JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 7, Nomor X, Bulan 2023, Page 999-999
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v5i1.2293

Simulasi Penerapan Keamanan Jaringan Menggunakan IPSec Dan GRE Pada Internet Of Things Menggunakan GNS3

Muhammad Rafi Irzam[1], Oktavia Ayu Permata[2], Kharisma Monika Dian Pertiwi[3]
[123] Fakultas Teknologi Informasi dan Bisnis, Teknologi Informasi, Institut Teknologi Telkom Surabaya, Surabaya, Indonesia
Email: [1]muhammad.rafi@student.ittelkom-sby.ac.id, [2]oktapermata@ittelkom-sby.ac.id, [3]kharismamonika@ittelkom-sby.ac.id
Email Penulis Korespondensi: muhammad.rafi@student.ittelkom-sby.ac.id

Abstrak−Internet of things (IoT) merupakan konsep dimana suatu objek ditanamkan teknologi seperti sensor dan software yang bertujuan untuk berkomunikasi, mengendalikan, menghubungkan, serta bertukar data melalui perangkat lain selama masih terhubung ke internet. Namun, tantangan keamanan yang muncul dalam lingkungan yang semakin terhubung ini menuntut solusi yang efektif. Salah satu bentuk solusinynya adalah menerapkan Virtual Private Network (VPN). Dalam konteks ini, penelitian ini bertujuan untuk menganalisis dan mengimplementasikan lapisan keamanan tambahan pada jaringan IoT menggunakan protokol Internet Protocol Security (IPSec) dan Generic Routing Encapsulation (GRE). Hasil pengujian menunjukkan bahwa penggunaan kombinasi protokol IPSec dan GRE memberikan hasil yang sangat baik dalam aspek keamanan dan QoS. Hal ini dilihat dari pengujian yang dilakukan dengan PING dan di analisa menggunakan aplikasi Wireshark dengan melihat parameter IP dan protokol, Quality of Service (QoS), keamanan data, dan rute. Penambahan protokol IPSec dan GRE tidak menyebabkan penurunan QoS pada jaringan yang signifikan. Hal ini berdasarkan data hasil perhitungan QoS yakni didapatkan rata – rata hasil throughput-nya adalah 986.5 bps, rata – rata hasil delay-nya adalah 1.03615 ms, rata – rata hasil packet loss-nya adalah 0%, dan rata – rata hasil jitter-nya adalah 3.35445 ms. Kesimpulannya, implementasi protokol IPSec dan GRE pada jaringan IoT menghasilkan lapisan keamanan yang efektif tanpa mengorbankan performa jaringan. Ini memberikan perlindungan yang memadai terhadap ancaman keamanan serta menjaga kualitas layanan dalam lingkungan jaringan yang semakin kompleks.

Kata Kunci: Internet of Things; IPSec; GRE; GNS3; Terowongan

Abstract−Internet of things (IoT) is a concept where an object is embedded with technology such as sensors and software that aims to communicate, control, connect, and exchange data through other devices as long as they are connected to the internet. However, the security challenges that arise in this increasingly connected environment demand effective solutions. One form of solution is to implement a Virtual Private Network (VPN). In this context, this research aims to analyze and implement an additional security layer on IoT networks using Internet Protocol Security (IPSec) and Generic Routing Encapsulation (GRE) protocols. The test results show that the use of a combination of IPSec and GRE protocols provides excellent results in terms of security and QoS. This can be seen from tests conducted with PING and analyzed using the Wireshark application by looking at IP and protocol parameters, Quality of Service (QoS), data security, and routes. The addition of IPSec and GRE protocols does not cause a significant decrease in QoS on the network. This is based on the data from the QoS calculation results, namely the average throughput result is 986.5 bps, the average delay result is 1.03615 ms, the average packet loss result is 0%, and the average jitter result is 3.35445 ms. In conclusion, the implementation of IPSec and GRE protocols in IoT networks produces an effective security layer without sacrificing security.

Keywords: Internet of Things, IPSec, GRE, GNS3, Tunnel

1. PENDAHULUAN

Saat ini kita berada pada era dimana saat suatu teknologi berkembang maka terdapat ancaman terhadap teknologi tersebut. Salah satu dari teknologi tersebut adalah Internet of Things (IoT), beberapa ancaman dapat terjadi pada IoT. IoT secara umum memiliki konsep kumpulan dari banyak objek, layanan, manusia, dan perangkat yang saling berhubungan yang dapat berkomunikasi, berbagi data, dan informasi untuk mencapai tujuan bersama di berbagai bidang dan aplikasi [1]. Pada tahun 2017, terjadi peningkatan serangan terhadap perangkat IoT sebesar 600% [2]. Hal tersebut dapat terjadi dikarenakan sebagian besar perusahaan yang memproduksi perangkat IoT tidak mempertimbangkan faktor keamanan dari sebuah perangkat namun lebih menekankan pada ukuran , biaya, dan kegunaan [2].

Beberapa bentuk ancaman pada teknologi IoT dapat berupa orang yang tidak berwenang mendapatkan akses untuk mengakses sebuah data dan menyalahgunakan informasi yang bersifat personal, penyerang membuat sistem mudah untuk diserang, serta ancaman kepada keselamatan pengguna [3]. Maka dari itu, diperlukan pengamanan yang dilakukan untuk mencegah hal tersebut terjadi. Salah satu upaya pengamanan tersebut adalah dengan mengamankan jaringan menggunakan Virtual Private Network (VPN) [4]. Dengan VPN, komunikasi atau transfer data lebih aman karena adanya sistem tunneling (terowongan) yang membuat data tersebut terenkripsi.

