IMPLEMENTASI *BACKBONE NETWORK SECURITY SISTEM* MENGGUNAKAN JARINGAN VPN PADA KOMUNIKASI *HYBRID* CIGRA D5 BERBASIS *WIREGUARD*

M tri saiful ulum [1)] imam ashar[2)]
[1)]Prodi Teknik Komunikasi Militer, Politeknik Angkatan Darat Jl. Raya Anggrek No.1 Junrejo, Batu, Indonesia
[2)] Sdirbindikjar Poltekad Kodiklatad
E - mail :[1)] sulum007@gmail.com, [2)]imamasharstmt@gmail.com

IMPLEMENTATION OF BACKBONE NETWORK SECURITY SYSTEM USING VPN IN HYBRID COMMUNICATION CIGRA D5-BASED WIREGUARD

Abstract: *The backbone network is the absolute path of a high-speed network because it uses fiber optics, so it often to connect local networks. The backbone network security site is also known as the data security process, so this method can be recommended for implementation in military communications systems. However, on the other hand, this network disconnection has a broad impact on connection disruptions in the areas served, therefore it is necessary to be equipped with a VPN (Virtual Private Network) for organized communication between devices and networks located in remote locations. In essence, a device is needed that has backbone network security features, which can be found in the Internet of Things system, IoT is a system that can transfer data using a Wi-Fi network so that it has an automatic system in the system.*
Keywords: *Backbone, Virtual Private Network, Internet of Things*

Abstrak: *Jaringan backbone merupakan lintasan mutlak suatu jaringan yang berkecepatan tinggi karena menggunakan fiber optic, sehingga kerap digunakan untuk menghubungkan antar jaringan local. Sistem keamanan jaringan backbone pun dikenal dengan proses pengamanan data, sehingga metode ini dapat dianjurkan untuk implementasikan pada sistem komunikasi di bidang militer. Namun disisi lain terputusnya jaringan ini berdampak luas akan gangguan koneksi pada wilayah yang dilayani, maka dari itu perlu dilengkapi dengan VPN (Virtual Private Network) guna penghubung koneksi yang terorganisir antar perangkat dengan jaringan yang berada di lokasi jauh. Pada intinya, diperlukan suatu device yang memiliki fitur keamanan jaringan backbone, yang mana hal tersebut dapat ditemui pada sistem Internet of Things. IoT merupakan sistem yang memiliki kemampuan mentransfer data dengan jaringan Wi-Fi sehingga memiliki sistem otomatis pada sistem.*
Kata kunci: Backbone, Virtual Private Network, Internet of Things

PENDAHULUAN

Bidang teknologi komunikasi instansi militer kini Tengah berfokus pada optimalisasi perangkat komunikasi yang bertujuan untuk tugas perang maupun bukan. Strategi pertahanan serta mencakup sistem

pecegahan pembobolan dan pencurian data menjadi tujuan utama dari sektor kounikasi militer saat ini. Mengatasi permasalahan tersebut diperlukan metode dalam prosesnya, penelitian ini menyarankan sistem keamanan jaringan backbone (Yamato,2021). Jaringan backbone merupakan koneksi dengan kecepatan tinggi yang menjadi jalur utama dan bertujuan mengatasi kecepatan interkoneksi jaringan local. Kecepatan tinggi pada jaringan bacxkbone diperoleh dari fiber optic.

Namun, apabila jarinagn koneksi terputus akan berdapak pada wilayah yang dilayani, maka dari itu VPN (Virtual Private Network) dapat menajdi terobosan bagi permasalahn tersebut. VPN merupakan sistem teknologi yang digunakan untuk melakukan komunikasi keamanan data dan keterttutupan transmisi data dari akses yang tidak berhak dalam transmisinya, serta dilengkapi dengan fitur enkrispsi dan tunnelling (Sari, 2020).

