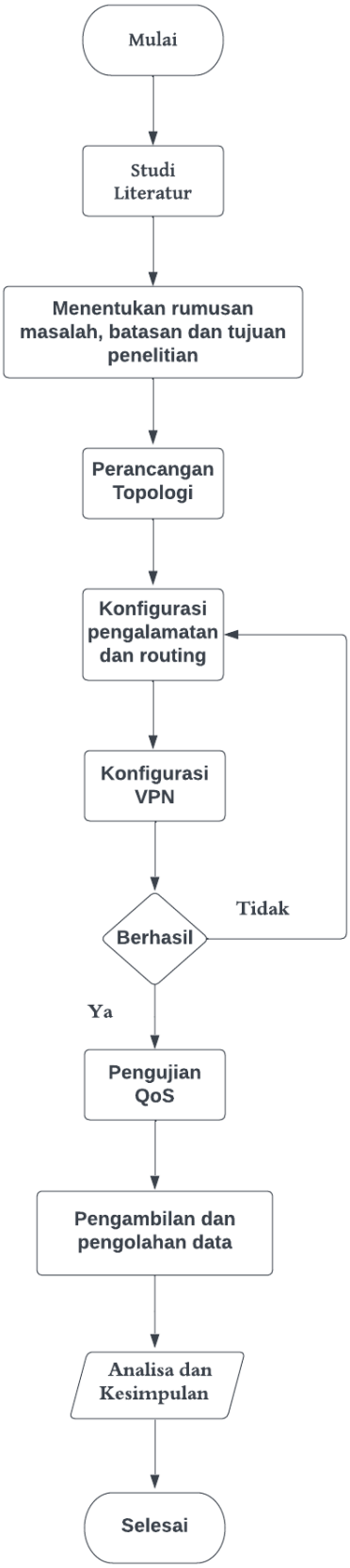
BAB 3
METODE PENELITIAN

3.1 ALUR PENELITIAN

Bagan alur *(flowchart)* pada penelitian dapat terlihat pada gambar 3.1. Penelitian dimulai dengan melakukan studi literatur untuk mendapatkan pengetahuan terkait penelitian yang akan dijalankan. Pengetahuan tersebut dapat mengenai topik permasalahan, perkembangan teknologi, dan penemuan-penemuan terbaru. Kemudian dari studi literatur, peneliti dapat memperoleh gambaran jelas sehingga mampu mengangkat sebuah rumusan masalah yang ada, menetapkan batasan dan tujuannya.

Kemudian dilanjutkan merancang topologi jaringan dan merancang sistem agar dapat membangun sebuah jaringan VPN IPsec dan WireGuard sehingga dapat dilakukan pengujian secara ilmiah. Topologi dan rancangan sistem tersebut kemudian diimplementasikan konfigurasi IP address dan *routing* untuk setiap perangkat. Jaringan yang dibangun kemudian diuji konektivitasnya IP Address nya dengan melakukan ping antar *point-to-point* dan memastikan setiap *router* telah terhubung internet.

Pengujian dilakukan dengan tanpa menggunakan protokol VPN untuk mengetahui performa QoS tanpa protokol VPN. Berikutnya pengujian menggunakan VPN IPsec dan WireGuard pada *router* mikrotik sesuai dengan topologi dan rancangan sistem yang telah dibuat. Apabila konfigurasi kedua VPN IPsec dan WireGuard telah berhasil dijalankan, maka melakukan pengujian QoS. Pengujian tersebut menghasilkan data-data yang kemudian disimpan untuk dianalisis dan diolah lebih lanjut sehingga menghasilkan sebuah pembahasan terhadap penelitian yang dilakukan. Dari hasil analisis dan pembahasan terhadap pengujian yang ada, maka penelitian dapat menarik sebuah kesimpulan yang mengikat keseluruhan proses penelitian.