Sebelumnya terdapat penelitian terdahulu yang telah dilakukan dengan judul "Pengembangan dan Penerapan Sistem Virtual Private Network (VPN) pada Internet of Things (IOT) Menggunakan Simulasi" [4]. Penelitian tersebut mengembangkan dan menerapkan sistem VPN pada IoT menggunakan simulasi GNS3 dan VM sebagai gambaran perangkat IoT. Penelitian ini menguji kinerja dan keamanan jaringan IoT dengan menggunakan empat jenis VPN, yaitu PPTP, L2TP, IPsec, dan L2TP IPsec. Jika dibandingkan dengan penelitian ini, perbedaan yang dilakukan dengan penelitian sebelumnya adalah protokolnya. Protokol yang digunakan untuk menguji kinerja dan keamanan jaringan IoT adalah GRE over IPSec dimana protokol Generic Routing Encapsulation (GRE)

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 7, Nomor X, Bulan 2023, Page 999-999
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v5i1.2293

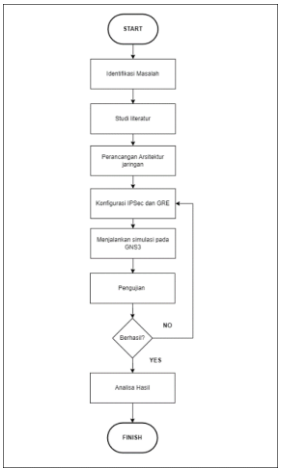
dikonfigurasikan bersama protokol IP Security (IPSec) dalam satu jaringan yang sama sehingga komunikasi antar perangkat lebih aman.

Dalam penelitian ini, tidak menggunakan perangkat IoT sesungguhnya namun berfokus pada simulasi keamanan jaringan menggunakan VPN IPSec dan GRE dengan simulator GNS3 yang diskenariokan seperti lingkungan IoT. Internet Protocol Security atau IPSec adalah protokol untuk mengamankan komunikasi pada Internet Protocol/IP dengan autentikasi dan juga melakukan enkripsi di setiap paket IP. Dan definisi Generic Routing Encapsulation (GRE) adalah protokol yang menggunakan teknologi tunneling sehingga dapat melakukan enkapsulasi berbagai protokol untuk kebutuhan link virtual point-to-point. Nantinya akan dilakukan konfigurasi pada Virtual PC Simulator (VPCS) sebagai gambaran perangkat IoT. Kemudian, untuk memeriksa trafik data, aplikasi yang digunakan adalah Wireshark. Trafik data yang dianalisis berupa throughput dan ping rata - rata.

Pada arsitektur IoT, terdapat application layer, network layer, dan sensing layer. Application layer merupakan lapisan yang menyediakan berbagai layanan dan fungsi untuk pengguna, seperti penyimpanan data, analisis data, visualisasi data, dan kontrol perangkat. Lapisan ini yang berinteraksi langsung dengan pengguna melalui aplikasi web atau aplikasi seluler. Application layer juga berinteraksi dengan lapisan jaringan untuk menerima dan mengirim data dari dan ke perangkat-perangkat IoT. Lapisan aplikasi biasanya menggunakan protokol seperti HTTP dan MQTT. Network layer adalah lapisan yang menyediakan konektivitas dan transmisi data antara perangkat-perangkat IoT. Network Layer menggunakan berbagai teknologi jaringan, seperti Wi-Fi, Bluetooth, atau seluler, untuk menghubungkan perangkat-perangkat IoT dengan router. Pada lapisan ini, menggunakan protokol seperti IP, TCP, UDP, atau 6LoWPAN untuk mengatur alamat, rute, dan format data yang dikirim dan diterima. Terakhir, Sensing layer atau lapisan sensor yang bertanggung jawab untuk mengumpulkan data dari lingkungan fisik, seperti suhu, kelembaban, cahaya, gerakan, atau suara. Lapisan ini juga bertugas untuk mengirim data ke lapisan jaringan atau menerima instruksi dari lapisan aplikasi untuk mengontrol perangkat-perangkat IoT.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian



Gambar 1.

Penelitian ini dimulai dengan identifikasi masalah tentang serangan terhadap perangkat IoT dan kurangnya keamanan pada perangkat IoT. Kemudian dilakukan studi literatur tentang penggunaan GNS3, IPSec, dan GRE sebagai metode penelitian. Selanjutnya dibuat rancangan arsitektur jaringan yang sesuai dengan studi kasus pada pabrik. Lalu dilakukan konfigurasi IPSec dan GRE pada routerOS dengan menggunakan command line pada Mikrotik Cloud Hosted Router. Terakhir dilakukan simulasi jaringan pada GNS3 dengan menggunakan node-node seperti VPCS dan Router Mikrotik CHR. Untuk lebih jelas mengenai tahapan tersebut berikut penjabarannya. Tahapan pertama dalam penelitian ini adalah identifikasi masalah, yaitu mendefinisikan masalah yang diteliti agar lebih terukur dan sebagai langkah awal penelitian. Masalah yang diidentifikasi adalah peningkatan serangan terhadap perangkat IoT dan kurangnya keamanan pada perangkat IoT. Langkah selanjutnya adalah studi literatur, yaitu mempelajari sumber-sumber yang relevan dengan penelitian untuk mendapatkan pemahaman lebih lanjut tentang metode yang digunakan dan referensi dari penelitian sebelumnya. Sumber-sumber yang dipelajari adalah jurnal nasional, jurnal internasional, atau buku yang berkaitan dengan penggunaan GNS3, IPSec, dan GRE. Langkah ketiga adalah perancangan arsitektur jaringan, yaitu membuat rancangan jaringan yang sesuai dengan studi kasus pada pabrik. Arsitektur jaringan ini melibatkan remote staff sebagai user yang mengontrol sensor dari jarak jauh melalui internet. Kemudia yang keempat adalah konfigurasi IPSec dan GRE, yaitu melakukan pengaturan pada routerOS untuk mengimplementasikan protokol IPSec dan GRE. Protokol IPSec digunakan untuk

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 7, Nomor X, Bulan 2023, Page 999-999
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v5i1.2293

mengamankan koneksi dengan enkripsi, sedangkan protokol GRE digunakan untuk mengamankan koneksi dengan tunneling. Konfigurasi ini dilakukan dengan menggunakan command line pada Mikrotik Cloud Hosted Router. Langkah terakhir adalah menjalankan simulasi pada GNS3, yaitu melakukan simulasi jaringan dengan menggunakan node-node yang telah ditambahkan pada GNS3. Node-node ini meliputi 2 VPCS sebagai remote staff dan sensor, dan 3 Router Mikrotik CHR sebagai routerOS. Simulasi ini melibatkan pendaftaran alamat IP, routing IP, pembuatan tunnel, dan konfigurasi protokol.

