MODUL 7

VPN DAN *FIREWALL*

7.1 Tujuan Praktikum

1. Mengetahui dan memahami apa itu VPN.
2. Mengetahui dan memahami apa itu *Firewall.*
3. Mampu melakukan instalasi dan konfigurasi dari VPN dan *Firewall.*
4. Mengetahui cara kerja dari *Firewall.*
5. Mampu membuat sebuah server menggunakan VPN dan *Firewall*.

7.2 Alat dan Bahan

1. Laptop
2. Mouse
3. Router Mikrotik
4. Winbox

7.3 Dasar Teori

7.3.1 Pengertian VPN

VPN atau Jaringan Pribadi Virtual (*Virtual Private Network*) membuat koneksi jaringan privat di antara beberapa perangkat melalui internet. VPN digunakan untuk mentransmisikan data secara aman dan anonym melalui jaringan public. VPN bekerja dengan cara menyembunyikan alamat IP pengguna dan meng-enskripsi data sehingga tidak dapat dibaca oleh siapa pun yang tidak berwenang untuk menerimanya.

7.3.2 Jenis Implementasi VPN

Pada implementasinya terdapat dua jenis VPN, yaitu *Remote Access VPN* dan *Site-to-Site VPN*.

1. *Remote Access VPN*

   Remote Access VPN disebut juga *Virtual Dial-Up Network* (VPDN). VPDN adalah jenis *user-to-LAN connection*, koneksi yang menghubungkan pengguna yang *mobile* dengan *Local Area Network* (LAN). Ini artinya, *user* dapat mengakses ke *private network* dari

manapun. Biasanya VPDN ini dimanfaatkan oleh para pegawai yang sedang berada di luar kantor dan memerlukan koneksi ke jaringan kantor perusahaannya. Biasanya Perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerja sama dengan *Enterprise Service Provider* (ESP). ESP akan memberikan suatu *Network Access Server* (NAS) bagi Perusahaan tersebut. ESP juga akan memberikan *software* khusus untuk komputer-komputer yang digunakan oleh pegawai Perusahaan tersebut.

Untuk mengakses jaringan lokal Perusahaan, pegawai terlebih dahulu terhubung ke NAS dengan men-*dial* nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan *software client* pegawai tersebut dapat terhubung ke jaringan lokal perusahaan.

2. *Site-to-Site VPN*

   Site-to-Site VPN digunakan untuk menghubungkan berbagai area yang sudah *fixed* atau tetap, VPN ini memanfaatkan perangkat *dedicated* yang dihubungkan melalui internet. Contoh implementasi VPN jenis ini adalah digunakan untuk menghubungkan antara dua kantor atau lebih yang letaknya berjauhan. Koneksi antara kantor tersebut secara terus menerus 24 jam. *Site-to-Site VPN* hanya menjadi dua, yaitu Extranet dan Intranet. Intranet yaitu di mana VPN hanya digunakan untuk menghubungkan berbagai lokasi yang masih satu instansi atau satu perusahaan. Seperti kantor pusat dihubungkan dengan kantor cabang. Dengan kata lain, *administrative control* dalam satu kendali. Sedangkan extranet adalah di mana saat VPN digunakan untuk menghubungkan Perusahaan satu dengan Perusahaan yang lain, misalnya mitra kerja, *supplier*, atau pelanggan. Dengan kata lain *administrative control* berada di bawah kendali beberapa instansi terkait.

7.3.3 Protokol VPN

1. PPTP

   PPTP (*Point-to-Point Tuneling Protocol*) merupakan protocol jaringan memungkinkan pengamanan transfer data dari *remote client* ke *server* pribadi Perusahaan dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan PPTP merupakan pengembangan *remote* dari *remote*

access Point-to-Point protocol yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). PPTP merupakan protocol jaringan yang merubah paket PPTP juga dapat digunakan pada jaringan *private LAN-to-LAN*. Fasilitas utama dari penggunaan PPTP adalah dapat digunakannua *Public-Switched Telephone Network* (PSTNs) untuk membangun VPN. Pembangunan PPTP yang mudah dan berbiaya murah untuk digunakan secara luas, menjadi solusi untuk *remote users* dan *mobile users* karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet.