Berdasarkan permasalahan yang telah dipaparkan, maka diperlukan device yang menunjang jaringan backbone, yang mana kini sistem IoT (Internet of Things) dapat menjadi salah satu Solusi. Internet of Things sendiri memiliki keunggulan dalam transmisi data melalui jaringan Wi-Fi, dan bertujuan memperluas konektivitas internet secara berkelanjutan. Terlebih, sistem IoT memiliki karakteristik otomatisasi yang memeprmudah kinerja manusia.

Berdasarkan dari latar belakang tersebut, maka dirumuskan beberapa permasalahan berikut: (hanya intinya saja)

1. Bagaimana implementasi sistem keamanan jaringan backbone terintegrasi dengan teknologi VPN?
2. Bagaimana server radio cigra hybrid D5 mampu memonitor *throughput, packet loss* dan *delay*?
3. Bagaimana server radio cighra hybrid D5 mampu mengirimkan notifikasi kepada operator apabila terjadi gangguan?

Pembahasan ini diharapakn pula lebih terarah sesuai dengan topik bahasan, maka dari itu diterapkan batasan permasalahan yang akan dibahas, yakni:

1. Membahas VPN berbasis Wireguard dalam mengatur akses user pada server.
2. Pada proses komunikasi membahas monitoring *throughput, packet loss,* dan *delay.*
3. Tidak membahas mekanika dari radio, interface, *gateway* serta komponen server.

Pembuatan tugas akhir ini juga harus mempunyai tujuan yang harus dicapai agar didalam pembuatannya menghasilkan suatu pencapaian yang maksimal. Tujuan penelitian dalam tugas akhir ini antara lain:

1. Untuk membuktikan sistem keamanan jaringan *backbone* yang telah terintegrasi VPN
2. Mendapatkan informasi yang ada pada server radio cighra *hybrid* D5 dan user berupa data *throughput, packet loss,* dan *delay.*
3. Untuk membuktikan server dapat mengirimkan notification ke operator apabila server mengalami *overload*.

digunakan pada "Implementasi *Backbone Network Security sistem* menggunakan jaringan VPN pada komunikasi *Hybrid* Cigra D5 Berbaiss *Wireguard*" sangat diperlukan untuk menciptakan sistem keamanan yang memiliki Tingkat keamanan yang memumpuni untuk mencegah kebocoran data sehingga komukasi berlangsung aman dan lancar, dan berpotensi untuk diaplikasikan pada sistem komunikasi jaringan di bidang militer.

METODE PENELITIAN

Penelitian ini menggunakan metode kuantitatif, hal tersebut untuk mengatasi gangguan pada kemampuas komunikasi,

Penelitian ini dilakukan di Laboratorium dan bengkel Telekomunikasi Poltekad Kodiklatad yang beralamatkan di jalan Anggrek Desa Pendem

Kecamatan Junrejo Kota Batu Jawa Timur. Atokası waktu yang di gunakan

untuk melakukan penelitian ini selama 10 bulan, yang di mulai dari bulan

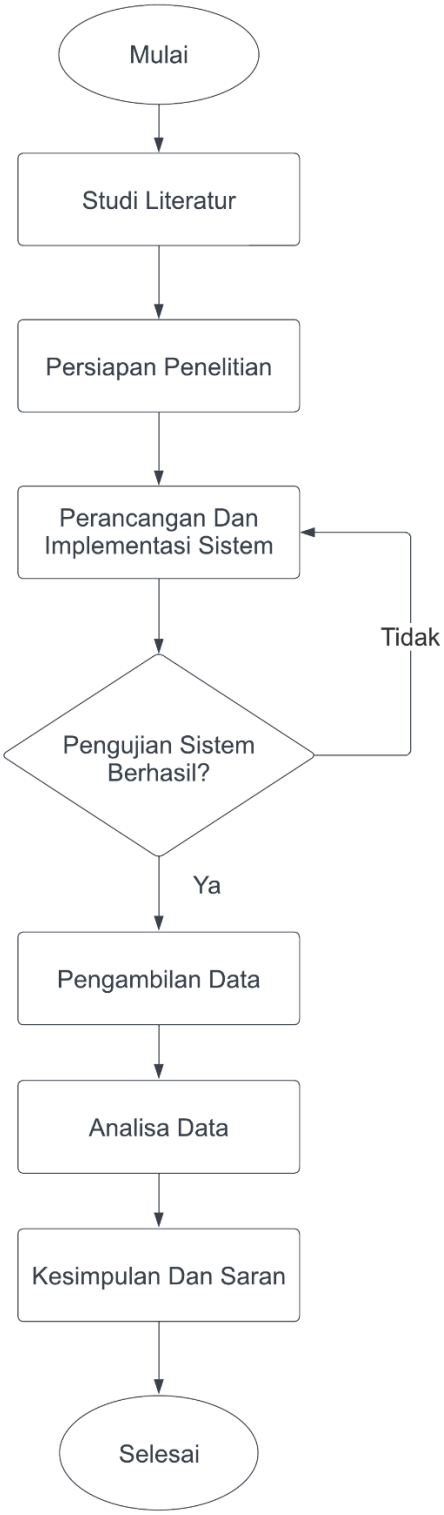
Agustus 2023 sampai dengan Mei 2024 Dengan rincian sebagat benkut.

