Indonesian Journal of Computer Science
ISSN 2302-4364 (*print*) dan 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam, No. 1, Padang, Indonesia, Telp. (0751) 7056199, 7058325
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

ANALISA PERBANDINGAN *QUALITY OF SERVICE* PROTOKOL VPN ANTARA PROTOKOL SSTP DAN OPEN VPN BERBASIS ROUTER MIKROTIK

Surono[1], Galet Guntoro S[2]
surono@usm.ac.id, galet@usm.ac.id
Universitas Semarang

Informasi Artikel

Diterima : 04 Mar 2022
Direview : 15 Mar 2022
Disetujui : 30 Apr 2022

Kata Kunci

VPN, Terenkripsi, QOS, *internet*, *routing*, NAT, VLAN

Abstrak

Internet sendiri merupakan jaringan publik yang bisa menghubungkan siapa saja kedalam jaringan yang sangat besar, dan tentunya terdapat ancaman – ancaman pencurian data didalamnya, VPN adalah teknologi komunikasi yang memungkinkan seorang pegawai yang berada di dalam kantor terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dalam jaringan lokal. Keuntungan VPN adalah data yang dikirimkan melalui VPN terenkripsi sehingga cukup aman dan rahasianya tetap terjaga meskipun melalui jaringan internet akan dilakukan analisa perbandingan performa VPN antar protokol SSTP (Secure Socket Tunneling Protocol) dengan protokol Open VPN untuk mengetahui performa *Quality Of Service* (Qos) dari kedua protokol tersebut di diperlukan suatu studi untuk menentukan penggunaan metode sehingga menghasilkan QOS (*Quality of Service*) yang optimal.

Keywords

VPN, Encrypted, QOS, internet, routing, NAT, VLAN.

Abstrak

The internet itself is a public network that can connect anyone into a very large network, and of course there are threats of data theft in it, VPN is a communication technology that allows an employee in the office to connect to a public network and use it to join the local network. . The advantage of a VPN is that the data sent via a VPN is encrypted so it is quite safe and the secret is maintained even though it is through the internet network, a comparison analysis of VPN performance between the SSTP (Secure Socket Tunneling Protocol) protocol and the Open VPN protocol will be carried out to determine the Quality Of Service (Qos) performance of both For this protocol, a study is needed to determine the use of the method so as to produce an optimal QOS (Quality of Service).

A. Pendahuluan

Pada era saat ini kita sudah masuk era digital dimana semua serba online untuk itu jaringan internet merupakan teknologi yang sangat di butuhkan. *Internet* saat ini menjadi suatu kebutuhan penting manusia dalam berbagai bidang terutama pada masa Pandemi Virus *Covid-19* saat ini. Teknologi internet sangat berpengaruh terhadap dunia industry atau dunia kerja secara global. Dengan memanfaatkan penggunaan jaringan internet, dapat membantu dalam mengatasi batasan jarak dan waktu. Kini seseorang dapat dengan mudah mengambil data atau mengolah data yang tersimpan di dalam jaringan lain, contohnya jaringan di dalam sebuah instansi seperti perusahaan baik negeri atau swasta juga dalam sebuah instansi yang bergerak dalam dunia pendidikan seperti sekolah dan perguruan tinggi, dari mana saja dan kapan saja. Hal tersebut dapat dilakukan jika jaringan tersebut terkoneksi dengan internet.

Karena internet sendiri merupakan jaringan publik yang bisa menghubungkan siapa saja kedalam jaringan yang sangat besar, dan tentunya terdapat ancaman – ancaman pencurian data didalamnya. Untuk mengatasi masalah keamanan setiap komunikasi data yang dilakukan melalui jaringan publik (*public network*) maka diperlukan suatu mekanisme yang memungkinkan koneksi antar workstation berjalan secara *private*, sehingga hanya workstation yang memiliki akses yang dapat saling terhubung, dengan cara memanfaatkan virtual private network atau VPN. Teknologi VPN, yaitu Teknik yang dapat menghubungkan beberapa jaringan local melalui jaringan publik (internet) dengan teknik VPN komunikasi seakan-akan kedua jaringan tersebut berada di dalam satu jaringan intranet yang besar [1].