Gambar 3.1 *Flowchart* Penelitian

3.2 PERSIAPAN PERANGKAT

Untuk mempersiapkan perangkat yang dibutuhkan, diperlukan sistem pendukung yang sesuai dengan kebutuhan dalam menerapkan skema yang akan dibuat. Sistem pendukung tersebut terdiri dari perangkat keras (*hardware*) dan perangkat lunak (*software*). Untuk menjalankan skema tersebut, diperlukan perangkat dengan spesifikasi sebagai berikut:

3.2.1 Spesifikasi *Hardware*

Penelitian ini menggunakan hardware berupa 2 buah PC, 2 buah Mikrotik, dan 4 kabel UTP untuk menghubungkan Miktotik dengan router utama dan Mikrotik dengan PC. Berikut adalah spesifikasi perangkat keras yang akan digunakan untuk melakukan penelitian ini:

Tabel 3.1 Spesifikasi *Hardware*

Hardware	Spesifikasi
Komputer 1	Windows 11, Intel Core i5-10500h 2,50 GHz, RAM 8 GB, SSD 256 GB
Komputer 2	Windows 10, Intel Core i7-7700 CPU 3.60 GHz, RAM 8 GB, HDD 1 TB
Router 1	Mikrotik RB952, *Router* OS 7.9
Router 2	Mikrotik RB952, *Router* OS 7.9

3.2.2 Spesifikasi *Software*

Berikut adalah spesifikasi perangkat lunak yang akan digunakan untuk melakukan penelitian ini:

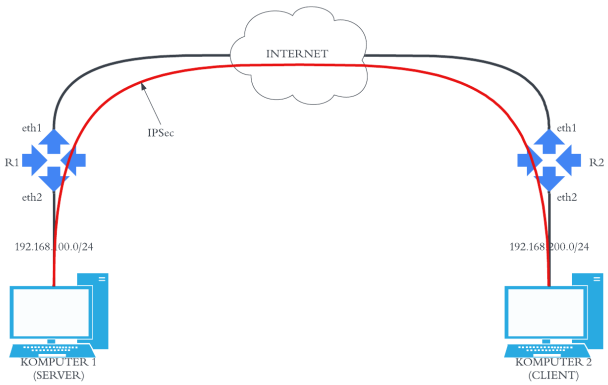
Tabel 3.2 *Software* yang Digunakan

Software	Versi	Fungsi
Winbox	3.3.7	Kontrol akses *router* mikrotik
Nping (Nmap)	7.94	Pengambilan data latensi, *jitter*, dan *packet loss*
JPerf	2.0.2	Pengambilan data *throughput*

Software	Versi	Fungsi
FileZilla Server	1.7.0	Pengujian jaringan VPN pada mekanisme transfer file
FileZilla *Client*	3.64.0	Pengujian jaringan VPN pada mekanisme transfer file.
Wireshark	4.0.5	Pengambilan *capture* data pada interface laptop.