2. L2TP

   L2TP (*Layer 2 Tunnel Protocol*) merupakan pengembangan dari PPTP ditambah L2F. *Network security protocol* dan enkripsi yang digunakan untuk autentikasi sama dengan PPTP. Akan tetapi untuk melakukan komunikasi, L2TP menggunakan UDP port 1701. Biasanya untuk keamaanan yang lebih baik, L2TP dikombinasikan dengan IPSec, menjadi L2TP/IPSec. L2TP biasa digunakan dalam membuat *Virtual Private Network* yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya. Umumnya, L2TP menggunakan port 1702 dengan protocol UDP untuk mengirimkan L2TP *encapsulated PPP frames* sebagai data yang di tunnel. Terdapat dua model *tunnel* yang dikenal, yaitu *compulsory* dan *voluntary*. Perbedaan utama keduanya terletak pada *end point tunnel*-nya. Pada *compulsaty tunnel*, ujung berada pada ISP, sedangkan pada *voluntary* ujung *tunnel* berada pada *client remote*.

3. IPSec

   IPsec merupakan *tunneling protocol* yang bekerja pada layer 3. IPSec menyediakan layanan sekuritas pada IP layer dengan mengizinkan sistem untuk memilih protokol keamanan yang diperlukan, memperkirakan algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. IPSec menyediakan layanan-layananm keamanan tersebut dengan menggunakan sebuah metode pengamanan yang bernama *Internet Key Exchange* (IKE). IKE bertugas untuk menangani protokol yang

bernegosiasi dan algoritma pengamanan yang diciptakan berdasarkan dari *policy* yang diterapkan. Dan pada akhirnya IKE akan menghasilkan sebuah sistem enkripsi dan kunci pengamanannya yang akan digunakan untuk otentikasi yang digunakan
pada sistem IPSec ini.

4. OpenVPN

   OpenVPN merupakan aplikasi *open source* untuk *Virtual Private Networking* (VPN), dimana aplikasi tersebut dapat membuat koneksi *point to-point tunnel* yang telah ter-enkripsi. OpenVPN menggunakan *private keys*, *certificate*, atau username/password untuk melakukan authentikasi dalam membangun koneksi. Di mana teknologi yang digunakan untuk enkripsi dalam jaringan OpenVPN ini menggunakan teknologi SSL dan untuk komunikasinya OpenVPN bergerak di Layer 2 dan 3 OSI Layer. Karena OpenVPN berbasis *protocol* SSL maka OpenVPN ini dapat digunakan di berbagai sistem operasi tanpa perbedaan yang signifikan.

7.3.4 Cara Kerja VPN

VPN merupakan koneksi virtual yang bersifat privat, maksud dari virtual sendiri adalah VPN menciptakan tunel atau terowongan virtual dalam jaringan publik yang tidak harus *direct* dengan menggunakan protokol-protokol seperti PPTP, L2TP, atau IPSec. Sedangkan privat maksudnya adalah data yang dikirimkan melalui tunel tersebut terenkripsi (terbungkus), sehingga tetap rahasia meskipun melewati *public network*. Dalam VPN terdapat VPN *Server* dan VPN *Client*, semua koneksi diatur oleh VPN *Server*. Pertama-tama VPN *Server* harus dikonfigurasikan terlebih dahulu, kemudian di *client* harus di install program VPN baru setelah itu bisa dikoneksikan. Di *client* nantinya akan muncul koneksi virtual, jadi dalam client akan muncul *network adapter* (LAN *Card*) tetapi virtual. Tugas VPN *Client* adalah untuk mengenkripsi/dekripsi dan autentikasi.

Contoh implementasinya, seorang *client* yang telah terhubung VPN akan mengakses suatu situs www.google.com. *Request* ini sebelum tersampaikan ke VPN *Server* terlebih dahulu dienkripsikan oleh VPN *Client*, misal dienkripsi dengan rumus A, karena sebelumnya telah dikonfigurasikan

antara VPN *server* dan *client* maka *server* dan *client* akan mempunyai algoritma yang sama untuk membaca sebuah enkripsi. Begitu juga sebaliknya *server* ke *client*.