Teknologi *private network* (jaringan pribadi) adalah suatu komunikasi dalam jaringan sendiri yang terpisah dari jaringan umum [2]. VPN adalah teknologi komunikasi yang memungkinkan seorang pegawai yang berada di dalam kantor terkoneksi ke jaringan publik dan menggunakannya untuk bergabung dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama ketika pegawai berada di kantor [3]. Keuntungan VPN adalah data yang dikirimkan melalui VPN terenkripsi [1] sehingga cukup aman dan rahasianya tetap terjaga meskipun melalui jaringan internet. VPN memiliki beberapa protokol yang dapat digunakan, diantaranya *Point to Point Tunneling Protocol* (PPTP) dan Layer 2 *Tunneling Protocol* (L2TP). Teknologi jaringan PPTP (*Point to Point Tunneling Protocol*) merupakan pengembangan dari *remote access point to point Protocol* yang dikeluarkan oleh internet *Engineering Task Force* (IETF).

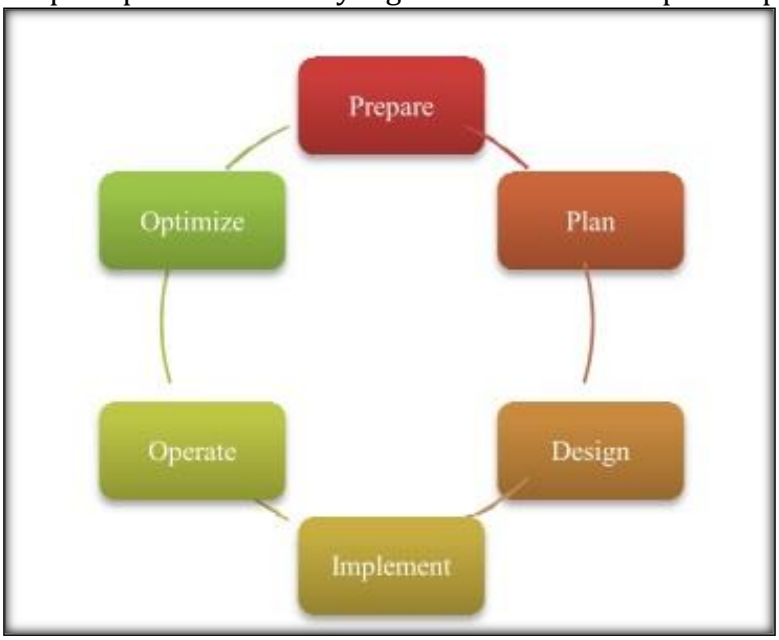
PPTP merupakan Protokol jaringan yang merubah paket PPP menjadi IP datagram agar dapat ditransmisi melalui internet. PPTP juga dapat digunakan pada jaringan private LAN to LAN. Sedangkan L2TP (Layer 2 *Tunneling Protocol*) adalah sebuah tunneling Protocol yang memadukan dan mengkombinasikan dua buah tunneling Protokol yaitu L2F (Layer 2 Forwarding) milik cisco sistem dengan PPTP *(Point to Point Tunneling Protocol*) milik Microsoft .

Pada Penelitian ini akan dilakukan analisa perbandingan performa VPN antar protokol SSTP **(Secure Socket Tunneling Protocol)** dengan protokol Open VPN untuk mengetahui performa *Quality Of Service* (Qos) dari kedua protokol tersebut di diperlukan suatu studi untuk menentukan penggunaan metode sehingga menghasilkan QOS (*Quality of Service*) yang optimal, dengan pengujian performa yaitu *Delay, trougput, packet loss, roundtrip* dan winSCP transfer, sedangkan untuk

keamanan adalah pengujian *denial of service* dan *sniffing* [5]. Pengujian perlu dilakukan untuk mengetahui protokol manakah yang menghasilkan performa terbaik pada jaringan VPN.

