Praktikum Jaringan Komputer
Pertemuan 11 – Konfigurasi Firewall pada Mikrotik

1.1. CAPAIAN PEMBELAJARAN

1. Memahami konsep Firewall;
2. Mampu Mengaplikasikan Firewall pada perangkat jaringan.

1.2. ALAT DAN BAHAN

1. Seperangkat komputer lengkap/Laptop dengan koneksi internet
2. Web Browser (Chrome/Firefox/Opera/Edge/Safari/dll)
3. Aplikasi Kantor (Microsoft Office/Libre Office/WPS Office/etc)
4. Router Mikrotik

1.3. DASAR TEORI

Firewall merupakan sistem keamanan jaringan yang dirancang untuk melindungi perangkat pengguna dari akses yang tidak sah. Kalau diibaratkan, firewall berfungsi seperti pagar atau gerbang keamanan yang memantau siapa saja yang melintas. Secara teknis, sistem ini memang bekerja untuk mengawasi data yang masuk atau keluar dari jaringan Anda. Firewall akan memeriksa tiap-tiapnya, lalu memastikan apakah data tersebut aman atau justru membawa virus atau malware. Apabila mendeteksi hal-hal yang mencurigakan, firewall akan langsung memblokir data tersebut agar tidak masuk ke perangkat Anda. Firewall sendiri bisa berupa hardware yang memiliki fitur keamanan, atau software yang diinstal di perangkat Anda. Setiap jenis ini bekerja sesuai aturan yang sudah ditetapkan, seperti izin akses untuk website tertentu atau memblokir aplikasi tertentu.

A. Fungsi Firewall

Firewall memiliki beberapa fungsi penting sebagai sistem keamanan jaringan, seperti:

1. Memberikan perlindungan dari ancaman cyber. Firewall mampu melindungi perangkat pengguna dari ancaman cyber dengan mengidentifikasi dan menghalau serangan jahat, seperti DDoS yang mengganggu kestabilan jaringan.
2. Mencegah akses yang tidak sah. Sistem ini akan memfilter dan memblokir aktivitas yang mencurigakan dari pihak luar yang mencoba mengakses jaringan tanpa izin. Hal ini sangat berguna untuk mengamankan data Anda dari hacker atau ancaman cyber lainnya.
3. Mengawasi traffic jaringan. Semua data di jaringan Anda akan diawasi oleh

firewall. Setiap data yang melewatinya akan diperiksa untuk memastikan tidak ada ancaman yang tersembunyi, seperti virus atau malware.

4. Mencegah kebocoran data. Selain paket data yang masuk ke jaringan, aliran data keluar juga akan diperiksa untuk memastikan bahwa hanya data yang aman saja yang bisa dikirim ke luar jaringan.
5. Membantu mengontrol akses internal. Firewall bisa membantu mengelola akses dalam jaringan Anda sendiri. Misalnya, Anda bisa menetapkan aturan agar hanya pengguna tertentu saja yang diizinkan mengakses sistem utama jaringan, yang berguna di lingkungan kantor atau perusahaan.
6. Mengatur penggunaan bandwidth. Anda bisa mengontrol penggunaan bandwidth melalui firewall dengan membatasi aplikasi atau layanan tertentu. Langkah ini akan memastikan penggunaan bandwidth yang efisien dan mencegah penyalahgunaan untuk aktivitas yang tidak penting.

B. Cara Kerja Firewall

Saat memantau dan mengontrol aliran data, ada beberapa tahap yang dilakukan oleh firewall dalam menjalankan tugasnya, berikut adalah penjelasan cara kerja firewall:

1. Firewall memantau aliran data.

   Firewall memantau semua paket data yang masuk dan keluar di jaringan Anda. Setiap paket data ini berisi informasi seperti alamat IP sumber dan tujuan, nomor port, serta protokol yang digunakan.
2. Aturan keamanan mulai diterapkan.

