

3. ANALISIS DAN DESAIN SISTEM

Bab ini akan menguraikan masalah yang dihadapi oleh perusahaan, serta kebutuhan yang perlu dipenuhi untuk meningkatkan infrastruktur perusahaan. Selain itu, akan dijelaskan desain sistem yang direncanakan untuk mencapai tujuan tersebut dan memperbaiki keadaan infrastruktur perusahaan.

3.1 Analisis Permasalahan dan Kebutuhan

Perusahaan menghadapi serangkaian masalah yang signifikan yang berdampak pada efisiensi operasional dan keamanan data. Salah satunya adalah masalah kecepatan dan kestabilan internet di kantor dan gudang yang tidak memadai. Kondisi ini menyulitkan karyawan dalam mengakses aplikasi berbasis web yang vital untuk menjalankan berbagai tugas sehari-hari. Ketika akses terhambat oleh koneksi internet yang tidak stabil, kinerja karyawan terganggu, menyebabkan penundaan dalam penyelesaian tugas. Sehingga, mereka membutuhkan koneksi internet yang cepat, stabil, dan cadangan untuk memastikan akses yang lancar dan kelangsungan operasional perusahaan.

Masalah kedua yang dihadapi oleh perusahaan adalah masalah penyimpanan email yang cepat terisi penuh di *Virtual Private Server* (VPS). Karyawan sering menggunakan email sebagai alat utama untuk berbagi dokumen, terutama file Excel atau PDF, antar departemen atau dengan rekan kerja lainnya. Akibatnya, kapasitas penyimpanan email cepat terpakai dan menyebabkan ketidakmampuan untuk menerima atau mengirim email baru. Kejadian seperti ini telah menyebabkan beberapa masalah, termasuk keterlambatan dalam tanggapan terhadap pelanggan dan kehilangan komunikasi penting antar karyawan. Sehingga mereka membutuhkan solusi alternatif untuk berbagi dokumen, yang memungkinkan karyawan untuk berbagi dan menyimpan dokumen dengan cara yang lebih terstruktur dan efisien.

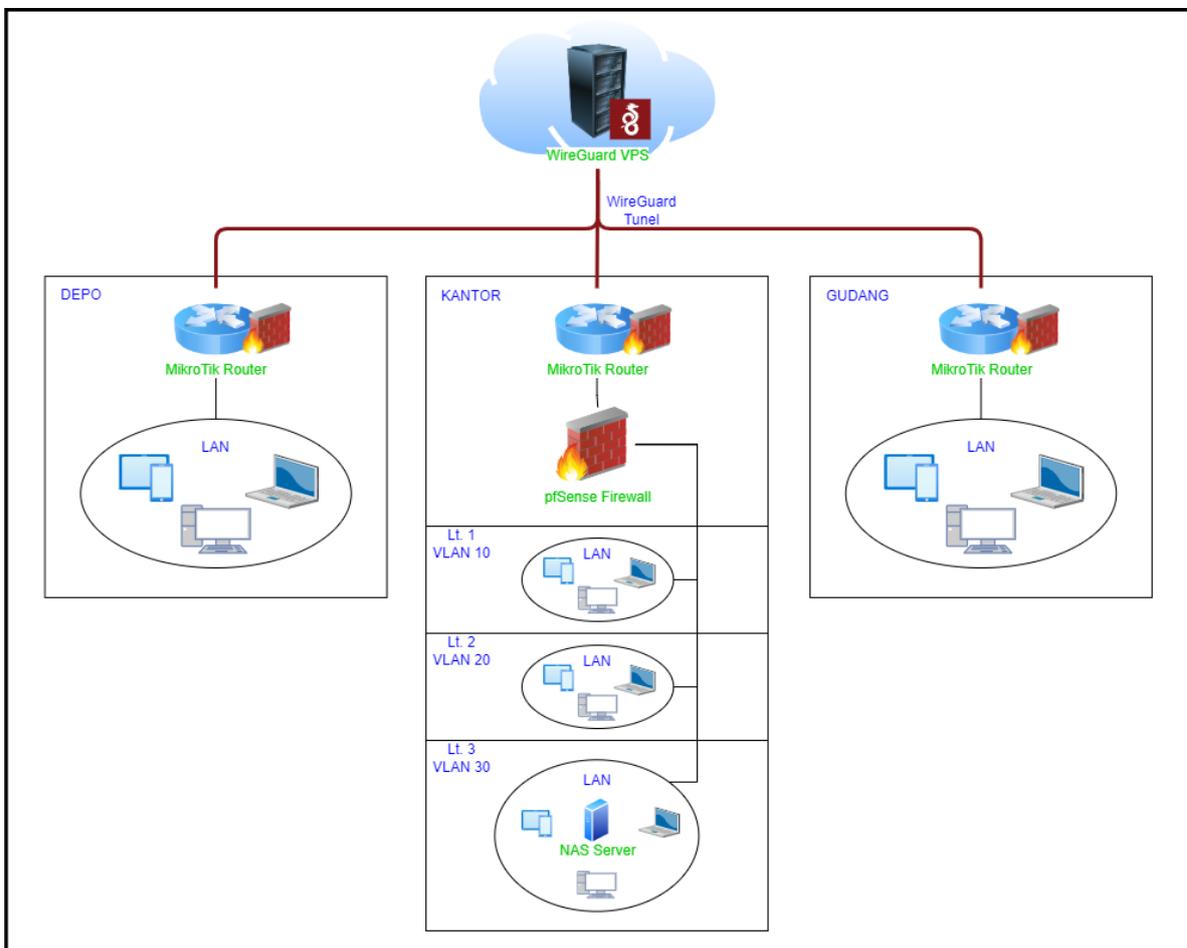
Masalah ketiga yang dihadapi oleh perusahaan adalah risiko keamanan yang timbul dari ketergantungan pada email sebagai saluran utama untuk menerima pesanan dari pelanggan. Karyawan harus secara manual mendownload lampiran email ke laptop mereka untuk memproses pesanan, meningkatkan risiko terhadap serangan keamanan atau kehilangan data sensitif. Terlebih lagi, data penting seperti informasi finansial dan informasi pelanggan berpotensi terkena risiko jika tidak ditangani dengan hati-hati. Oleh karena itu, diperlukan

sebuah solusi yang dapat meningkatkan keamanan jaringan perusahaan, mengurangi risiko terhadap serangan keamanan atau kehilangan data sensitif.