B. Metode Penelitian

Dari data yang terkumpul kemudian dilakukan pengembangan suatu sistem menggunakan *Prepare, Plan, Design, Implement, Operate, and Optimize* (PPDIOO) *Network Lifecycle* seperti pada Gambar 3 yang terdiri dari beberapa tahap, yaitu:



Gambar 1. Metode PPDIOO

1. Prepare

Dalam model pengembangan sistem PPDIOO fase pertama dimulai dari fase prepare, melakukan proses penelitian dan menganalisa terhadap masalah yang ada, serta bagaimana cara administrator jaringan maupun program serta Sebagian karyawan yang di beri akses ke data base dapat mengakses server server secara aman dan lokal meskipun memakai jaringan di luar kantor dalam hal ini di rumah.

2. *Planning*

Untuk tahap selanjutnya adalah tahap *plan*, merencanakan kebutuhan baik *hardware* maupun *software* yang akan digunakan untuk konfigurasi SSTP dan OpenVpn yang ada di Universitas Semarang serta konfigurasi yang akan dilakukan pada perangkat router.

3. *Implement*

Tahap selanjutnya adalah tahap implementasi. Dalam tahap ini menerapkan semua yang telah direncanakan, mencakup instalasi serta konfigurasi terhadap rancangan topologi, dan konfigurasi yang dilakukan pada masing-masing perangkat. Pada tahap konfigurasi *Router* .

4. *Operate*

Dalam tahap ini melakukan pemantauan terhadap jaringan vpn yang menggunakan metode SSTP selama paling tidak 1 (satu bulan) dan melakukan pemantauan terhadap jaringan yang menggunakan metode OpenVpn selama paling tidak 1 (satu bulan). Data dicatat sesuai dengan parameter yang telah ditentukan dengan melakukan pengujian ke vpn server server yang di ada lokal atau di dlaam area kantor dari masing – masing *user* yang di beri akses tersebut dapat melihat hasilnya, sehingga dari hasil tersebut dapat dibandingkan perbedaan antara kedua metode protokol vpn tersebut

5. *Optimize*

Tahap OptimezeDari hasil uji , dilakukan konfigurasi untuk metode yang hasil ujinya lebih baik sehingga dapat menghasilkan QOS jaringan *internet* yang optimal. Perawatan, pemeliharaan, dan pengelolaan terhadap penggunaan kedua metode VPN tersebut .

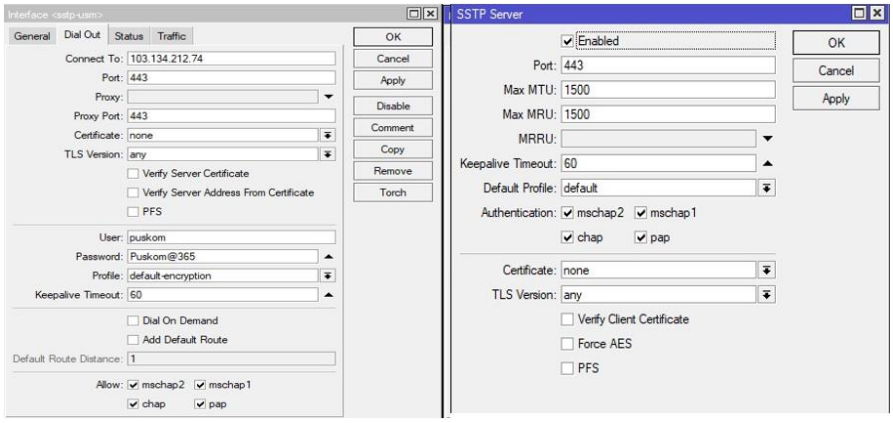
C. Hasil dan Pembahasan

1. Implementasi

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan local . Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik. Penggunaan Virtual Private Network merupakan salah satu untuk membangun jalur komunikasi yang aman client dan remote server melalui jaringan public.