   Berdasarkan informasi dalam paket data tersebut, firewall kemudian menerapkan aturan keamanan yang sudah ditentukan. Misalnya, kalau ada paket data dari sumber yang tidak dikenal atau menggunakan port yang tidak diizinkan, firewall akan memblokirnya.
3. Paket data akan difilter.

   Setelah menerapkan aturan keamanan, firewall akan memutuskan apakah paket data diizinkan atau ditolak. Pada tahap ini, firewall akan menggunakan metode filtering yang meliputi:

   - Packet filtering. Metode ini memeriksa header paket data untuk menentukan apakah paket tersebut sesuai dengan aturan yang ditetapkan.

- Stateful inspection. Menganalisis status koneksi untuk memastikan bahwa paket data berasal dari koneksi yang valid.
- Proxy service. Bertindak sebagai penengah antara pengguna dan resource yang diakses sehingga data tidak langsung masuk ke jaringan internal.

4. Firewall mengambil keputusan.

   Setelah menyelesaikan tahap penyaringan paket data, firewall akan menetapkan keputusan berikut:

   - Allow. Paket data diizinkan untuk diteruskan ke tujuannya.
   - Deny. Menolak paket data, yang kemudian diblokir dan tidak diteruskan.
   - Limit. Mengizinkan penerusan paket data, tapi dengan batasan tertentu seperti kecepatan transfer.

5. Mencatat dan memantau data.

   Terakhir, firewall akan mencatat semua aktivitas data, termasuk paket yang diblokir atau diizinkan. Anda bisa mengecek log ini untuk melihat apakah ada anomali, atau untuk mendeteksi ancaman serupa di lain waktu.

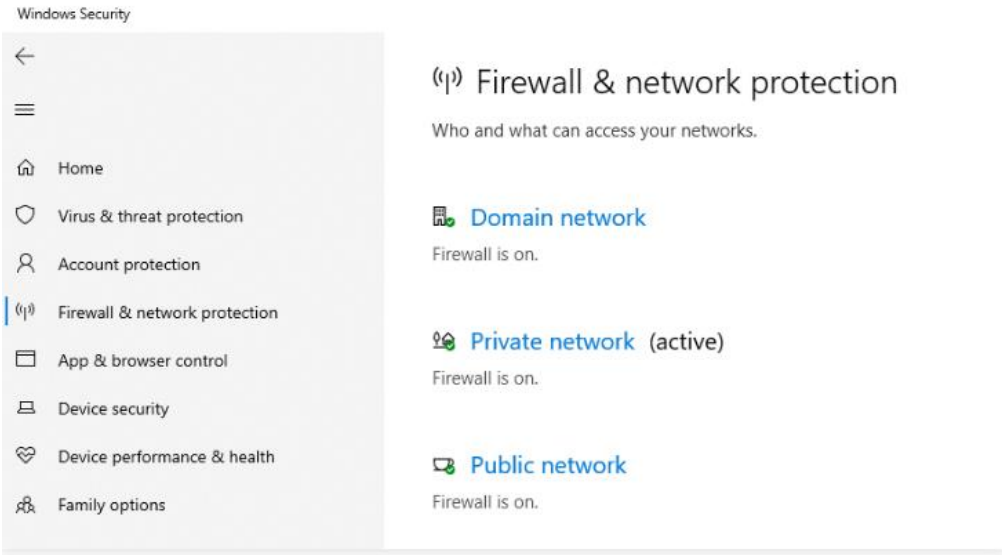
C. Jenis-Jenis Firewall

1. Hardware Firewall

Hardware firewall adalah firewall berbentuk fisik yang terpisah dari perangkat yang dilindunginya. Biasanya, perangkat ini terletak di antara jaringan internal dan internet, yang berfungsi untuk mengamankan seluruh jaringan.