7.3.5 Pengertian *Firewall*

Firewall atau tembok-api 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 tembok-api diterapkan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (*gateway*) antara jaringan lokal dan jaringan lainnya. Tembok-api umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah *firewall* menjadi istilah lazim 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 berbadan hukum di dalamnya, maka perlindungan terhadap modal digital perusahaan tersebut dari serangan para peretas, pemata-mata, ataupun pencuri data lainnya, menjadi hakikat.

7.3.6 Jenis-Jenis *Firewall*

1. *Personal Firewall*

   Personal Firewall didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki. *Firewall* jenis ini akhir-akhir ini ber-evolusi menjadi sebuah kumpulan program yang bertujuan untuk mengamankan komputer secara total, dengan ditambahkannya beberapa fitur pengaman tambahan semacam perangkat proteksi terhadap *virus*, *anti-spyware*, *antispam*, dan lainnya. Bahkan beberapa produk *firewall* lainnya dilengkapi dengan fungsi pendeteksian gangguan keamanan jaringan (*Intrusion Detection System*). Contoh dari *firewall* jenis ini adalah *Microsoft Windows Firewall*. *Personal Firewall* secara umum hanya memiliki dua fitur utama, yakni *Packet Filter Firewall* dan *Stateful Firewall.*

2. *Network Firewall*

   Network Firewall didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni sebuah perangkat terdedikasi atau sebagai sebuah perangkat lunak yang di-instalasikan dalam sebuah *server*. Contoh dari *firewall* ini adalah IPTables dalam sistem operasi GNU/Linux. *Network Firewall* secara umum memiliki beberapa fitur utama, yakni apa yang dimiliki oleh *personal firewall* (*packet filter firewall* dan *stateful firewall*), *Circuit Level Gateway*, *Application Level Gateway*, dan juga NAT *Firewall*. *Network Firewall* umumnya bersifat transparan (tidak terlihat) dari pengguna dan menggunakan teknologi routing untuk menentukan paket mana yang diizinkan, dan mana paket yang akan ditolak.

7.3.7 Fungsi *Firewall*

- Mengatur dan mengontrol lalu lintas jaringan.
- Melakukan autentikasi terhadap akses.
- Melindungi sumber daya dalam jaringan private.
- Mancatat semua kejadian, dan melaporkan kepada administrator.

7.3.8 Cara Kerja *Firewall*

Pada bentuknya yang paling sederhana, sebuah *firewall* adalah sebuah router atau komputer yang dilengkapi dengan dua buah NIC (*Network Interface Card*, kartu antarmuka jaringan) yang mampu melakukan penapisan atau penyaringan terhadap paket-paket yang masuk. Perangkat jenis ini umumnya disebut dengan *packet-filtering router*. *Firewall* jenis ini bekerja dengan cara membandingkan alamat sumber dari paket-paket tersebut dengan kebijakan pengontrolan akses yang terdaftar dalam *Access Control List firewall*, *router* tersebut akan mencoba memutuskan apakah hendak meneruskan paket yang masuk tersebut ke tujuannya atau menghentikannya. Pada bentuk yang lebih sederhana lagi, *firewall* hanya melakukan pengujian terhadap alamat IP atau nama domain yang menjadi sumber paket dan akan menentukan apakah hendak meneruskan atau menolak paket tersebut. Meskipun demikian, *packet-filtering router* tidak dapat digunakan untuk

memberikan akses (atau menolaknya) dengan menggunakan basis hakhak yang dimiliki oleh pengguna.

Packet-filtering router juga dapat dikonfigurasikan agar menghentikan beberapa jenis lalu lintas jaringan dan tentu saja mengizinkannya. Umumnya, hal ini dilakukan dengan mengaktifkan/menonaktifkan *port* TCP/IP dalam sistem firewall tersebut. Sebagai contoh, port 25 yang digunakan oleh Protokol SMTP (*Simple Mail Transfer Protocol*) umumnya dibiarkan terbuka oleh beberapa *firewall* untuk mengizinkan surat elektronik dari Internet masuk ke dalam jaringan private, sementara *port* lainnya seperti port 23 yang digunakan oleh Protokol Telnet dapat dinonaktifkan untuk mencegah pengguna Internet untuk mengakses layanan yang terdapat dalam jaringan *private* tersebut. Firewall juga dapat memberikan semacam pengecualian (*exception*) agar beberapa aplikasi dapat melewati *firewall* tersebut. Dengan menggunakan pendekatan ini, keamanan akan lebih kuat tapi memiliki kelemahan yang signifikan yakni kerumitan konfigurasi terhadap *firewall*: daftar *Access Control List firewall* akan membesar seiring dengan banyaknya alamat IP, nama domain, atau port yang dimasukkan ke dalamnya, selain tentunya juga *exception* yang diberlakukan.