2. Konfigurasi VPN Protokol SSTP di USM

Tahap implementasi VPN SSTP meliputi pembangunan SSTP server dan client. Pada kedua sisi, dilakukan manajerial jaringan agar router server dan router client dapat berkomunikasi melalui tunnel VPN, Dengan Mode GUI server dan CLI sebagai berikut :



Dengan mode CLI :

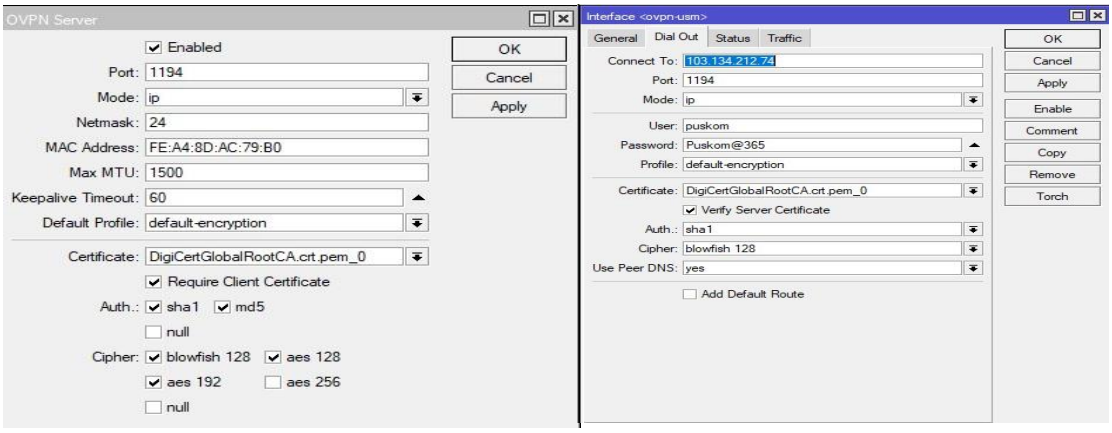
```
/interface ethernet
set [ find default-name=ether1 ] speed=100Mbps
set [ find default-name=ether2 ] speed=100Mbps
```

```
set [ find default-name=ether3 ] speed=100Mbps
set [ find default-name=ether4 ] speed=100Mbps
set [ find default-name=ether5 ] speed=100Mbps
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=dhcp_pool0 ranges=192.168.199.2-192.168.199.254
/ip dhcp-server
add address-pool=dhcp_pool0 disabled=no interface=ether5
name=dhcp1
/ppp profile
add local-address=192.168.199.1 name=profile1 remote-
address=dhcp_pool0
set *FFFFFFFE idle-timeout=1h session-timeout=1h
/snmp community
set [ find default=yes ] addresses=0.0.0.0/0
/user group
set full
policy=local,telnet,ssh,ftp,reboot,read,write,policy,test,winbox,passw
ord,web,sniff,sensitive,api,romon,dude,tikapp
/ip neighbor discovery-settings
set discover-interface-list=!dynamic
/interface l2tp-server server
set enabled=yes ipsec-secret=usmjaya1** keepalive-timeout=6 use-
ipsec=yes
/interface ovpn-server server
set certificate=DigiCertGlobalRootCA.crt.pem_0 enabled=yes
/interface sstp-server server
set enabled=yes
/ip address
add address=103.134.214.78/30 disabled=yes interface=ether1
network=103.134.214.76
add address=103.134.212.74/29 interface=ether1
network=103.134.212.72
add address=192.168.199.1/24 interface=ether5
network=192.168.199.0
add address=103.134.212.75/29 interface=ether1
network=103.134.212.72
/ip dhcp-server network
add address=192.168.199.0/24 gateway=192.168.199.1
/ip dns
set allow-remote-requests=yes servers=103.134.215.132
/ip firewall nat
add action=dst-nat chain=dstnat disabled=yes dst-port=53
protocol=udp to-addresses=103.30.181.1 to-ports=53
add action=accept chain=dstnat disabled=yes dst-
address=112.78.40.99 dst-port=443,80 protocol=tcp
```

```
add action=accept chain=dstnat disabled=yes dst-address=103.30.180.101 dst-port=443,80 protocol=tcp
add action=src-nat chain=srcnat dst-address=172.16.99.4 to-addresses=172.16.99.1
add action=dst-nat chain=dstnat dst-address=103.134.212.75 dst-port=8298 protocol=tcp to-addresses=172.16.99.4 to-ports=161
add action=dst-nat chain=dstnat dst-address=103.134.212.75 dst-port=8298 protocol=udp to-addresses=172.16.99.4 to-ports=161
add action=dst-nat chain=dstnat dst-address=103.134.212.75 protocol=icmp to-addresses=172.16.99.4
add action=src-nat chain=srcnat to-addresses=103.134.212.74
/ip route
add distance=1 gateway=103.134.212.73
/ip service
set telnet port=9923
set ftp disabled=yes
set www port=9980
set ssh disabled=yes
set api disabled=yes
set winbox port=1810
set api-ssl disabled=yes
/ppp secret
add local-address=172.16.99.1 name=bowo password="Semarang\?\?08" profile=default-encryption remote-address=172.16.99.2
add local-address=172.16.99.1 name=surono password=Puskom@365 profile=default-encryption remote-address=172.16.99.3
add local-address=172.16.99.1 name=alang password=//alang** profile=default-encryption remote-address=172.16.99.4
add name=puskom password=Puskom@365 profile=profile1
/system clock
set time-zone-name=Asia/Jakarta
/system identity
set name=ro-vpn-usm
[u5m@ro-vpn-usm] >
```