3.2 Desain Sistem

Desain sistem akan membahas desain topologi jaringan untuk ketiga cabang, desain VLAN untuk jaringan kantor, desain sistem WireGuard untuk keperluan VPN *site-to-site*, desain sistem RADIUS dan *hotspot*, desain sistem Zabbix, dan desain *whitelist* untuk IP dan *port* di *firewall* pfSense.

3.2.1 Topologi Keseluruhan Jaringan

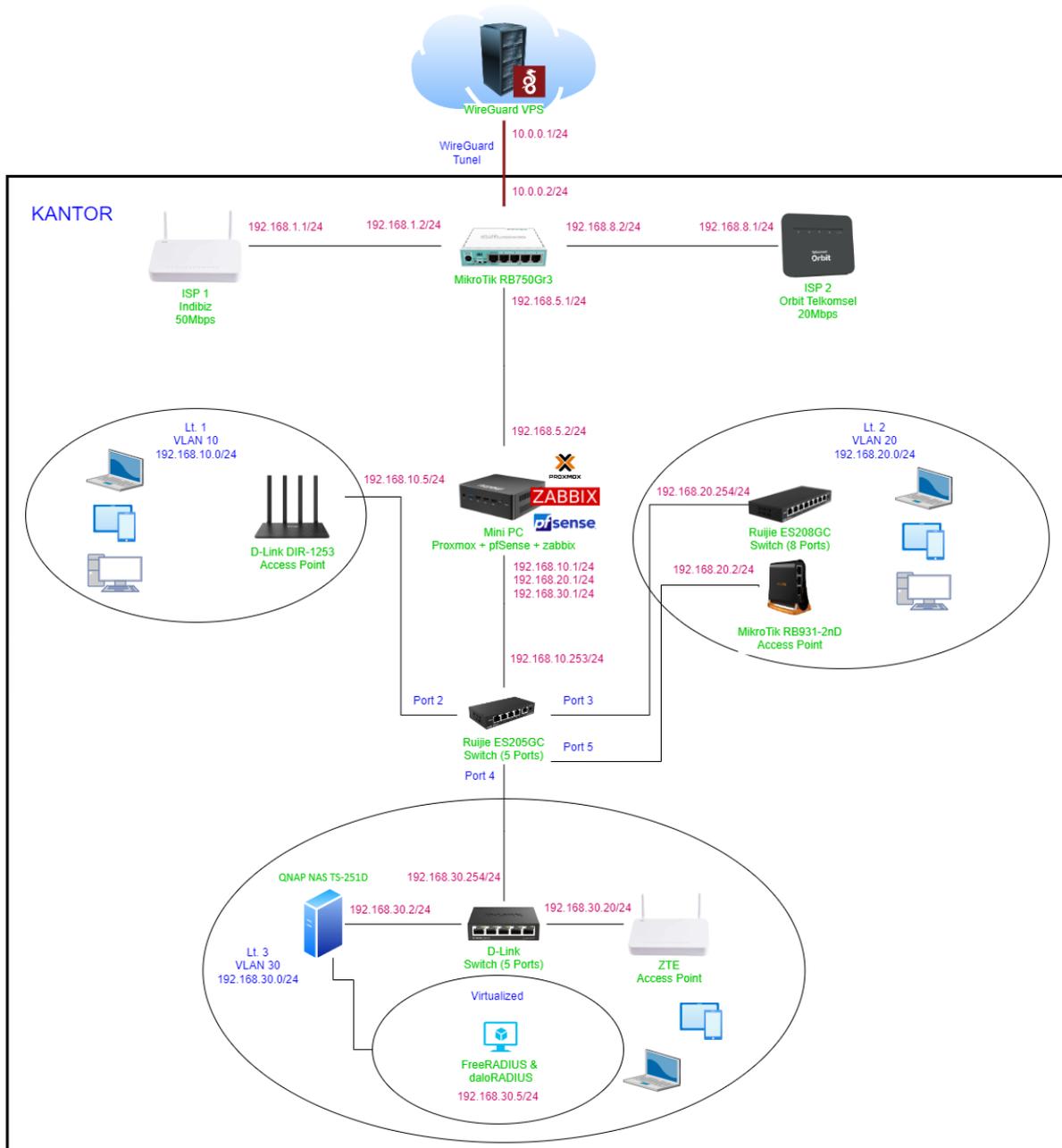


Gambar 3.2.1 Topologi Keseluruhan Jaringan

Pada gambar 3.2.1, terdapat sebanyak tiga cabang perusahaan yang topologi jaringannya digambarkan, yaitu cabang kantor, cabang gudang, dan cabang depo. Karena perusahaan ingin mengimplementasi sebuah area penyimpanan yang terpusat, maka

dibentuklah jaringan VPN *site-to-site* tersebut agar *server* NAS yang ada di kantor dapat diakses dari cabang lainnya. Sebenarnya NAS tersebut memiliki kemampuan untuk diakses secara *cloud*, namun secara keamanan tidak baik bagi perusahaan, karena dapat diakses dari manapun dan akan rentan terhadap *brute force*. Untuk setiap cabang dapat dilihat bahwa akan dipasang sebuah MikroTik *router* yang nantinya akan menjadi sebuah WireGuard *client* yang akan terkoneksi dengan WireGuard *server* yang dipasang di sebuah VPS. VPS tersebut akan berfungsi sebagai jembatan yang akan menghubungkan ketiga jaringan tersebut. Untuk jaringan kantor akan diimplementasikan juga sebuah VLAN untuk setiap lantai, lantai 1 adalah karyawan-karyawan dari divisi *marketing*, lantai 2 adalah karyawan-karyawan dari divisi *accounting*, dan lantai 3 adalah divisi *management*. VLAN digunakan agar dapat dengan lebih mudah mengatur *security policy* untuk setiap divisi tersebut serta juga agar dengan lebih mudah mengisolasi sumber masalah jika terjadi masalah di jaringan.

