Pengembangan dan Penerapan Sistem *Virtual Private Network* (VPN) pada *Internet of Things* (IOT) Menggunakan Simulasi

Ilmalik Muhammad Alviendra, Eko Setijadi dan Gatot Kusrahardjo
Departemen Teknik Elektro, Institut Teknologi Sepuluh Nopember (ITS)
e-mail: ekoset@ee.its.ac.id

***Abstrak*—Internet Of Things (IOT) mengacu kepada penggunaan beberapa perangkat yang terhubung dan sistem untuk menggunakan data yang diperoleh dari sensor dan aktuator dan objek fisik lainnya.. Wireless Sensor Network merupakan salah satu aspek penting dalam IOT.. Dalam proses ini diperlukan kapasitas penyimpanan serta networks untuk mendukung lancarnya komunikasi antara user dengan perangkat itu tersendiri.WSN sendiri lebih rentan terhadap serangan dibandingkan jaringan lainnya. Pada penelitian ini telah dilakukan simulasi menggunakan Graphical Network Simulator 3(GNS3) dan di konfigurasikan Virtual Machine(VM)sebagai gambaran perangkat IOT. VM tersebut dihubungkan menuju router dimana router tersebut adalah Gateway menuju internet dan jaringan lainnya. Dikonfiguasikan pula Network Address Translation (NAT) agar simulasi dapat serupa dengan kasus nyata. Kemudian dikonfigurasikan VPN Server jenis PPTP,L2TP,IPsec dan L2TP IPSec. Pada percobaan PPTP server yang terhubung langsung pada router Gateway didapatkan bahwa data terenkripsi dan IP telah terselubung pada jaringan internal namun IP masih tetap akan berubah ketika sudah menuju Internet. Pada percobaan L2TP IP telah berhasil terselubung dari intranet dan ketika menuju internet juga telah terselubung namun belum terenkripsi. Pada percobaan IPSec data telah berhasil terenkripsi dan alamat IP tidak berubah. Pada percobaan L2TP IPsec data telah berhasil ternekripsi dan alamat IP berubah ketika menuju internet.**

***Kata Kunci*—Virtual Private Network (VPN), Internet of Things (IoT), Network Address Translation(NAT), Graphical Network Simulator-3 (GNS3),Virtual Machine (VM) Wireshark.**

I. PENDAHULUAN

DALAM sebuah IOT, pasti ada sebuah Wireless Sensor Netwok yaitu beberapa sensor yang terhubung dengan jaringan. Sensor yang terpasang untuk mencatat data dari sebuah objek yang kemudian akan dihubungkan pada aktuator dan data akan terus direkam dan disimpan pada memori kemudian ketika sebuah keadaan terjadi seperti di set oleh user maka sensor akan melakukan sesuatu berdasarkan feedback dari objek tersebut, atau mengirimkan data kepada user melalui proses signal processing didalam semua proses yang terjadi, ada kemungkinan terjadinya serangan dimulai dari eavesdropping, MITM Attack, sampai DOS. Salah satu metode untuk mengamankan jaringan ialah dengan Firewall, penginstalan anti-virus, dan penggunaan VPN yang dikonfigurasikan secara manual.

VPN sendiri merupakan sebuah hal yang sudah ada sejak jaman 1993 diawali dengan swIPe yang ditemukan oleh John Ioannidis PPTP (Point to Point Tunnelling Protocol) lalu kemudian IPsec dan kemudian berkembang lagi sampai tersedia nya OpenVPN. Dari cara pemasangannya, VPN dapat dipasang melalui komputer langsung, melalui router,single board circuit seperti Raspberry PI, dan banyak lagi. Oleh karena itu apabila sebuah WSN dibuat maka harus ada sumber jaringan dan perintah nya. Hal yang diharapkan dari penelitian ini ialah serangan akan gagal dikarenakan IP address baik dari Sensor maupun User akan disembunyikan pada server VPN. Dalam Tugas Akhir ini akan di fokuskan pada router IoT yang akan digunakan dua konfigurasi VPN yaitu PPTP dan L2TP. Selanjutnya akan dillihat mengenai IP adress dan isi paket pada topologi jaringan yang akan di monitor kemudian diperiksa keterbacaan isi paketnya serta terlacak atau tidaknya Alamat IP. Simulasi akan menggunakan software GNS3 (Graphical Network Simulator-3) dengan menggunakan router,host,internet,dan attacker yang di dalam nya terkonfigurasi IP Address. Untuk penelitian akan berfokus kepada *Router Gateway* dan pada sisi client.

Beberapa parameter yang diambil ialah tahun tercipta karena teknologi berkembang pada setiap waktu, lalu keamanan dimana faktor ini merupakan opsi keamanan yang dapat digunakan baik berupa enkripsi maupun tunnelling nya, kecepatan sebagai parameter kualitas layanan apabila di simulasikan VPN dan terakhir adalah kompabilitas nya terhadap Operating System.

Metode yang digunakan untuk melakukan pemeriksaan keamanan akan menggunakan applikasi *Wireshark* dimana pada applikasi tersebut akan diperlihatkan isi-isi data yang ada lengkap dengan alamat IP, isi data, dan lainnya. Untuk data yang digunakan ialah data *PING (Packet Internet or Inter-Network Groper)* dimana data dalam PING tersebut adalah 26 huruf alfabet yang tersusun sesuai dengan operating system.

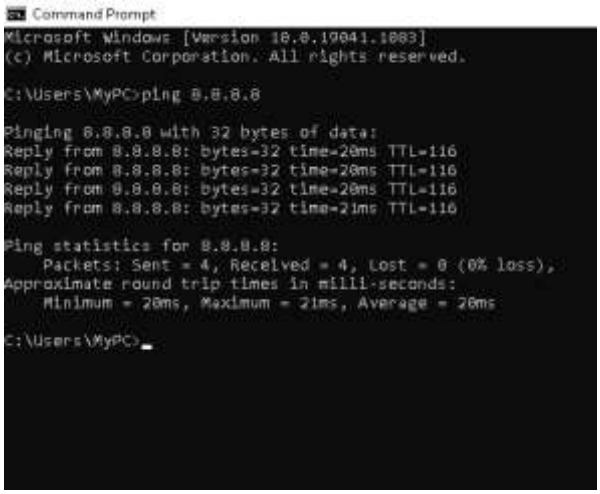
II. TINJAUAN PUSTAKA

A. Router

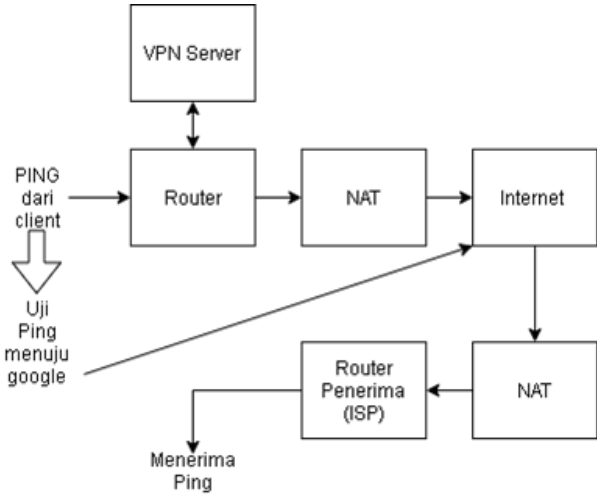
Router merupakan sebuah perangkat yang berfungsi mengirimkan dan menerima paket data melalui jaringan yang khusus disebutkan atau internet menuju tujuannya, melalui proses yang dikenal sebagai routing.Proses routing terjadi pada layer 3 OSI Layer [1]. Fungsi utama dari router ialah penghubung antara sebuah jaringan dengan jaringan lainnya agar bisa bertukar data.