a. Pengumpulan data dilaksanakan pada bulan Agustus 2023
b. Pembuatan Proposal dilaksanakan pada bulan Agustus 2023
c. Seminar Proposal dilaksanakan pada bulan Agustus 2023
d. Proses Bimbingan dilaksanakan pada bulan September 2023 September 2023 sarpai dengan Mei 2024
e. Pembuatan alat dilaksanakan pada bulan Januan sampai dengan April 2024
f. Pengambilan data akhir dilaksanakan pada bulan April sampai denqan Mei 2024
g. Seminar hasil dilaksanakan pada bulan Mei 2024
h. Sidang Tugas Akhir dilaksanakan pada bulan Juni 2024
i. Perbaikan naska dilaksanakan pada bulan Juni 2024

Variabel Bebas

1. Internet Protocol (IP)
2. SSH (Secure Shell) Protocol
3. Protocol SIP

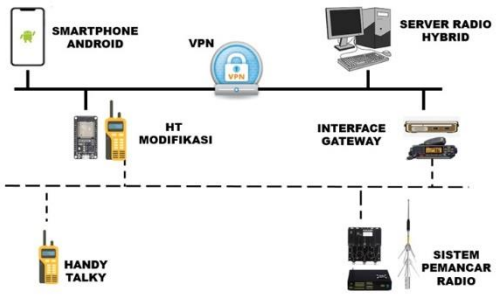
Diagram alir penelitian ditampilkan pada Gambar 1



Gambar 1. Diagram alir

Diagram alir tersebut menjabarkan tahapan penelitian mulai dari studi literatur yang bertujuan memperoleh landasan teori dan refrensi pendukung penelitian, kemudian menyiapkan alat dan bahan serta komponen yang diperlukan dan dirancang, kemudian mengimplementasikan sistem. Setelah sistem berjalan lancer, amak data diambil dan dianalisis agar mengahsilkan kesimpulan. Berdasarkan kesimpulan yang diperoleh maka terbentukalah saran sebagai bentuk evaluasi agar penelitian kedepannya memperoleh hasil yang lebih baik

Perancangan sistem measuring frame yang diusulkan peneliti dapat dilihat pada Gambar 2



Gambar 2. Perancangan sistem

Gambar 2 merupakan blok diagram sistem komunikasi yang menjabarkan konsep komunikasi Radio Hybrid. Pertama, dimulai dari input suara yang masuk ke microphone radio kemudian diterima oleh sinyal penerima antena yakni 458.025.000 MHz. Selanjutnya masuk ke duplexer dan diolah agar dapat melewati sinyal kecil yang diterima dari antena ke repeater.

Pada rangkaian *interface* berfungsi merubah frekuensi digital menjadi analog maupun sebaliknya. Konsep kerjanya adalah jika server mengeluarkan audio maka port akan menerima data yang menggerakkan relay sehingga membuat radio rig berfungsi seperti *repeater* karena memancarkan Kembali audio yang diterima dari server.

