# 1. PENDAHULUAN

## 1.1 Latar Belakang Masalah

Dalam era digital yang terus berkembang, perusahaan-perusahaan di seluruh dunia semakin bergantung pada infrastruktur teknologi informasi yang canggih untuk mendukung operasi bisnis mereka. Khususnya, bagi perusahaan dengan beberapa cabang atau lokasi yang tersebar, memiliki infrastruktur TI yang handal dan terintegrasi menjadi suatu keharusan. Infrastruktur TI multicabang yang efisien dan aman memainkan peran yang sangat penting dalam menjaga kinerja operasional, mengoptimalkan sumber daya, dan melindungi aset data perusahaan.

PT Kris Cargo Bahtera, dalam hal ini, adalah salah satu contoh perusahaan yang seringkali mengalami masalah di jaringan mereka, terutama di kantor utama mereka. Masalah yang mereka sering hadapi adalah koneksi internet yang lambat dan tidak stabil. Koneksi internet sangat vital bagi perusahaan tersebut karena para karyawan harus mengakses aplikasi berbasis web yang ada di web hosting. Sehingga, jika koneksi ke internet down, maka karyawan tidak akan bisa bekerja dan akan berdampak buruk pada bisnis perusahaan tersebut. Selain itu mereka juga memiliki masalah dalam hal storage yang ada di VPS mereka, karena sering kali terjadi forward email ke antar akun email internal, sehingga membuat storage di VPS penuh dan alhasil tidak dapat menerima email dari client. Yang terakhir, untuk masalah keamanan, karena media utama mereka dalam berinteraksi dengan customer adalah melalui email, maka tidak jarang karyawan mendapatkan email phishing/attachment yang mengandung malware/trojan sehingga perlu sebuah mekanisme untuk mendeteksi dan mencegah program berbahaya tersebut agar tidak meng-compromise jaringan mereka.

Dalam konteks menghadapi masalah ketersediaan, kecepatan, dan stabilitas layanan internet, penggunaan teknologi seperti load balancing, failover, VLAN, network monitoring software, pemblokiran konten yang memakan banyak bandwith, pemakaian RADIUS dalam hal penggunaan internet, serta penggunaan queue sebagai alat QoS (Quality of Service) untuk pembagian bandwidth yang merata dapat memberikan solusi bagi perusahaan agar dapat meningkatkan performa layanan internet secara keseluruhan. Selain itu untuk mengefisiensikan storage, penggunaan NAS (Network Attached Storage), dapat membantu untuk menyediakan penyimpanan terpusat yang efisien serta VPN site-to-site yang memungkinkan komunikasi aman dan akses terhadap NAS secara aman antara cabang-cabang yang terpisah geografis. Dalam

konteks keamanan, (Mukkamala, 2020) menjelaskan bahwa penggunaan firewall, IDS, dan IPS dapat melindungi jaringan dari traffic yang malicious seperti brute force, Nmap, dan traffic malicious lainnya. Oleh karena itu, pemasangan firewall, IDS, dan IPS merupakan kebutuhan mendasar bagi sebuah perusahaan untuk melindungi jaringan mereka agar aset perusahaan bisa lebih terjamin keamanannya.

Hal yang sama telah diterapi oleh (Sholihah, Rizaldi, & Novianty, 2019) yang dipublikasikan di 2018 International Conference of Computer and Informatics Engineering di mana peneliti mengalami masalah dalam melakukan monitoring dan troubleshooting jaringan dari kantor mereka untuk jaringan di Gelora Bung Karno. Oleh karena masalah tersebut, akhirnya peneliti menggunakan solusi VPN site-to-site untuk mengkoneksikan antara jaringan kantor dengan jaringan yang ada di Gelora Bung Karno agar bisa efisien dalam mengawasi dan menangani masalah-masalah jaringan yang ada. Dari penelitian ini, penggabungan network yang terpisah secara geografis menjadi satu kesatuan sangat memungkinkan dengan adanya teknologi VPN.

Dalam penelitian ini, akan dilakukan perancangan dan implementasi infrastruktur teknologi informasi multicabang yang melibatkan komponen-komponen untuk meningkatkan ketersediaan, kecepatan, dan stabilitas layanan internet seperti load balancing dan failover menggunakan MikroTik, VLAN, network monitoring software menggunakan Zabbix, pemblokiran konten yang memakan banyak bandwith, menggunakan RADIUS (FreeRADIUS dan daloRADIUS) dalam hal penggunaan internet, dan penggunaan queue sebagai alat QoS untuk pembagian bandwidth secara merata. Selain itu komponen-komponen seperti VPN site-to-site menggunakan WireGuard dan Network Attached Storage (NAS) digunakan untuk mengefisiensikan penggunaan storage. Yang terakhir, komponen keamanan akan meliputi penggunaan firewall, IDS, dan IPS menggunakan pfSense dan Suricata untuk membuat jaringan yang aman. Dengan demikian, penelitian ini diharapkan dapat membantu PT Kris Cargo Bahtera dalam mengoptimalkan infrastruktur TI mereka sehingga dapat meningkatkan produktivitas perusahaan.