B. Routing

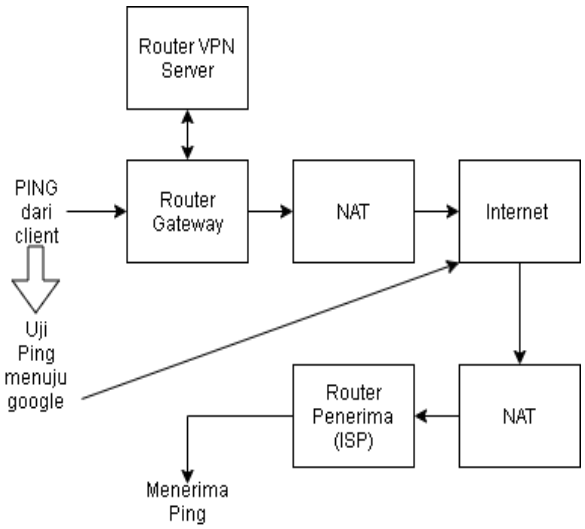
Sebuah Router memiliki kapabilitas untuk mengetahui kemana rute perjalanan sebuah informasi (paket) dari sumber akan diteruskan, kemampuan ini dinamakan Routing. Routing dapat diteruskan untuk perangkat atau host yang



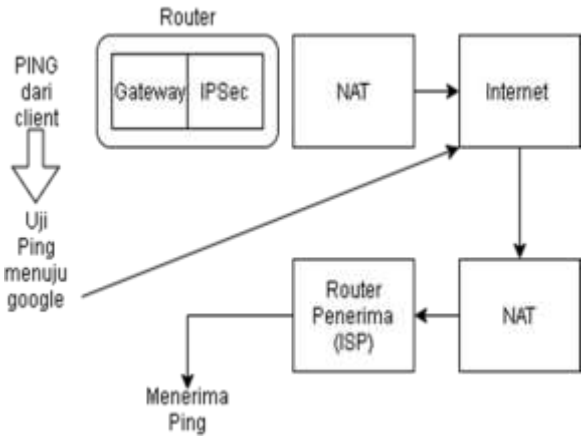
Gambar 1. PING pada Windows.



Gambar 2. Desain Simulasi Penelitian.



Gambar 3. Desain PPTP menggunakan router ketiga.



Gambar 4. Desain IPSec serta Gateway dalam satu router.

berada pada satu jaringan atau berada di jaringan lainnya. Jika sebuah paket data ditunjukkan untuk suatu perangkat yang berada pada jaringan luar router maka paket akan diizinkan untuk penerusan menuju alamat tersebut dan jika paket ditunjukkan pada alamat yang salah maka paket tersebut akan ditolak dan tidak dapat keluar.

Routing terbagi menjadi tiga jenis yaitu Routing Statis, Routing Dinamis, dan Routing Default [1]. Routing statis adalah pembuatan dan pengubahan serta pemasukkan routing table secara manual. Staric routing tidak akan merubah informasi yang ada pada table routing secara otomatis, sehingga pengguna harus melakukan merubah tabel routing secara manual apabila topologi jaringan berubah.

Dynamic Routing adalah router yang memiliki kemampuan untuk membuat tabel routing secara otomatis berdasarkan trafik jaringan dan router yang terhubung. Jika diartikan, dinamis adalah bisa berubah-ubah.

C. IP Address

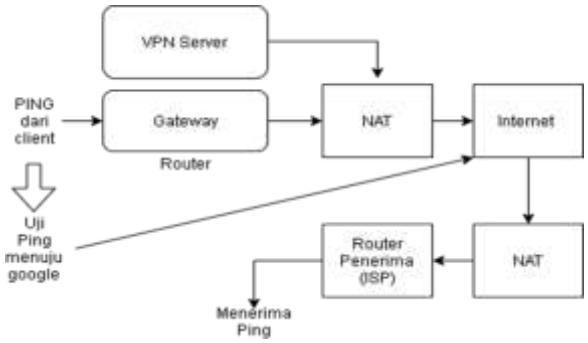
IP Address adalah singkatan dari Internet Protocol Address. IP address digunakan sebagai metode untuk memeriksa perangkat yang dapat mengakses internet yang berbasis TCP/IP. IP address berisi deretan angka biner [2]. Terdapat dua jenis IP Addres yaitu IP versi 4 (IPv4) dan IP versi 6 (IPv6) dimana perbedaannya berada pada jumlah biner yang digunakan. IP address memiliki dua fungsi yaitu, sebagai alamat dan kedua sebagai identifikasi

Fungsi IP address sebagai alamat lokasi jaringan dapat digambarkan seperti halnya alamat pada rumah dimana digambarkan data sebagai tukang pos atau pengirim barang dan untuk mengirimkan maupun menerima data maka seorang pemilik rumah wajib memiliki alamat agar pengirim barang tersebut dapat mengirim atau memberi paket, sebuah alamat untuk mengetahui di mana website tersebut, dan juga sebuah rute agar dapat mencari alamat tersebut [3].

D. Network Address Translation

NAT (Network Address Translation) adalah sebuah proses dimana sebuah jaringan privat dapat menggunakan IP Public untuk mengirimkan data, dimana memungkinkan untuk sebuah perangkat privat dapat mengakses jaringan publik [4]. Dengan kata lain NAT akan menerjemahkan alamat IP privat menjadi satu IP Public yang dapat mengakses internet atau WAN (Wide Area Network). NAT memiliki beberapa jenis konfigurasi di antaranya NAT Statis, NAT Dinamis, Overloading NAT, Overlapping NAT [5].

