MAKALAH

MENGENAL FIREWALL DAN CARA KERJANYA

Disusun Guna Memenuhi Tugas Mata Jaringan komputer

Dosen Pengampu:

Adi Widharma, S.Si., M.Kom

Disusun Oleh :

Amanda Zaskya	5242451004
Anggi Syahputri	5242451003
Asjad Iman Nazeb Zebua	5243151011
Fikri Najwan Arfi	5243151018
M. Khairiel Darmawan	5241151014
Nabila Atifah	5243151044

PROGRAM STUDI PENDIDIKAN TEKNOLOGI INFORMATIKA DAN KOMPUTER

FAKULTAS TEKNIK

UNIVERSITAS NEGERI MEDAN

2025

KATA PENGANTAR

Puji dan syukur saya panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga saya dapat menyelesaikan menyelesaikan tugas mata kuliah Keamanan Jaringan, dengan judul makalah "Mengenal Firewall dan Cara kerja firewall "

Demikianlah sekapur sirih dari saya, apabila ada tutur kata yang tidak berkenan di hati pembaca mohon di maafkan sebagaimana saya hanyalah manusia biasa yang tak pernah luput dari kesalahan. Kesempurnaan hanya milik Allah. Semoga makalah ini dapat bermanfaat baik bagi kita semua. Aamiin

Medan, 10 Maret 2025

Penyusun

Kelompok 3

DAFTAR ISI

BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Di era internet yang semakin canggih ini, setiap komputer dapat terhubung dengan komputer lainnya secara mudah. Pertukaran file atau dokumen pun semakin tanpa batas dan dapat dilakukan oleh siapa saja. Tentunya hal ini membawa dampak positif yang juga diiringi dengan dampak negatif. Positifnya, orang semakin dimudahkan untuk berbagi berbagai dokumen yang diperlukan. Namun negatifnya, tidak semua orang berbagi dengan tujuan baik. Beberapa berusaha untuk menyerang komputer sebagai hacker, memata-matai (spionase) komputer tertentu demi kepentingan pribadi, atau bahkan mencuri data yang ada dalam suatu komputer. Untuk mencegah dampak negatif tersebut, dibutuhkan firewall sebagai pengatur sistem komunikasi antara dua buah jaringan.

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. Mengingat saat ini banyak perusahaan yang memiliki akses ke Internet dan juga tentu saja jaringan korporat di dalamnya, maka perlindungan terhadap aset digital perusahaan tersebut dari serangan para hacker, pelaku spionase, ataupun pencuri data lainnya, menjadi esensial.Karena kurangnya pengetahuan tentang firewall maka penulis mengangkat materi tentang firewall untuk membantu pembaca mengetahui tentang firewall.

1.2 TUJUAN MAKALAH

a. Mengetahui apa itu firewall
b. Untuk mengetahu apa saja fungsi-fungsi firewall
c. Membahas mengenai firewall baik itu jenis, tipe, prinsip kerja, dll.

1.3 MANFAAT

a. Pembaca dapat mengetahui tentang firewall dan jenis - jenisnya

b. Pembaca dapat mengetahui tentang cara kerja firewall

BAB II

PEMBAHASAN

2.1 Konsep Dasar Firewall

Firewall adalah sistem keamanan jaringan komputer yang mampu melindungi dari serangan virus, malware, spam, dan berbagai jenis serangan internet lainnya. Dapat dikatakan juga bahwa, firewall merupakan perangkat lunak untuk mencegah akses yang dianggap ilegal atau tidak sah dari jaringan pribadi (private network).

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. Namun, masih terdapat beberapa orang atau user yang belum aware dengan adanya sistem ini dan cenderung mengabaikan dari sistem keamanan pada jaringan komputer. Selain itu, firewall juga mempunyai peranan penting dalam menjaga keamanan lalu lintas pada jaringan internet yang terhubung dengan perangkat komputer anda.

Firewall secara umum di peruntukkan untuk melayani :

1.mesin/komputer

Setiap individu yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.

2.Jaringan

Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang di miliki oleh perusahaan organisasi dsb.