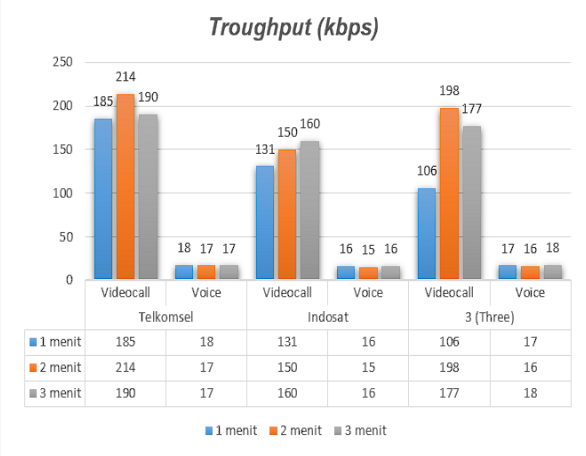
HASIL DAN PEMBAHASAN

Pada tahap ini akan ditampilkan hasil dari penerapan sistem jaringan wireguard yang di buat sebelumnya.

Selanjutnya penulis akan melakukan pengujian pada sistem untuk mengakses sistem pada jaringan komunikasi radio *hybrid* cigra D5 yaitu pengujian data *troughput, packet loss*, dan *delay*.

Pada tahap ini dari peneliti melakukan pengujian sebanyak 3 kali dengan menggunakan provider yang berbeda pengujian dengan provider telkomsel, indosat, dan 3 (three). Aplikasi yang digunakan adalah *wireshark*. Sehingga memperoleh hasil berikut :

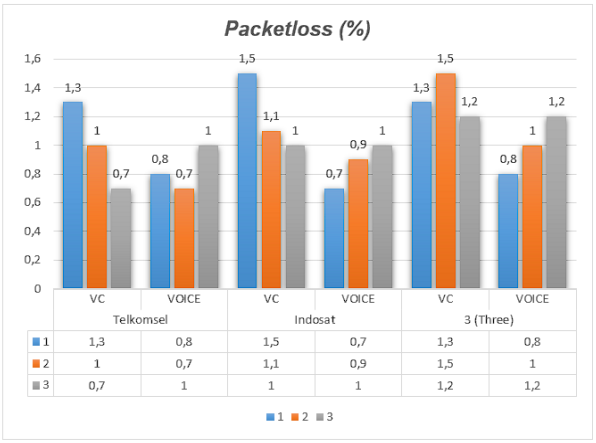
1. Pengujian *throughput* (kbps).



Gambar 2. *Throughput*

Data hasil *throughput* pada komunikasi memperoleh rata-rata pada pagi hari sebesar 17.8 kbps, rata-rata pada siang hari sebesar 17.3 kbps, dan rata-rata dimalam hari sebesar 15.7 kbps. Hal ini menunjukan bahwa komunkasi yang dilakukan pada pagi hari lebih efektif dibandingkan pada siang hari ataupun malam hari.

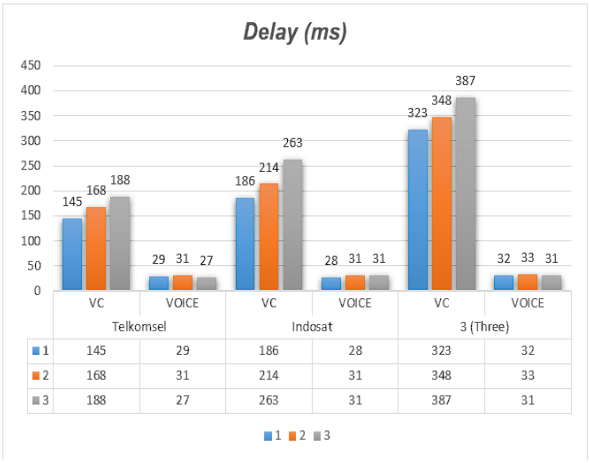
2. *Packet loss*



Gambar 2.*Packet loss*

Data hasil pengujian *packet loss* pada komunikasi memperoleh rata-rata pada pagi hari sebesar 0.79%, rata-rata pada siang hari sebesar 0.9 %, dan rata-rata pada malam hari sebesar 1.05 %. Hasil percobaan tersebut membuktikan bahwa komunikasi yang dilakukan pada pagi hari menghasilkan *packet loss* lebih kecil daripada komunikasi yang dilakukan di siang hari atau pada malam hari.

