BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi jaringan komputer menunjukkan peningkatan yang sangat pesat seiring dengan semakin meningkatnya kebutuhan akan terhubungnya lokasi–lokasi yang terpisah secara jarak namun ingin tetap berbagi informasi dan menikmati layanan yang sama. Kebutuhan akan terhubungnya antar lokasi ini dirasakan benar pada level perusahaan. Sebuah perusahaan yang memiliki sejumlah unit usaha tentunya ingin agar setiap unit usahanya tersebut terhubung satu sama lain agar dapat bertukar informasi dan memiliki akses yang sama ke internet. Oleh karena itu, dibutuhkan suatu sistem jaringan komputer untuk menghubungkan kantor pusat dengan kantor cabang yang letaknya berjauhan agar dapat saling bertukar informasi secara *internal*. Dalam melakukan komunikasi dan pengolahan informasi antara kantor pusat dengan kantor cabang yang tersebar di lokasi yang terpisah, dibutuhkan suatu jaringan yang terkoneksi secara sistematis dengan internet, sehingga jaringan yang berbeda tadi terhubung dalam satu sistem jaringan komputer secara luas dan aman. Sistem jaringan yang terpasang nantinya akan menjadi kerangka awal untuk pembangunan ataupun pengembangan jaringan ke depannya sehingga akan lebih mudah untuk perancangan pada pengembangan selanjutnya. Hal ini juga dapat memberi petunjuk bagi para pengguna jaringan agar tidak salah dalam menggunakan layanan yang tersedia pada sebuah jaringan. Pembangunan jaringan ini juga terpacu berdasarkan pada mekanisme pembangunan jaringan secara virtual dan dalam hal ini khusus tentang *Virtual Private Network* (VPN). VPN banyak digunakan untuk meningkatkan keamanan data-data komunikasi yang bersifat rahasia (Hidayatulloh dkk, 2013).

Dengan dikembangkannya jaringan *Virtual Private Network* (VPN) yang teraplikasi pada jaringan *Wide Area Network* (WAN) proses pengaksesan data dapat dilakukan dimana saja selama terkoneksi dengan *internet*, sehingga memungkinkan komunikasi data jarak jauh yang relevan. Karena memiliki manfaat sangat yang baik, kemudian dikembangkan berbagai jenis VPN seperti PPP, Winsock, IPsec dan OpenVPN (Hidayatulloh, 2013).

Dengan dikembangkannya keamanan jaringan juga dapat diartikan sebagai proses untuk mengidentifikasi dan mencegah adanya *user* yang tidak mempunyai izin (penyusup) dari sistem jaringan komputer. Tujuan dibangunnya suatu sistem keamanan jaringan adalah untuk menanggulangi dan mencegah ancaman dari jaringan luar yang dapat berupa ancaman logik atau fisik. Ancaman logik adalah sebuah ancaman yang berupa pengambilan data secara tidak sah atau pencurian data oleh penyusup dengan cara mencari celah yang terbuka pada sistem keamanan jaringan, sedangkan ancaman fisik yaitu sebuah ancaman yang bertujuan untuk merusak sistem jaringan dari sisi *hardware* sebuah komputer (Candra, 2019).

Pfsense adalah *software* atau distribusi perangkat lunak komputer berdasarkan FreeBSD. Pfsense dapat diinstalasi pada komputer fisik atau mesin virtual untuk membuat *firewall* khusus atau *router* untuk jaringan. Fitur-fitur tersebut disediakan Pfsense diantaranya kemudahan penggunaan dan biaya yang relatif kecil karena sifatnya yang *open source*. Dapat dikonfigurasi dan *upgrade* melalui anatar muka berbasis *web*, dan tidak memerlukan pengetahuan tentang sistem FreeBSD yang juga merupakan kelebihan penggunaan Pfsense. Pfsense umumnya digunakan sebagai perimeter, *router*, titik akses nirkabel, DHCP, DNS dan sebagai VPN *end point*. Pfsense juga mendukung instalasi paket pihak ke-3 seperti *Snort* atau *Squid* melalui *Package Manager*-nya.

Router adalah sebuah alat jaringan komputer yang digunakan untuk menghubungkan 2 buah *subnet* yang berbeda. Untuk melakukan konfigurasi terhadap sebuah *router*, biasanya masih dilakukan dengan menggunakan *Command Line Interface (CLI)* atau *console.* Hal inilah yang dirasa cukup sulit untuk melakukan konfigurasi terhadap sebuah *router*, baik itu berupa konfigurasi *bandwidth* atau hanya sekedar serta *filtering* beberapa situs yang dilarang oleh Menkominfo yang disinyalir berbau pornografi, perjudian, SARA, terorisme dan lain sebagainya (Irawan, 2014).