- **Fungsi Firewall**

1. Mengatur dan mengontrol lalu lintas jaringan

Fungsi pertama yang dapat dilakukan oleh firewall adalah firewall harus dapat mengatur dan mengontrol lalu lintas jaringan yang diizinkan untuk mengakses jaringan privat atau komputer yang dilindungi oleh firewall. Firewall melakukan hal yang demikian, dengan melakukan inspeksi terhadap paket-paket dan memantau koneksi yang sedang dibuat, lalu melakukan

penapisan (filtering) terhadap koneksi berdasarkan hasil inspeksi paket dan koneksi tersebut.

2. Melakukan autentikasi

Fungsi fundamental firewall yang kedua adalah firewall dapat melakukan autentikasi terhadap akses. Protokol TCP/IP dibangun dengan premis bahwa protokol tersebut mendukung komunikasi yang terbuka. Jika dua host saling mengetahui alamat IP satu sama lainnya, maka mereka diizinkan untuk saling berkomunikasi. Pada awal-awal perkembangan Internet, hal ini boleh dianggap sebagai suatu berkah. Tapi saat ini, di saat semakin banyak yang terhubung ke Internet, mungkin kita tidak mau siapa saja yang dapat berkomunikasi dengan sistem yang kita miliki. Karenanya, firewall dilengkapi dengan fungsi autentikasi dengan menggunakan beberapa mekanisme autentikasi, sebagai berikut:

Firewall dapat meminta input dari pengguna mengenai nama pengguna (user name) serta kata kunci (password). Metode ini sering disebut sebagai extended authentication atau xauth. Menggunakan xauth pengguna yang mencoba untuk membuat sebuah koneksi akan diminta input mengenai nama dan kata kuncinya sebelum akhirnya diizinkan oleh firewall. Umumnya, setelah koneksi diizinkan oleh kebijakan keamanan dalam firewall, firewall pun tidak perlu lagi mengisikan input password dan namanya, kecuali jika koneksi terputus dan pengguna mencoba menghubungkan dirinya kembali.

Metode kedua adalah dengan menggunakan sertifikat digital dan kunci publik. Keunggulan metode ini dibandingkan dengan metode pertama adalah proses autentikasi dapat terjadi tanpa intervensi pengguna. Selain itu, metode ini lebih cepat dalam rangka melakukan proses autentikasi. Meskipun demikian, metode ini lebih rumit implementasinya karena membutuhkan banyak komponen seperti halnya implementasi infrastruktur kunci publik.

Metode selanjutnya adalah dengan menggunakan Pre-Shared Key (PSK) atau kunci yang telah diberitahu kepada pengguna. Jika dibandingkan dengan sertifikat digital, PSK lebih mudah diimplenentasikan karena lebih sederhana, tetapi PSK juga mengizinkan proses autentikasi terjadi tanpa intervensi pengguna. Dengan menggunakan PSK, setiap host akan diberikan sebuah kunci yang telah ditentukan sebelumnya yang kemudian digunakan untuk proses autentikasi. Kelemahan metode ini adalah kunci PSK jarang sekali diperbarui dan banyak organisasi sering sekali menggunakan kunci yang sama untuk melakukan koneksi terhadap host-host yang berada pada jarak jauh, sehingga hal ini sama saja meruntuhkan proses autentikasi. Agar tercapai sebuah

derajat keamanan yang tinggi, umumnya beberapa organisasi juga menggunakan gabungan antara metode PSK dengan xauth atau PSK dengan sertifikat digital.

3. Melindungi sumber daya dalam jaringan privat

Salah satu tugas firewall adalah melindungi sumber daya dari ancaman yang mungkin datang. Proteksi ini dapat diperoleh dengan menggunakan beberapa peraturan pengaturan akses (access control), penggunaan SPI, application proxy, atau kombinasi dari semuanya untuk mencegah host yang dilindungi dapat diakses oleh host-host yang mencurigakan atau dari lalu lintas jaringan yang mencurigakan. Meskipun demikian, firewall bukanlah satu-satunya metode proteksi terhadap sumber daya, dan mempercayakan proteksi terhadap sumber daya dari ancaman terhadap firewall secara eksklusif adalah salah satu kesalahan fatal. Jika sebuah host yang menjalankan sistem operasi tertentu yang memiliki lubang keamanan yang belum ditambal dikoneksikan ke Internet, firewall mungkin tidak dapat mencegah dieksploitasinya host tersebut oleh host-host lainnya, khususnya jika exploit tersebut menggunakan lalu lintas yang oleh firewall telah diizinkan (dalam konfigurasinya).