2.2 Konfigurasi IPSec dan GRE

2.2.1 Konfigurasi IPSec

Konfigurasi protokol IPSec dilakukan pada operating system (OS) router dan konfigurasi tersebut berupa command line. Internet Protocol Security atau IPSec merupakan serangkaian protokol untuk komunikasi protokol Internet (IP) aman yang bekerja dengan mengautentikasi dan mengenkripsi setiap paket IP dari sesi komunikasi [5]. RouterOS yang digunakan adalah Mikrotik Cloud Hosted Router. Pertama masuk ke dalam config IP, kemudian masuk ke config IPSec. Konfigurasi protocol IPSec terdiri dari 2 phase, yakni phase 1 membuat profile IPSec dan phase 2 membuat proposal. Pada phase 1, pembuatan profile dimulai dengan menambahkan property dh-group (Diffie–Hellman), enc-algorithm, dan nama dari profile. Selanjutnya pada phase 2, pembuatan proposal menambahkan property enc-algorithms, pfs-group, dan nama proposal. Dilanjutkan dengan membuat ip peer yang menambahkan ip address dari remote router serta memberikan nama peer seperti nama profile yang telah dibuat. Tahap selanjutnya adalah membuat identity, dimana pada tahap ini menambahkan peer dan juga secret. Semua config dilakukan pada masing – masing router.

2.2.2 Konfigurasi GRE

Seperti pada IPSec, konfigurasi pada GRE dilakukan pada OS router dan konfigurasi berupa command line. Generic Routing Encapsulation (GRE) merupakan metode standar yang dijelaskan oleh Internet Engineering Task Force (IETF) dan merupakan protokol terowongan yang dapat membawa lebih dari satu jenis protokol alamat komunikasi [6]. Pertama masuk ke dalam mode configuration interface. Dilanjutkan masuk ke configuration GRE kemudian menambahkan remote dan local address dan memberi nama dari interface GRE. Semua konfigurasi dilakukan pada kedua router, setelah itu menambahkan alamat ip untuk tunnel dan didaftarkan pada interface yang telah dibuat. Tahap selanjutnya, melakukan routing IP.

2.2 Skenario Pengujian

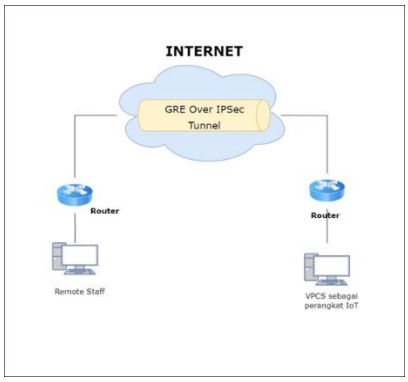
Proses pengujian untuk pemeriksaan keamanan akan menggunakan aplikasi Wireshark, dari aplikasi tersebut dapat melihat isi - isi data yang lengkap seperti alamat IP, jenis protokol, dan lainnya. Telah dijelaskan pada proses simulasi, data yang digunakan adalah data PING. PING atau Packet Internet Groper adalah perangkat lunak yang bekerja dengan protokol Internet Control Message Protocol (ICMP) untuk mengontrol koneksi antara dua komputer di internet. PING berjalan dengan mengirimkan paket ke alamat tujuan dan menunggu respon dari host tujuan [17].

Pengujian dilakukan sebanyak 20 kali pengiriman PING dengan tujuan untuk mendapatkan rata - rata keberhasilan proses enkapsulasi dan enkripsi alamat IP. Hasil pengujian berupa IP address pada trafik akan berubah dan tidak sama dengan data PING yang sebenarnya dan juga keterangan protokol akan berbeda. Hal tersebut terjadi karena data - data tersebut telah dienkripsi oleh IPSec, protokol pada saat melakukan PING umumnya menggunakan ICMP namun ketika telah dienkripsi protokol yang muncul akan menjadi ESP. Artinya data tersebut berhasil untuk diamankan.

2.2 Desain Topologi Jaringan

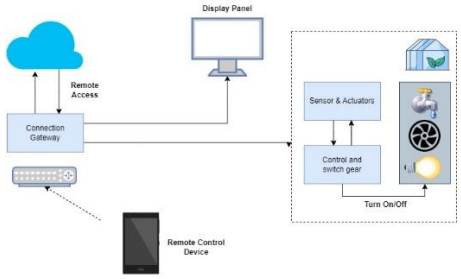
Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 7, Nomor X, Bulan 2023, Page 999-999
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v5i1.2293



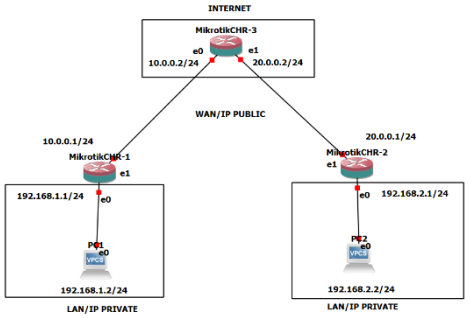
Gambar 2. Arsitektur Jaringan IPSec dan GRE

Arsitektur jaringan akan menggunakan studi kasus pada pabrik dimana perangkat IoT akan berada pada lingkungan pabrik, salah satu contoh perangkat tersebut adalah sensor. Remote staff sebagai user yang mengatur sensor tersebut dari jarak jauh dan dapat melakukannya dimana saja karena telah tersambung pada internet, contohnya jika akan menghidupkan dan mematikan mesin, monitoring kinerja alat, dan mendeteksi kerusakan pada alat.