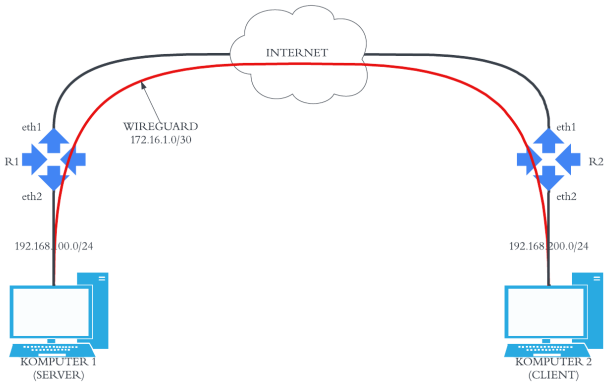
3.3 PERANCANGAN TOPOLOGI JARINGAN

Topologi jaringan adalah suatu penentuan mengenai bagaimana struktur jaringan yang cocok untuk sistem yang sedang dikembangkan. Hal ini bertujuan agar dapat memberikan gambaran yang jelas mengenai sistem yang akan dibangun. Jaringan VPN merupakan sebuah mekanisme yang menghubungkan dua jaringan secara privat melalui jaringan publik. Pada topologi jaringan yang ditampilkan pada gambar 3.2 terdapat 2 PC yang berfungsi yaitu komputer 1 berfungsi sebagai *server* kemudian komputer 2 berfungsi sebagai *client*, terdapat juga 2 *router* yang memiliki fungsi masing-masing. *Router* R1 dan R2 merupakan *router* yang akan menjalankan protokol IPsec. Kemudian jaringan lab untuk merepresentasikan jaringan publik internet, yang mana dengan internet jaringan publik tersebut akan menghubungkan R1 dan R2. Pada jaringan VPN IPsec yang terbentuk untuk koneksi *peer*ing tidak memiliki IP *point-to-point*. Mekanisme enkripsi pada jaringan IPsec yakni pada fase pembentukan *peer* dan pengiriman data



Gambar 3.2 Topologi Jaringan IPsec

Kemudian pada gambar 3.3 adalah topologi jaringan untuk menerapkan jaringan VPN WireGuard. Router R1 sebagai VPN host yang kemudian akan diterima oleh router R2 sebagai VPN host juga. Kedua VPN pada router tersebut akan membentuk *direct peering* satu sama lain dengan menggunakan sebuah interface WireGuard yang telah terbentuk. Internet sebagai representasi dari jaringan publik. Untuk perangkat router dan komputer dibuat identik agar menghindari terdapat sesuatu hal diluar perancangan. Mekanisme enkripsi pada WireGuard adalah dengan mengunci *peer* menggunakan *public key* berdasarkan kode enkripsi MD5.



Gambar 3.3 Topologi Jaringan WireGuard

Tabel 3.3 Pengalamatan IP *Address*

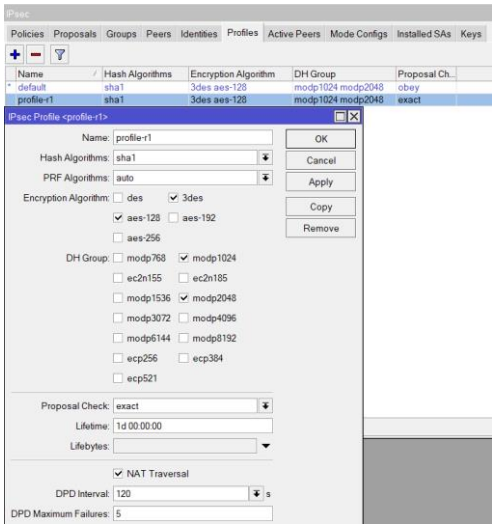
Perangkat	***Interface***	**IP *Address***
Komputer 1	ether	192.168.100.254
Komputer 2	ether	192.168.200.254
R1	Ether1	10.212.16.67/23
	Ether2	192.168.100.1/24
	IPsec	-
	WireGuard	172.16.1.1/30
R2	Ether1	10.212.16.68/23
	Ether2	192.168.200.1/24
	IPsec	-
	WireGuard	172.16.1.2/30

3.4 KONFIGURASI IPSEC

Untuk menghubungkan dua jaringan lokal pada *site* yang berbeda, digunakan *tunneling* VPN menggunakan protokol IPsec. Tahapan dalam melakukan konfigurasi IPsec adalah:

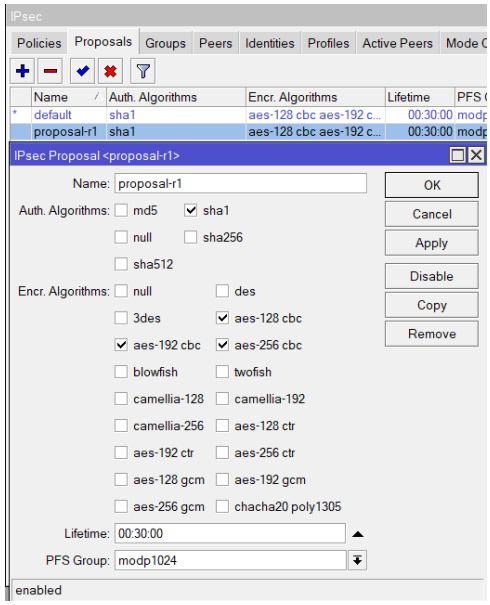
1) Konfigurasi pada R1

Pertama adalah melakukan konfigurasi pada *router* R1. Dalam konfigurasi IPsec dalam Mikrotik, langkah pertama adalah pembuatan *profile* dan proposal. *Profile* mendefinisikan berbagai set parameter yang digunakan untuk negosiasi IKE fase 1. Sedangkan untuk proposal berisi informasi yang akan dikirimkan ke daemon IKE untuk membentuk SA untuk kebijakan tertentu.



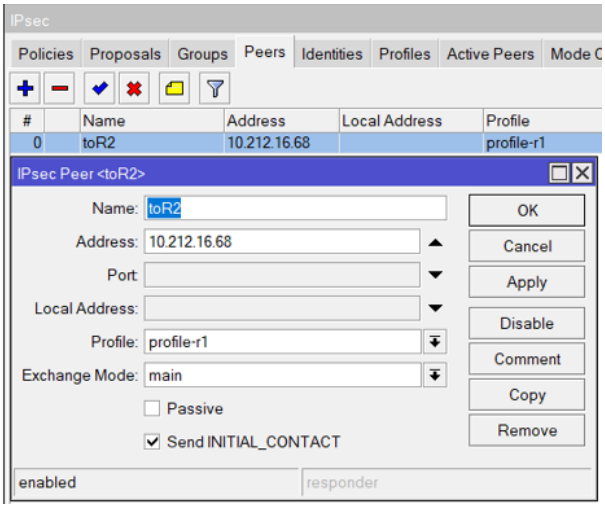
Gambar 3.4 Konfigurasi IPsec *Profile* Pada R1

Pada Gambar 3.4, diperlihatkan bahwa algoritma enkripsi yang dipilih dan digunakan dalam sistem tersebut adalah AES-128 dan 3DES. Kedua algoritma ini memiliki keunggulan dan keamanan masing-masing dalam melakukan enkripsi data. Selain itu, untuk menjamin keamanan pertukaran kunci, konfigurasi DH (Diffie-Hellman) Group yang diterapkan menggunakan dua jenis modulasi, yaitu modp1024 dan modp2048. Hal ini dilakukan untuk memberikan fleksibilitas dalam pemilihan tingkat keamanan yang diinginkan. Terakhir, adanya Checklist NAT (Network Address Translation) Traversal memiliki tujuan khusus, yaitu memastikan bahwa router VPN yang telah dikonfigurasi dengan fitur NAT dapat berfungsi dengan baik dan kompatibel saat digunakan bersamaan dengan teknologi VPN berbasis IPsec. Dengan demikian, komunikasi antar jaringan dapat berjalan lancar tanpa hambatan.



Gambar 3.5 Konfigurasi IPsec Proposal Pada R1

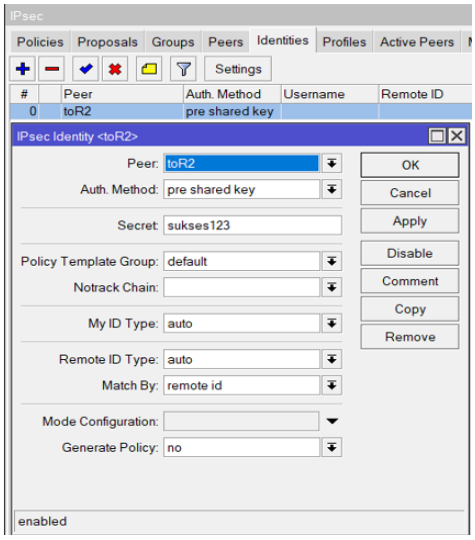
Pada gambar 3.5 adalah konfigurasi untuk proposal yang mana untuk algoritma autentikasi nya menggunakan sha1 dan algoritma enkripsinya menggunakan aes-128 cbc, aes-192 cbc dan aes-256 cbc. *Lifetime* disini berarti koneksi proposal akan terus dijaga selama 30 menit.