3. Implementasi OpenVPN

OpenVPN adalah aplikasi open source SSL VPN yang mampu memberikan banyak konfigurasi terhadap VPN seperti remote access, site-to-site VPN, kemanan Wi-Fi dan remote access berskala enterprise. OpenVPN bekerja dengan cara membuat koneksi point-to-point tunnel yang telah dienkripsi menggunakan OpenSSL. OpenVPN menggunakan private keys, certificate, atau username/password untuk melakukan autentikasi dalam membangun koneksi. Berikut konfiguras dengan metode GUI dan CLI sisi server dan client :



interface ovpn-server server set
certificate=DigiCertGlobalRootCA.crt.pem_0
cipher=blowfish128,aes128,aes192 default-profile=default-encryption enabled=yes require-client-certificate=yes
/interface sstp-server server
set enabled=yes
/ip address
add address=103.134.214.78/30 disabled=yes interface=ether1 network=103.134.214.76
add address=103.134.212.74/29 interface=ether1 network=103.134.212.72
add address=192.168.199.1/24 interface=ether5 network=192.168.199.0
add address=103.134.212.75/29 interface=ether1 network=103.134.212.72
/ip dhcp-server network
add address=192.168.199.0/24 gateway=192.168.199.1
/ip dns
set allow-remote-requests=yes servers=103.134.215.132
/ip firewall nat
add action=dst-nat chain=dstnat disabled=yes dst-port=53 protocol=udp to-addresses=103.30.181.1 to-ports=53
add action=accept chain=dstnat disabled=yes dst-address=112.78.40.99 dst-port=443,80 protocol=tcp
add action=accept chain=dstnat disabled=yes dst-address=103.30.180.101 dst-port=443,80 protocol=tcp
add action=src-nat chain=srcnat dst-address=172.16.99.4 to-addresses=172.16.99.1
add action=dst-nat chain=dstnat dst-address=103.134.212.75 dst-port=8298 protocol=tcp to-addresses=172.16.99.4 to-ports=161
add action=dst-nat chain=dstnat dst-address=103.134.212.75 dst-port=8298 protocol=udp to-addresses=172.16.99.4 to-ports=161
add action=dst-nat chain=dstnat dst-address=103.134.212.75 protocol=icmp to-addresses=172.16.99.4