Gambar 3. Contoh ilustrasi jaringan IoT

Gambar 3 merupakan salah satu contoh arsitektur jaringan IoT, *remote control* akan tersambung dengan *router* agar terhubung dengan internet kemudian melalui internet akan menghubungkan pada sensor yang ada pada pabrik. Pengamanan dilakukan pada koneksi antara *remote control* dan sensor. Dengan diterapkannya keamanan pada koneksi tersebut diharapkan dapat meminimalisir serangan pada perangkat – perangkat IoT yang terdapat pada pabrik.



Gambar 4. Arsitektur jaringan tanpa IPSec dan GRE

Gambar 4 merupakan topologi jaringan yang dimana belum dikonfigurasikan protokol GRE dan IPSec jadi pengiriman data melewati router ke router tanpa melewati tunnel. Pembagian IP dalam jaringan yang disimulasikan ditunjukkan pada Tabel 1

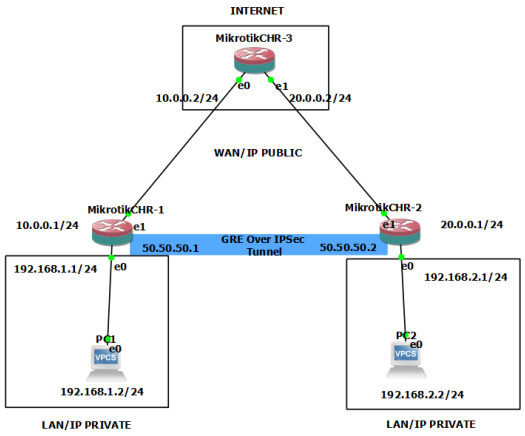
Tabel 1. Keterangan Topologi

Nama Perangkat	Interface	IP Address
PC1	e0	192.168.1.2/24
PC2	e0	192.168.2.2/24
Mikrotik CHR-1	e0	192.168.1.1/24
	e1	10.0.0.1/24

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

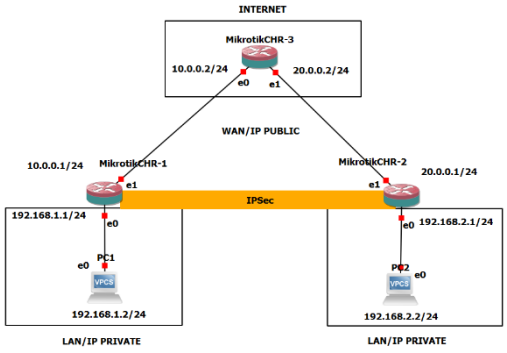
JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 7, Nomor X, Bulan 2023, Page 999-999
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v5i1.2293

Nama Perangkat	Interface	IP Address
Mikrotik CHR-2	e0	192.168.2.1/24
	e1	20.0.0.1/24
Mikrotik CHR-3	e0	10.0.0.2/24
	e1	20.0.0.2/24



Gambar 5. Arsitektur jaringan IPSec dan GRE

Topologi pada Gambar 5 dibuat pada aplikasi GNS3, dalam pembuatan topologi tersebut dibutuhkan node 2 VPCS dan 3 router Mikrotik CHR versi 6.49.8 stable yang sebelumnya telah didaftarkan pada GNS3. Router Mikrotik CHR-3 dianggap sebagai internet sehingga router Mikrotik CHR-1 dan Mikrotik CHR-2 tersambung seperti melalui internet. Pada router Mikrotik CHR-1 dan Mikrotik CHR-2 dibuatkan tunnel dengan menggunakan GRE Over IPSec, dimana protokol GRE dikonfigurasikan dengan protokol IPSec agar lebih aman saat kedua router saling berkomunikasi. Informasi nama perangkat, interface dan IP Address dipaparkan pada tabel 1.



Gambar 6. Arsitektur jaringan IPSec

Gambar 6 merupakan topologi jaringan yang dikonfigurasikan hanya dengan protokol IPSec, jadi pengiriman data akan melewati alamat IP peer dari tunnel IPSec yang telah dikonfigurasikan.

3. HASIL DAN PEMBAHASAN

3.1 Konfigurasi RouterOS dan VPCS

Pada tahapan ini dilakukan pendaftaran Alamat IP pada masing – masing routerOS dan VPCS sesuai pada desain topologi jaringan yang telah dibuat kemudian dilakukan *routing IP address* agar semua perangkat dapat terhubung dan saling berkomunikasi. Router yang digunakan adalah Mikrotik RouterOS. MikroTik RouterOS merupakan sistem operasi dan perangkat lunak yang mengubah PC biasa atau perangkat keras MikroTik Routerboard menjadi router [7]. Berikut untuk tabel routing Alamat IP pada perangkat *Mikrotik CHR-1*:

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 7, Nomor X, Bulan 2023, Page 999-999
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v5i1.2293

Tabel 2 *Keterangan Routing IP RouterOS Mikrotik CHR-1*

No.	DST-ADDRESS	PREF-SRC	GATEWAY	DISTANCE
1.	0.0.0.0/0	-	10.0.0.2	1
2.	10.0.0.0/24	10.0.0.1	ether2	0
3.	50.50.50.2/32	50.50.50.1	gre-tunnel	0
4.	192.168.1.0/24	192.168.1.1	ether1	0
5.	192.168.2.0/24	-	50.50.50.2	1

Dst-address adalah alamat IP dari jaringan tujuan yang ingin dicapai oleh paket. Pref-src adalah alamat IP yang digunakan sebagai sumber paket yang dikirimkan oleh router. Gateway adalah alamat IP dari perangkat selanjutnya yang harus dilewati oleh paket untuk mencapai jaringan tujuan.. Distance adalah nilai yang menunjukkan seberapa jauh atau seberapa baik rute tersebut dibandingkan dengan rute lain yang menuju ke jaringan tujuan yang sama. Nilai 0 berarti rute langsung tanpa melewati perangkat lain, dan nilai 1 berarti rute dengan satu lompatan atau satu perangkat lain.