## 1.2 Perumusan Masalah

Berdasarkan latar belakang diatas, dapat dirumuskan rumusan masalahnya sebagai berikut:

1. Bagaimana dampak sebelum dan sesudah implementasi failover, load balancing, VLAN, penggunaan network monitoring software, pemblokiran

konten yang memakan banyak bandwith, pemakaian RADIUS server dalam penggunaan internet, dan penggunaan queue sebagai alat QoS untuk pembagian bandwidth secara merata dalam infrastruktur TI multicabang PT Kris Cargo Bahtera terhadap ketersediaan layanan dan pengatasan potensi gangguan dalam jaringan?

2. Sejauh mana penggunaan teknologi VPN *site-to-site* pada infrastruktur TI multicabang PT Kris Cargo Bahtera dapat memastikan kelancaran komunikasi antar cabang serta bagaimana pengaruhnya terhadap kinerja jaringan & layanan-layanan NAS saat diakses dari cabang lainnya?
3. Bagaimana ketahanan jaringan dan serangan jaringan apa saja yang dapat dicegah setelah dipasang *firewall*, IDS, dan IPS di jaringan perusahaan?

## 1.3 Tujuan Penelitian

Tujuan dari skripsi ini adalah merancang dan mengimplementasikan infrastruktur TI multicabang dengan load balancing, failover, VLAN, network monitoring software, pemblokiran konten yang memakan banyak bandwith, pemakaian RADIUS server dalam penggunaan internet, penggunaan queue sebagai alat QoS untuk pembagian bandwidth secara merata, VPN site-to-site, NAS, serta firewall, IDS, dan IPS pada PT Kris Cargo Bahtera untuk meningkatkan efisiensi, kecepatan, ketersediaan, dan keamanan jaringan.

## 1.4 Ruang Lingkup

- Ruang lingkup dibatasi pada:
    - Narasumber adalah pemilik dari PT Kris Cargo Bahtera yaitu Wirawan Tedja
    - Sisi Desain:
        1. Desain topologi infrastruktur teknologi informasi multicabang menggunakan GNS3 menggunakan perangkat utama yaitu MikroTik yang mencakup *load balancing*, *failover*, VLAN, pemblokiran konten tertentu, RADIUS *server*, queue (QoS), serta perangkat pfSense dan Suricata untuk mengimplementasi *firewall*, IDS, dan IPS di ketiga cabang perusahaan. Ini akan mencakup perencanaan konsep dan arsitektur keseluruhan infrastruktur.

2. Pemilihan perangkat keras yang sesuai untuk mendukung fitur-fitur yang sudah disebutkan di atas. Ini termasuk pemilihan perangkat seperti *router*, *switch,* dan *mini PC* yang mendukung fitur-fitur ini.
3. Desain teknologi VPN *site-to-site* menggunakan WireGuard di semua cabang PT Kris Cargo Bahtera untuk memastikan keamanan dan kerahasiaan komunikasi antar cabang. Ini mencakup konfigurasi VPN dan pengaturan keamanan.
4. Desain VLAN (*Virtual Local Area Network*) di kantor utama PT Kris Cargo Bahtera untuk memisahkan *traffic* jaringan ke dalam segmen-segmen terisolasi di setiap lantai, meningkatkan keamanan, dan mempermudah manajemen jaringan lokal. Ini melibatkan konfigurasi perangkat *switch, router,* dan *mini PC* di kantor utama.
5. Desain konfigurasi *Network Attached Storage* (NAS) di kantor utama PT Kris Cargo Bahtera sebagai solusi penyimpanan terpusat yang dapat diakses dari semua cabang perusahaan.
6. Desain konfigurasi *firewall*, IDS, dan IPS apa saja yang akan sesuai untuk diterapkan di jaringan.

- Sisi Implementasi:
    1. Implementasi *load balancing* di kantor utama PT Kris Cargo Bahtera untuk mendistribusikan *traffic* jaringan secara merata dengan dua ISP dan meningkatkan kinerja jaringan. Ini mencakup konfigurasi perangkat keras dan perangkat lunak yang dibutuhkan.
    2. Implementasi *failover* di kantor utama PT Kris Cargo Bahtera untuk memastikan ketersediaan layanan yang tinggi dengan mengalihkan *traffic* ke sumber daya cadangan saat terjadi gangguan pada ISP utama. Ini akan melibatkan konfigurasi dan pengujian dari mekanisme *failover*.
    3. Implementasi VLAN yang telah didesain di kantor utama untuk setiap lantai.