Gambar 3.6 Konfigurasi *Peers*

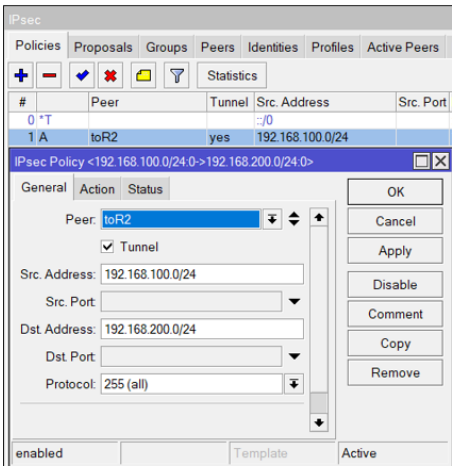
Kemudian selanjutnya adalah pembuatan *peer* yang terdokumentasi pada gambar 3.6 Konfigurasi *peer* bertujuan untuk membentuk koneksi antar daemon IKE. Lebih sederhananya bahwa *peer* ini menetapkan koneksi VPN pada R2. Pencantuman alamat IP pada *peer* merupakan IP Publik dari R2

(yakni 192.168.1.22). (Pada IP Publik menggunakan IP *Private* 192.168.1.0/24).



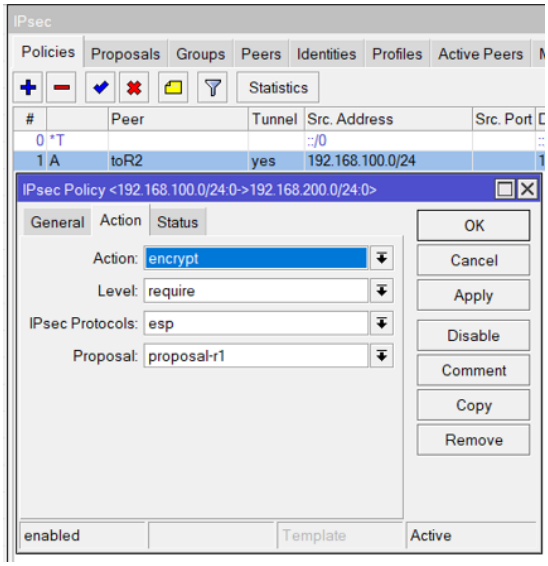
Gambar 3.7 Konfigurasi *Identities* Pada R1

Kemudian melakukan konfigurasi *policies* terhadap *peer* yang telah disetting. Konfigurasi *policies* menyangkut alamat *source address* dan *dst address. Source address* pada R1 adalah alamat IP distribusi R1 (yakni 192.168.100.0/24). Sedangkan pada R2 adalah alamat IP distribusi R2 (yakni 192.168.200.0.24).



Gambar 3.8 Konfigurasi *Policies* Pada R1

Kemudian pada *policies*, disetting *action*=encrypt, proposal adalah settingan proposal1, kemudian untuk kolom yang lain dibiarkan default.



Gambar 3.9 Konfigurasi *Action* Pada *Policies* R1

2) Konfigurasi pada R2

Untuk konfigurasi pada R2, untuk pembuatan IPsec *profile* dan proposal serupa dengan R1. Kemudian untuk pembuatan *peer* ke R1, dilakukan konfigurasi seperti pada konfigurasi R1. Pencantuman IP 192.168.1.21 merupakan IP Publik dari *Router* R1. Kemudian untuk konfigurasi Identity R2, serupa dengan konfigurasi IPsec pada R1. Untuk *secret* disamakan yakni "sukses123". Dengan menset *peer* sama dengan "to-R1". Kemudian konfigurasi IPsec *policies* pada R2. Untuk *source address* merupakan IP *Address* distribusi yang dimiliki oleh R2, sedangkan *dst address* adalah IP *Address* distribusi yang dimiliki oleh R1. Penetapan alamat *source address* dan *dst address* untuk mendefinisikan IP Distribusi mana saja yang dapat dipertukarkan melalui jaringan VPN IPsec.