Tabel 3 *Keterangan Routing IP RouterOS Mikrotik CHR-2*

No.	DST-ADDRESS	PREF-SRC	GATEWAY	DISTANCE
1.	0.0.0.0/0	-	20.0.0.2	1
2.	20.0.0.0/24	20.0.0.1	ether2	0
3.	50.50.50.1/32	50.50.50.2	gre-tunnel	0
4.	192.168.1.0/24	-	50.50.50.1	1
5.	192.168.2.0/24	192.168.2.1	ether1	0

Tabel 4 *Keterangan Routing IP RouterOS Mikrotik CHR-3*

No.	DST-ADDRESS	PREF-SRC	GATEWAY	DISTANCE
1.	10.0.0.0/24	10.0.0.2	Ether1	0
2.	20.0.0.0/24	20.0.0.2	Ether2	0
3.	192.168.1.0/24	-	10.0.0.1	1
4.	192.168.2.0/24	-	20.0.0.1	1

3.2 Konfigurasi GRE

Untuk membuat tunnel GRE antara dua router MikroTik, terdapat beberapa langkah yang meliputi pembuatan interface GRE, penambahan IP peer, routing, dan konfigurasi firewall. Langkah pertama adalah membuat interface GRE dengan menentukan nama, alamat lokal, alamat remote, dan parameter keepalive yang menentukan durasi dan jumlah pengulangan untuk menjaga koneksi tunnel. Langkah kedua adalah menambahkan IP peer pada interface GRE dengan menentukan alamat IP point-to-point dan network dari router lawan. Langkah ketiga adalah melakukan routing dengan menentukan alamat jaringan tujuan dan gateway dari router lawan. Langkah keempat adalah mengkonfigurasi firewall dengan menambahkan aturan NAT untuk menyembunyikan alamat IP privat dan menandai trafik yang keluar dari interface GRE.Berisi hasil implementasi aplikasi ataupun hasil program (yang penting saja), ataupun hasil dari pengujian metode.

3.3 Konfigurasi IPSec

Terdapat beberapa tahapan untuk mengkonfigurasi protokol IPSec antara dua router MikroTik adalah sebagai berikut. Membuat profile, proposal, IP peer, identity, dan policy yang menentukan parameter-parameter untuk mengatur koneksi IPSec. Profile menentukan algoritma enkripsi, grup Diffie-Hellman, dan durasi koneksi. Proposal menentukan jenis-jenis algoritma yang akan digunakan untuk mengenkripsi data. IP peer menentukan alamat IP publik dari router lawan. Identity menentukan kunci rahasia yang akan digunakan untuk mengautentikasi koneksi. Policy menentukan aturan-aturan untuk mengirim dan menerima data melalui IPSec.

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 7, Nomor X, Bulan 2023, Page 999-999
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v5i1.2293

Untuk membuat profile, dilakukan pendaftaran nama, alamat lokal, alamat remote, dan parameter keepalive pada masing-masing router. Untuk membuat proposal, perlu memberikan nama, algoritma enkripsi, dan grup Perfect Forward Secrecy (PFS) pada masing-masing router. Untuk menambahkan IP peer, perlu memberikan nama, alamat IP, profile, dan proposal pada masing-masing router. Untuk menambahkan identity, perlu memberikan nama peer dan secret pada masing-masing router. Untuk menambahkan policy, caranya dengan memberikan alamat IP sumber, alamat IP tujuan, mode tunnel, aksi enkripsi, proposal, dan peer pada masing-masing router.

3.4 Konfigurasi Hasil Pengujian

Pada pengujian dibuat menjadi 3 kondisi yakni, pengujian sebelum dan sesudah diterapkannya GRE over IPSec ditambahkan pengujian sesudah diterapkan IPSec saja. Terdapat pengujian dan analisa pada masing – masing kondisi yaitu pengujian PING antar VPCS, analisa IP & protokol, analisa QoS, analisa keamanan, dan analisa rute

3.4.1 Pengujian PING

Setelah masing – masing perangkat telah dikonfigurasi, memiliki alamat IP dan di routing maka selanjutnya dilakukan pengujian dari PC1 ke PC2 begitu juga sebaliknya. Pengujian PING dilakukan dari PC1 ke PC2 dan dilakukan hingga 20 packet, pengujian ini dilakukan dengan tujuan apakah kedua VPCS telah dapat berkomunikasi dan terhubung. PING atau Packet Internet Groper adalah perangkat lunak yang bekerja dengan protokol Internet Control Message Protocol (ICMP) untuk mengontrol koneksi antara dua komputer di internet. PING berjalan dengan mengirimkan paket ke alamat tujuan dan menunggu respon dari host tujuan [8]. Didapatkan rata – rata waktu yang dibutuhkan untuk packet bisa sampai ke tujuan adalah 7.62 ms pada kondisi sebelum penerapan IPSec dan GRE. Pada kondisi setelah penerapan IPSec dan GRE didapatkan rata – rata waktunya adalah 9.15 ms. Untuk kondisi setelah penerapan IPSec saja didapatkan rata – ratanya adalah 7.415 ms. Dari pengujian PING yang dilakukan pada 3 kondisi, terlihat jika pengiriman data yang paling lambat adalah pada kondisi penerapaan GRE dan IPSec.