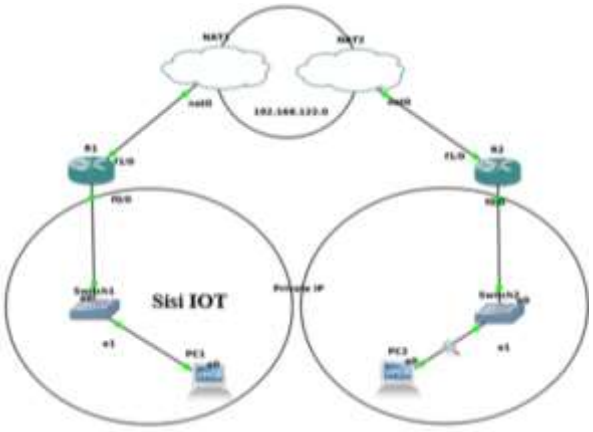
NAT sendiri memiliki beberapaka kelebihan salah satunya adalah dengan adanya NAT dapat menghemat alamat IPv4 yang jumlahnya makin sedikit seiring berjalannya waktu dan kebutuhan mengakses dunia digital. Di samping itu selain memiliki kelebihan NAT juga mempunyai beberapa kelemahan.yaitu setiap kali sebuah komputer ingin terhubung



Gambar 5. Desain L2TP/IPSec.

Tabel 1.
Parameter penelitian

Nomor	Parameter	Keterangan
1	IP Address	Identitas alamat sebuah perangkat jaringan
2	Protokol	Sebuah aturan yang mendefinisikan sebuah pengiriman data
3	Throughput	Kecepatan pengiriman dan penerimaan data dari pengiriman dan penerimaan
4	Keamanan data	Berupa enkripsi yang disediakan pada jaringan yang telah terhubung dengan VPN



Gambar 6. Topologi Jaringan Simulasi.

dengan computer lainnya, baik untuk mendapatkan data atau mengirimnya dari atau keluar harus melewati gateway. Kemudian harus juga mengupdate akses list (access-list). Selain itu, sebuah hardware yang sudah di-NAT akan dapat menggunakan Port Translations atau membaca atau mengirim alamat IP seperti IP lain.

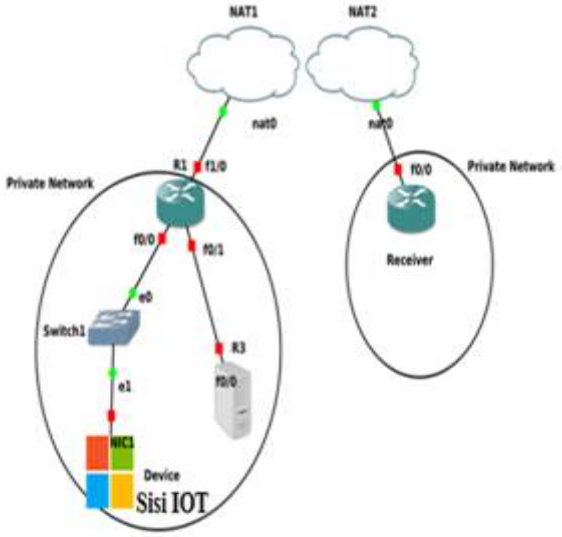
Pada NAT ada dua jenis interface yaitu inside dan outside. Inside yang dimaksud disini adalah alamat asal atau alamat asli dari sebuah perangkat , sedangkan Outside adalah IP yang ada pada router yang telah dikonfiguraskan dengan NAT. Secara mudahnya, semua IP yang akan menuju outside akan diubah menjadi IP pada nat outside

E. PING (Pack Internet or Inter-Network Gropher)

PING adalah utilitas perangkat lunak administrasi jaringan komputer yang digunakan untuk menguji keterjangkauan suatu host pada jaringan Internet Protocol (IP) dan untuk mengukur pengaruh waktu sebagai parameter dari kualitas pelayanan. Nama ini berasal dari terminologi sonar aktif yang mengirimkan pulsa suara dan mendengarkan gema untuk mendeteksi objek di bawah air. Namun, backronym "PING"

Tabel 2.
Keterangan Topologi

R1(Router Gateway IOT)	
f1/0	192.168.122.124
f0/0	192.168.8.1
PC 1	192.168.8.2 (DHCP)
R2 (Router ISP atau penerima)	
f1/0	192.168.122.244
f0/0	192.168.10.1
PC 2	192.168.10.2(DHCP)



Gambar 7. Topologi dengan PPTP Server.

Tabel 3.
Alamat IP Percobaan PPTP

PPTP Server	
f 0/0	192.168.1.2
VPN Pool	172.16.1.2 s.d 172.16.1.10
Loopback	172.16.1.1
Gateway Router	
f 0/0	192.168.8.1
f 0/1	192.168.1.1
f 1/0	192.168.122.100
IOT Device	
IP Address	192.168.8.2

yang berarti "Packet InterNet Groper" telah digunakan sejak awal komputasi untuk pengujian dan pengukuran jaringan. dan Internet. Parameter-parameter yang berada dalam ping ialah “round-trip time” atau waktu sebuah paket dikirimkan dan di terima kembali [6]. Pada awalnya, pengguna ping akan mengirimkan beberapa data (dalam default windows dikirimkan data sebesar 32 byte) kemudian data tersebut akan diterima oleh alamat tujuan ping, alamat yang menerima tadi akan mengirimkan pong (terminologi atau balasan dari ping) menuju pengguna ping tadi kemudian akan muncul parameter-parameter Round-trip Time.

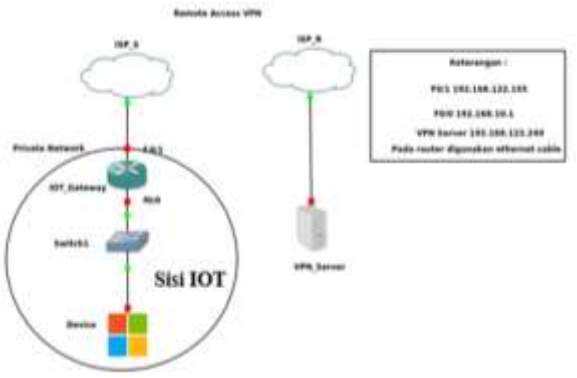
Dari gambar 1 dapat dilihat bahwa RTT dari ping ke ip 8.8.8.8 (google) ialah 20milisecond dari 32 bytes yang dikirimkan, dengan hal yang kita ketahui tersebut kita dapat mengetahui throughput dari jaringan kita dengan rumus:

$$Throughp = \frac{Jumlah\ data\ yang\ dikirim(bytes)}{Waktu\ RTT\ (second)} \quad (6)$$

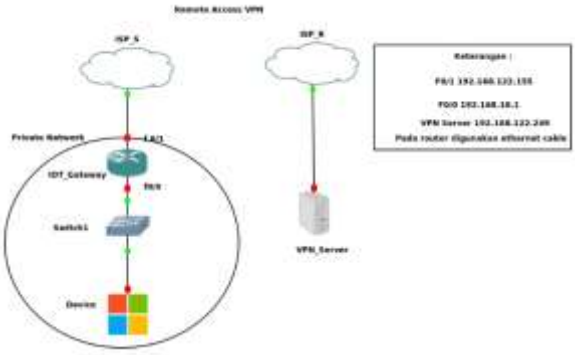
Dari rumus diatas bisa kita hitung hasil dari ping yang ada di gambar 1.