4. Koneksi dan Keadaan Koneksi

Agar dua host TCP/IP dapat saling berkomunikasi, mereka harus saling membuat koneksi antara satu dengan lainnya. Koneksi ini memiliki dua tujuan: Komputer dapat menggunakan koneksi tersebut untuk mengidentifikasikan dirinya kepada komputer lain, yang meyakinkan bahwa sistem lain yang tidak membuat koneksi tidak dapat mengirimkan data ke komputer tersebut. Firewall juga dapat menggunakan informasi koneksi untuk menentukan koneksi apa yang diizinkan oleh kebijakan akses dan menggunakannya untuk menentukan apakah paket data tersebut akan diterima atau ditolak. Koneksi digunakan untuk menentukan bagaimana cara dua host tersebut akan berkomunikasi antara satu dengan yang lainnya (apakah dengan menggunakan koneksi connection-oriented, atau connectionless). Kedua tujuan tersebut dapat digunakan untuk menentukan keadaan koneksi antara dua host tersebut, seperti halnya cara manusia bercakap-cakap. Jika Amir bertanya kepada Aminah mengenai sesuatu, maka Aminah akan meresponsnya dengan jawaban yang sesuai dengan pertanyaan yang diajukan oleh Amir; Pada saat Amir melontarkan pertanyaannya kepada Aminah, keadaan percakapan tersebut adalah Amir menunggu respons dari Aminah. Komunikasi di jaringan juga mengikuti cara yang sama untuk memantau keadaan percakapan komunikasi yang terjadi.

5. Proses inspeksi Paket

Inspeksi paket (‘packet inspection) merupakan proses yang dilakukan oleh firewall untuk ‘menghadang’ dan memproses data dalam sebuah paket untuk menentukan bahwa paket tersebut diizinkan atau ditolak, berdasarkan kebijakan akses (access policy) yang diterapkan oleh seorang administrator. Firewall, sebelum menentukan keputusan apakah hendak menolak atau menerima komunikasi dari luar, ia harus melakukan inspeksi terhadap setiap paket (baik yang masuk ataupun yang keluar) di setiap antarmuka dan membandingkannya dengan daftar kebijakan akses. Inspeksi paket dapat dilakukan dengan melihat elemen-elemen berikut, ketika menentukan apakah hendak menolak atau menerima komunikasi:

- Alamat IP dari komputer sumber
- Port sumber pada komputer sumber
- Alamat IP dari komputer tujuan
- Port tujuan data pada komputer tujuan
- Protokol IP
- Informasi header-header yang disimpan dalam paket

6. Stateful Packet Inspection

Ketika sebuah firewall menggabungkan stateful inspection dengan packet inspection, maka firewall tersebut dinamakan dengan Stateful Packet Inspection (SPI). SPI merupakan proses inspeksi paket yang tidak dilakukan dengan menggunakan struktur paket dan data yang terkandung dalam paket, tapi juga pada keadaan apa host-host yang saling berkomunikasi tersebut berada. SPI mengizinkan firewall untuk melakukan penapisan tidak hanya berdasarkan isi paket tersebut, tapi juga berdasarkan koneksi atau keadaan koneksi, sehingga dapat mengakibatkan firewall memiliki kemampuan yang lebih fleksibel, mudah diatur, dan memiliki skalabilitas dalam hal penapisan yang tinggi. Salah satu keunggulan dari SPI dibandingkan dengan inspeksi paket biasa adalah bahwa ketika sebuah koneksi telah dikenali dan diizinkan (tentu saja setelah dilakukan inspeksi), umumnya sebuah kebijakan (policy) tidak dibutuhkan untuk mengizinkan komunikasi balasan karena firewall tahu respons apa yang diharapkan akan diterima. Hal ini memungkinkan inspeksi terhadap data dan perintah yang terkandung dalam sebuah paket data untuk menentukan apakah sebuah koneksi diizinkan atau tidak, lalu firewall akan secara otomatis memantau keadaan percakapan dan secara dinamis mengizinkan lalu lintas yang sesuai dengan keadaan. Ini merupakan peningkatan yang cukup signifikan jika dibandingkan dengan firewall dengan inspeksi paket biasa. Apalagi, proses ini diselesaikan tanpa adanya kebutuhan untuk mendefinisikan sebuah kebijakan untuk mengizinkan respons dan

komunikasi selanjutnya. Kebanyakan firewall modern telah mendukung fungsi ini

- **Manfaat Firewall**

Firewall adalah sistem keamanan jaringan yang berfungsi sebagai penghalang antara jaringan internal yang aman dan jaringan eksternal yang tidak aman (seperti internet). Berikut adalah beberapa manfaat utama firewall:

1. Melindungi Jaringan dari Ancaman Berbahaya

Firewall dapat mencegah akses tidak sah dari pihak luar ke jaringan internal. Ini membantu mengurangi risiko serangan seperti hacking, malware, ransomware, dan DDoS (Distributed Denial of Service).