3.4.2 Analisa IP & Protokol

Analisa Alamat IP dan protokol pada tahapan pengujian dianalisa pada aplikasi *Wireshark*. *Wireshark* adalah salah satu analisis paket bebas serta sumber terbuka [9]. Aplikasi ini mampu menangkap paket - paket data yang ada pada jaringan tersebut. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa [9]. Analisa ini bertujuan untuk melihat protokol apa yang muncul pada saaat komputer saling berkomunikasi dan mengetahui dari mana dan kemana komunikasi tersebut berlangsung. Setelah dilakukan analisa pada *wireshark,* didapatkan hasil dari masing – masing kondisi pengujian. Pada kondisi sebelum penerapan IPSec dan GRE, pada *wireshark* muncul protokol *Internet Control Message Protocol* (ICMP) juga alamat IP asli dari perangkat asal dan tujuan masih tertampil. Pada kondisi setelah penerapan IPSec dan GRE, protokol yang muncul pada *wireshark* adalah GRE dan Encapsulation Security Payload (ESP). ESP merupakan sebuah protokol dalam IPSec yang menyediakan layanan enkripsi, integritas, dan autentikasi untuk data yang dikirim melalui jaringan internet [10]. Alamat IP asal dan tujuan yang tertampil bukan dari alamat asli dari masing – masing perangkat melainkan digantikan alamat IP local dan remote yang sebelumnya telah dikonfigurasikan. Hasil analisa tersebut sama seperti penerapan protokol IPSec dan yang menjadi pembeda hanya tidak munculnya protokol GRE.

3.4.3 Analisa QoS

Untuk mengetahui performa pada protokol - protokol tersebut terdapat beberapa parameter yang diperhatikan mengacu pada data yang tertangkap menggunakan aplikasi wireshark. Salah satu parameter yang diteliti adalah *Quality of Service* (QoS), pada QoS terdapat aspek yang dilihat seperti *throughput*, *delay*, *packet loss*, dan *jitter*.

Quality of Service (QoS) merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari satu servis [11]. Pada masing – masing aspek QoS, diberikan standar penilaian parameter QoS yang dikeluarkan oleh *European Telecommunication Standards Institute* yaitu *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON). Berikut penjelasan mengenai aspek pada QoS :

a. Throughput
   Throughput adalah laju data yang dikirim melalui jaringan, biasanya diekspresikan dalam satuan *bits per second* (bps) atau *byte per second* (Bps) [12]. Untuk mendapatkan nilai throughput, dilakukan perhitungan dan ditunjukkan pada persamaan (1) sebagai berikut :

$$\text{Throughput} = \frac{Jumlah\ data\ yang\ dikirim}{waktu\ pengiriman\ data} \quad \textbf{(1)}$$

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 7, Nomor X, Bulan 2023, Page 999-999
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v5i1.2293

Tabel 5 *Kategori Throughput menurut Standar TIPHON*

Kategori Throughput	Throughput (bps)	Indeks
Sangat Bagus	100	4
Bagus	75	3
Sedang	50	2
Jelek	<25	1

(sumber : TIPHON)

b. Delay

Delay adalah waktu yang dibutuhkan sebuah data untuk menempuh jarak dari asal ke tujuan [13]. Untuk mendapatkan nilai delay, dilakukan perhitungan dan ditunjukkan pada persamaan (2) sebagai berikut :

$$\text{Delay} = \frac{waktu\ pengiriman\ data}{total\ paket\ yang\ terkirim} \quad \textbf{(2)}$$

Tabel 6 *Kategori Delay menurut Standar TIPHON*

Kategori Delay	Besar Delay (ms)	Indeks
Sangat Bagus	< 150 ms	4
Bagus	150 ms s/d 300 ms	3
Sedang	300 ms s/d 450 ms	2
Jelek	> 450 ms	1

(sumber : TIPHON)

c. Packet Loss

Packet Loss merupakan suatu parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang, dapat terjadi karena collision dan congestion pada jaringan [14].Untuk mendapatkan nilai packet loss, dilakukan dengan perhitungan pada persamaan (3) sebagai berikut :

$$\text{Packet Loss} = \frac{(paket\ data\ dikirim) - (paket\ data\ diterima)}{paket\ data\ yang\ dikirim} \text{ x } 100\% \quad \textbf{(3)}$$

Tabel 7 *Kategori Packet Loss menurut Standar TIPHON*

Kategori Packet Loss	Packet Loss (%)	Indeks
Sangat Bagus	0	4
Bagus	3	3
Sedang	15	2
Jelek	25	1

(sumber : TIPHON)

d. Jitter

Jitter atau variasi delay adalah variasi dari delay atau selisih antara delay pertama dengan delay selanjutnya [15]. Untuk mendapatkan nilai jitter, dapat lakukan perhitungan yang ditunjukkan pada persamaan (4) sebagai berikut :

$$\text{Jitter} = \frac{total\ variasi\ delay}{total\ paket\ yang\ diterima - 1} \quad \textbf{(3)}$$

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 7, Nomor X, Bulan 2023, Page 999-999
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v5i1.2293

***Tabel 3. 1** Kategori Jitter menurut Standar TIPHON*

Kategori Jitter	Jitter (ms)	Indeks
Sangat Bagus	0 ms	4
Bagus	0 ms s/d 75 ms	3
Sedang	75 ms s/d 125 ms	2
Jelek	125 ms s/d 225 ms	1

(sumber : TIPHON)

Tabel 5. Hasil pengujian Quality of Service setelah penerapan GRE dan IPSec

Rute Pengujian	Parameter Quality Of Service			
	Throughput (bps)	Delay (ms)	Packet Loss (%)	Jitter (ms)
PING dari PC1 ke PC2	1376	0.8893	0	4.5539
PING dari PC2 ke PC1	597	1.183	0	2.155

Berdasarkan tabel 5, di dapatkan bahwa nilai throughput terkategori sangat bagus dengan nilai 1376 bps dan 597 bps, nilai delay terkategori sangat bagus dengan nilai 0.8893 ms dan 1.183 ms, nilai packet loss dalam pengujian ini juga mendapatkan hasil yang baik dengan nilai 0% dan Jitter dengan nilai 4.5539 ms dan 2.155 ms.