Tabel 4.
Alamat IP pada Percobaan L2TP

L2TP Server (R4)	
f 0/0	192.168.2.2
VPN Pool	172.16.2.2 s.d 172.16.1.10
Loopback	172.16.2.2
Gateway Router (R2)	
f 0/0	192.168.10.1
f 0/1	192.168.2.1
f 1/0	192.168.122.244
IOT Device	
IP Address	192.168.10.2



Gambar 8. Topologi IPSec.



Gambar 9. Topologi L2TP/IPSec.

$$Throughp = \frac{32(bytes)}{0.02\ (second)} = 1.6\ kilobytes$$

F. *Internet Of Things*

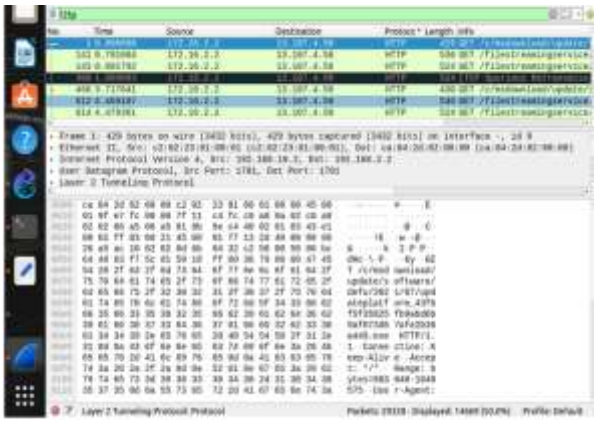
IoT (Internet of Things) merupakan sebuah perangkat dan system yang disusun sedemikian rupa dan saling terhubung serta menyediakan data yang dapat digunakan untuk keperluan-keperluan penggunanya. Dengan IOT, maka terjadi integrasi perangkat menjadi sebuah perangkat yang dapat dikendalikan dari jauh, Kerjasama antar perangkat dan pembagian data. Untuk bisa menggunakan IoT tentu saja harus memiliki beberapa persyaratan diantaranya adalah Sensor, Perangkat IOT, IOT Gateways, IOT Backend [7].

Secara arsitektur, IoT dapat terbagi menjadi beberapa banyak layers. Namun proses utama yang dilakukan ialah data diterima oleh sensor, kemudian data tersebut diproses dan diolah kemudian siap untuk dikirimkan melalui IoT Gateways. IoT gateways ini dapat berupa bluetooth, router dan lainnya. Kemudian setelah data tersebut disiapkan akan dikirim dan disimpan pada cloud, setelah data tersebut dikirimkan ke cloud maka akan dikirimkan kembali kepada back end atau user dari IoT tersebut [8].

Tabel 5.
Alamat IP pada Percobaan L2TP IPSec

L2TP Server (R2)	
f 0/0	192.168.122.249
VPN Pool	192.168.11.1 s.d 192.168.11.10
Loopback	192.168.11.20
Gateway Router (R1)	
f 0/0	192.168.10.1
f 1/0	192.168.122.155
IOT Device	
IP Address	192.168.10.2

Gambar 10. Hasil penangkapan dari Gateway menuju ISP.

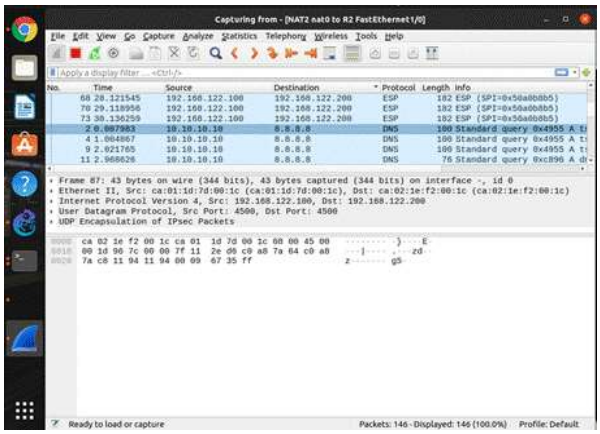


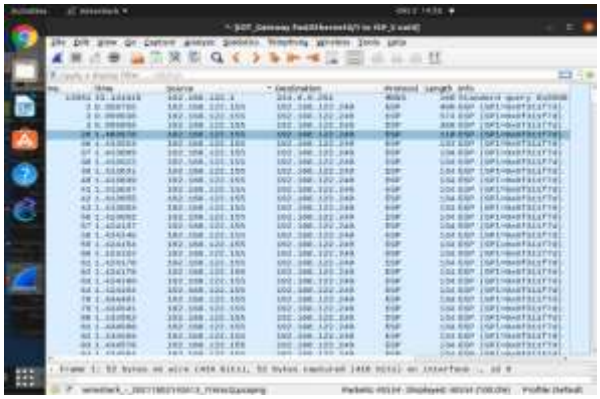
Gambar 11. Hasil Penangkapan protokol L2TP.

G. *Virtual Private Network (VPN)*

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk sebuah pengguna agar dapat terhubung ke jaringan publik dan menggunakannya untuk bergabung dengan jaringan lokal [9]. Dengan cara tersebut maka akan didapatkan sebuah keleluasan pribadi dimana pada jaringan publik Ketika ada seseorang yang mencari maka akan sulit untuk ditemukan. Adapun untuk lebih lengkapnya VPN menggunakan tunneling yaitu , melalui server VPN yang menyembunyikan komunikasi melalui public internet dengan cara tunnelling dan enkripsi dari sebuah VPN. Tunnelling adalah sebuah protokol dimana tunnel akan menyediakan suatu koneksi point-to-point logis selama jaringan IP-nya bersifat connectionless [10].

Tunnelling merupakan suatu proses pemgbungkusan dan pengiriman data yang masuk dan keluar pada osi layer. Alasan disebut *Tunnel* karena koneksi point-to-point tersebut sebenarnya terbentuk melalui jaringan trafik umum, namun


Gambar 12. Penangkapan pada percobaan IPSec.


Gambar 13. Hasil Percobaan L2TP/IPSEC.

Tabel 6.
Perbandingan Protokol

Protokol	Perubahan IP	Keamanan	Delay	Thoroughput
PPTP	Tidak	Terenkripsi	2 ms	17.490 (byte/s)
L2TP	Ya	Tidak	8 ms	16.789 (byte/s)
IPSec	Tidak	Terenkripsi	10 ms	25.296 (byte/s)
L2TP IPSec	Ya	Terenkripsi	3 ms	55.503 (byte/s)

koneksi tersebut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari penggunanya [11].