3.2.2 Desain Jaringan Kantor



Gambar 3.2.2 Topologi Jaringan Kantor

Pada gambar 3.2.2, mulai dari paling atas, dapat dilihat bahwa sebuah MikroTik dengan model RB750Gr3 digunakan dan tersambung dengan sebuah WireGuard server yang dipasang di sebuah VPS. MikroTik tersebut terhubung dengan WireGuard server tersebut melalui *public* IP dari VPS tersebut. Jika nanti sudah terhubung, maka WireGuard server dan WireGuard *client* (MikroTik) akan berkomunikasi dengan *private* IP yang sudah di-*set*, yaitu 10.0.0.1 untuk server

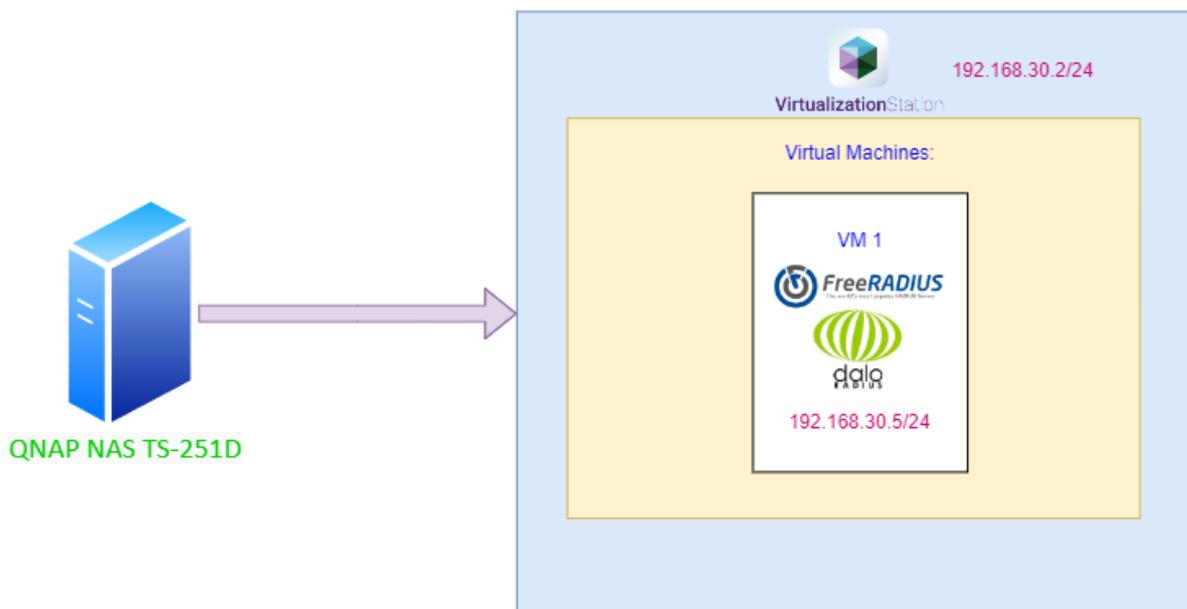
dan 10.0.0.2 untuk *client*. MikroTik tersebut juga harus memiliki versi RouterOS minimum 7, karena fitur WireGuard baru ditambahkan di versi 7.

Selain sebagai sebuah alat untuk menjalankan fungsi VPN *site-to-site*, MikroTik tersebut juga akan menjadi sebuah alat untuk menjalankan fungsi *load balancing* dan *failover*. Oleh sebab itu, alat tersebut terhubung dengan 2 *internet service provider*, ISP 1 yaitu Indibiz dan ISP 2 atau ISP cadangan adalah Orbit dari Telkomsel. Untuk IP *default* dari Indibiz adalah 192.168.1.1, oleh karena itu untuk sisi MikroTik akan diberi IP 192.168.1.2. Untuk IP default dari Orbit adalah 192.168.8.1, oleh karena itu untuk sisi MikroTik akan diberikan IP 192.168.8.2. Di kantor terdapat sebanyak 16 orang, dan setiap orang memiliki 2 perangkat, yaitu *laptop* dan *smartphone*. Setiap pekerja membutuhkan minimum sekitar 4Mbps, sehingga jika semua *user* dalam satu waktu menggunakan internet, maka akan membutuhkan sekitar 64Mbps. Oleh karena itu, di cabang kantor, karena Orbit memiliki kecepatan rata-rata sebesar 20Mbps, maka jika digabungkan (*load balancing*) dengan ISP Indibiz yang memiliki kecepatan 50Mbps, maka akan mendapatkan kecepatan total sebesar 70Mbps. Selain untuk meningkatkan total *bandwidth*, alasan lainnya adalah karena dengan desain yang baru ini untuk melakukan login *hotspot* seluruh cabang harus mengontak server RADIUS yang ada di kantor dan juga karena cabang-cabang lainnya juga harus mengakses NAS yang ada di cabang kantor, harus dipastikan bahwa server-server tersebut akan selalu *available*, dan salah satu caranya adalah untuk menggunakan 2 ISP agar jika salah satu ISP mati, masih ada ISP *backup* yang dapat digunakan.

MikroTik tersebut juga akan terhubung dengan sebuah *Mini PC* dengan model AWOW AK10. *Mini PC* tersebut akan dipasang sebuah *platform* untuk menjalankan virtualisasi yaitu Proxmox VE. *Firewall* pfSense akan dipasang di atas Proxmox tersebut sebagai sebuah *virtual machine*. Selain itu juga akan di pasang zabbix sebagai *network monitoring system*. *Firewall* tersebut dipasang di sisi LAN kantor agar *firewall* serta IPS (Suricata) dapat melindungi server-server penting yang ada di kantor seperti QNAP, RADIUS server, aplikasi internal kantor, dan lain-lainnya. *Mini PC* tersebut memiliki 2 *port* gigabit ethernet yang nantinya akan terhubung dengan MikroTik dan juga dengan perangkat-perangkat LAN. Untuk sisi koneksi dengan MikroTik, akan menggunakan IP di *network* 192.168.5.0/24, untuk pfSense akan menggunakan IP 192.168.5.2 dan untuk MikroTik akan menggunakan IP 192.168.5.1. Lalu untuk sisi LAN, dia akan memiliki 3 buah *gateway* karena dia akan memiliki 3 *network* yang terpisah secara VLAN. Untuk VLAN 10 akan berada di *network* 192.168.10.0/24, VLAN 20 di *network* 192.168.20.0/24, dan VLAN 30 akan berada di *network* 192.168.30.0/24. *Mini PC* tersebut akan memiliki *gateway* 192.168.10.1 untuk VLAN 10, 192.168.20.1 untuk VLAN 20, dan 192.168.30.1 untuk VLAN 30.

