list. [access-list] adalah perintah untuk konfigurasi access list, [100] merupakan nomer access list atau dapat dikatakan ID access list, [deny] merupakan aksi untuk menolak network yang pengguna perintah nantinya, [tcp] merupakan target protocol yang akan pengguna block nantinya, [192.168.20.0] merupakan gateway ip address dari client perusahaan, [0.0.0.255] adalah wildcard yang diperoleh dari pengurangan subnet mask 255.255.255.255-255.255.255.0, [host 192.168.10.1] merupakan ip address dari Server perusahaan, [eq] untuk menandakan port dan protocol yang diperbolehkan/dilarang, [FTP] merupakan target port yang akan diblock. Pada baris ke 4 memiliki pembeda pada perintah sebelumnya, yaitu dimana dapat pengguna simpulkan bahwa perintah access list 100 memperbolehkan sumber paket(selain 192.168.20.0) dan tujuan paket data yang menerima. Pada baris ke 5 pengguna akan menentukan interface yang akan diatur untuk dijadikannya tempat filter paket data, berdasarkan gambar 4.1 interface terdekat dari sumber adalah FastEthernet0/1, untuk baris ke 6 pengguna akan konfigurasi access group dimana seluruh ip address dari jalur terdekat yang dapat melewatinya kecuali ip address yang telah dideny pada baris 3.

2) *Penerapan Firewall (Server)*

Pada tahap ini, penerapan Firewall bertujuan untuk menambahkan aturan yang memungkinkan atau memblokir pada protokol atau port tertentu dapat diamati pada aturan masuk yang ditampilkan pada Gbr 7.

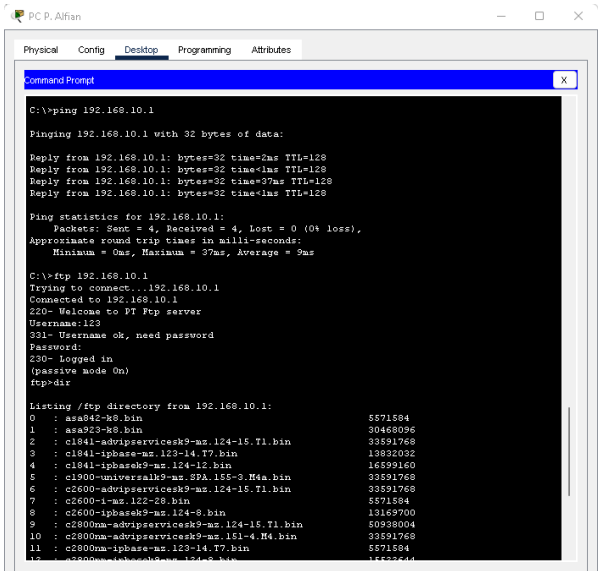


Gbr 7. Penerapan Firewall pada Server

Gbr 7. merupakan tampilan desktop dari firewall pada Server yang akan di setting. Untuk langkah awal agar firewall dapat berjalan, pengguna diharuskan mengaktifkan dengan memilih ON pada bagian service, selanjutnya pada kolom action pengguna akan memberikan perintah mengizinkan atau memblock (allow/deny), kemudian pada kolom Protocol pengguna akan diminta untuk memilih 4 protocol(IP/ICMP/TCP/UDP) yang nantinya akan pengguna block, selanjutnya pada kolom Remote IP merupakan target host dengan ip address yang nantinya akan pengguna izinkan atau blokir, untuk pemberian wildcard mask pengguna gunakan metode pengurangan subnet mask seperti pada settingan access list sebelumnya, untuk Remot port merupakan port yang akan pengguna jadikan sebagai target nantinya.