Hal ini sama dengan seperti penggunaan jalur pesepeda khusus dimana jalur yang digunakan ialah jalur raya namun dibuat sebuah jalur khusus dimana hanya sepeda yang dapat lewat. Selain itu, VPN juga akan mengubah IP address yang kita miliki dengan cara mengirimkan sebuah IP address dimana IP address tersebut yang akan digunakan untuk mengirimkan dan menerima data [12].

III. METODE PENELITIAN

A. Perancangan Desain Simulasi

Dalam tugas akhir ini akan dilakukan serangkaian proses yang terlihat pada gambar 2. Gambar 2 merupakan alur proses data yang digunakan pada penelitian ini secara umum**.**

Pada desain gambar 3 adalah sebuah router yang dipasang pada router gateway. Fungsi dari router ini adalah menyediakan layanan PPTP VPN kepada client nya. Client disini adalah sebuah perangkat yang tahu alamat IP asal dari VPN tersebut, ketika koneksi sudah terhubung maka router Server VPN akan memberikan IP address yang baru serta meng enkripsikan data yang ingin dikirim oleh client keluar dari router gateway

Pada gambar 8 Router VPN Server adalah sebuah router dimana dapat dikonfigurasikan protokol antara L2TP atau PPTP. Ketika Client sudah terhubung kepada Router VPN Server, maka server VPN akan menerima permintaan tunnel dari Client kemudian akan disediakan sebuah IP Address VPN dan juga enkripsi MPPE jika menggunakan protokol PPTP dan tidak terenkripsi jika menggunakan L2TP. Kemudian ketika Client mengirimkan PING menuju penerima, paket tersebut dihubungkan terlebih dahulu menuju Router VPN Server sebelum dikirimkan pada Public Internet. IP yang digunakan akan diselubungkan dan data akan dienkripsikan. Protokol PING yang awalnya berupa ICMP akan berubah menjadi PPP dan PPTP.

Pada awal jenis VPN yang digunakan adalah menggunakan PPTP kemudian setelah itu akan dirancang kembali jaringan yang serupa dengan PPTP akan tetapi menggunakan protokol L2TP. Untuk informasi dan topologi akan dibahas pada sub-bab selanjutnya. Setelah menguji kedua protokol tersebut maka protokol selanjutnya yang akan dicoba ialah IPSec, lebih rinci lagi ialah IPSec dengan *mode transport.*

Hampir mirip dengan alur sebelumnya namun, pada alur ini pengamanan terjadi ketika Paket yang ingin dikirimkan akan diteruskan. Ketika menggunakan protokol IPSec maka sebelumnya harus lah digenerasikan sebuah kunci atau Pre-shared key agar dapat menggunakan protokol ini. Lalu diperlukan juga IP address dari router Gateway agar client dapat melakukan dial-up untuk mendapatkan enkripsi dari IPSec. Berbeda dari protokol L2TP dan PPTP, IPSec tidak akan mengubah IP Address dari pengirimnya melainkan mengubahnya menjadi alamat IP dari IP yang dihubungi oleh client, khusus pada kasus NAT, maka IP yang digunakan adalah IP dari Router Gateway menuju outside NAT. Gambar 4 adalah contoh desain IPSec pada router gateway.

Awalnya, client akan melakukan proses dial-up pada IPSec, IPSec sendiri akan menggunakan IP dari Gateway. Setelah terhubung maka client harus memasukkan Pre-Shared key agar dapat menggunakan layanan IPSec tersebut. Setelah koneksi terjalin, client akan melakukan PING menuju Gateway, karena IPSec menggunakan IP Gateway maka IPSec juga akan mengenkripsikan tiap trafik yang keluar dari gateway. Data dari PING yang berasal dari client akan tetap sampai menuju ISP namun, ketika dicoba untuk menangkap trafik dari router menuju internet dan seterusnya, data yang didapatkan tidak akan sama dengan data PING asli yang dikirim oleh client dan diterima oleh penerima PING. Protokol PING pada standarnya berupa ICMP namun dapat berubah menjadi ESP dikarenakan beberapa pengaturan keamanan IPSec.

Lalu ketika IPSec sudah selesai disimulasikan dan dianalisa maka simulasi selanjutnya ialah mencoba untuk menyisipkan keamanan IPSec pada protokol L2TP atau sering disebut L2TP/IPSec, hal lalu kemudian meletakkan VPN Server terpisah dari jaringan client, dengan kata lain hal ini dapat disebut dengan *Remote AccessVPN*. Pada desain kali ini, IP Gateway akan dihubungkan pada VPN Server jenis

L2TP dan IPSec, dimana kedua protokol ini akan menggunakan IP untuk dial-up dari client. L2TP akan memberikan VPN IP pada client dan IPSec akan mengenkripsikan data-data yang dirikimkan dari client menuju internet dan seterusnya. Gambar 5 adalah alur data PING dengan menggunakan L2TP+IPsec atau L2TP over IPSec pada router Gateway.

Client akan melakukan proses dial-up dengan IP VPN Server, setelah koneksi VPN terjalin maka client akan menggunakan Pre-shared key dalam konfigurasi VPN nya kemudian ketika sudah dilakukan maka terciptalah tunnel yang akan menyelubungi serta mengenkripsi data-data yang dikirimkan dari client menuju penerima. Awalnya PING akan diselubungkan IP nya dengan IP yang di dapat dari VPN Server (L2TP) kemudian data PING tersebut akan dibungkuskan pada IPSec menggunakan metode enkripsi antara 3DES atau AES. Data PING yang dikirimkan tetap akan diterima oleh ISP namun ketika di coba untuk menangkap trafik data maka protokol yang akan muncul adalah ESP, dimana sebelumnya pada PING jenis protokol yang tertangkap trafiknya seharusnya ICMP lalu IP Address yang awalnya berupa IP client akan menjadi IP yang diberikan dari VPN server. Dalam metode ini, posisi pada VPN Server berada pada ISP yang lain, hal ini dapat digunakan sebagai penggambaran remote access VPN.

B. Parameter Penelitian

Parameter untuk mengetahui performasi dari pemasangan protokol-protokol VPN mengacu pada data-data yang tertangkap menggunakan Wireshark. Adapun parameter penangkapan trafik berada pada Tabel 1.

Perhitungan *thoroughput* akan dilakukan ketika pengujian sudah berhasil dengan cara mengirimkan *PING* menuju *DNS Google* yaitu 8.8.8.8. Protokol akan membandingkan kecepatan antar VPN dan tanpa VPN. Sementara keamanan data adalah tingkat seberapa amannya data yang dapat dibaca melalui applikasi *Wireshark*.