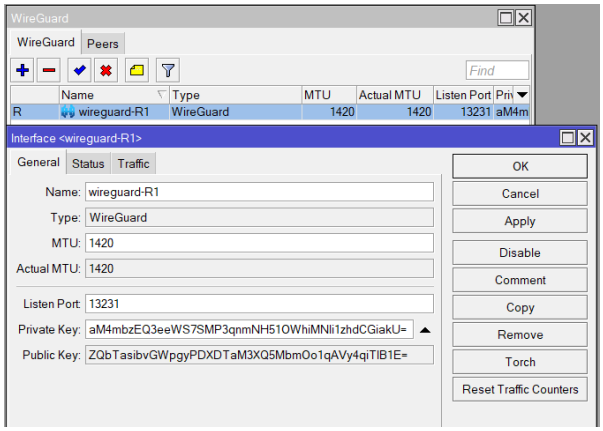
3.5 KONFIGURASI WIREGUARD

Untuk menghubungkan dua jaringan lokal pada *site* yang berbeda, digunakan *tunneling* VPN menggunakan protokol WireGuard. Tahapan dalam melakukan konfigurasi WireGuard adalah:

1) Konfigurasi pada R1

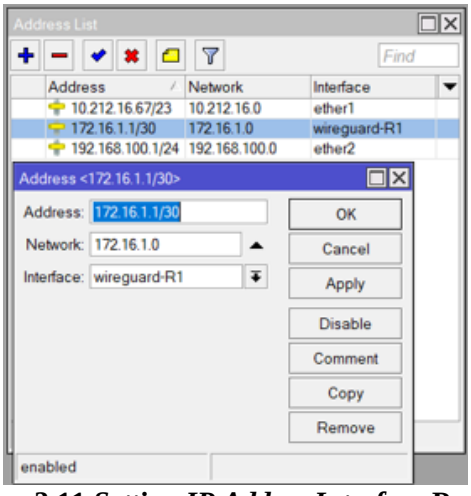
Pada menu di *route* R1, klik add *interface*. Untuk parameter *listen port* secara default adalah 13231. Untuk pengujian VPN port akan dibiarkan *default*.

Kemudian untuk R2 langkah pembuatan *interface* sama dengan untuk R1. Apabila sudah di-*apply*, maka pembuatan *interface* akan me-generate *private key* dan *public key* yang berbeda antara R1 dan R2. Kemudian lakukan konfigurasi IP *Address* untuk VPN untuk R1 dengan IP 172.16.1.1/30 dan R2 dengan IP 172.16.1.2/30.



Gambar 3.10 Konfigurasi *Interface* Pada Mikrotik

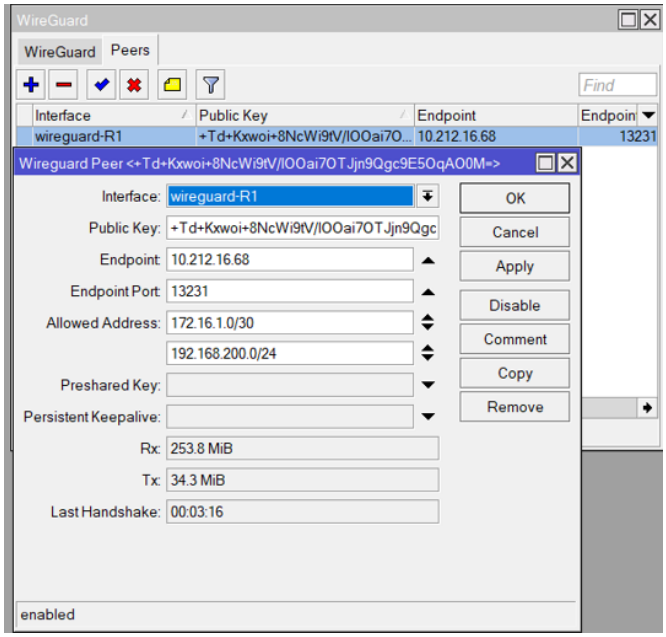
Apabila sudah diapply, maka pembuatan *interface* akan me-generate *private key* dan *public key* yang berbeda antara R1 dan R2. Kemudian lakukan konfigurasi IP *Address* untuk VPN untuk R1 dengan IP 172.16.1.1/30 dan R2 dengan IP 172.16.1.2/30.