2. Mengontrol Akses Jaringan

Firewall memungkinkan administrator untuk menetapkan aturan siapa yang boleh mengakses jaringan dan layanan tertentu. Dengan fitur filtering, firewall dapat membatasi akses berdasarkan alamat IP, domain, atau aplikasi tertentu.

3. Meningkatkan Privasi dan Keamanan Data

Firewall mencegah kebocoran data dengan mengontrol lalu lintas keluar dan masuk. Ini sangat penting bagi organisasi yang menangani data sensitif seperti informasi pelanggan atau data keuangan.

4. Mendeteksi dan Mencegah Ancaman Secara Real-time

Beberapa firewall modern dilengkapi dengan fitur Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) yang dapat mendeteksi, memonitor, dan mencegah aktivitas mencurigakan secara otomatis.

5. Mengurangi Risiko Serangan Phishing dan Malware

Firewall dapat memblokir situs web berbahaya dan email yang mencurigakan untuk mencegah

karyawan atau pengguna mengakses situs yang bisa menyebarkan malware atau melakukan phishing.

6. Mengoptimalkan Penggunaan Bandwidth

Dengan firewall, perusahaan dapat mengatur penggunaan bandwidth dengan membatasi akses ke situs atau layanan tertentu seperti streaming, media sosial, atau torrent, yang dapat mengganggu produktivitas.

7. Menyediakan Keamanan dalam Jaringan Wi-Fi Publik

Firewall membantu mencegah akses tidak sah ke perangkat yang terhubung dalam jaringan Wi-Fi publik, melindungi dari serangan Man-in-the-Middle (MitM) dan packet sniffing.

8. Memastikan Kepatuhan terhadap Regulasi Keamanan

Banyak industri memiliki regulasi keamanan seperti GDPR, HIPAA, atau ISO 27001 yang mengharuskan organisasi menggunakan firewall untuk melindungi data pelanggan dan sistem mereka.

- **Jenis-jenis Firewall**

Sebagai sistem keamanan perangkat, terdapat beberapa jenis firewall yang dapat disesuaikan dengan kebutuhan. Berikut merupakan jenis-jenis firewall yang dapat diketahui:

1. Packet Filtering Firewall

Packet Filtering Firewall bekerja pada lapisan jaringan (Network Layer) dan Transport Layer dalam model OSI. Firewall ini menyaring lalu lintas berdasarkan header paket, seperti alamat IP sumber dan tujuan, port, serta protokol. Jika paket sesuai dengan aturan yang ditetapkan, paket akan diteruskan; jika tidak, paket akan diblokir. Kelebihannya adalah cepat dan sederhana karena hanya memeriksa header paket serta memiliki konsumsi sumber daya rendah. Namun, kekurangannya adalah tidak dapat menganalisis isi paket (payload) serta rentan terhadap serangan seperti spoofing atau fragmented attacks. Contoh implementasinya adalah Access Control Lists (ACL) pada router dan firewall sederhana.

2. Stateful Inspection Firewall

Stateful Inspection Firewall selain memeriksa header paket, juga melacak status koneksi dalam tabel sesi untuk memastikan bahwa paket yang masuk sesuai dengan sesi yang sudah ada. Ini membuatnya lebih aman dibandingkan Packet Filtering Firewall karena memahami konteks koneksi dan dapat mencegah paket tidak sah yang mencoba menyamar sebagai koneksi yang sah. Namun, firewall ini memerlukan lebih banyak sumber daya karena harus menyimpan informasi sesi dan rentan terhadap serangan DDoS jika tidak dikonfigurasi dengan benar. Contoh implementasi firewall jenis ini adalah iptables (Linux) dan Windows Defender Firewall.

