BAB V

PENUTUP

5.1. Kesimpulan

Dari hasil implementasi dan pengujian konfigurasi *Load Balancing* dan *Failover* berbasis Mikrotik pada jaringan PT. ABB Sakti Industri, diperoleh kesimpulan sebagai berikut:

1. Sistem jaringan yang sebelumnya hanya bergantung pada satu ISP memiliki risiko *downtime* tinggi dan tidak efisien dalam distribusi *trafik.*
2. Implementasi metode *Load Balancing* berhasil mendistribusikan *trafik* secara proporsional ke dua jalur ISP, sehingga meningkatkan efisiensi dan stabilitas koneksi.
3. Fitur *failover* yang dikonfigurasi menggunakan *Netwatch* dan *script* Mikrotik mampu mendeteksi gangguan koneksi ISP dan melakukan pengalihan secara otomatis dalam waktu kurang dari 5 detik.
4. Hasil pengujian menunjukkan peningkatan performa jaringan, baik dari sisi waktu *respon (ping),* efisiensi jalur *(traceroute),* maupun kestabilan koneksi.
5. Manajemen jaringan menjadi lebih terstruktur dengan adanya *monitoring, logging,* dan sistem otomatisasi yang mendukung operasional TI.

5.2. Saran

Untuk mendukung pengembangan dan pemeliharaan sistem jaringan di masa mendatang, penulis menyampaikan beberapa rekomendasi sebagai berikut:

5.2.1. Saran dari Aspek Manajerial

1. Perusahaan perlu menyusun SOP Manajemen Jaringan, yang mencakup prosedur penanganan gangguan, alur eskalasi, dokumentasi perubahan *konfigurasi,* serta standar pemeliharaan perangkat. Dengan adanya SOP yang baku, proses penanganan insiden dapat berjalan lebih cepat, terukur, dan tidak bergantung pada teknisi tertentu.

2. Perlu pembentukan tim atau penanggung jawab khusus jaringan, yang fokus pada monitoring, perencanaan kapasitas (*capacity planning*), dan pengelolaan dua ISP agar kinerja jaringan tetap terjaga secara konsisten.

3. Disarankan melakukan pelatihan berkala, untuk tim IT terkait konfigurasi Mikrotik, pemahaman *redundancy*, teknik *troubleshooting*, dan manajemen keamanan jaringan guna meningkatkan kompetensi teknis dalam operasional jangka panjang.

4. Evaluasi dan audit jaringan secara periodik minimal, setiap 6 bulan untuk menilai efektivitas *load balancing*, kinerja ISP, tren penggunaan *bandwidth*, serta menilai apakah diperlukan peningkatan kapasitas atau perubahan desain jaringan.

5.2.2. Saran dari Aspek Sistem

1. Perlu menambah sistem monitoring terpusat, seperti *Zabbix, The Dude*, atau PRTG untuk memantau performa router, kualitas koneksi ISP, penggunaan *bandwidth,* serta memberikan notifikasi otomatis apabila terjadi gangguan.

2. Implementasikan segmentasi jaringan berbasis VLAN, yang lebih ketat pada setiap divisi untuk meningkatkan keamanan, mengurangi *broadcast domain*, dan mengatur prioritas trafik secara lebih efisien.

3. Perangkat router atau switch inti perlu disiapkan *redundancy*, (misalnya menggunakan dua *router* Mikrotik dengan metode VRRP atau *failover hardware*) untuk menghindari *single point of failure*.

4. Penerapan IDS/IPS, (*Intrusion Detection/Prevention System*) sangat disarankan untuk meningkatkan keamanan jaringan terhadap ancaman internal maupun eksternal.

5. Optimalkan *Quality of Service* (QoS), untuk memprioritaskan trafik penting seperti ERP, VoIP, dan *Microsoft Teams* sehingga aplikasi kritikal tetap berjalan optimal meskipun terjadi beban tinggi.

5.2.3. Saran untuk Penelitian Selanjutnya

1. Penelitian berikutnya dapat melakukan pengujian menggunakan metode *load balancing* lain, seperti: ECMP (*Equal-Cost Multi Path*), *Bonding*, Metode NTH

sehingga hasilnya dapat dibandingkan dengan metode PCC yang digunakan pada penelitian ini.

2. Disarankan menambah simulasi dengan jumlah pengguna lebih banyak (50–200 user) untuk mengukur skalabilitas sistem dan melihat dampaknya terhadap *throughput*, *latency*, dan *packet loss*.

3. Penelitian lebih lanjut dapat mengevaluasi kinerja ISP dalam jangka panjang, seperti stabilitas harian, fluktuasi *latency*, dan waktu *downtime*, sehingga dapat menentukan ISP mana yang paling optimal untuk diterapkan sebagai jalur utama.

4. Implementasi berikutnya dapat mencoba mengintegrasikan *load balancing* dan *failover* dengan sistem keamanan lanjutan, seperti VPN *site-to-site* atau *SD-WAN*, agar jaringan menjadi lebih stabil, aman, dan fleksibel.