BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi telah membawa perubahan besar dalam dunia bisnis dan operasional perusahaan. Kini, hampir semua aspek pekerjaan terhubung dengan jaringan internet, mulai dari komunikasi antar karyawan, pengelolaan data, hingga Customer Service. Namun, di balik kemudahan dan kenyamanan yang ditawarkan, integrasi teknologi informasi juga membawa berbagai tantangan, terutama dalam hal keamanan jaringan [1, 2].

Serangan siber menjadi ancaman serius bagi perusahaan, baik yang berasal dari luar (ancaman eksternal) maupun dari dalam organisasi sendiri (ancaman internal). Ancaman eksternal dapat berupa peretasan, penyebaran malware, pencurian data seperti serangan Man-in-the-Middle. Sementara itu, ancaman internal sering kali terjadi tanpa disengaja, misalnya karyawan yang tanpa sadar mengklik tautan phishing dalam email atau mengunduh file yang mengandung virus.

Selain risiko keamanan, penggunaan internet di lingkungan kerja juga menghadirkan tantangan lain. Tanpa pengawasan yang memadai, karyawan dapat menghabiskan waktu kerja untuk hal yang tidak produktif, seperti bermain game, menonton video, atau mengakses media sosial secara berlebihan. Hal ini tidak hanya menurunkan efisiensi kerja, tetapi juga dapat menghabiskan sumber daya jaringan perusahaan, memperlambat koneksi internet yang seharusnya digunakan untuk keperluan bisnis.

Lebih dari itu, tanpa adanya kontrol yang baik, perusahaan juga rentan terhadap penyebaran informasi sensitif secara tidak sengaja. Misalnya, seorang karyawan yang mengakses data penting dari jaringan perusahaan menggunakan perangkat pribadi tanpa perlindungan yang memadai dapat membuka celah bagi peretas untuk mencuri informasi tersebut.

Untuk mengatasi berbagai tantangan ini, perusahaan perlu menerapkan sistem keamanan jaringan yang efektif. Salah satu solusi utama yang digunakan dalam keamanan jaringan adalah firewall. Firewall berfungsi sebagai lapisan pertahanan pertama yang mengontrol lalu lintas data yang masuk dan keluar dari jaringan perusahaan, dengan tujuan mencegah akses yang tidak sah dan melindungi

sistem dari ancaman eksternal maupun internal [3].

Namun, seiring dengan berkembangnya teknik serangan siber yang semakin canggih, firewall tradisional yang hanya berfungsi sebagai pemfilter lalu lintas berdasarkan alamat IP dan port tidak lagi cukup efektif. Oleh karena itu, banyak perusahaan kini beralih menggunakan Next-Generation Firewall (NGFW) yang dapat menyediakan proteksi lebih menyeluruh untuk perusahaan.

1.2 Maksud dan Tujuan Kerja Magang

Kegiatan magang ini dilaksanakan dengan maksud tertentu yang menjadi dasar dalam proses pelaksanaannya. Berikut adalah maksud yang ingin dicapai melalui kegiatan magang ini.

1. Menerapkan softskill dan hardskill yang telah dipelajari di kampus ke dalam praktik di dunia kerja.
2. Mengembangkan pengalaman profesional, khususnya sebagai persiapan sebelum terjun sepenuhnya ke dunia karier.
3. Menambah pengetahuan dalam bidang network security, baik dengan memperoleh pengetahuan baru atau memperluas pengetahuan yang sudah ada.

Berdasarkan permasalahan yang telah diidentifikasi dalam keamanan jaringan perusahaan, tujuan dari kerja magang ini adalah implementasi dan konfigurasi kebijakan keamanan menggunakan perangkat FortiGate, yang mencakup Firewall Policy, IPS (Intrusion Prevention System), Web Filtering, Application Control, Antivirus, Traffic Shaping, dan VPN (Virtual Private Network). Langkah ini diharapkan dapat meningkatkan perlindungan terhadap ancaman siber, memastikan efisiensi lalu lintas jaringan, serta menjaga keamanan data perusahaan.

1.3 Waktu dan Prosedur Pelaksanaan Kerja Magang

Berdasarkan kontrak yang telah disepakati, kegiatan magang dimulai pada tanggal 3 Februari 2025 dan berakhir pada 31 Mei 2025. Program magang ini diterapkan dengan sistem bekerja di kantor (WFO). Secara rinci, sistem kerja ini diterapkan setiap minggu mulai dari hari Senin hingga Jumat. Jam kerja ditetapkan

dari pukul 09:00 WIB hingga 18:00 WIB setiap harinya, dengan waktu istirahat yang berlangsung selama satu jam, dimulai dari pukul 12:00 WIB hingga 13:00 WIB. Untuk absensi pada hari kerja di kantor, digunakan sistem absensi face recognition untuk memastikan presensi yang tepat.