3. Proxy Firewall

Proxy Firewall (Application Layer Firewall) bertindak sebagai perantara (proxy) antara pengguna dan layanan yang diakses. Firewall ini memeriksa lalu lintas hingga lapisan aplikasi (Application Layer) untuk mendeteksi ancaman tersembunyi dalam data. Pengguna tidak langsung terhubung ke server tujuan; firewall akan menerima permintaan, memverifikasinya, lalu meneruskannya ke server jika aman. Kelebihannya adalah memberikan perlindungan tingkat tinggi dengan analisis mendalam pada data serta dapat menyembunyikan alamat IP pengguna, meningkatkan anonimitas dan keamanan. Namun, kelemahannya adalah dapat menyebabkan keterlambatan dalam koneksi karena perlu memproses setiap permintaan serta membutuhkan daya komputasi yang lebih besar dibandingkan firewall lainnya. Contoh firewall jenis ini adalah Squid Proxy dan Blue Coat ProxySG.

4. Next-Generation Firewall (NGFW)

Next-Generation Firewall (NGFW) adalah firewall modern yang menggabungkan fitur dari firewall sebelumnya dengan tambahan keamanan tingkat lanjut seperti Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Deep Packet Inspection (DPI), serta analisis berbasis AI dan Machine Learning. NGFW mampu mengidentifikasi dan menghentikan serangan secara real-time, serta memfilter lalu lintas berdasarkan aplikasi, pengguna, dan jenis ancaman. Kelebihannya adalah perlindungan menyeluruh terhadap berbagai ancaman siber, mendukung kontrol aplikasi (Application Control), serta memiliki kapabilitas inspeksi mendalam terhadap lalu lintas jaringan. Namun, kelemahannya adalah membutuhkan biaya tinggi serta konfigurasi yang kompleks. Contoh firewall jenis ini adalah Palo Alto Networks, Cisco Firepower, dan Fortinet FortiGate.

2.2 Implementasi Firewall Berbasis Perangkat Lunak

Firewall berbasis perangkat lunak adalah aplikasi yang diinstal pada komputer atau server untuk mengawasi dan mengendalikan lalu lintas jaringan berdasarkan aturan keamanan yang telah ditetapkan. Tujuannya adalah melindungi sistem dari akses yang tidak sah dan ancaman siber.

Fungsi Utama Firewall Berbasis Perangkat Lunak:

1. Mencegah Akses Tidak Sah: Firewall memblokir percobaan akses oleh pengguna atau sistem yang tidak diotorisasi, menjaga integritas dan kerahasiaan data.

2. Memfilter Lalu Lintas Jaringan: Dengan menetapkan aturan spesifik, firewall dapat mengizinkan atau menolak paket data berdasarkan alamat IP, nomor port, atau protokol tertentu.

3. Mendeteksi dan Memblokir Aktivitas Mencurigakan: Firewall dapat mengenali pola lalu lintas yang tidak biasa atau berpotensi berbahaya, seperti serangan malware atau upaya peretasan, dan mengambil tindakan pencegahan.

4. Mengontrol Akses Aplikasi ke Internet: Firewall memungkinkan pengaturan izin bagi aplikasi tertentu untuk mengakses internet, sehingga dapat mencegah aplikasi berbahaya mengirim atau menerima data tanpa sepengetahuan pengguna.

Jenis-Jenis Firewall Berbasis Perangkat Lunak:

1. Firewall Berbasis Host (Host-based Firewall): Terpasang langsung pada komputer individu untuk melindungi perangkat tersebut dari ancaman jaringan. Contohnya adalah Windows Defender Firewall dan ZoneAlarm.

2. Firewall Berbasis Jaringan (Network-based Firewall): Dipasang pada server atau gateway untuk melindungi seluruh jaringan dari ancaman eksternal. Contohnya adalah pfSense dan IPFire.

3. Firewall Generasi Berikutnya (Next-Generation Firewall - NGFW): Menggabungkan fitur firewall tradisional dengan kemampuan tambahan seperti sistem pencegahan intrusi (IPS) dan

inspeksi paket mendalam (deep packet inspection) untuk memberikan perlindungan yang lebih komprehensif.

Contoh Firewall Berbasis Perangkat Lunak yang Populer:

Windows Defender Firewall: Firewall bawaan pada sistem operasi Windows yang memberikan perlindungan dasar terhadap ancaman jaringan.

ZoneAlarm: Firewall pihak ketiga yang menawarkan fitur tambahan seperti perlindungan terhadap phishing dan kontrol aplikasi.

pfSense: Sebuah firewall open-source yang berbasis FreeBSD, sering digunakan untuk keperluan jaringan yang lebih kompleks.

