TEKNIS DAN DETAIL PEKERJAAN UNTUK PROJECT AKHIR

LOAD BALANCING & FAILOVER MIKROTIK & RUIJIE

Tujuan Proyek :

1. Mengimplementasikan mekanisme Load Balancing pada MikroTik / Ruijie untuk mendistribusikan trafik internet secara optimal.
2. Menerapkan Failover untuk memastikan konektivitas tetap berjalan meskipun salah satu jalur internet mengalami gangguan.
3. Mengoptimalkan performa jaringan untuk pengguna akhir.

Kebutuhan Teknis Minimal :

1. **Perangkat :**
   - ☑ Router MikroTik : RB4011, RB AC Series, RB AX Series atau Ruijie yang mendukung kebutuhan proyek.
   - ☑ Internet : Minimal 2 koneksi ISP dengan kecepatan berbeda.
   - ☑ Jaringan Internal : Jaringan LAN dengan perangkat klien.
2. Topologi Jaringan :
   - ☑ WAN: Dua atau lebih ISP (misal: ISP1 dan ISP2).
   - ☑ LAN: Terhubung ke switch untuk mendistribusikan koneksi ke klien.

Lingkup Pekerjaan :

1. Setup Perangkat MikroTik :
   - ☑ Mengonfigurasi router MikroTik sebagai load balancer dan failover.
2. Konfigurasi Load Balancing :
   - ☑ Metode yang digunakan PCC dan ECMP (jika menggunakan MikroTik)
   - ☑ Metode yang digunakan Based on Link, Based on Src and Dst IP Address (jika menggunakan Ruijie)
   - ☑ Membagi trafik pengguna berdasarkan algoritma yang dipilih.
3. Implementasi Failover :
   - ☑ Menyiapkan skrip failover otomatis menggunakan Netwatch atau Routing Table (jika menggunakan MikroTik)
   - ☑ Memastikan failover berjalan mulus jika salah satu ISP mengalami gangguan.
4. Pengujian Sistem :
   - ☑ Menguji distribusi beban trafik melalui 2 jalur ISP.
   - ☑ Menguji failover dengan simulasi putusnya salah satu jalur ISP.
5. Dokumentasi :
   - ☑ Dokumentasi teknis konfigurasi dan panduan troubleshooting dan pengelolaan sistem.

TEKNIS DAN DETAIL PEKERJAAN UNTUK PROJECT AKHIR

SISTEM MONITORING JARINGAN (ZABBIX)

Tujuan Proyek :

1. Mengimplementasikan Zabbix sebagai solusi monitoring jaringan untuk memantau kinerja perangkat dan layanan jaringan.
2. Menyediakan notifikasi dan pelaporan otomatis untuk mendeteksi masalah secara cepat.
3. Mengoptimalkan performa dan pemeliharaan infrastruktur jaringan melalui analisis data monitoring.

Kebutuhan Teknis Minimal :

1. Perangkat :
   - ☑ Server fisik atau virtual
   - ☑ Perangkat Target : Router, Switch, dan Access Point
2. Sistem Operasi dan Software :
   - ☑ OS: Linux (Ubuntu, CentOS, atau Debian).
   - ☑ Zabbix Server: Versi terbaru (sesuai kebutuhan proyek).
   - ☑ Database: MySQL, PostgreSQL, atau MariaDB.
   - ☑ Web Server: Nginx atau Apache.

Lingkup Pekerjaan :

1. Persiapan Infrastruktur :
   - ☑ Instalasi server Zabbix.
   - ☑ Konfigurasi database untuk menyimpan data monitoring.
   - ☑ Setup perangkat target untuk dipantau.
2. Implementasi Sistem Monitoring :
   - ☑ Konfigurasi template untuk perangkat jaringan.
   - ☑ Pengaturan notifikasi untuk alur eskalasi (email/Telegram/WA/SMS).
   - ☑ Pembuatan grafik, laporan, dan dashboard.

     Gunakan template bawaan Zabbix atau buat template khusus untuk :

     (CPU Usage, Memory Usage, Network Traffic, Disk Utilization)
3. Uji Coba Sistem Monitoring :
   - ☑ Pengujian koneksi antara server Zabbix dan perangkat target.

     (Pengujian notifikasi, Pengujian Dasboard & Reporting)
   - ☑ Simulasi gangguan untuk memastikan sistem mendeteksi dan memberikan notifikasi.
4. Dokumentasi dan Evaluasi :
   - ☑ Penyusunan panduan implementasi.
   - ☑ Laporan hasil pengujian performa sistem.