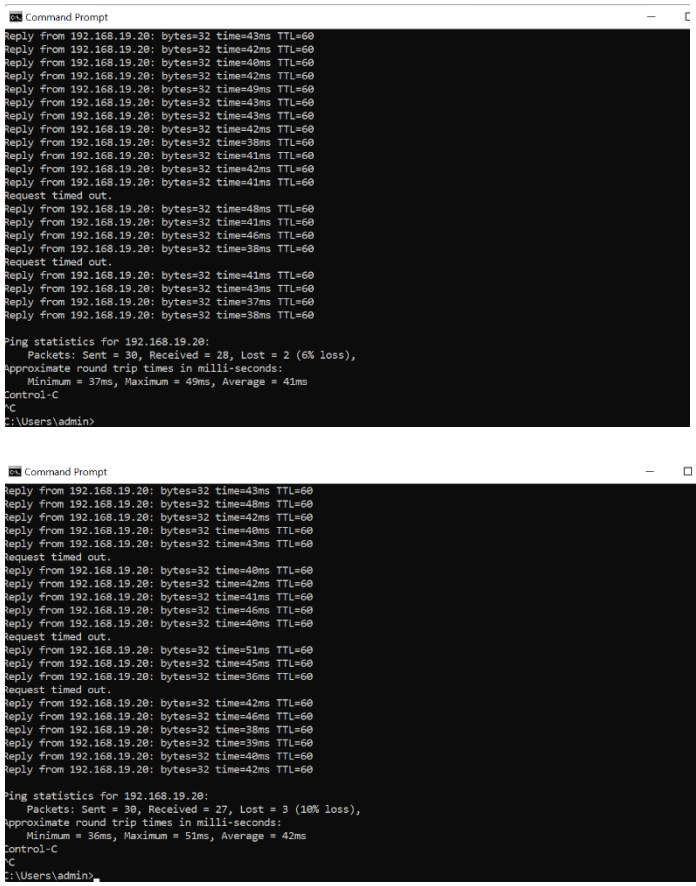
```
add action=src-nat chain=srcnat to-addresses=103.134.212.74
/ip route
add distance=1 gateway=103.134.212.73
/ip service
set telnet port=9923
set ftp disabled=yes
set www port=9980
set ssh disabled=yes
set api disabled=yes
set winbox port=1810
set api-ssl disabled=yes
/ppp secret
add local-address=172.16.99.1 name=bowo password="Semarang\?\?08" profile=default-encryption remote-address=172.16.99.2
add local-address=172.16.99.1 name=surono password=Puskom@365 profile=default-encryption remote-address=172.16.99.3
add local-address=172.16.99.1 name=alang password=//alang** profile=default-encryption remote-address=172.16.99.4
add name=puskom password=Puskom@365 profile=profile1
/system clock
set time-zone-name=Asia/Jakarta
/system identity
set name=ro-vpn-usm
[u5m@ro-vpn-usm]
```

4. Analisa dan Pengujian Parameter QoS

Nilai QoS (Quality of Service) dari kedua metode VPN dalam penelitian ini dapat di lakukan dengan software Wireshark untuk mengetahui metode VPN mana yang paling baik, untuk pengujian dalam metode ini antara lain *Packetloss, Rountrip, winscp transfer*, sedangkan untuk keamanan menggunkan *denial of service.*

a. Packet Loss

Packet tidak dapat menyimpan data dalam jumlah besar, mereka dapat memuat 65.535 byte (atau 0,065 megabyte) informasi di dalamnya. biasanya, paket internet hanya menyimpan 1.500 byte (0,0015 megabyte) data, server dan komputer mengirim lebh dari satu packet dalam berinteraksi sehingga *packetLoss* sangat mungkin terjadi, pada pengujian ini bertujuan untuk memantau rata-rata, minimum dan maksimum *packetloss* yang melalui tunnel VPN.