Mini PC tersebut akan terhubung dengan *switch* (*port* 1 dengan mode *trunk*) terlebih dahulu di mana *switch* tersebut akan di-*set* untuk memiliki VLAN 10 dan memiliki IP *address* 192.168.10.253.

Untuk *port* kedua *switch* tersebut akan terhubung dengan *access point* lantai 1, sehingga *port* tersebut akan berjalan dalam mode akses dengan VLAN 10. Untuk *port* ketiga, *switch* tersebut akan terhubung dengan *switch* di lantai 2, sehingga kedua *port switch* tersebut akan berjalan di mode *trunk*. Lalu, untuk menjamin *availability* jaringan Wi-Fi di seluruh kantor, akan ditarik kabel langsung dari *port* kelima (berjalan dalam mode akses dengan VLAN 20) *switch* dari lantai 1, ke *access point* lantai 2, sehingga tidak ada *intermediary device* lain yang dapat berpotensi menyebabkan kegagalan. Hal ini dilakukan karena Wi-Fi di lantai 2 dapat meng-*cover* untuk Wi-Fi di lantai 1 dan lantai 3. Sehingga jika terjadi kegagalan di Wi-Fi lantai 1 atau lantai 3, maka pengguna-pengguna Wi-Fi tersebut dapat beralih ke Wi-Fi di lantai 2 agar tetap dapat terkoneksi ke jaringan. Lalu untuk *port* terakhir yaitu *port* keempat akan terhubung dengan *switch* di lantai 3. *Switch* di lantai 3 lalu akan terhubung dengan *access point* agar user di lantai 3 dapat terhubung ke jaringan secara *wireless*.

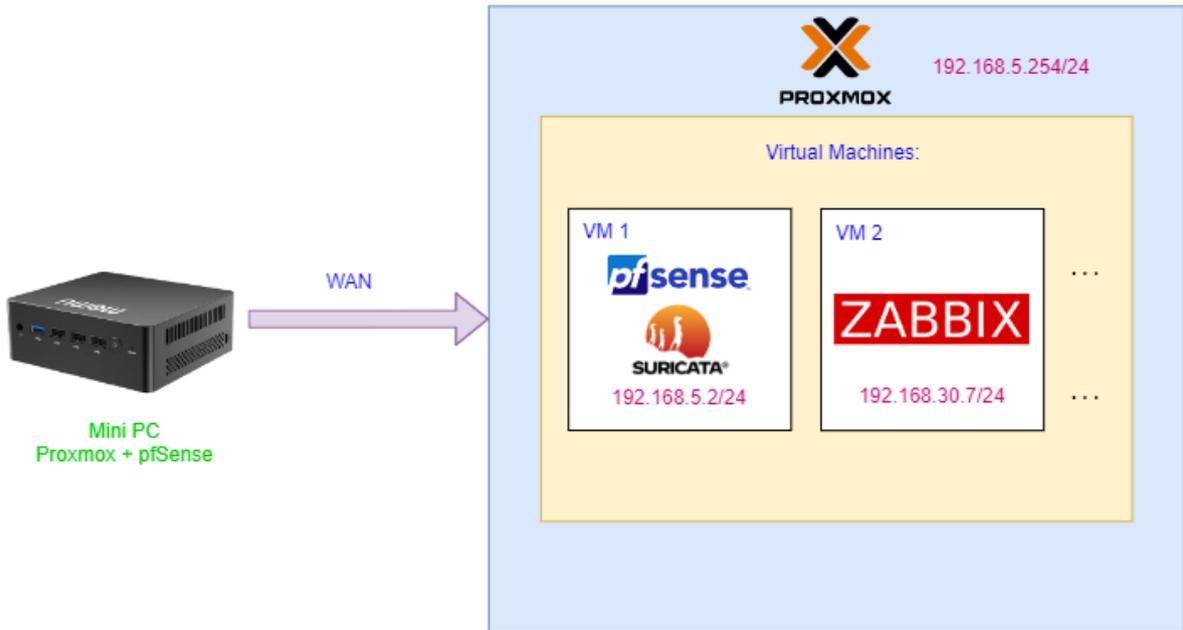


Gambar 3.2.3 Sistem Virtualisasi QNAP NAS

Lalu untuk di lantai 3 juga akan ada perangkat *network attached storage* (NAS) dengan model QNAP TS-251D. Perangkat tersebut memiliki CPU Intel Celeron dengan 2 *cores* dan memiliki kecepatan hingga 2,9Ghz. Perangkat tersebut juga memiliki RAM sebesar 8GB. NAS tersebut memiliki gigabit *ethernet port* dan akan memiliki IP *address* 192.168.30.2. NAS tersebut