4. Mengimplementasi *network monitoring software* menggunakan Zabbix untuk memonitor semua jaringan cabang.
5. Mengimplementasi pemblokiran konten tertentu yang memakan *bandwith* banyak seperti youtube, tiktok, dan aplikasi-aplikasi sosial media lainnya.
6. Memasang RADIUS server beserta dengan QoS untuk membatasi bandwidth setiap user menggunakan FreeRADIUS dan daloRADIUS yang dipasang menggunakan sebuah *virtual machine* di NAS.
7. Menginstal dan mengkonfigurasi *server* VPN WireGuard di sebuah VPS.
8. Mengimplementasi VPN *site-to-site* dengan mengkonfigurasi WireGuard di setiap *router* MikroTik di setiap cabang agar terkoneksi ke WireGuard *server* yang sudah terpasang di sebuah VPS.
9. Instalasi dan konfigurasi QNAP NAS di kantor utama yang dapat diakses oleh cabang-cabang lainnya.
10. Instalasi dan konfigurasi *Mini PC* menggunakan proxmox sebagai *virtualisation platform* untuk menjalankan pfSense sebagai *firewall* yang nantinya akan dipasang *package* Suricata sebagai IDS dan IPS nya.
11. Mengimplementasi audit jaringan untuk mencari kelemahan jaringan sebelum dan setelah dipasang IDS dan IPS.

- Tools yang digunakan
    A. Hardware
        1. MikroTik *router* (RB750Gr3, RB951Ui-2nD, RBmAPL-2nD)
        2. D-Link DIR-1253 *access point*
        3. D-Link *switch*
        4. QNAP NAS TS-251D
        5. Ruijie *switch*
        6. AWOW *Mini* PC AK10
    B. Software

1. RouterOS 7
2. Winbox
3. Zabbix
4. GNS3
5. Fing
6. Ruijie Cloud
7. WireGuard VPN
8. Ubuntu (VPS)
9. QTS-Linux
10. Proxmox VE
11. pfSense
12. Suricata
13. Nmap
14. Hping3
15. Kali Linux
16. FreeRADIUS + daloRADIUS
17. OpenVAS (*Open Vulnerability Assessment Scanner*) atau yang sekarang dikenal dengan GVM (*Greenbone Vulnerability Manager*)

- Rencana pengujian
    1. Untuk fitur *failover*, pengujian dilakukan dengan cara mematikan salah satu sumber internet dengan cara mematikan/mencabut kabel dari MikroTik dan menguji apakah internet kantor masih berjalan. Untuk fitur *load balancing* diuji dengan cara melakukan *download/upload* file yang besar yang melalui jalur internet dan memonitor *load traffic* dari dua *interface* yang terkoneksi dengan sumber internet yang berbeda dengan aplikasi winbox. Untuk *network monitoring software* akan diuji juga untuk kemampuan Zabbix (*network monitoring software* yang digunakan) dalam mendeteksi perangkat yang mati *service* nya atau pun mati secara keseluruhan. Untuk pemblokiran konten yang memakan *bandwith* banyak akan diuji pembukaan *website*/aplikasi yang sudah diblokir di jaringan dan melihat apakah masih dapat dibuka atau tidak. Untuk fitur RADIUS *server* akan diuji kemampuannya dalam membatasi

jumlah *device* yang dapat login dan bandwidth dalam mengakses internet. Untuk *queue* akan diuji kemampuannya dalam membatasi *bandwidth* setiap perangkat dengan melakukan *speed test* di perangkat-perangkat yang terkoneksi ke jaringan. Akan menggunakan fitur data yang dikoleksi oleh NMS zabbix yang ada untuk men-*generate* statistik mengenai kecepatan rata-rata internet dan *detail* lain-lainnya.