Tabel 6 Hasil pengujian Quality of Service setelah penerapan IPSec

Rute Pengujian	Parameter Quality Of Service			
	Throughput (bps)	Delay (ms)	Packet Loss (%)	Jitter (ms)
PING dari PC1 ke PC2	341	0.4868	0	- 9.5
PING dari PC2 ke PC1	346	0.4796	0	- 1.77

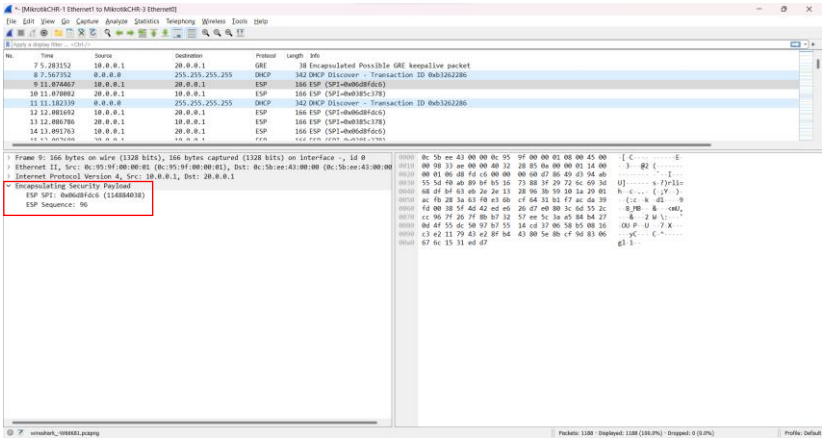
Berdasarkan tabel 6, di dapatkan bahwa nilai throughput terkategori sangat bagus dengan nilai 341 bps dan 346 bps, nilai delay terkategori sangat bagus dengan nilai 0.4868 ms dan 0.4796 ms, nilai packet loss dalam pengujian ini juga mendapatkan hasil yang baik dengan nilai 0% dan Jitter dengan nilai – 9.5 ms dan – 1.77 ms. Hasil perhitungan jitter bernilai minus hasil maka dianggap sangat bagus karena menurut *European Telecommunications Standards Institute* (ETSI) jitter negatif menunjukkan bahwa jaringan dapat mengirimkan data dengan lebih cepat dan lebih stabil.

3.4.4 Analisa Keamanan

Analisa keamanan dilakukan dengan tujuan untuk mengetahui apakah hasil konfigurasi telah berhasil diterapkan atau belum. Analisa dilakukan pada aplikasi *wireshark.* Setelah dilakukan pengujian, pada kondisi setelah penerapan GRE dan IPSec terlihat pada *wireshark* muncul keterangan *Security Parameter Index* (SPI). *Security Parameter Index* atau Indeks Parameter Keamanan adalah pengidentifikasi yang digunakan untuk mengidentifikasi secara unik Asosiasi Keamanan IPSec yang dibentuk secara manual dan dinamis [16]. Pada bagian *protocol* muncul protokol ESP. ESP merupakan salah satu jenis header IPSec yang menyediakan kerahasiaan (enkripsi), dan pembatasan aliran lalulintas kerahasiaan. Pada keterangan source dan destination di wireshark, telah terganti alamat IP local dan remote dari tunnel jadi bukan alamat IP asli dari masing – masing perangkat yang berarti data telah berhasil terenkripsi.

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 7, Nomor X, Bulan 2023, Page 999-999
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v5i1.2293



Gambar 7 Detail Informasi Protocol pada Wireshark sesudah penerapan GRE dan IPSec

3.4.5 Analisa Rute

Traceroute adalah perintah yang digunakan untuk melacak jalur yang dilalui packet data menuju ip/host tertentu di internet [17]. Setelah protokol GRE dan IPSec berjalan, rute yang dilalui paket data akan melewati alamat tunnel yang telah dikonfigurasikan sebelumnya. Hal tersebut membuktikan jika tunnel telah berhasil dibuat dan komunikasi antar perangkat melewato *tunnel* atau terowongan GRE.

```
PC1> trace 192.168.2.2
trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
 1   192.168.1.1   1.209 ms  1.014 ms  1.036 ms
 2   50.50.50.2   4.129 ms  3.686 ms  3.287 ms
 3   *192.168.2.2   5.123 ms (ICMP type:3, code:3, Destination port unreachable)
```

Gambar 8 Keterangan hasil traceroute setelah penerapan GRE dan IPSec

4. KESIMPULAN

Berdasarkan simulasi dan pengujian yang telah dilakukan, dibagi menjadi dua kondisi yakni kondisi sebelum dan sesudah diterapkannya GRE & IPSec. Dalam mengamankan jaringan IoT dapat dilakukan dengan mengimplementasikan tunnelling menggunakan protokol IPSec dan GRE. Hal ini dikarenakan protokol GRE mengenkapsulasi data saat dikirim ditambah protokol IPSec mengenkripsi data tersebut. Proses tersebut dapat dibuktikan dengan analisa pada aplikasi Wireshark, ketika pengiriman data berlangsung source dan destination alamat IP yang terlihat adalah local dan remote address dari tunnel yang telah dibuat. Dapat dilihat juga ketika dianalisa melali traceroute, data akan melewati 3 rute juga melewati alamat IP dari tunnel.