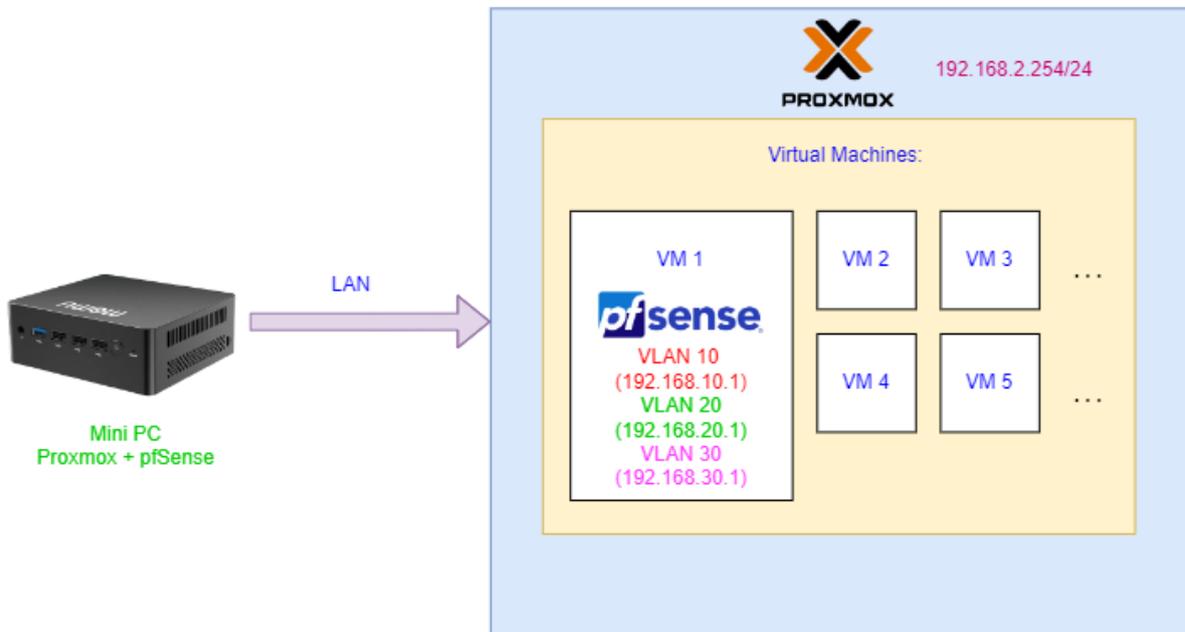
juga memiliki aplikasi bernama *Virtualization Station* yang dapat berfungsi untuk menjalankan *virtual machine* di dalamnya. Sehingga, akan dijalankan *virtual machine* untuk kepentingan jaringan perusahaan tersebut, yaitu VM untuk kepentingan RADIUS, sehingga akan dipasang FreeRADIUS dan juga dalorRADIUS sebagai *web GUI* untuk mengkonfigurasi FreeRADIUS tersebut. VM untuk RADIUS tersebut akan memiliki IP *address* 192.168.30.5.

3.2.2.1 Sistem Virtualisasi Proxmox



Gambar 3.2.4 Sistem Virtualisasi *Mini PC* Sisi WAN

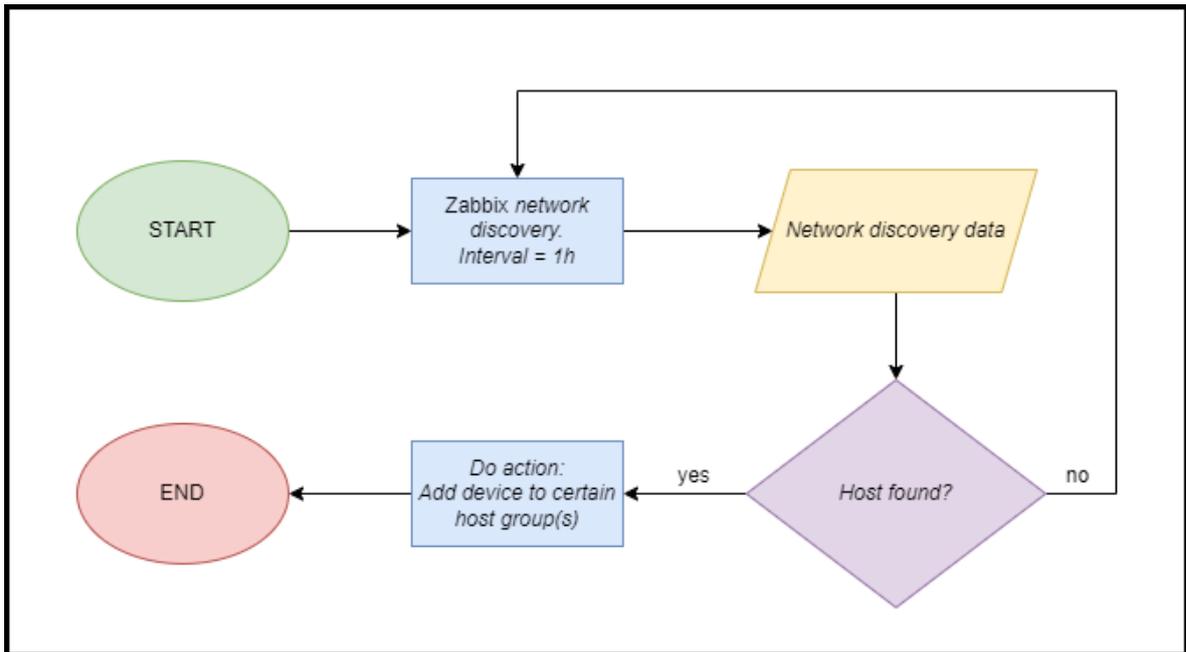
Mini PC tersebut memiliki CPU Intel N100 dengan 4 cores dan kecepatan hingga 3,4Ghz. *Mini PC* tersebut juga memiliki RAM 8GB DDR5 4800MHz. Dengan spesifikasi tersebut, tentunya akan sia-sia jika hanya di-*install* pfSense secara *bare metal*, oleh karena itu *Mini PC* tersebut dipasang dengan Proxmox VE terlebih dahulu agar selain bisa menjalankan pfSense sebagai sebuah *virtual machine*, alat tersebut akan juga bisa menjalankan mesin-mesin lainnya sesuai dengan kebutuhan perusahaan yang selalu menambah. Alat tersebut memiliki 2 gigabit *port ethernet* sehingga untuk *port* yang mengarah ke WAN akan memiliki IP address 192.168.5.254 untuk platform Proxmox dan untuk VM pfSense akan memiliki IP address 192.168.5.2. Lalu untuk VM kedua akan menjalankan Zabbix sebagai *network monitoring software* untuk memonitor jaringan seluruh cabang perusahaan. VM tersebut akan memiliki IP address 192.168.30.7.



Gambar 3.2.5 Sistem Virtualisasi *Mini PC* Sisi LAN

Lalu untuk sisi LAN, akan dibuat 3 VLAN di VM pfSense tersebut, sehingga nantinya di pfSense akan muncul 3 *interface* di mana untuk *interface* pertama akan memiliki VLAN 10, *interface* kedua akan memiliki VLAN 20, dan *interface* ketiga akan memiliki VLAN 30. Lalu untuk setiap *interface* yang telah dibuat tersebut, untuk VLAN 10 akan diberi IP *address* 192.168.10.1, untuk VLAN 20 akan diberi IP *address* 192.168.20.1, dan untuk VLAN 30 akan diberi IP *address* 192.168.30.1.