TEKNIS DAN DETAIL PEKERJAAN UNTUK PROJECT AKHIR

BISNIS RT/RW NET

Tujuan Proyek :

1. Membangun infrastruktur jaringan untuk layanan internet skala RT/RW.
2. Memastikan distribusi bandwidth yang adil dan stabil untuk seluruh pelanggan.
3. Memberikan sistem pengelolaan pengguna dan keamanan jaringan yang efektif.

Kebutuhan Teknis Minimal :

1. Router MikroTik Router RB2011, RB AC Series, RB AX Series untuk manajemen bandwidth dan routing.
2. Switch unmanaged atau managed untuk distribusi kabel ke pelanggan.
3. Wireless AP (contoh: Ubiquiti, TP-Link, atau MikroTik) untuk area yang membutuhkan koneksi nirkabel.
4. Peralatan Pendukung:
   - ☑ Kabel UTP Cat6 untuk koneksi kabel.
   - ☑ Antena wireless (jika cakupan area luas).

Lingkup Pekerjaan :

1. Perancangan Infrastruktur Jaringan :
   - ☑ Membuat topologi jaringan RT/RW Net.
   - ☑ Menentukan perangkat keras dan perangkat lunak yang dibutuhkan.
2. Implementasi Jaringan :
   - ☑ Instalasi dan konfigurasi perangkat jaringan.
   - ☑ Distribusi internet ke pelanggan melalui kabel atau nirkabel (wireless) menggunakan metode PPPoE Server & Client
3. Manajemen Bandwidth :
   - ☑ Membagi bandwidth berdasarkan :
     - ✓ Skema Berbasis Fixed Bandwidth Per User
     - ✓ Skema Berbasis Prioritas Pengguna (Premium, Reguler & Basic)
   - ☑ Menerapkan mekanisme QoS (Quality of Service).
4. Keamanan Jaringan :
   - ☑ Mengamankan jaringan dari ancaman eksternal (firewall, filtering).
   - ☑ Membuat sistem autentikasi pengguna.
5. Pengujian Sistem :
   - ☑ Menguji konektivitas dan performa jaringan.
   - ☑ Simulasi skenario gangguan untuk memvalidasi stabilitas jaringan.
6. Dokumentasi dan Laporan :
   - ☑ Menyusun panduan implementasi dan hasil pengujian jaringan.

TEKNIS DAN DETAIL PEKERJAAN UNTUK PROJECT AKHIR

IDS MENGGUNAKAN MIKROTIK

Tujuan Proyek :

1. Mengidentifikasi dan mencatat aktivitas mencurigakan pada jaringan.
2. Memberikan peringatan dini terhadap ancaman keamanan.
3. Mencegah serangan lebih lanjut dengan aturan yang sesuai.

Kebutuhan Teknis Minimal :

1. Router MikroTik yang mendukung firewall.
2. Perangkat Uji berupa Komputer atau server untuk simulasi serangan (menggunakan tools seperti hping3, Nmap, atau Metasploit).

Lingkup Pekerjaan :

1. Perancangan Sistem IDS:
   - ☑ Menentukan jenis ancaman yang akan dideteksi (DoS, scanning, dll.).
   - ☑ Merancang konfigurasi deteksi berbasis firewall MikroTik.
2. Implementasi IDS pada MikroTik:
   - ☑ Menggunakan fitur firewall, mangle, dan address-list untuk mendeteksi ancaman.

     IDS akan mendeteksi :
     - ✓ Port Scanning :

       Deteksi upaya pemindaian port yang sering dilakukan oleh penyerang.
     - ✓ DoS/DdoS :

       Deteksi lalu lintas berlebihan dari satu atau beberapa sumber.
     - ✓ Brute Force :

       Deteksi banyak upaya koneksi gagal ke layanan tertentu.
   - ☑ Mencatat log aktivitas ke telegram/email.
3. Pengamanan Tambahan (jika diperlukan) :
   - ☑ Memblokir sementara sumber serangan menggunakan address-list.
4. Pengujian Sistem:
   - ☑ Simulasi serangan jaringan untuk menguji efektivitas IDS.
5. Dokumentasi dan Laporan:
   - ☑ Panduan konfigurasi IDS.
   - ☑ Laporan hasil pengujian.