C. Penyusunan Topologi Awal

Pada program simulasi yang dilakukan pada penelitian Tugas Akhir ini, akan digunakan salah satu network simulation tools yaitu GNS3(Graphical Network Simulator 3). GNS3 merupakan aplikasi emulator jaringan (Graphic Simulator Network) berbasis GUI yang berarti emulator ini akan memberikan kenyamanan lebih pada sisi topologi, GNS3 di rilis pada tahun 2008.

Agar menyerupai sebuah aliran data pada IoT menggunakan router gateway, maka akan digunakan sebuah router direpresentasikan dengan R1, selanjutnya pada topologi akan ada client dimana client-client tersebut adalah sebuah komputer atau device IOT dengan sistem operasi

Windows 10, maka akan digunakan switch sebagai pembagi jaringan menuju router, guna switch disini adalah menyambungkan beberapa device (many) menuju R1 (one). Kemudian setelah tersusun maka akan dihubungkan R1 dengan NAT yang sebelumnya diunduh pada subbab 3.4.2 NAT pada topologi ini berarti router telah terhubung langsung dengan internet namun diperlukan beberapa konfigurasi khusus agar client dan router dapat tersambung pada internet. Lalu pada sisi yang berbeda akan diletakkan Router ISP atau sebuah router yang akan mengantarkan paket menuju penerima. Router ini direpresentasikan dengan R2. R2 disini juga akan dihubungkan kepada NAT agar dapat menggambarkan kasus dimana banyak device end user IOT yang lebih dari satu. Jika dilihat pada contoh kasus nyata di dunia sehari-hari penggunaan IPv4 yang banyak sejak munculnya internet mendatangkan krisis alamat IP Address, oleh karena itu NAT diciptakan. NAT mencabangkan sebuah IP dari publik kemudian menyediakan IP Private pada jaringan-jaringan yang terhubung ke sebuah router NAT. Gambar 6 merupakan Topologi yang akan digunakan untuk simulasi Tugas Akhir ini.

Dengan keterangan sebagai pada Tabel 2 Dimana pada topologi ini digunakan dua PC yaitu PC1 sebagai representasi perangkat IOT dan PC 2 sebagai penerima. Ketika konfigurasi pada router telah berhasil dilakukan maka PC 1 akan diganti dengan *Virtual Machine* dengan sistem operasi windows dan PC2 akan dihilangkan.

Dikarenakan menggunakan NAT pada percobaan kali ini, maka gate menuju internetnya adalah sama ialah 192.168.122.0. Ini merupakan network yang merepresentasikan akses Internet bagi Router,Device, serta End-user.

Setelah Topologi tersusun maka langkah selanjutnya adalah melakukan konfiguasi pada router diantaranya adalah konfigurasi *IP Address, Network Address Translation (NAT), dan DHCP Server.* Setelah semua konfigurasi telah dilakukan maka langkah selanjutnya adalah konfigurasi jenis-jenis VPN diantaranya adalah *Point-To-Point Tunnelling Protocol (PPTP), Layer Two Tunnelling Protocol (L2TP) , IPSecurity (IPSec), dan Layer Two Tunnelling Protocol Over IPSec(L2TP Over IPSec).*

D. Konfigurasi dan Pengujian VPN

Ketika sudah melakukan konfigurasi untuk setiap IP Address, DHCP Server sekaligus NAT, akan dikonfigurasikan VPN Server. Pada tiap konfigurasi PPTP, L2TP, IPSec, L2TP IPSec akan digunakan jenis IP VPN yang berbeda beserta konfigurasi pengguna yang berbeda. Hal ini karena fungsi GNS3 yaitu emulator, memakan penyimpanan yang banyak dimana jika ingin digunakan satu topologi yang sama akan memakan banyak memori, oleh karena itu ketika suatu percobaan telah dilakukan dan di ambil datanya, maka akan di simpan konfigurasi pada plain-text dan screenshoot kemudian file mengenai percobaan akan dihapus. Pada bagian ini akan dibahas cara menghubungkan antara client dengan VPN Server dimana apabila suatu IOT device dapat melakukan proses dial-up maka device tersebut dapat menggunakan layanan Virtual Private Network.

Pada konfigurasi PPTP, topologi yang akan digunakan adalah topologi dimana server VPN terhubung secara langsung pada Router Gateway namun berbeda network dengan sisi DHCP Servernya. Topologi dengan PPTP server dapat dilihat pada Gambar 7.

Pada topologi diatas ada 3 router, dimana R1 merupakan Router Gateway, R2 merupakan Receiver dan R3 merupakan Server VPN. Adapun fungsi dari f1/0 R1 adalah router NAT dimana IP pada network dibelakangnya akan di translasikan, kemudian pada node f0/0 R1 adalah DHCP Server yang dihubungkan pada switch, hal ini agar semua device yang terhubung pada switch tersebut akan mendapatkan akses menuju internet. Kemudian f0/1 adalah penghubung agar dapat mengakses VPN Server. Ketika client sudah melakukan

proses dial-up menuju R3, maka semua data yang akan keluar dari R1 akan diubah terlebih dahulu alamat IP nya dan diberikan enkripsi oleh R3 dan kemudian dikirimkan keluar. Agar VPN tidak bertumpang tindih dengan proses NAT maka harus diberikan aturan tambahan pada R1 agar tidak mentranslasikan beberapa protokol. Contohnya disini ialah PPTP dimana PPTP menggunakan protokol *GRE(Generic Routing Encapsulation)* dengan protocol 47 dan PPP (Point to Point Protocol) dengan port 1723 Adapun konfigurasi PPTP pada VPN Server dapat dilihat pada Tabel 3.

Pada simulasi kali ini,vpn server terhubung langsung dengan Router gateway IOT. Proses agar client dapat menggunakan jasa VPN adalah dengan cara melakukan *dial-up* pada VPN Server, dimana IP yang akan dimasukkan dalam dial-up ialah IP f0/0 dari VPN Server.

Setelah beberapa konfigurasi yang dilakukan pada VPN Server, langkah selanjutnya adalah melakukan proses *dial-up* dari client. Proses ini adalah proses agar client dapat menggunakan layanan VPN Server. Hal yang perlu dilakukan ialah menghubungkan dari client, sebuah koneksi menuju VPN Server kemudian memasukkan parameter-parameter keamanan yang telah diterapkan oleh VPN Server. Beberapa parameter yang ada contohnya adalah *Username & Password, Pre-shared keys, certificate,RADIUS, dan masih banyak lagi parameter lainnya.* Pada percobaan kali ini yang digunakan ialah *Username & Password* yaitu *admin dan admin01*. Kemudian setelah parameter dimasukkan maka client dapat mendapatkan layanan seperti pada protokol dalam kasus ini, protokolnya adalah PPTP dengan enkripsi *MPPE* dan dengan IP Address seperti yang tertera pada Tabel 3.