Cara kerjanya mirip seperti router, tapi lebih rumit karena jenis firewall ini bisa memfilter data berdasarkan aturan tertentu. Hardware firewall juga bisa mengamankan banyak perangkat sekaligus sehingga banyak digunakan oleh perusahaan.

2. Software Firewall



Software firewall langsung terinstal di perangkat yang dilindunginya, seperti komputer atau server. Pengguna bisa menetapkan aturan khusus untuk aplikasi tertentu, atau membatasi akses port tertentu agar hanya program tepercaya saja yang bisa berjalan.

Jenis firewall ini biasanya lebih fleksibel sehingga cocok untuk satu perangkat atau jaringan kecil. Contohnya adalah Windows Defender Firewall, yang sudah terinstal di sistem operasi Windows.

3. Packet-filtering Firewall

Packet-filtering firewall memfilter data berdasarkan alamat IP sumber, tujuan, port, dan protokol. Firewall jenis ini bekerja dengan memeriksa header setiap paket data, kemudian hanya mengizinkan paket yang sesuai dengan aturan yang ditetapkan.

Namun, karena data diperiksa pada tingkat paket, firewall jenis ini kurang optimal dalam mendeteksi ancaman kompleks meskipun bisa bekerja lebih cepat.

Packet-filtering firewall bisa ditemukan pada router yang menerapkan Access Control List (ACL). Router bisa diatur agar mengizinkan traffic HTTP dari port default (80), tapi memblokir koneksi FTP dari port 21.

4. Circuit-level Gateway

Circuit-level gateway bekerja dengan memeriksa koneksi antarperangkat untuk memastikan komunikasi yang aman. Berbeda dengan jenis lainnya, firewall ini lebih difokuskan untuk memantau sesi koneksi guna memastikan bahwa koneksi tersebut bukanlah sesi berbahaya.

Firewall ini cocok untuk jaringan yang membutuhkan kecepatan dan stabilitas, karena proses pengecekan tidak dilakukan satu-satu untuk setiap paket data.

5. Stateful Inspection Firewall

   Stateful inspection firewall bekerja dengan mengawasi seluruh sesi koneksi dan memblokir aktivitas yang mencurigakan. Bisa dibilang, jenis firewall ini adalah gabungan dari packet-filtering firewall dan circuit-level gateway yang mampu memeriksa status koneksi. Jenis firewall ini mampu membedakan paket yang aman dan paket yang berpotensi berbahaya.

6. Proxy Firewall

   Seperti proxy server pada umumnya, jenis firewall ini berfungsi sebagai jembatan antara jaringan internal dan internet. Ketika perangkat mengirimkan permintaan data keluar, proxy firewall akan menanganinya dan meneruskannya ke jaringan eksternal dengan menyamarkan IP perangkat.

   Oleh karena itu, jenis firewall ini cocok untuk jaringan yang memerlukan privasi ketat, seperti layanan keuangan atau pemerintahan.

7. Next Generation Firewall

   Next-generation firewall (NGFW) adalah firewall canggih yang memiliki mekanisme keamanan paling lengkap. Jenis firewall ini menerapkan pemeriksaan paket data yang ketat, deteksi ancaman, serta sistem pencegahan serangan sekaligus.

   Selain itu, NGFW juga bisa memeriksa status koneksi, mendeteksi malware, dan menganalisis aplikasi.

   Jenis firewall ini paling cocok untuk perusahaan yang membutuhkan keamanan tingkat lanjut untuk menghalau serangan yang lebih canggih, serta melindungi seluruh sistem dengan konfigurasi yang bisa diatur sesuai kebutuhan.

8. Cloud Firewall

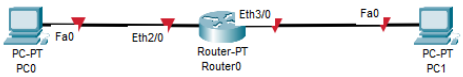
   Cloud firewall menerapkan sistem perlindungan melalui layanan berbasis cloud tanpa perangkat fisik sehingga lebih fleksibel dan bisa diakses dari mana saja. Firewall jenis ini mampu memberikan perlindungan dengan cepat sesuai kebutuhan. Biasanya, cloud firewall digunakan untuk mengamankan aplikasi web dan layanan cloud sehingga cocok untuk perusahaan yang menggunakan layanan berbasis cloud.