7.3.9 Perbedaan Antara VPN dan *Firewall*

VPN	FIREWALL
Fungsi Utama: VPN digunakan untuk meng-enkripsi lalu lintas internet dan membuat terowongan aman antara perangkat dan server VPN.	**Fungsi Utama:** *firewall* adalah alat yang digunakan untuk melindungi jaringan dari ancaman eksternal dengan memantau dan mengontrol lalu lintas masuk dan keluar.
Privasi dan Anonimitas: VPN menggantikan alamat IP dengan alamat IP dari server VPN, menyembunyikan identitas dan lokasi fisik.	**Pengaturan dan Kontrol Lalu Lintas:** *Firewal* memberikan kontrol atas jenis lalu lintas yang diizinkan dan diblokir, serta mengatur aturan akses terhadap aplikasi dan layanan tertentu.
Melintasi Pembatasan Geografis: VPN memungkinkan untuk mengakses komten yang mungkin terbatas di wilayah geografis tertentu.	**Deteksi dan Pencegahan Serangan:** *Firewall* memiliki kemampuan untuk mendeteksi dan mencegah serangan, seperti serangan DDoS, serangan berbasis protokol, dan upaya masuk yang mencurigakan.
Keamanan di Jaringan Publik: Saat terhubung ke jaringan WiFi publik, VPN membantu melindungi data dari potensi ancaman keamanan, seperti peretasan atau pencurian data.	**Proteksi Terhadap Ancaman Langsung:** *Firewall* melindungi jaringan dan perangkat dari ancaman yang mungkin merusak atau mencuri data.
Bypass Sensor dan Pemantauan: Di beberapa negara, VPN dapat membantu menghindari sensor dan pemantauan oleh pemerintah atau penyedia layanan internet, sehingga memungkinkan akses ke informasi dan konten tanpa pembatasan.	**Kontrol Keamanan Jaringan:** *Firewall* membantu dalam manajemen jaringan, memprioritaskan lalu lintas yang sah, dan mengelola *bandwidth.*

7.3.10 Alasan Mengapa Menggunakan VPN dan *Firewall* Diwaktu yang Sama

1. Dengan menggunakan VPN dan *firewall*, menciptakan lapisan keamanan yang jauh lebih baik karena *firewall* melindungi jaringan dari serangan langsung dan ancaman eksternal dan VPN melindungi data saat berkomunikasi melalui jaringan publik.
2. Dengan menggunakan VPN dan *firewall*, privasi akan lebih kuat. Dan VPN membantu menyembunyikan alamat IP serta melindungi identitas serta lokasi fisik. Dan *firewall* memberika kontrol lebih lanjut atas lalu linta yang masuk dan keluar, memastikan bahwa data yang sensitif tidak ter-ekspos.
3. Dengan menggunakan VPN dan *firewall*, perlindungan dari ancaman dari berbagai jenis *firewall* jauh lebih baik. Dengan *firewall* dapat mencegah ancaman langsung yang mungkin merusak atau mengancam jaringan.
4. Dengan menggunakan VPN dan *firewall* dapat melihat lalu lintas VPN yang masuk dan keluar, serta memonitor aktivitas jaringan melalui *firewall*.
5. Dengan menggunakan VPN dan *firewall* dapat menangani koneksi VPN yang lebih tepat karena *firewall* dapat dikonfigurasi untuk mengizinkan koneksi VPN melalui aturan yang sesuai.
6. Dengan menggunakan VPN dan *firewall* dapat memiliki kebebasan berbicara dan berpendapat.
7. Dengan menggunakan VPN dan *firewall* saat terhubung ke jaringan WiFi publik, VPN dan *firewall* bekerjasama untuk melindungi data dari ancaman keamanan yang mungkin muncul di lingkungan jaringan publik.