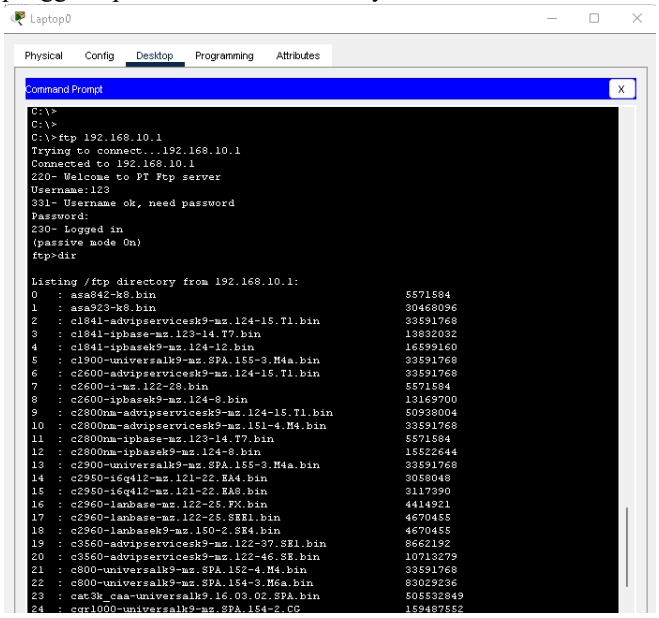
3) Pengujian Jaringan

Gbr 8 merupakan tampilan desktop dari firewall pada Server yang akan di setting. Untuk langkah awal agar firewall dapat berjalan, pengguna diharuskan mengaktifkan dengan memilih ON pada bagian service, selanjutnya pada kolom action pengguna akan memberikan perintah mengizinkan atau memblock (allow/deny), kemudian pada kolom Protocol pengguna akan diminta untuk memilih 4 protocol(IP/ICMP/TCP/UDP) yang nantinya akan pengguna block, selanjutnya pada kolom Remote IP merupakan target host dengan ip address yang nantinya akan pengguna izinkan atau blokir, untuk pemberian wildcard mask pengguna gunakan metode pengurangan subnet mask seperti pada settingan access list sebelumnya, untuk Remot port merupakan port yang akan pengguna jadikan sebagai target nantinya.



Gbr 8. Pengujian Jaringan

Pada Gbr 8, pc perusahaan melakukan ping pada ip address Server dan memasuki FTP Server, dan dapat pengguna perhatikan bahwa hasilnya diizinkan.



Gbr 9. Tampilan Attacker saat mengakses FTP Server sebelum Penerapan Firewall

Gbr 9. merupakan tampilan Command Prompt dengan percobaan koneksi FTP ke alamat IP 192.168.10.1. Koneksi berhasil dengan pesan "220-Welcome to PT FTP server" dan pengguna berhasil login. Selanjutnya, ditampilkan daftar file dalam direktori FTP dari 192.168.10.1, termasuk nama file dan ukuran masing-masing file.

Gbr 10. Tampilan Attacker saat melakukan ping dan Mencoba Mengakses FTP

Pada Gbr 10, dapat diperhatikan bahwa attacker atau tamu melakukan percobaan ping ke alamat IP 192.168.10.22 dan 192.168.10.1 yang gagal dengan 100% kehilangan paket, serta percobaan koneksi FTP yang juga tidak berhasil saat setelah diterapkannya firewall.

Gbr 11. Tampilan Attacker Mencoba Mengakses Web Server Setelah Diterapkan Firewall

Pada Gbr 11 merupakan tampilan dimana attacker atau tamu masih dapat memasuki Web Server perusahaan saat firewall telah diterapkan.

V. KESIMPULAN

Setelah melakukan simulasi penerapan firewall pada Server FTP, ditemukan bahwa seluruh pihak yang terhubung pada jaringan internet di area perusahaan dapat memasuki Server tanpa adanya hambatan. Selain itu, setelah menerapkan sistem keamanan menggunakan Firewall pada jaringan PT. Alfian Jaya Abadi, attacker atau perangkat yang tidak dikenali tidak dapat terhubung pada beberapa port pada jaringan perusahaan. Kesimpulan dari penelitian ini menunjukkan bahwa penerapan firewall security port dapat meningkatkan keamanan jaringan di PT. Alfian Jaya Abadi dan memberikan perlindungan yang optimal terhadap akses yang tidak sah serta potensi serangan cyber.

REFERENSI

[1] A. O., O., Nureni, Y., Akinwole, A. & O, O., 2021. Firewall Approach To Computer Network Security: Functional Viewpoint. *Int. J. Advanced Networking and Applications,* 13(03), pp. 4993-5000.

[2] Ahmed, A. H. & Al-Hamadani, M. N. A., 2021. Designing a secure campus network and simulating it using Cisco packet tracer. *Indonesian Journal of Electrical Engineering and Computer Science,* 23(1), pp. 479-489.

[3] Indonesiabaik.id, 2023. *Pengguna Internet di Indonesia Makin Tinggi.* [Online] Available at: https://indonesiabaik.id/infografis/pengguna-internet-di-indonesia-makin-tinggi.

[4] Islam, M. S. et al., 2022. Analysis and Evaluation of Network and Application Security Based on Next Generation Firewall. *International Journal of Computing and Digital Systems,* 13(1).

[5] Manuaba, I. B. V. H., Hidayat, R. & Kusumawardani, S. S., 2012. Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus: Kantor Pusat Fakultas Teknik Universitas Gadjah Mada).

[6] Barney, N. & Lutkevich, B., 2023. *network security.* [Online] Available at: https://www.techtarget.com/searchnetworking/definition/network-security

[7] Nur, M. et al., 2023. The Effectiveness of the Port Knocking Method in Computer Security. *Internasional Journal of Integrative Sciences (IJIS),* 2(6), pp. 873-880.

[8] Point, C., 2023. *What is Network Security?.* [Online] Available at: https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/

[9] Cisco, 2023. *Configuring Port Security.* [Online] Available at: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/sec_port.html

[10] Cisco, 2023. *What Is Network Security?.* [Online] Available at: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html.

[11] Sartomo, S. & Sulistyo, W., 2022. Model Keamanan Jaringan Menggunakan Firewall Port Blocking. *KreaTIF,* 10(1), pp. 10-18.