Gambar 3.11 *Setting IP Addres Interface* Pada R1

Agar VPN antar *router* Mikrotik R1 dan R2 dapat terjalin maka perlu dilakukan konfigurasi *peer* pada setiap *router*. Konfigurasi *peer* memerlukan

public key dari *router* pasangannya. Untuk pertama melakukan konfigurasi *peer* pada R1. Parameter *public key* pada R1 diisikan *public key* yang ter-generate pada R2. Kemudian untuk *Endpoint* adalah alamat IP Publik dari R2 yakni 192.168.1.22. *Endpoint* port adalah port pada R2 yakni 13231. Untuk alamat yang dizinkan (*allowed address*), kita isi alamat LAN distribusi R2 yakni 192.168.200.0/24 dan alamat *peer*ing yakni 172.16.1.0/30. Kemudian untuk konfigurasi pada R2 serupa dengan langkah-langkah pada R1. Untuk *public*k *key* pada *peer* diisikan *public key interface* R1. Untuk *endpoint* diisikan IP *Public* dari R1 yakni 192.168.1.21. Kemudian untuk *endpoint* port nya adalah 13231 yang merupakan port R1. Untuk *Allowed Address* diisikan alamat IP *Address* jaringan distribusi LAN R1 yakni 192.168.100.0/24 dan alamat *peer*ing yakni 172.16.1.0/30.



Gambar 3.12 Konfigurasi Peers Pada R1

Dari kedua konfigurasi tersebut, maka *tunnelling* sudah terbentuk. Untuk pembuktiannya dapat melakukan *ping* dari R1 ke R2 menggunakan IP *Peer*ing *router* berlawanan dan menggunakan IP *address* dari LAN Distribusi R2. Terlihat bahwa untuk IP *Peer*ing sudah dapat dilakukan *Ping* pada R1, namun pada LAN Distribusi R2 belum dapat dilakukan.

Gambar 3.13 Static Route Pada R1

Sehingga untuk pengujian *ping* terhadap LAN distribusi R2 pada R1, dapat dilakukan. Terlihat R1 dapat melakukan *ping* ke 192.169.200.1 menggunakan source *address* 172.16.1.1. Pada *router* Mikrotik R2 juga perlu ditambahkan *static route* untuk mengenalkan jaringan 192.168.100.0/24 (LAN Distribusi R1) melalui *interface* 1. Jikalau melakukan *ping* pada R2 yakni dengan IP tujuan 192.168.100.1 dan source *address*nya adalah 172.16.1.2, maka *ping* dapat dilakukan. Pada *router* Mikrotik R2 juga perlu ditambahkan *static route* untuk mengenalkan jaringan 192.168.100.0/24 (LAN Distribusi R1) melalui *interface* 1. Jikalau melakukan *ping* pada R2 yakni dengan IP tujuan 192.168.100.1 dan source *address*nya adalah 172.16.1.2, maka *ping* dapat dilakukan.

2) Konfigurasi pada *Site* B kurang lebih sama dengan konfigurasi pada *Site* A, yang membedakan adalah *rules* yang dipakai dalam *router* ini.