1.4. PRAKTIKUM

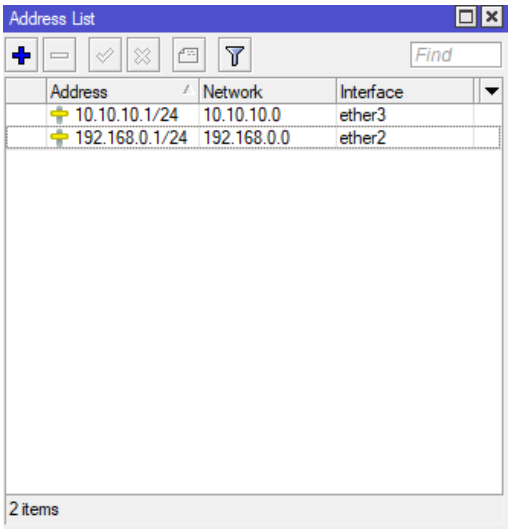
Konfigurasi Firewall pada Mikrotik

A. Manajemen Akses Router Mikrotik dengan Filter Rules

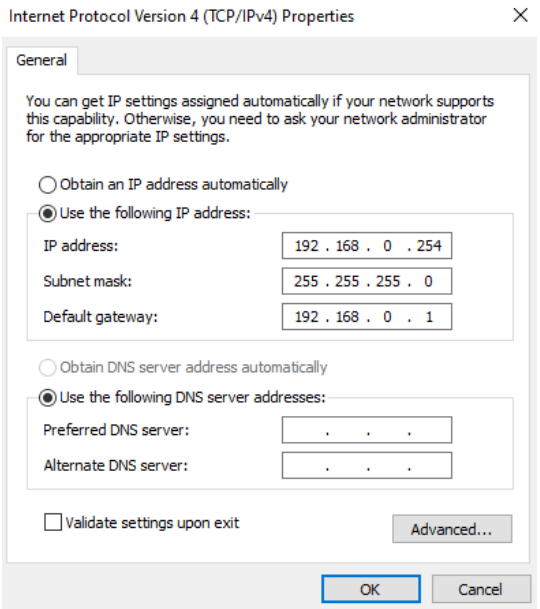
1. Hubungkan Router dengan 2 buah *end devices* seperti pada tolopogi berikut:



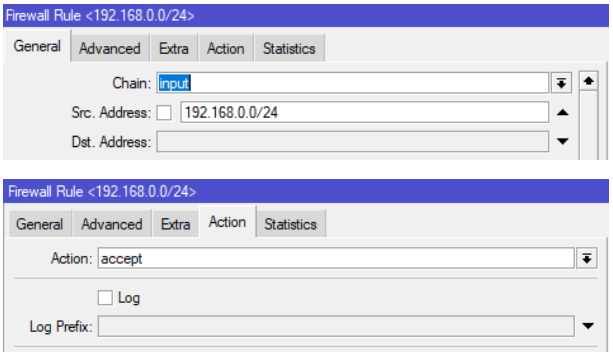
2. Buka winbox menggunakan salah satu PC melalui akses MAC Address
3. Buka menu **IP** > **Addresses**, kemudian tambahkan IP pada ethernet 2 dan ethernet 3 (Alamat IP menyesuaikan dengan NPM)