2. Pengujian kinerja jaringan setelah memasangkan VPN *site-to-site* akan dilakukan menggunakan *network monitoring software* untuk memantau CPU dan RAM dari setiap *router* di cabang, selain itu juga memantau rata-rata kecepatan internet dari setiap cabang. Akan dilakukan juga pengujian VPN *site-to-site* dengan cara memantau kecepatan *download*/*upload file* saat mengakses NAS dari cabang lain.
3. Mencoba untuk menyerang jaringan menggunakan Kali Linux dengan serangan-serangan umum yang biasanya terjadi seperti Nmap, Ping of Death, DoS, dan juga serangan-serangan umum lainnya menggunakan OpenVAS (*Open Vulnerability Assessment Scanner*) atau sekarang yang dikenal dengan GVM (*Greenbone Vulnerability Manager*) untuk mencari tahu serangan apa saja yang bisa dideteksi dan dicegah oleh *firewall* serta IDS dan IPS agar bisa mengetahui seberapa efektif perangkat *security* yang terpasang di jaringan dalam mengamankan jaringan dari serangan-serangan yang sering dilakukan.

## 1.5 Metodologi Penelitian

Langkah-langkah dalam pengerjaan skripsi:

1. Studi literatur tentang:
    1.1 Load balancing dan Failover
    1.2 VLAN
    1.3 GNS3
    1.4 Zabbix
    1.5 WireGuard VPN

1.6 QNAP NAS

1.7 pfSense

1.8 Suricata

1.9 FreeRADIUS

1.10 daloRADIUS

1.11 Proxmox VE

1.12 OpenVAS (*Open Vulnerability Assessment Scanner*) atau yang sekarang dikenal dengan GVM (*Greenbone Vulnerability Manager*)

2. Perencanaan dan pembuatan sistem:

2.1 Desain dan implementasi topologi jaringan yang baru

2.2 Memasang dan mengkonfigurasi *router* MikroTik di ketiga cabang

2.3 Mengatur VLAN di cabang kantor utama

2.4 Mengatur konfigurasi untuk *load balancing* dan *failover*

2.5 Menginstal VPN WireGuard di sebuah VPS yang menggunakan OS linux

2.6 Mengkonfigurasi setiap router MikroTik dengan VPN WireGuard server

2.7 Mengatur pemblokiran konten di jaringan

2.8 Memasang dan mengkonfigurasi NAS dengan FreeRADIUS dan daloRADIUS

2.9 Memasang dan mengkonfigurasi Mini PC yang sudah dipasang dengan proxmox yang akan menjalankan pfSense dan Suricata

3. Pengujian dan analisis sistem

3.1 Pengujian performa jaringan dengan menjalankan speedtest (tanpa

limitasi bandwidth oleh queue) untuk menguji performa load balancing, mematikan salah satu sumber ISP untuk menguji failover, kemampuan Zabbix (network monitoring software yang digunakan) dalam mendeteksi perangkat yang mati service nya atau pun mati secara keseluruhan, membuka website yang sudah diblokir untuk menguji efektivitas pemblokiran, menguji performa limitasi bandwidth yang menggunakan RADIUS dan queue dengan melakukan speedtest menggunakan user yang dibatasi bandwidth nya.

3.2 Pengujian performa VPN site-to-site dalam kecepatan, stabilitas, dan resource yang digunakan di setiap router MikroTik yang ada di setiap cabang menggunakan Zabbix dan akan juga dilakukan tes kecepatan download/upload file saat mengakses NAS dari cabang lain.

3.3 Pengujian ketahanan jaringan dengan cara menyerang jaringan dengan serangan-serangan yang biasanya umum dilakukan seperti DoS, Ping of Death, Nmap menggunakan Kali Linux dan juga serangan-serangan umum lainnya menggunakan OpenVAS (*Open Vulnerability Assessment Scanner*) atau sekarang yang dikenal dengan GVM (*Greenbone Vulnerability Manager*).

4. Pengambilan kesimpulan
5. Pembuatan laporan

## 1.6 Sistematika Penulisan

Penulisan laporan skripsi ini dibagi menjadi beberapa bab, yaitu:

- Bab I: Pendahuluan

  Bab ini berisikan judul, latar belakang, perumusan masalah, ruang lingkup, tujuan skripsi, dan metodologi penelitian yang akan digunakan dalam skripsi ini.
- Bab II: Landasan Teori

  Bab ini berisikan teori-teori yang digunakan dan diterapkan dalam skripsi ini.
- Bab III: Analisis dan Desain Sistem

Bab ini menjelaskan analisis masalah yang dihadapi dan perencanaan pembuatan keseluruhan sistem dalam aplikasi yang akan dibuat.

- Bab IV: Implementasi Sistem

  Bab ini berisikan tentang implementasi sistem berdasarkan desain.

- Bab V: Pengujian Sistem

  Bab ini berisi tentang hasil pengujian yang dilakukan terhadap aplikasi yang telah dibuat berdasarkan implementasi pada system yang telah dirancang dan dibuat pada Bab IV.

- Bab VI: Kesimpulan

  Bab ini berisikan kesimpulan yang dapat diambil terhadap hasil yang dicapai.