3. *Delay*



Gambar 4. *Delay*

Data hasil pengujian *delay* pada komunikasi memperoleh rata-rata pada pagi hari sebesar 339 ms, rata-rata pada siang hari sebesar 399 ms, dan pada malam hari memperoleh rata-rata 420 ms. Hasil tersebut menunjukan bahwa komunikasi yang dilakukan pada pagi

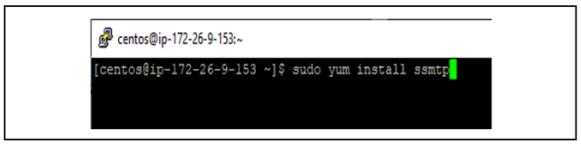
memperoleh delay yang lebih kecil dibandingkan dengan komunikasi yang dilakukan pada siang ataupun malam hari.

Pembahasan Notifikasi Zabbix

Selanjutnya peneliti akan melakukan pembahasan tentang kinerja *server dengan menggunakan Zabbix*.

Pada tahap ini akan dilaksanakan beberapa Langkah diantaranya:

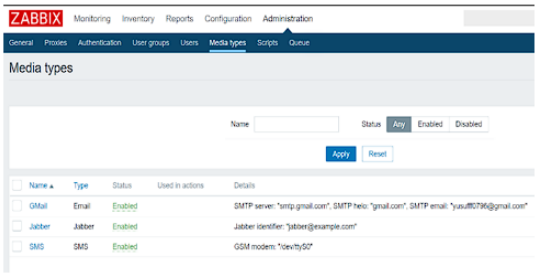
1. Install ssmpt pada *centos server* yang digunakan.



Gambar 5. Ssmpt

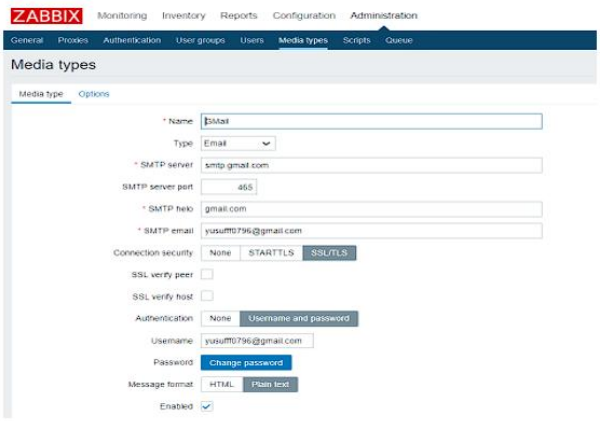
Pemasangan ssmtp berfungsi sebagai pembantu proses pengiriman surat elektronik lebih cepat, mudah dan terjaga kerahasiaannya

2. *Media Types*



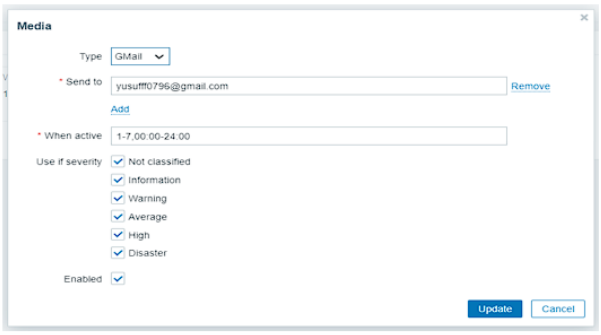
Gambar 6. Media types

Selanjutnya membuka media type dengan masuk ke *Zabbix* dan pilih administration kemudian pilih media types langkah selanjutnya yaitu memastikan *e-mail* yang tadi sudah di inputkan sudah masuk ke dalam tabel. Jika belum ada maka bisa menambahkannya dengan cara pengaturan seperti gambar dibawah