Pengujian dilakukan dengan melakukan PING dari PC1 ke PC2 dan sebaliknya. Terdapat beberapa parameter yang di analisa pada penelitian ini , yaitu : Analisa IP dan Protokol, Analisa Quality of Service, Analisa Keamanan data, dan Analisa Rute. Dari pengujian Quality of Service, penambahan protokol IPSEc dan GRE tidak menyebabkan penurunan QoS pada jaringan yang signifikan. Hal ini berdasarkan data hasil rata – rata throughput dan delay berstatus sangat bagus, Packet loss menunjukkan 0 % yang artinya data diterima dengan baik oleh perangkat tujuan, nilai jitter berstatus sangat bagus.. Dapat dilihat juga dari analisa keamanan, pada aplikasi wireshark ketika pengiriman data berlangsung alamat IP source dan destination yang muncul bukan alamat IP asli dari masing – masing perangkat melainkan alamat IP local dan remote dari tunnel yang telah dibuat. Protokol GRE digabungkan protokol IPSec merupakan kombinasi yang tepat dalam mengamankan data juga efektif.

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

REFERENCES

[1] Y. Fatma Andriani, M. Fajrian Noor, and A. S. Salim, “INTERNET OF THINGS (IoT)-TANTANGAN DAN KEAMANAN IOT MENGGUNAKAN ENKRIPSI AES,” 2019.

[2] I. Ahmad, M. S. Niazy, R. A. Ziar, and S. Khan, “Survey on IoT: Security threats and applications,” *Journal of Robotics and Control (JRC)*, vol. 2, no. 1. Department of

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

Volume 7, Nomor X, Bulan 2023, Page 999-999
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v5i1.2293

Agribusiness, Universitas Muhammadiyah Yogyakarta, pp. 42–46, Jan. 01, 2021. doi: 10.18196/jrc.2150.

[3] W. Najib, T. Ancaman dan Solusi Keamanan, S. Sulistyo, and K. Kunci, "Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things (Review on Security Threat and Solution of Internet of Things Technology)," 2020.

[4] "Pengembangan dan Penerapan Sistem Virtual Private Network (VPN) pada Internet of Things (IOT) Menggunakan Simulasi".

[5] Vega Augusto, Pradip Bose, and Buyuktosunoglu Alper, *Rugged embedded systems*. Morgan Kaufmann, 2016.

[6] R. M. Arifin, E. Dwi Wardhani, and S. Beta, "Implementasi Tunnel GRE pada Jaringan Ring dan Mesh Perangkat Metro-E Nokia (Implementation of GRE Tunnel on Ring and Mesh Network Nokia Metro-E Devices)," 2021.

[7] D. A. Jakaria, "IMPLEMENTASI FIREWALL DAN WEB FILTERING PADA MIKROTIK ROUTEROS UNTUK MENDUKUNG INTERNET SEHAT DAN AMAN (INSAN)," *JUTEKIN (Jurnal Teknik Informatika)*, vol. 8, no. 2, Nov. 2020, doi: 10.51530/jutekin.v8i2.480.

[8] H. Fiyono, L. A. Syamsul, I. Akbar, and A. S. Rachman, "MONITORING PING REPLY PADA SAAT KEGIATAN INSTALASI JARINGAN ANTENA MENGGUNAKAN SMS GATEWAY INSTALATION OF ANTENNA NETWORK USED PING REPLY MONITORING WITH SMS GATEWAY."

[9] F. Rizqi Nurdiana, I. Gunawan, R. Cahya Viollita, Ma. Faizal, D. Nurcahyadi abcde Teknik informatika, and S. Tinggi Teknologi Ronggolawe Cepu Penulis Korenspondensi, "Analisis Keamanan Jaringan Wifi Menggunakan Wireshark," 2021. [Online]. Available: http://searchsecurity.techtarget.com/tip/Wireshark-tutorial-

[10] P. Thiruvasagam and K. Jijo George, "IPSec: Performance analysis in IPv4 and IPv6," *Journal of ICT Standardization*, vol. 7, no. 1, pp. 59–76, 2019, doi: 10.13052/jicts2245-800X.714.

[11] M. Hasbi and N. R. Saputra, "ANALISIS QUALITY OF SERVICE (QOS) JARINGAN INTERNET KANTOR PUSAT KING BUKOPIN DENGAN MENGGUNAKAN WIRESHARK," 2021. [Online]. Available: https://jurnal.umj.ac.id/index.php/just-it/index

[12] Vanny Andini, Lipur Sugiyanta, and Bachren Zaini, "ANALISIS KINERJA PARAMETER THROUGHPUT DAN DELAY AKSES INETRNET DI SMK KARYAGUNA JAKARTA SELATAN," *PINTER : Jurnal Pendidikan Teknik Informatika dan Komputer*, vol. 4, no. 2, pp. 41–44, Dec. 2020, doi: 10.21009/pinter.4.2.8.

[13] S. Wisnu Pamungkas and E. Pramono, "Analisis Quality of Service (QoS) Pada Jaringan Hotspot SMA Negeri XYZ," 2018.

[14] "ANALISA KEHANDALAN JARINGAN INTERNET DENGAN PENDEKATAN QUALITY OF SERVICE PADA RS. KUSTA DR. RIVAI ABDULLAH PALEMBANG".

[15] H. F. Fakultas, "ANALISIS QOS (QUALITY OF SERVICE) PENGUKURAN DELAY, JITTER, PACKET LOST DAN THROUGHPUT UNTUK MENDAPATKAN KUALITAS KERJA RADIO STREAMING YANG BAIK ANALYSIS QOS (QUALITY OF SERVICE) MEASUREMENT OF DELAY , JITTER, PACKET LOST AND THROUGHPUT TO GET GOOD QUALITY OF RADIO STREAMING WORK," 2018.

[16] IBM, "What is a Security Parameter Index (SPI)?" https://www.ibm.com/support/pages/what-security-parameter-index-spi (accessed Aug. 22, 2023).

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 7, Nomor X, Bulan 2023, Page 999-999
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v5i1.2293

[17] "ANALISIS DAN PERANCANGAN JARINGAN KOMPUTER DENGAN MENGGUNAKAN METODE TOP DOWN".

Submitted: **dd/mm/yyyy**; Accepted: **dd/mm/yyyy**; Published: **dd/mm/yyyy**