Untuk Layer 2 Tunnelling Protocol (L2TP) Proses yang dilakukan hampir sama dengan PPTP. Perbedaannya hanya pada konfigurasi VPDN, dan konfigurasi VPN pada client. Tabel 4 adalah konfigurasi pada percobaan menggunakan L2TP.

Untuk perbedaan yang pertama pada konfigurasi adalah jenis protokol yang digunakan pada *VPDN (Virtual Private Dial-up Network) setup* dimana pada PPTP menggunakan protokol PPTP sementara pada L2TP akan menggunakan protokol L2TP. Sedangkan perbedaannya pada sisi client ialah melakukan pengaturan pada jaringan VPN nya bahwa jenis VPN yang digunakan adalah Layer Two Tunnelling Protocol (L2TP) kemudian mengijinkan *Microsoft CHAP Version 2(MS Chap v2)* atau pada jenis sistem operasi lain untuk mengijinkan autentikasi jenis ini atau jika tidak maka harus diberi autentikasi lain pada sisi VPN Server. Berbeda pada topologi sebelumnya dimana ada router ketiga, pada IPSec topologi yang akan digunakan adalah topologi seperti pada Gambar 8.

Pada IPSec, digunakan sebuah peta kripto atau *crypto map* yang akan di konfigurasikan pada jalur keluar NAT, pada simulasi kali ini peta tersebut akan diletakkan pada node f1/0 R1. Adapun yang harus dilakukan agar IPSec dapat digunakan adalah *policy, pre-shared keys, enrcyption, hash,* dan yang utama adalah mode dimana dapat dipilih antara mode *tunnel* atau mode *transport.* Perbedaan dari kedua mode ini adalah mode *tunnel* akan membuat sebuah terowongan antara titik A dengan titik B dimana pada jaringan ialah IP yang keluar dari IPSec dan titik B adalah titik tujuan dimana ketika tunnel tersebut terjadi akan ada IP Header tambahan pada tunnel tersebut. Walaupun mode *transport* tidak memberikan IP Header tambahan, namun pada mode transport akan mengamankan payload atau traffik dari client yang bekerja dibalik IPSec. Dengan kata lain, akan lebih kuat terhadap serangan *Eavesdropping.*

Lalu setelah itu maka, kita akan melakukan proses dial-up pada IP yang didalamnya tersedia crypto map yaitu f1/0. Setelah dilakukan dial-up maka langkah selanjutnya adalah memasukkan pre-shared keys yang telah diterapkan pada router.

Pada percobaan terakhir yaitu L2TP over IPSec topologi telah diubah dan dimodifikasi menjadi *remote access* dimana VPN Server berada pada jaringan yang berbeda dengan client. Gambar 9 akan menunjukan topologi yang digunakan untuk percobaan ini. Kemudian berikut adalah tabel keterangan untuk IP Address dari topologi dapat dilihat pada Gambar 9. Tabel 5 merupakan alamat IP pada PercobaanL2TPSec.

IV. HASIL SIMULASI DAN ANLISA

A. Percobaan Point-to-Point Tunneling Protocol

Pada protokol Point-to-Point Tunneling Protocol (PPTP) ketika client telah melakukan proses dial-up dan terhubung dengan VPN Server maka data yang dikirim dari client akan dialihkan terlebih dahulu menuju VPN Server. Topologi yang digunakan untuk simulasi ini menghubungkan VPN Server dibelakang network Router gateway.

Jika diuruti dari awal, yang terjadi adalah terjadi enkapsulisasi PPP dari R1 (Gateway Router) menuju R3 (VPN Server) kemudian setelah itu akan terjadi enkripsi data yang masih berada dalam private network dan kemudian setelah itu maka VPN Server akan memberikan IP samaran pada client. Ketika proses hubungan dilakukan keluar menuju public network maka IP yang terdeteksi adalah IP dari Outside NAT tersebut. Pada gambar 10 adalah hasil penagkapan traffik dari router gatewau menuju ISP dan dapat dilihat walaupun perubahan IP gagal karena NAT, namun enkripsi masih tetap utuh.

Lalu dilakukan pengujian kecepatan dan delay dengan menggunakan PING. Didapatkan *thoroughput* PING awal adalah 537,815 bytes dan ketika memakai protokol PPTP menjadi 520,325 bytes. Jika dihitung dari delay maka terjadi delay sebesar 2 millisecond, sedangkan pada thoroughput nya mengalami penurunan sebesar 17.49 bytes

B. Percobaan Layer-two Tunneling Protocol (L2TP)

Ketika proses dial-up terjadi, dan sudah didapatkan IP Address, tidak seperti PPTP dimana jika kita melakukan PING terhadap loopback akan terdeteksi, pada L2TP berada keamanan lebih pada sisi IP nya. Dari kekurangannya dapat dilihat pada gambar 11 dimana pada router gateway menuju ISP akan terubah IP Header nya namun data yang ada tidak terenkripsi

Dapat dilihat pada gambar 11 bahwa ketika menggunakan protokol L2TP maka IP akan tetap tersamarkan namun data masih dapat dibaca. Kecepatan yang di dapatkan ketika menggunakan L2TP tidak berubah terlalu signifikan. Jika dihitung thoroughput nya maka akan di dapatkan delay sebesar 8 millisecond dan thoroughput nya berkurang sebesar 16.789 bytes

C. Percobaan IP Security (IPSec)

Pada simulasi kali ini, jenis enkripsi yang dipilih adalah 3DES(Triple Data Encryption Standard) , sedangkan untuk hash nya adalah SHA(Secure Hashing Algorithm). Enkripsi yang didapatkan dapat dikatakan memadai dibanding dengan enkripsi pada PPTP, namun untuk melakukan konfigurasi pada IPSec akan sedikit lebih rumit namun pada sisi positifnya, NAT tidak akan mengganggu protokol ini.

Setelah client memasukkan Pre-shared-key dan terhubung dengan IPSec, ,maka semua jenis protokol yang terdapat pada traffik akan berupa ESP (Encapsulating Security Payload) dimana data didalamnya akan tersembunyikan walaupun IP yang ada masih sama. Gambar 12 akan diperlihatkan hasil penangkapan traffik pada percobaan IPSec

Kecepatan yang di dapatkan ketika menggunakan IPSec hampir tidak berubah. Dengan rumus menghitung thoroughput maka dapat diketahui delay sebesar 10 millisecond dan thoroughput nya berkurang sebesar 25.296 bytes.