4. Konfigurasi IP pada PC yang terhubung dengan ethernet 2 agar berada dalam 1 jaringan dengan router



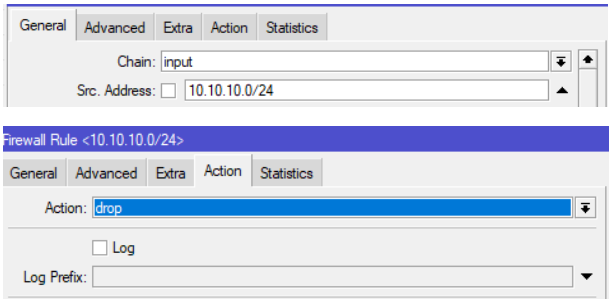
5. Lakukan hal serupa dengan PC yang terhubung pada ethernet 3
6. Buka **IP** > **Firewall** > **Filter Rules**, klik ikon plus (+) untuk menambahkan rule sebagai berikut:
   a. Rule untuk mengizinkan akses ke router bagi jaringan ethernet 2 melalui IP Address (layer 3 – OSI layer): Konfigurasi dilakukan pada tab **General** dan **Action**



   - Chain > Input : Memproses trafik yang masuk ke router
   - Src. Address : Alamat sumber paket data
   - Action > Accept : Paket diterima

   Penjelasan : Pada rules tersebut berarti router akan menerima paket data yang masuk dari seluruh alamat IP yang berada pada jaringan 192.168.0.0/24

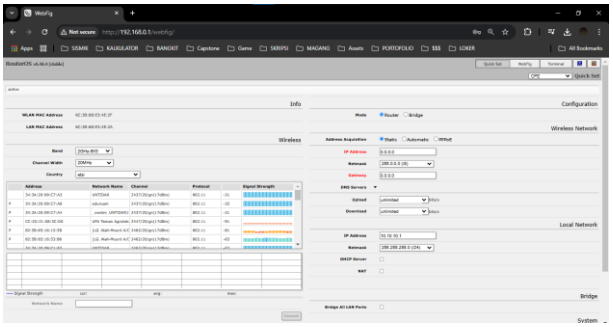
   b. Rule untuk menolak akses ke router dari jaringan ethernet 3 melalui IP Address (layer 3 – OSI layer): Konfigurasi dilakukan pada tab **General** dan **Action**



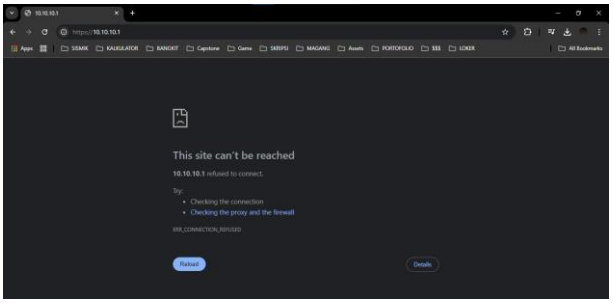
   - Chain > Input : Memproses trafik yang masuk ke router
   - Src. Address : Alamat sumber paket data
   - Action > Drop : Paket ditolak tanpa keterangan

   Penjelasan : Pada rules tersebut berarti router akan menolak paket data yang masuk dari seluruh alamat IP yang berada pada jaringan 10.10.10.0/24.

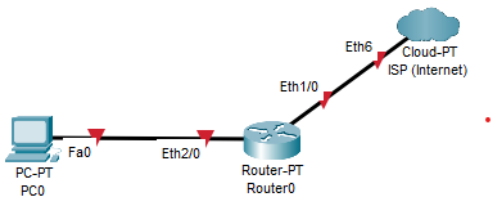
7. Cek status konfigurasi:
    a. Cek PC ethernet 2 akses ke mikrotik bisa dilakukan dengan mengetikkan alamat IP port ethernet 2 pada web browser PC yang terhubung dengan jaringan ethernet 2 router. Jika konfigurasi berhasil maka perangkat boleh mengakses router dan akan muncul tampilan seperti berikut



