BAB 1

PENDAHULUAN

1.1 Latar Belakang

Pada zama modern ini kemudahan dan ke akuratan dalam memperoleh informasi sangat diperlukan oleh manusia agar dalam melakukan pekerjaan lebih efisien peyampaian sebuah informasi dapat diperoleh menggunakan internet tidak terlepas dari komputerisasi dalam pengelolaan data yang dilakukan sebagian besarnya menggunakan komputer .

Terhubungnya antar lokasi dirasakan 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.

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 computer. (NOVIAN CANDRA, 2018)

OpenVPN menggunakan protocol komunikasi TCP (Transmission Control Protocol) dan UDP (User Datagram Protocol). Sebagian besar penyedia VPN memungkinkan Anda memilih di antara ke 2 protokol tersebut. Tetapi, hanya sedikit yang menjelaskan perbedaan OpenVPN TCP vs UDP dan kelebihan yang dimiliki masing-masing protocol tersebut . Fungsi kedua protocol tersebut

adalah untuk membagi data menjadi paket kecil yang dapat dikirim TCP atau UDP dapat memiliki dampak yang sangat nyata pada seberapa baik penggunaan ke 2 protokol tersebut. (Tremblay, n.d.)

Protokol TCP memungkinkan menangani masalah.

- **Data Duplication** – Pengiriman Data memungkinkan bagi penerima untuk mendapatkan paket dua kali , bahkan jika dikirim sekali , nomor urut memungkinkan penerima utuk mengabaikan data apapun yang sudah di proses.
- **Data Loss -** Ketika penerima tidak mendapatkan paket, ia tidak bisa mengakui kedatangannya ke pengirim. Beberapa saat setelah meneruskan data, jika pengirim tidak melihat pemberitahuan, ia hanya akan mengirim kembali informasi yang sama. Dengan cara ini setiap paket dijamin (pada akhirnya) mencapai tujuan.
- **Data Seqencing** – urutan paket data juga sering rusak . memiliki urutan yang terpasang masing-masing memungkinkan penerima untuk merakit kembali ke urutan yang benar.

Kelemahan Protokol TCP.

- **High Overhead** – Mekanisme protocol TCP mengorbankan kecepatan . untuk setiap paket yang keluar , pengirim harus melihat pemberitahuan dari penerima sebelum dapat meneruskan lebih banyak data.
- **Lag** – Menggunakan Koneksi Internet tidak Stabil , protocol TCP akan mengirim ulang paket data yang terjatuh menciptakan penundaan untuk sebagian besar data statis yang dapat diterima (mengunduh file) Tetapi untuk streming video dan audio jauh lebih baik untuk data yang hilang .

Protokol UDP memungkinkan menangani masalah .

- **Dealing with a slow connection** – dalam beberapa keadaan seperti protokol TCP yang Overhead dapat menghasilkan kinerja koneksi yang sangat rendah . menggunakan Protokol UDP dapat mempercepat dengan

mengurangi pemrosesan tambahan dan penundaan koreksi kesalahan yang dating dengan yang terakhir

- **Transmitting Time-Sensitive Data** - Jika Anda mengirim atau menerima lalu lintas VoIP atau video langsung melalui koneksi VPN Anda, paket yang dijatuhkan tidak masalah seperti halnya hanya sekedar mendapatkan data. Hal yang sama berlaku untuk streaming video dan audio.

Kelemahan Protokol UDP

Meskipun UDP menawarkan keunggulan kecepatan yang signifikan dibandingkan kekurangan UDP adalah .

- **Less Reliability** - Mengirim informasi menggunakan protokol UDP dengan risiko data akan hilang atau rusak ketika kondisi jaringan tidak ideal. Hal itu dapat mengakibatkan unduhan yang gagal atau koneksi terputus saat kesalahan menumpuk hingga tidak dapat dikelola.

- **Compatibility Issues** - Dalam lingkungan jaringan tertentu, lalu lintas masuk dan keluar terbatas untuk menjaga keamanan jaringan. UDP biasanya lebih terbatas daripada TCP. Menggunakannya dalam keadaan seperti itu dapat menyebabkan koneksi OpenVPN gagal.

Pengertian Pfsense (id.wikipedia.org, n.d.) **& (** *Keyword :, Pfsense)*

Pfsense adalah open source firewall / router distribusi perangkat lunak komputer berdasarkan FreeBSD. Hal ini diinstal pada komputer fisik atau mesin virtual untuk membuat firewall khusus / router untuk jaringan dan telah dicatat untuk kehandalan dan menawarkan berbagai fitur. Hal ini dapat dikonfigurasi dan ditingkatkan melalui web, dan tidak memerlukan pengetahuan tentang sistem FreeBSD yang mendasari untuk mengelola. Pfsense umumnya digunakan sebagai firewall perimeter, router, titik akses nirkabel , DHCP Server merupakan singkatan dari Dinamyc Host Configuration Protocol. DHCP merupakan sebuah layanan yang secara otomatis memberikan nomor IP kepada komputer yang memintanya. Komputer yang memberikan nomor IP inilah yang disebut sebagai DHCP server, DNS Server (Domain Name Server) adalah server yang digunakan untuk mengetahui IP Address suatu *host* lewat *host name*-nya, dan sebagai VPN endpoint

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 Open VPN menggunakan Protokol TCP pada Pfsens.
2. Menganalisis Performa Open VPN menggunakan Protokol UDP pada Pfsens.
3. Menganalisis kinerja Ke 2 Protokol Open VPN pada Pfsens untuk Remote akses.

1.3 Rumusan Masalah

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

1. Bagaimana Performa Open VPN menggunakan Protokol TCP pada Pfsens.
2. Bagaimana Performa Open VPN menggunakan Protokol UDP pada Pfsens.
3. Bagaimana kinerja Ke 2 Protokol Open VPN pada Pfsens untuk Remote akses.

1.4 Batasan Masalah

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

1. Menganalisis performa dari Open VPN dengan protocol TCP pada Pfsense.
2. Menganalisis performa dari Open VPN dengan protocol UDp pada Pfsense
3. Komunikasi jaringan yang sudah di setting ip untuk terkoneksi ke Open VPN dalam jaringan tersebut.
4. Lingkungan jaringan yang digunakan dalam simulasi ini adalah pada satu WAN.
5. Implementasi menggunakan Pfsense.
6. Parameter yang digunakan adalah Bandwitdh , packet loss, dan delay.

1.5 Tujuan dan Manfaat

1.5.1 Tujuan

Penelitian ini bertujuan untuk :

1. Mengetahui Hasil Implementasi OpenVPN pada Router Pfsense
2. Menganalisis performa dari Open VPN dengan protocol TCP pada Pfsense.
3. Menganalisis performa dari Open VPN dengan protocol UDP pada Pfsense.
4. Untuk mengetahui kinerja Open VPN pada Pfsense untuk remote akses.

1.5.2 Manfaat

Adapun manfaat penelitian ini adalah sebagai berikut:

1. Untuk mengetahui dan memberikan informasi tentang performa Open VPN dengan protocol TCP pada Pfsense.
2. Untuk mengetahui dan memberikan informasi tentang performa Open VPN dengan protocol UDP pada Pfsense.
3. Untuk mengetahui dan memberikan informasi tentang performa dari kinerja penggunaan Open VPN pada Pfsense untuk remote akses.