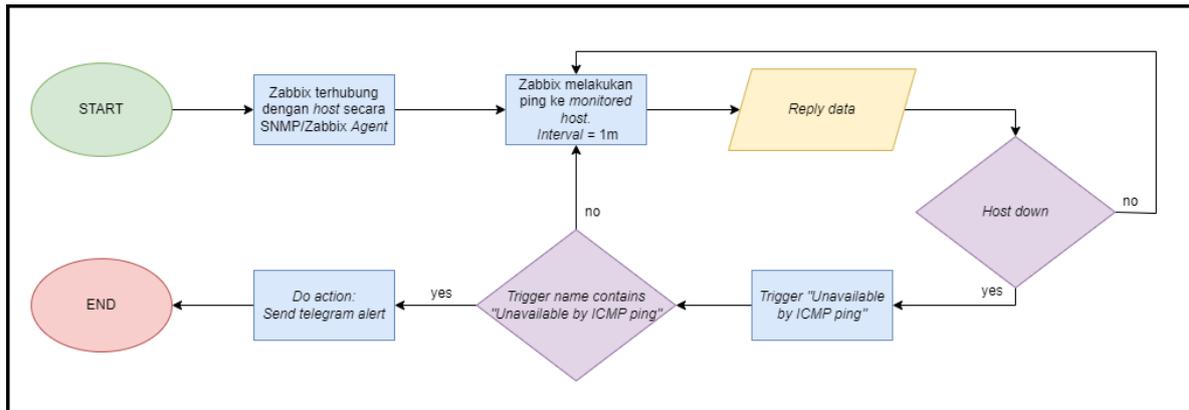
3.2.2.2 Sistem Network Monitoring Zabbix



Gambar 3.2.6 Zabbix Network Discovery Action

Gambar 3.6 merupakan *flowchart* proses *network discovery* yang akan dijalankan Zabbix yang merupakan sebuah *network monitoring system*. Berikut adalah penjelasan lebih rinci untuk setiap langkah yang ada pada *flowchart* tersebut:

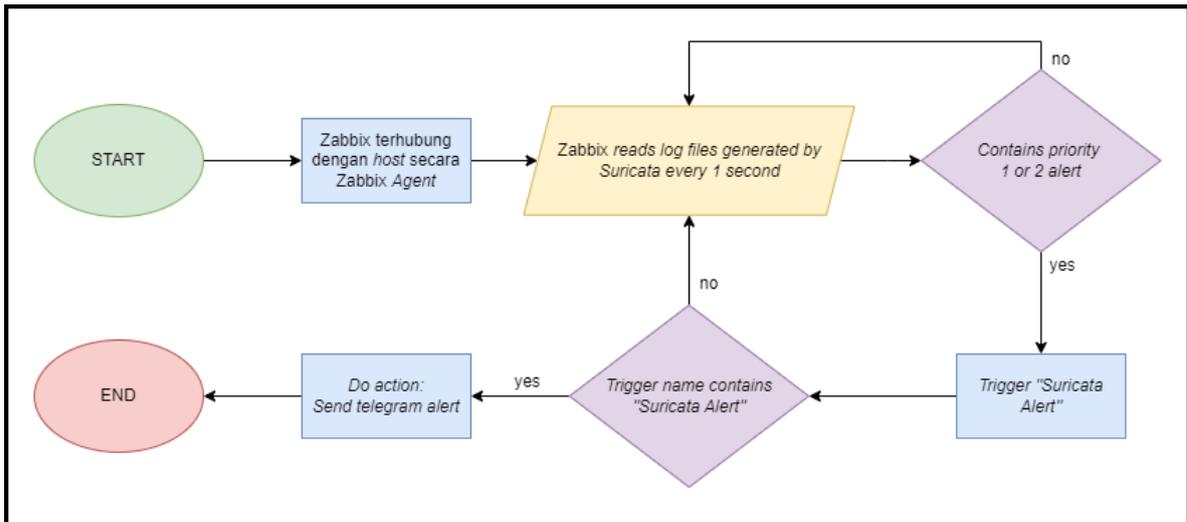
1. *Zabbix network discovery*, Interval = 1h. Pada tahap ini, jika server Zabbix sudah dikonfigurasi untuk melakukan *scanning* terhadap *network* dengan *interval* misal 1 jam, maka Zabbix server akan melakukan *network discovery* pada *network range* yang sudah ditentukan dengan mengirim ping terhadap seluruh IP *address* di *network range* tersebut.
2. *Network discovery data*. Tahap ini melambangkan bahwa Zabbix sudah selesai memproses dan sudah mendapatkan data dari proses *network discovery* tersebut.
3. *Do action: Add device to certain host group(s)*. Jika Zabbix menemukan *host* dari proses *network discovery* tersebut, maka Zabbix bisa dikonfigurasi untuk menambahkan *device* tersebut ke sebuah atau beberapa *host group* yang sudah dibuat. Jadi, misal untuk proses *network discovery* di IP *range* 192.168.40.0/24, maka jika ada *host* yang ditemukan di *network range* tersebut, maka tambahkan ke *host group* "Depo".



Gambar 3.2.7 Zabbix *Host Down Alert*

Gambar 3.7 merupakan *flowchart* proses Zabbix dalam melakukan proses *alerting* jika ada *host* yang dimonitor *down*. Berikut adalah penjelasan lebih rinci untuk setiap langkah yang ada pada *flowchart* tersebut:

1. Zabbix terhubung dengan *host* secara SNMP/Zabbix Agent. Di tahap ini, Zabbix akan melakukan proses untuk menghubungkan dirinya dengan *host* secara SNMP atau secara Zabbix Agent. Sebelum proses ini tentunya harus dikonfigurasi dahulu di kedua sisi agar bisa terhubung. Di skripsi ini akan ada beberapa *host* yang dimonitor yang akan terhubung secara SNMPv3 dan juga secara Zabbix Agent.
2. Zabbix melakukan ping ke monitored host, Interval = 1m. Jika sudah dikonfigurasi *host* mana yang ingin dijaga/monitor maka Zabbix akan mengirim ping ke *host* tersebut dengan *interval default* yaitu 1 menit.
3. *Reply data*. Di tahap ini, Zabbix akan mendapatkan data apakah *host tersebut* me-*reply*.
4. *Host down & Trigger "Unavailable by ICMP ping"*. Di tahap ini, Zabbix akan mengevaluasi, jika *host* tersebut tidak me-*reply* sebanyak 3 kali (ini adalah *default*), maka dia akan melakukan *Trigger "Unavailable by ICMP ping"*.
5. *Trigger name contains "Unavailable by ICMP ping" & Do action: Send telegram alert*. Karena ada banyak macam *trigger name* yang dapat dikeluarkan oleh Zabbix, maka untuk *action* harus dikonfigurasi untuk mengirim *alert* ke telegram beserta informasi nama *host*, IP dari *host*, dan informasi penting lainnya jika ada *trigger* yang mengandung kata-kata "*Unavailable by ICMP ping*".