IPFire: Firewall open-source yang fokus pada keamanan dan fleksibilitas, cocok untuk berbagai jenis jaringan.

Langkah-Langkah Implementasi Firewall Berbasis Perangkat Lunak:

1. Instalasi dan Konfigurasi Awal:
Unduh dan instal perangkat lunak firewall yang sesuai dengan kebutuhan dan kompatibel dengan sistem operasi yang digunakan Setelah instalasi, lakukan konfigurasi awal dengan menetapkan aturan dasar untuk mengizinkan atau memblokir lalu lintas jaringan.

2. Penetapan Aturan Penyaringan (Filtering Rules):
Tentukan kebijakan keamanan yang jelas, seperti mengizinkan akses hanya dari alamat IP tertentu atau memblokir port yang tidak digunakan. Aturan penyaringan harus disesuaikan dengan kebutuhan spesifik jaringan dan risiko yang mungkin dihadapi.

3. Pemantauan dan Pencatatan (Monitoring and Logging):
Aktifkan fitur logging untuk mencatat semua aktivitas jaringan yang melewati firewall. Secara rutin tinjau log untuk mendeteksi aktivitas mencurigakan atau upaya akses yang tidak sah.

4. Pembaruan dan Pemeliharaan Berkala:

Pastikan perangkat lunak firewall selalu diperbarui ke versi terbaru untuk mendapatkan fitur keamanan terkini dan perbaikan bug. Lakukan pengujian berkala terhadap aturan yang diterapkan untuk memastikan efektivitasnya dalam menghadapi ancaman baru.

2.3 Konfigurasi dan Manajemen Firewall

Konfigurasi firewall merupakan bagian penting dalam mengamankan aset jaringan. Namun, pertahanan firewall terkuat sekalipun akan gagal jika tidak dikonfigurasi dengan benar. Pakar keamanan Gartner berpendapat bahwa 99% pelanggaran firewall disebabkan oleh kesalahan konfigurasi , bukan kelemahan dalam sistem firewall. Cara pengguna mengatur sistem firewall mereka membuat perbedaan besar pada postur keamanan mereka secara keseluruhan.

Hal ini penting karena firewall merupakan bagian utama dari sistem keamanan siber. Firewall menyaring lalu lintas jaringan yang masuk dan keluar. Firewall hanya mengizinkan lalu lintas yang disetujui untuk mengakses sumber daya. Firewall juga memblokir koneksi yang tidak dikenal, sehingga mencegah penyerang jahat masuk.

Firewall hanya dapat menjalankan fungsi-fungsi ini dengan kebijakan yang tepat. Kebijakan firewall adalah serangkaian aturan keamanan yang menyatakan kondisi untuk masuk ke jaringan . Kebijakan ini mencakup port yang diizinkan dan alamat IP atau nama domain yang disetujui. Kebijakan ini juga menerapkan zona keamanan untuk melakukan segmentasi jaringan. Menerapkan kebijakan ini dengan benar merupakan tantangan utama konfigurasi firewall . Jika filter terlalu luas, penyerang mungkin dapat mengakses jaringan. Namun, kontrol yang terlalu ketat dapat mengakibatkan masalah kinerja bagi pengguna yang sah. Mari kita bahas cara meningkatkan konfigurasi firewall Anda

BAB III
PENUTUP

3.1 Kesimpulan

Firewall merupakan suatu sistem proteksi untuk melaksanakan pengawasan lalu lintas paket data menuju atau meninggalkan sebuah jaringan computer sehingga paket data yang telah diperiksa dapat diterima, ditolak atau bahkan dimodifikasi terlebih dahulu sebelum memasuki atau meninggalkan jaringan tersebut.

3.2 Saran

Diharapkan para pembaca bisa memahami apa itu firewall dan bagaimana cara kerjanya.

DAFTAR PUSAKA

https://congwong.blogspot.com/2024/10/menganalisis-konsep-dan-implementasi.html?utm_source=chatgpt.com&m=1

https://nordlayer.com/learn/firewall/configuration/

Adi, D. W., Irawan, F., Athallah, Z. R., & Neyman, S. N. (2024). Implementasi firewall menggunakan fitur dari IPTables pada sistem operasi Linux. Journal of Internet and Software Engineering.