Untuk hasil yang di dapat dalam pengujian ini dapat di lihat pada tabel di bawah ini :

Tabel 1. Tabel Hasil Packet Loss

Jenis VPN	IP Sumber	IP Tujian	Packet Loss
Open Vpn	172.16.99.3	192.168.19.20	6%
SSTP	172.16.99.4	192.168.19.20	10%

b. Round Trip

Round Trip Delay Time atau biasa disebut dengan Round-Trip Time (RTT) adalah lama waktu yang dibutuhkan sebuah jaringan untuk mengirim sebuah paket data ketujuan tertentu ditambah dengan lama waktu yang dibutuhkan saat jaringan asal menerima informasi dari tempat tujuan yang dituju sebelumnya.Pengujian ini dilakukan bersamaan dengan packetloss.pada table 2 di bawah ini menunjukan hasil dari pengujian :

Tabel 2. Tabel Round Trip Delay

Jenis VPN	IP Sumber	IP Tujian		Min Latency	Max Latency	Rata-rata Latency
Open Vpn	172.16.99.3	192.168.19.20		37	49	41
SSTP	172.16.99.4	192.168.19.20		36	51	42

c. WinSCP Transfer

Kegunaan dari WinSCP ini adalah sebagai alat untuk transfer, atau lebih familiar kita kenal dengan sebutan upload dan download file melalui protokol ftp dan secure shell (SSH), Dengan WinSCP kita juga dapat melakukan editorial seperti mengedit isi file, merubah nama file menghapus file dan lain sebagainya

Berikut adalah hasil dari pengujian download dan upload file pada kedua VPN.

Tabel 3. Hasil Pengujian Download

Data Upload Jenis VPN	IP Sumber	IP Tujian	Time Span (s)	Average Rate (bit)	Packet Drop (%)
Open Vpn	172.16.99.3	192.168.19.20	67,880	1764k	0
SSTP	172.16.99.4	192.168.19.20	68,625	1691k	0

Tabel 4. Data Download

Jenis VPN	IP Sumber	IP Tujian	Time Span (s)	Average Rate (bit)	Packet Drop (%)
Open Vpn	172.16.99.3	192.168.19.20	34,551	3249k	0
SSTP	172.16.99.4	192.168.19.20	22,975	4844k	0

d. WinSCP Transfer

Kegunaan dari WinSCP ini adalah sebagai alat untuk transfer, atau lebih familiar kita kenal dengan sebutan upload dan download file melalui protokol ftp dan secure shell (SSH), Dengan WinSCP kita juga dapat melakukan editorial seperti mengedit isi file, merubah nama file menghapus file dan lain sebagainya

Berikut adalah hasil dari pengujian download dan upload file pada kedua VPN.

Tabel 5. Hasil Pengujian Download

Data Upload Jenis VPN	IP Sumber	IP Tujian	Time Span (s)	Average Rate (bit)	Packet Drop (%)
Open Vpn	172.16.99.3	192.168.19.20	67,880	1764k	0
SSTP	172.16.99.4	192.168.19.20	68,625	1691k	0

Tabel 6. Data Download

Jenis VPN	IP Sumber	IP Tujian	Time Span (s)	Average Rate (bit)	Packet Drop (%)
Open Vpn	172.16.99.3	192.168.19.20	34,551	3249k	0
SSTP	172.16.99.4	192.168.19.20	22,975	4844k	0

e. Denial of Service

Pengujian pada Denial of Service atau DoS ini bertujuan untuk mencegah pengguna menikmati layanan yang diberikan suatu server dan pada akhirnya server tersebut akan down, pada penggujian menggunakan size 1300 Bytes dengan jumlah paket yang akan dikirim 100, memperoleh hasil sebagai berikut:

a. Hasil pengujian DOS OpenVPN menunjukkan pada paket 50 terjadi packet loss sebesar 5% dan kemudian pada pengujian lain menunjukkan paket 100 terjadi packet loss sebesar 8%. Koneksi OpenVPN mengalami RTO namun tidak terputus dari server

b. Hasil pengujian DOS SSTP menunjukkan pada paket 50 terjadi packet loss sebesar 8% dan kemudian pada pengujian lain menunjukkan paket 100 terjadi packet loss sebesar 6%. Koneksi SSTP mengalami RTO namun tidak terputus dari server