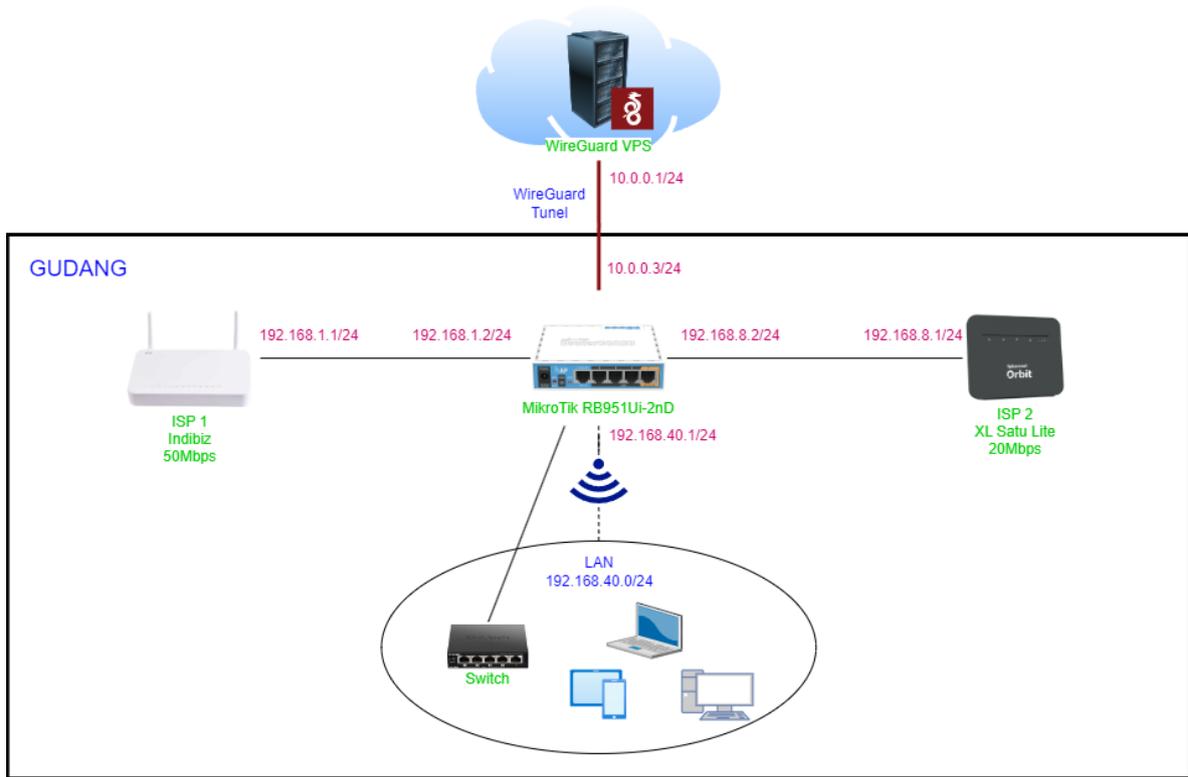
Gambar 3.2.8 Zabbix Suricata Alert

Gambar 3.8 merupakan *flowchart* proses Zabbix dalam melakukan proses *alerting* jika ada *alert* dari Suricata dari *host* pfSense yang dapat berpotensi menjadi ancaman keamanan jaringan. Berikut adalah penjelasan lebih rinci untuk setiap langkah yang ada pada *flowchart* tersebut:

1. Zabbix terhubung dengan *host* secara Zabbix Agent. Di tahap ini, Zabbix akan melakukan proses untuk menghubungkan dirinya dengan *host* pfSense yang menjalankan Suricata secara Zabbix Agent. Sebelum proses ini tentunya harus dikonfigurasi dahulu di kedua sisi agar bisa terhubung.
2. Zabbix reads log files generated by Suricata every 1 second. Zabbix dapat dikonfigurasi untuk membaca *alert* yang di-generate oleh Suricata yang berjalan di *host* pfSense paling cepat adalah setiap 1 detik. Jadi, karena setiap *alert* yang di-generate oleh Suricata akan masuk ke dalam sebuah *log file*, maka karena *host* pfSense sudah di-install Zabbix agent, Zabbix server dapat membaca *log file* tersebut dan dapat mengetahui *alert* apa saja yang dikeluarkan oleh Suricata tersebut.
3. Contains priority 1 or 2 alert & Trigger "Suricata Alert". Jadi, karena *alert* yang ada di *log file* tersebut memiliki *pattern*, jadi untuk *alert* yang berbahaya akan mengandung "[Priority: 1]" atau "[Priority: 2]", maka jika saat membacanya Zabbix server menemukan *term* tersebut, Zabbix akan langsung melakukan *trigger* "Suricata Alert".
4. Trigger name contains "Suricata Alert" & Do action: Send telegram alert. Lalu, akan dicek apakah *trigger name* mengandung kata-kata "Suricata Alert" dan jika mengandung, maka Zabbix dapat dikonfigurasi untuk melakukan *action* untuk mengirim *alert* melalui

media telegram beserta informasi yang ada di *log file* Suricata tersebut dan informasi penting lain-lainnya seperti tanggal kejadian *alert* tersebut.