Pandangan Islam pada OpenVPN adalah bentuk atau cara individu dalam melakukan keamanan atau privasi untuk melindungi dari hal-hal buruk dan mengharapkan ridho dan pahala dari Allah SWT.

Wahai orang-orang yang beriman kepada Allah dan RasulNya serta melaksanakan syariatNya, janganlah kalian memasuki rumah-rumah yang bukan milik kalian, hingga kalian meminta izin kepada penghuninya untuk masuk dan mengucapkan salam pada

mereka. Bunyi ucapan salam adalah, “Assalamu’alaikum, apakah saya boleh masuk?” permintaan izin masuk itu lebih baik bagi kalian, supaya kalian menjadi ingat perintah-perintah Allah dengan perbuatan kalian meminta izin, sehingga kalian taat kepadanya.

Jika tidak meminta izin terdapat banyak mafsadat, di antaranya dapat melihat aurat yang ada dalam rumah, karena rumah merupakan aurat bagi seseorang seperti halnya pakaian yang menjadi penutup bagi auratnya. Di samping itu, tanpa meminta izin dapat menimbulkan keraguan, tuduhan buruk terhadapnya sebagai pencuri misalnya, dsb. Hal itu, karena masuk secara diam-diam menunjukkan keburukan. Allah sebut meminta izin dengan isti’zan, karena dengan meminta izin, maka akan membuat nyaman penghuni rumah setelah merasakan ketidaknyamanan. Allah berfirman dalam (QS. An-Nuur(24) : 27); sebagaimana dijelaskan dalam fiman Allah SWT:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ لَا تَدۡخُلُواْ بُيُوتًا غَيۡرَ بُيُوتِكُمۡ حَتَّىٰ تَسۡتَأۡنِسُواْ وَتُسَلِّمُواْ عَلَىٰٓ أَهۡلِهَاۚ ذَٰلِكُمۡ خَيۡرٞ لَّكُمۡ لَعَلَّكُمۡ تَذَكَّرُونَ ٢٧

Artinya :

“Hai orang-orang yang beriman, janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu (selalu) ingat.” (QS. An-Nuur(24) : 27)

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dijelaskan di atas, identifikasi masalah yang ada dalam penelitian ini adalah sebagai berikut :

1. Menganalisis performa dari OpenVPN dengan protocol TCP pada Pfsense.
2. Menganalisis kinerja dari OpenVPN pada Pfsense untuk akses *remote*.
3. Menganalisis kinerja dari OpenVPN pada Pfsense menurut Islam.

1.3 Rumusan Masalah

Dari identifikasi masalah yang telah dipilih maka dapat dirumuskan permasalahan penelitian ini yaitu :

1. Bagaimana performa dari OpenVPN dengan protocol TCP pada Pfsense ?
2. Bagaimana kinerja dari OpenVPN pada Pfsense untuk akses *remote* ?
3. Bagaimana kinerja dari OpenVPN pada penggunaan Pfsense menurut Islam ?

1.4 Batasan Masalah

Agar penelitian ini lebih terarah, terfokus, dan tidak meluas, maka batasan masalahnya adalah:

1. Menganalisis performa dari OpenVPN dengan protocol TCP pada Pfsense.
2. Komunikasi jaringan yang sudah diset IP untuk terkoneksi ke OpenVPN dalam jaringan tersebut.
3. Lingkungan jaringan yang digunakan dalam simulasi ini adalah pada satu WAN.
4. Implementasi menggunakan Pfsense.
5. Parameter kinerja yang diteliti adalah *bandwidth, packet loss,* dan *delay*.

1.5 Tujuan

Penelitian ini bertujuan untuk :

1. Menganalisis performa dari OpenVPN dengan protocol TCP pada Pfsense.
2. Untuk mengetahui kinerja OpenVPN pada Pfsense untuk akses *remote*.
3. Memahami pandangan Islam terhadap penggunaan OpenVPN pada Pfsense untuk akses *remote*.

1.6 Manfaat

Adapun manfaat penelitian ini adalah sebagai berikut:

1. Untuk mengetahui dan memberikan informasi tentang performa OpenVPN dengan protocol TCP pada Pfsense.
2. Untuk mengetahui dan memberikan informasi tentang performa dari kinerja penggunaan OpenVPN pada Pfsense untuk akses *remote*.
3. Memahami pandangan Islam terhadap penggunaan OpenVPN pada Pfsense untuk akses *remote*.