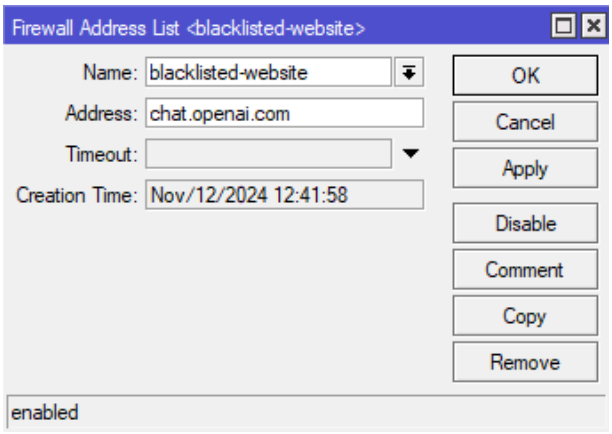
    b. Cek PC ethernet 3 akses ke mikrotik bisa dilakukan dengan mengetikkan alamat IP port ethernet 3 pada web browser PC yang terhubung dengan jaringan ethernet 3 router. Jika konfigurasi berhasil maka perangkat tidak diizinkan untuk mengakses router dan akan muncul tampilan seperti berikut



B. Manajemen Akses Website dengan Filter Rules
1. Buatlah jaringan dengan topologi seperti berikut:

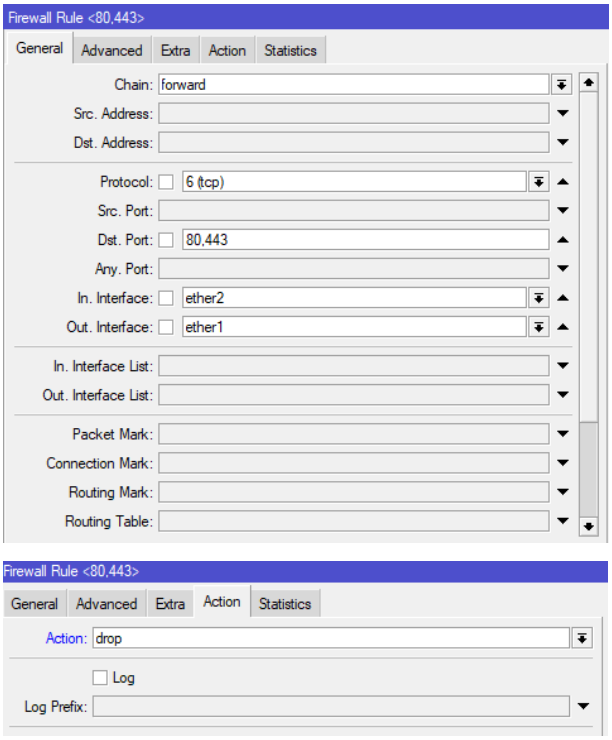


2. Konfigurasi DHCP dan NAT agar PC terhubung dengan internet
3. Buka **IP** > **Firewall** > **Address Lists**, tambahkan website yang ingin diblokir. Pada praktikum ini akan memblokir akses ke website chat.openai.com untuk membatasi penggunaan chatgpt



- Name : Berisi nama dari address list yang dibuat
- Address : Berisi alamat website yang dituju

4. Buat rule pada Firewall Rule yang berisi perintah untuk menolak akses ke Address List yang telah dibuat



- Chain > Forward : Mengelola trafik paket data yang melewati router
- Protocol > 6 (tcp) : Rule yang dibuat akan diterapkan pada jaringan yang meggunakan protokol TCP
- Dst. Port : Port destinasi atau website. 80 merupakan port untuk HTTP, sedangkan 443 merupakan port untuk HTTPS
- In. Interface > ether2 : Rule berlaku untuk jaringan yang masuk dari ethernet 2 (jaringan lokal)

- Out. Interface > ether1 : Rule berlaku untuk jaringan yang keluar melalui ethernet 1 (ISP)
- Action > Drop : Menolak trafik

5. Setelah rule berhasil dibuat, cek status konfigurasi dengan membuka website yang diblokir, jika berhasil maka website tersebut akan gagal untuk diakses.