3.2.3 Desain Jaringan Gudang



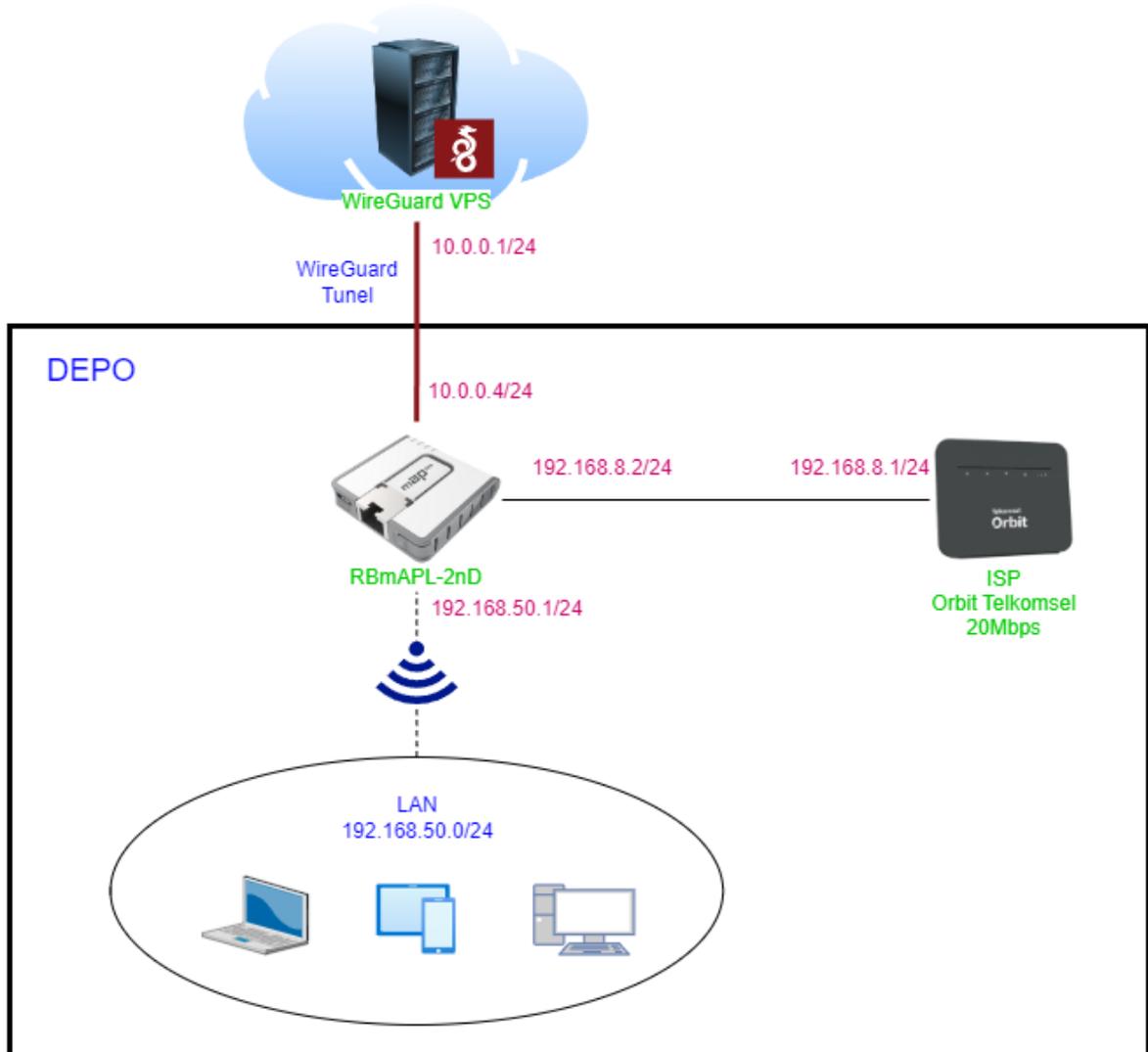
Gambar 3.2.9 Topologi Jaringan Gudang

Pada gambar 3.2.9, mulai dari paling atas, dapat dilihat bahwa sebuah MikroTik dengan model RB951Ui-2nD digunakan dan tersambung dengan sebuah WireGuard server yang dipasang di sebuah VPS. Sama halnya dengan MikroTik kantor, MikroTik di gudang akan juga memiliki *private* IP yakni 10.0.0.3 setelah berhasil tersambung dengan WireGuard server yang ada di VPS dan akan bisa berkomunikasi dengan jaringan cabang-cabang lain melalui jalur VPN tersebut.

Lalu, dapat dilihat bahwa untuk cabang gudang dipasangkan juga dua ISP, ISP utama menggunakan Indibiz dan ISP kedua menggunakan XL Satu Lite. Untuk kecepatan rata-rata XL Satu Lite kurang lebih sama dengan Orbit, yaitu sebesar 20Mbps. Jika digabung dengan Indibiz yang memiliki kecepatan 50Mbps, akan mendapatkan sekitar 70Mbps. Di gudang hanya terdapat sebanyak 7 orang dan 14 perangkat. Alasan utama cabang gudang dipasangkan 2 ISP adalah karena cabang tersebut sering memiliki gangguan dengan ISP utamanya. Sehingga, walaupun kecepatannya sudah memadai, harus ada ISP kedua yang dapat mem-*backup* jika terjadi masalah dengan ISP utamanya. Untuk sisi LAN akan menggunakan Wi-Fi untuk perangkat-perangkat seperti *laptop* dan *smartphone* dan untuk perangkat-perangkat seperti CCTV akan

menggunakan kabel *ethernet* yang terhubung dengan *switch*. Untuk IP akan menggunakan IP *address* yang ada di *network* 192.168.40.0/24.

3.2.4 Desain Jaringan Depo



Gambar 3.2.10 Topologi Jaringan Depo

Pada gambar 3.2.10, mulai dari paling atas, dapat dilihat bahwa sebuah MikroTik dengan model RBmAPL-2nD digunakan dan tersambung dengan sebuah WireGuard server yang dipasang di sebuah VPS. Sama halnya dengan MikroTik kantor, MikroTik di gudang akan juga memiliki *private* IP yakni 10.0.0.4 setelah berhasil tersambung dengan WireGuard server yang ada di VPS dan akan bisa berkomunikasi dengan jaringan cabang-cabang lain melalui jalur VPN tersebut.

Untuk cabang depo, hanya memiliki sebanyak 5 karyawan saja dan sekitar 10 perangkat, sehingga menggunakan 1 ISP saja yaitu Orbit yang memiliki kecepatan 20Mbps akan cukup. Untuk sisi LAN hanya akan menggunakan Wi-Fi dan akan menggunakan IP *address* di *network* 192.168.50.0/24.