Gambar 7. Pengisian Form

3. *Edit User Profile*



Gambar 8. *Edit User Profil*

selanjutnya yaitu menambahkan *e-mail* pada user dengan cara membuka tab media. Pada tab media ini operator dapat memilih type dari *e-mail*. Disini peneliti menggunakan type gmail. Selain itu operator juga bisa menambahkan kepada siapa saja notifikasi tersebut dapat dikirimkan. Kemudian operator juga bisa mengatur kapan notifikasi ini diaktifkan dan kapan notifikasi ini dimatikan. Setelah selesai melakukan konfigurasi pada profil, maka semua proses konfigurasi sudah selesai. *Zabbix* akan melakukan perintah sesuai dengan konfigurasi yang telah dibuat Semua masalah yang terjadi pada host tersebut akan otomatis terkirim notifikasinya melalui *e-mail*. Untuk melakukan pengujian peneliti membuat triger masalah seperti melakukan *shutdown* pada host yang dimonitor. Sehingga, *Zabbix* akan menganggap bahwa *host* tersebut mati sehingga notifikasi masalah.

Kesimpulan

Berdasarkan pengimplementasian alat ini dapat disimpulkan bahwa system yang telah di buat mampu untuk di akses, membatasi hak akses, dan mampu berjalan dengan baik begitu juga dengan percobaan menggunakan aplikasi *wireshark* dan dapat diketahui perbandingan *throughput, packet loss,* dan *delay* dengan menggunakan tiga provider yang berbeda. Saran dari peneliti untuk penelitian selanjutnya adalah perlu dilakukan pembaruan menggunakan fitur VPN yang baru agar system keamanan pada server radio hybrid cigra D5 dapat mengikuti perkembangan teknologi sehingga keamanan dan kinerja pada server dapat berjalan dengan lebih optimal.

DAFTAR PUSTAKA

A. I. A. Rifa., Firdaus., I. Eka., N. Ida. 2017. Perancangan Jaringan Backbone Dan Distribusi 4G LTE Di Sleman Berbasis Jaringan Optik. Yogyakarta. Indonesia.

Jasa Lie. 2017. Modifikasi Handy Talky (HT) Sebagai Telealarm Pengaman Benda-Benda Suci Pratiam Di Pura Dari Tindakan Pencurian. Bali. Indonesia.

P. A. Fajar., P. Agus., D. A. Eko. 2018. Optimalisasi Jaringan Menggunakan Firewall. Jawa Barat. Indonesia.

E. Yoyon. 2018. Internet of Things (IoT) Sistem Pengendalian Lampu Menggunakan Raspberry PI Berbasis Mobile. Riau. Indonesia.

H. Yasdinul., Adri. M., A. Yoharmen. Perancangan Aplikasi Client Untuk Jaringan VOIP (Voice Over Internet Protocol) Berbasis Arduino. Sumatera Barat. Indonesia.

A. Abbyzar., N. Wahyu. F. 2019. Pola Komunikasi Militer Dalam Program Swasembada Pangan Di Wiliyah Koramil 1607/-01 Sumbawa. Sumbawa. Indonesia.

W. B. Fajar., S. R. S. Rummi. 2019. Perancangam Sistem Monitoring Suhu Ruangan Menggunakan Handy Talkie. Jakarta. Indonesia.

D. Sari., R. Fajar., S. Tika., H. Noer. 2020. Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point to Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis.

S. S. Hanhan., B. P. M. Imam., G. K. Petrus. 2020. Analisa Performansi Jaringan Kabel Fiber Optik Link Backbone Ungaran-Krapyak. Purwokerto. Indonesia.

M. Alexander., G. Christina. 2021. A WireGuard Exploration. West Lafayette. USA.

Yamato., A. Nurul. F., M. Achmad. 2021