D. Percobaan L2TP Over IPSec (L2TP/IPSec)

Pada simulasi kali ini, digunakan sebuah router yang akan bertindak sebagai VPN server, router ini terdapat L2TP dan IPSec hal ini agar proses enkripsi dan enkapsulasi terjadi pada satu router yang sama dalam satu proses. Karena jika salah satu konfigurasi berada pada router lainnya akan mengakibatkan double encapsulation dan menambah lambat kecepatan.

data PING yang ada tidak terdeteksi lagi oleh wireshark. Hal ini terjadi karena IPSec telah menyelubungkan paket-paket yang ada menjadi ESP. L2TP bekerja pada inside network, mengubah jenis-jenis IP yang ada sekaligus menambah enkripsi nya. Aspek lain yang akan diteliti ialah jika dikirimkan sebuah paket menuju keluar melalui VPN Server. Data tersebut tidak akan terenkripsikan maupun terubah IP nya dikarenakan pada dasarnya, ketika terjadi dial-up maka pengamanan akan terfokus melalui satu tunnel.

Jika dilihat bahwa pada gateway terjadi enkripsi yang sangat banyak, namun IP Address masih tidak berubah. Namun hal ini cukup mengamankan device dikarenakan data tidak dapat diakses oleh penyerang dan jika digunakan DDoS maka device akan tetap aman walaupun router gateway dapat terserang.

Gambar 13 akan menunjukan hasil penangkapan dari router gateway menuju ISP. Setelah dilakukan beberapa percobaan dan didapatkan hasil, protokol-protokol yang telah diuji akan diletakkan pada tabel beserta dengan aspek-aspek penting pada percobaan ini seperti *thoroughput*, delay, keamanan data , dan perubahan IP. Tabel 6 merupakan perbandingan protokol.

V. KESIMPULAN?RINGKASAN

Setelah dilakukan pengkajian, penyusunan topologi, simulasi, dan pembahasan hasil yang diperoleh terkait dengan judul tugas akhir “Pengembangan dan Penerapan Sistem Virtual Private Network (VPN) pada Internet Of Things (IOT) Menggunakan Simulasi” maka dapat diambil kesimpulan sebagai berikut;(1)Untuk menghubungkan IOT terhadap VPN harus menggunakan sebuah opsi connect untuk mencari alamat IP dari VPN Server dan mengakses layanan.(2)Letak Server VPN akan memengaruhi kecepatan transmisi data pada client yang terhubung pada VPN. Jika jaraknya berada dibelakang sebuah router maka kecepatan tidak akan berkurang secara signifikan, namun ketika diletakkan diluar sebuah router yang di dalamnya terkonfigurasi NAT maka kecepatan akan berubah menjadi tidak stabil.(3)Berdasarkan kecepatan yang diteliti, protokol yang paling sedikit terpengaruh pada thoroughput adalah VPN dengan protokol Point-to-Point Tunneling Protocol (PPTP) dengan pengurangan sebesar 17.49 bytes dan delay 2ms dibandingkan dengan L2TP, IPSec, dan L2TP IPSec).(4)IPSec dapat digunakan untuk mengenkripsikan data.(5)Jika data yang berada tidak terlalu tinggi tingkat kepentingannya, maka dapat digunakan L2TP untuk menambah keamanan pada IP.(6)Berdasarkan keamanannya, tipe L2TP IPSec adalah yang paling aman karena ketika dalam private network Router Gateway terjadi enkripsi dan IP terganti serta traffik untuk ICMP tidak ditemukan.(7) VPN dapat digunakan untuk mengamankan IOT. Lebih spesifiknya lagi pengamanan terjadi pada layer dua dan tiga. Untuk device bisa diamankan dari perangkat, switch,sampai ke router.

DAFTAR PUSTAKA

[1] I. Marzuki, “Perancangan dan simulasi routing static berbasis IPV4 menggunakan router cisco,” *Energy*, vol. 5, no. 2, pp. 47–52, 2015, [Online]. Available: https://adoc.tips/perancangan-dan-simulasi-routing-static-berbasis-ipv4-menggu.html.

[2] W. Huitao, Y. Ruopeng, Wufan, and Z. Xiaofei, “Research on IP address allocation of tactical communication network,” *J. Phys. Conf. Ser.*, vol. 1187, no. 4, 2019, doi: 10.1088/1742-6596/1187/4/042105.

[3] L. E. Nuryanto, “Konsep subnetting Ip address untuk efisiensi internet,” *Orbith*, vol. 11, no. 1, pp. 68–73, 2015, [Online]. Available: https://www.scribd.com/doc/55681626/Konsep-Subnetting-IP-Address-Untuk-Effisiensi-Internet.

[4] R. Wijaya, “Analisis dan Perancangan Jaringan Network Address Translation (nat) pada Jaringan Internal yang Memiliki Lebih dari Satu Router Menggunakan Mikrotik,” Universitas Internasional Batam, 2020.

[5] A. Bansal and P. Goel, “Simulation and analysis of network address translation (NAT) & port address translation (PAT) techniques,” *Int. J. Eng. Res. Appl.*, vol. 07, no. 07, pp. 50–56, 2017, doi: 10.9790/9622-0707025056.

[6] A. Hafiz and D. Susianto, “Analysis of internet service quality using internet control message protocol,” *J. Phys. Conf. Ser.*, vol. 1338, no. 1, pp. 1–6, 2019, doi: 10.1088/1742-6596/1338/1/012055.

[7] E. Setijadi *et al.*, “Design of Large Scale Structural Health Monitoring System for Long-Span Bridges Based on Wireless Sensor Network,” *2013 Int. Jt. Conf. Aware. Sci. Technol. Ubi-Media Comput. Can We Realiz. Aware. via Ubi-Media?, iCAST 2013 UMEDIA 2013*, pp. 169–173, 2013, doi: 10.1109/ICAwST.2013.6765428.

[8] N. M. Kumar and P. K. Mallick, “The internet of things: insights into the building blocks, component interactions, and architecture layers,” *Procedia Comput. Sci.*, vol. 132, pp. 109–117, 2018, doi: 10.1016/j.procs.2018.05.170.

[9] M. Pudelko, “Performance Analysis of VPN Gateways,” Technical University of Munich, 2018.

[10] M. Varvello, I. Q. Azurmendi, A. Nappa, P. Papadopoulos, G. Pestana, and B. Livshits, “A Privacy-Preserving Decentralized Virtual Private Network,” in *IFIP Networking Conference, IFIP Networking 2021*, 2021, pp. 1–7, doi: 10.23919/IFIPNetworking52078.2021.9472843.

[11] J. Triwanto and E. A. Setiawan, “Penggunaan virtual private network untuk pengamanan komunikasi pada VoIP,” *Tesla*, vol. 16, no. 1, pp. 25–32, 2014, [Online]. Available: https://www.journal.untar.ac.id/index.php/tesla/article/view/354/295.

[12] S. H. Kurniadi, E. Utami, and F. W. Wibowo, “Building dynamic mesh VPN network using mikroTik router,” *J. Phys. Conf. Ser.*, vol. 1140, no. 1, 2018, doi: 10.1088/1742-6596/1140/1/012039.