1 PENDAHULUAN

1.1 Latar Belakang

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) merupakan asosiasi yang bertujuan untuk mengatur jasa tarif internet di Indonesia. APJII dibentuk pada tanggal 15 Mei 1996 dan telah mengalami banyak perubahan pemimpin. Pemilihan pemimpin APJII diadakan setiap tiga tahun sekali. Saat ini APJII dipimpin oleh Jamalul Izza (Masa kerja: Sejak tahun 2015 sampai dengan 2018). APJII memiliki banyak sekali *device* yang digunakan untuk menyambungkan antara satu ISP dengan ISP yang lainnya. Oleh sebab itu keamanan jaringan sangatlah dibutuhkan untuk melindungi tiap-tiap *device* dari segala macam kemungkinan yang akan terjadi ke depannya (APJII 2014).

Pada *data center* terdapat banyak sekali *router* yang aktif akan tetapi ada beberapa *router* yang tidak memiliki keamanan jaringan *bloking port.* Fungsi dari mem-*block port* aktif agar keamanan *router* saat transmisi dalam keadaan yang aman. APJII hanya membutuhkan *port* HTTP dan HTTPS dikarenakan semakin banyak *port* yang aktif maka semakin lemah pertahanan *router* dan semakin tinggi kesempatan peretas untuk mengakses kedalam *port* yang aktif di *router*. Alasan mengapa APJII hanya membuka akses HTTP, HTTPS dan menutup seluruh *port* adalah untuk menjaga keamanan dari *router* dan tidak membutuhkan *port* lainnya saat melakukan transmisi.

Alasan untuk pengembang jaringan menggunakan *firewall* adalah untuk melindungi *network* dari *user* yang tidak berkepentingan. *Firewall* merupakan solusi perangkat keras dan perangkat lunak yang akan mememberikan keamanan jaringan dengan *policies. Firewall* diibaratkan sebagai kunci pada sebuah bangunan. Apabila kunci tersebut tidak cocok dengan lubang kuncinya maka pintu tidak akan bisa terbuka. Namun, apabila kunci dan lubangnya cocok maka pintu akan terbuka (Andy 2000).

Salah satu solusi yang dapat diterapkan pada masalah tersebut adalah dengan perancangan *blocking port* untuk melindungi suatu jaringan dari para pengguna *network* yang tidak bertanggung jawab. Sehingga *user* akan merasa lebih aman saat menggunakan internet.

1.2 Tujuan

Adapun tujuan dari keamanan jaringan dan *virtual private network* (VPN) yaitu:

1. Mematikan *port* pada router selain *port* HTTP dan HTTPS pada *router.*
2. Melindungi *device* dari serangan peretas.
3. Membuat sebuah jaringan VPN yang hanya dapat diakses oleh *user* tertentu.

1.3 Manfaat

Adapun manfaat dari keamanan jaringan dan *virtual private network* (VPN), tu:

Mencegah *console router* oleh pihak luar.
Membuat kebijakan pada *router*.
Melindungi *device* saat karyawan mengakses internet.
Melindungi jaringan internal dari serangan peretas.
Menjaga keamanan *router* VyOS APJII.
Membuat kebijakan *route* pada akses jaringan internet dan intranet.

1.4 Ruang Lingkup

Ruang lingkup dalam Keamanan Jaringan dan *Virtual Private Network* di osiasi Penyelenggara Internet Indonesia adalah sebagai berikut:

Implimentasi dilakukan pada fitur keamanan *firewall rules.*
Implementasi dilakukan menggunakan *software* PuTTY
Hasil *blocking port* dapat diuji menggunakan CMD.
Jaringan komputer yang ada di APJII diterapkan menggunakan simulator jaringan.

2 METODE KERJA

2.1 Lokasi dan Waktu PKL

Pelaksanaan kegiatan Praktik Kerja Lapangan (PKL) dilakukan di Kantor osiasi Penyelenggara Jasa Internet Indonesia yang beralamat di Gedung Cyber 1 Jl Kuningan Barat No. 8 Kuningan Barat – Mampang Prapatan Jakarta. PKL aksanakan selama 45 hari masa kerja terhitung mulai tanggal 1 Februari 2018 ngga 6 April 2018. Waktu dan pelaksanaan PKL adalah pada hari Senin hingga nat dan jam bekerjanya tergantung kepada *shift* apa yang didapat pada satu nggu tersebut. Terdapat 3 *shift* atau yang biasa disebut jam kerja yaitu:

Shift 1 pada pukul 07.00 sampai dengan 16.00 WIB.
Shift 2 pada pukul 14.00 sampai dengan 23.00 WIB.
Shift 3 pada pukul 23.00 sampai dengan 08.00 WIB.

2.2 Metode Bidang Kajian

Metode yang digunakan dalam mengimplementasi Sistem Keamanan ingan dan *Virtual Private Network* (VPN) menggunakan VyOS terdiri atas