5. Simpulan

Implementasi VPN dengan menggunakan metode OpenVPN dan SSTP bertujuan untuk mengetahui efisiensi dari metode tersebut. Hasil yang diperoleh dari implementasi dan pengujian metode VPN tersebut, dapat disimpulkan sebagai berikut:

a. VPN menggunakan OpenVPN dan SSTP dapat diimplementasikan pada jaringan server sehingga user atau client dapat mengakses server privat dimana saja dan kapan saja melalui jaringan internet.

b. Pengujian yang dilakukan pada performa menghasilkan perbedaan yang tidak begitu signifikan. Pada pengujian packet loss dan round trip peforma OpenVPN lebih unggul dibandingkan SSTP yang ditunjukan dengan packet loss dan latency yang lebih kecil. Pada pengujian WinSCP, ketika upload file metode OpenVPN lebih unggul dibandingkan SSTP dan ketika download lebih unggul SSTP dibandingkan dengan OpenVPN. Pada pengujian DOS kedua metode VPN tidak putus dari server namun mengalami RTO, ketika paket sebesar 50 packet loss pada

OpenVPN lebih kecil dibandingkan dengan SSTP dan ketika paket sebesar 100 packet loss SSTP lebih kecil daripada OpenVPN.

6. Ucapan Terima Kasih

Kami panjatkan puji syukur kehadirat Tuhan Yang Maha Kuasa yang telah memberikan kami semangat untuk menyusun laporan penelitian kami dengan baik. Selain itu kami selaku tim peneliti berterima kasih kepada beberapa pihak yang telah mendukung terlaksananya penelitian ini, yaitu kepada:

1. Dr. Supari, S.T., M.T., selaku Rektor Universitas Semarang.
2. Prof. DR. Ir. Mudjiastuti Handajani, MT selaku Ketua Lembaga Peneltian dan Pengabdian kepada Masyarakat (LPPM) Universitas Semarang.
3. Seluruh rekan pengajar dan staff di lingkungan Fakultas Teknologi Informasi dan Komunikasi (FTIK) Universitas Semarang.
4. Ilham Radianto dan Retomika selaku mahasiswa yang membantu dalam penelitian ini.
5. Keluarga yang selalu menjadi sumber semangat dan support bagi tim peneliti.
6. Seluruh pihak yang tidak dapat kami sebutkan satu per satu yang telah ikut serta membantu dalam penelitian ini.

7. Referensi

[1] S. Surono, F. W. Christanto, and C. Maulana, "Uji Komparasi Quality of Service Antara Metode Routing dan VLAN pada Distribusi Paket Data Jaringan Internet," *JPRT (Pengembangan Rekayasa dan Teknologi)*, vol. 16, no. 2, pp. 183–190, 2020.

[2] D. Dahnial, "Analisa Perbandingan Quality Of Service Antara Protokol PPTP dan L2TP Pada Virtual Private Network Berbasis Router Mikrotik," *Jurnal Ilmiah Informatika Global*, vol. 10, no. 2, pp. 107–113, 2019, doi: 10.36982/jig.v10i2.858.

[3] W. Amayreh, N. Alqahtani, and B. Al-Balawi, "Analysis of the Vlan Network Delay Performance to Improve Quality of Services (QOS)," *Communications on Applied Electronics*, vol. 5, no. 9, pp. 51–54, 2016, doi: 10.5120/cae2016652378.

[4] J. L. Putra, L. Indriyani, and Y. Angraini, "Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna," *IJCIT (Indonesian Journal on Computer and Information Technology*, vol. 3, no. 2, pp. 260–267, 2018.

[5] P. Margana and M. M. Saonari, "VPN Jurnal,"

[6] R. B. Santoso, "PERBANDINGAN KINERJA JARINGAN VPN BERBASIS MIKROTIK MENGGUNAKAN PROTOKOL PPTP dan L2TP SEBAGAI MEDIA TRANSFER DATA."