3.6 SKENARIO PENGAMBILAN DATA

Tahap selanjutnya adalah pengambilan data, dimana data yang dibutuhkan pada penelitian ini adalah *throughput*, *delay*, *jitter* dan *packet loss*.

1) Prngambilan dan pengolahan parameter *delay* dan *packet loss* menggunakan tools Nping

   Parameter data *delay, jitter,* dan *packet loss* akan diambil menggunakan aplikasi Nping. Aplikasi Nping merupakan aplikasi yang termasuk pada tools

Nmap. Nping dapat melakukan ping secara *advanced* karena dapat mengatur interval, size, dan waktu.

Gambar 3.14 Mekanisme Penggunaan Aplikasi Nping

Gambar 3.14 menunjukan mekanisme pengambilan data yakni Komputer 1 dan Komputer 2 akan dipasang aplikasi Nping. Kemudian akan dilakukan ping dari Komputer 1 ke Komputer 2 dan sebaliknya sesuai dengan variabel interval, size dan waktu yang telah ditentukan pada jaringan menggunakan VPN IPsec dan VPN WireGuard. Pengujian akan dilakukan dengan beberapa variabel tersebut seperti pada tabel 3.4.

Tabel 3.4 Skenario Pengujian

VPN	*Interval*	*Size*	*Count*
IPsec /WireGuard	150 ms	512/1024/2048/4096 B	100/300/500
	50 ms	512/1024/2048/4096 B	100/300/500
	1 ms	512/1024/2048/4096 B	100/300/500
	0,5ms	512/1024/2048/4096 B	100/300/500

2) Pengambilan dan pengolahan data *throughput* menggunakan Jperf

Parameter data *throughput* akan diambil menggunakan aplikasi Jperf. Aplikasi tersebut berfungsi untuk melakukan *bandwidth test* dari sisi *server* ke *client* dengan cara me-*generate traffic*. Pada JPerf terdapat berbagai pengaturan yang dipakai untuk yakni dapat menggunakan protokol TCP/UDP, *bitrate*, *size*, hingga periode waktu pengetesan. Pengujian akan dilakukan menggunakan VPN IPsec dan WireGuard.

Gambar 3.15 Mekanisme Penggunaan Aplikasi Jperf

Gambar 3.15 menunjukan mekanisme pengambilan data yakni Komputer 1 dan Komputer 2 akan dipasang aplikasi Jperf. Jperf pada Komputer 1 akan sebagai *server* yang akan me-*generate traffic* dengan port tertentu. Jperf pada Komputer 2 sebagai *client* yang akan menerima *traffic* dari Komputer 1 pada port yang telah ditentukan. Sebagai catatan bahwa mikrotik pengujian untuk setiap port interface hanya mendukung 100 Mbps, sehingga untuk *data rate* dikonfigurasi di bawah 100 Mbps. Pengujian pada Jperf akan menggunakan protokol TCP dan UDP. Pengujian akan dilaksanakan dengan beberapa variabel seperti pada tabel 3.5.

Tabel 3.5 Skenario Pengujian

VPN	**Protokol**	***Paralel Stream* (Sisi Client)**	**Waktu**
IPsec /WireGuard	TCP/UDP	1/5/10	10/30/60 detik
		1/5/10	10/30/60 detik
		1/5/10	10/30/60 detik

3) Pengambilan dan pengolahan data *jitter* menggunakan wireshark dan filezilla
Parameter data *jitter* akan diambil menggunakan aplikasi wireshark dan filezilla. Aplikasi filezilla server (ftp server) akan terpasang pada komputer 1 dan filezilla client (ftp client) akan terpasang pada komputer 2. Hasil dari pengujian tersebut kemudian akan diujikan berdasarkan parameter *jitter*. Pada sisi komputer 1 akan dijalankan aplikasi wireshark yang berfungsi untuk meng-*capture* paket data ftp yang diterima dari interface ethernet komputer terdapat pada gambar 3.16.

Gambar 3.16 Mekanisme Penggunaan Aplikasi FileZilla