BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi yang sangat pesat dan tak luput dari inovasi serta riset yang berlangsung, tentu ada sisi positifnya seperti kemudahan dalam melakukan komunikasi dan pertukaran data, dan sisi negatifnya adalah adanya kejahatan siber yaitu serangan dan pencurian data. Hal tersebut sangat menarik perhatian publik dikarenakan semakin maju teknologi, maka serangan dan pencurian data menjadi semakin tinggi dengan model yang canggih. Salah satu bentuk kejahatan siber adalah serangan zero day, di mana serangan tersebut merupakan ancaman yang berpotensi tinggi karena memanfaatkan kerentanan yang belum pernah diketahui. (Yasin, n.d.).

Dampak negatif dari perkembangan teknologi tersebut dapat mengakibatkan kerugian khusunya yang berhubungan dengan sejumlah data-data yang merupakan informasi penting dan hanya diperbolehkan untuk diketahui oleh orangorang tertentu di dalam sebuah perusahaan. Selain itu, serangan zero day juga dapat merusak reputasi perusahaan dan mengganggu operasional bisnis secara keseluruhan. Oleh karena itu, penting bagi perusahaan untuk memiliki sistem keamanan yang kuat dan terus memperbarui perlindungan mereka terhadap serangan semacam ini. Kasus kebocoran data terbesar di dunia berdasarkan laporan CSO yaitu kebocoran data Yahoo pada agustus 2013 di mana ada sekitar 3 miliar akun yang berada di layanan mereka bocor (Khalisah & Kirana, 2022), sehingga keamanan data adalah prioritas utama untuk diperhatikan dari kerusakan ataupun penyalahgunaan dari pihak tanggung jawab.

Salah satu langkah yang dapat digunakan untuk mencegah adanya pencurian data atau informasi dalam suatu jaringan, yaitu dengan menggunakan teknologi firewall(Ramos Brandao & Almeida, 2021). Fungsi firewall adalah menjaga jaringan dari trafic yang berbahaya, di mana bentuk dari firewall dapat berupa hardware maupun software. Jika diilustrasikan firewall dapat digambarkan seperti pintu gerbang. Jadi ketika kita mengirimkan paket dari internet, sebelum sampai dikirimkan kepada user, firewall menyarinng paket tersebut dan memutuskan

apakah paket tersebut diterima atau ditolak.

Firewall merupakan suatu sistem yang dapat menerapkan access control policy pada lalu lintas jaringan, yang dapat membantu melindungi dari serangan lalu lintas jaringan dan serangan lainnya, serta dapat memfilter lalu lintas jaringan yang masuk pada jaringan. Implementasi firewall sangat penting diterapkan pada perangkat komputer untuk menghindari dari pencurian data-data yang ada di dalam perangkat yang sifatnya rahasia. Implementasi firewall penting untuk diterapkan pada jaringan untuk menjaga dari ancaman serangan. Dasar kinerja yang dimiliki firewall, yaitu dapat mendeteksi traffic jaringan yang sah. Seingga dapat diberikan akses ke dalam sistem dengan melewati firewall untuk dibatasi. Pembatasan akses yang masuk ke dalam jaringan lokal, kemudian melakukan pencegahan jaringan yang tidak terdaftar pada sistem. Pembatasan dilakukan dengan diaturnya rules atau policy pada konfigurasi firewall. The next-generation firewall (NGFW).

Next Generation Firewall merupakan firewall yang memiliki kemampuan dalam mendeteksi dan memblokir suatu serangan yang berbahaya. Kemampuan NGFW dengan memberikan proteksi dan perlindungan yang tinggi, serta dapat menerapkan keamanan yang terdapat pada tingkat protocol, port, dan aplikasi. Next generation firewall adalah bagian dari generasi ketiga firewall, perbedaan paling jelas antara keduanya adalah kemampuan next generation firewall untuk menyaring setiap trafic berdasarkan aplikasi. Pengguna next generation firewall dapat menggunakan white list atau signature-based IPS untuk membedakan antara aplikasi yang aman dan yang tidak aman, dan juga next generation firewall dapat membuat policy sampai Layer 7 dengan menggabungkan konten AI (IPS, Antivirus, Antispyware, dll) dalam policy.

Berdasarkan fenomena kasus di atas yaitu, rentannya pencurian data dan kebocoran data sehingga saya mengangkat judul tentang implementasi next generation firewall dan cara kerjanya untuk bertahan terhadap serangan Jurnal Informatika Universitas Dikarenakan next generation firewall memiliki fitur yang lebih kompleks dalam pertahanan terhadap malware, saya menggunakan next generation firewall pada penelitian ini.

Pada penelitian ini saya memilih mengamankan sistem dengan next generation firewall dibandingkan dengan firewall tradisional dikarenakan firewall tradisional

tidak dapat memblokir malware (PENGAMANAN SISTEM JARINGAN KOMPUTER DENGAN TEKNOLOGI FIREWALL I Gede Suputra Widharma and The A Team, n.d.). Penelitian ini melakukan implementasi seperti penelitian, yaitu melakukan implementasi web filter, antivirus, IPS, dan antiDDoS. Pada penelitian ini, juga melakukan pengujian ketahanan next-generation firewall terhadap serangan malware.

Pengujian ketahanan terhadap serangan malware pada next generation firewall pada penelitian ini menggunakan randsomware, Wannacry, dan malware lainnya. Penelitian ini menggunakan Wannacry dikarenakan menurut laporan ancaman ransomware unit 42 paloalto, mengemukakan bahwa trend randsomware terus meningkat. Jika diilihat dari laporan pada tahun 2022, kasus randsomware meningkat 144% dari tahun sebelumnya dan terdapat 85% jumlah peningkatan korban.

Wannacry terjadi pada sejak mei 2017 sampai saat ini telah melumpuhkan lebih dari 200.000 komputer di lebih dari 150 negara, dengan estimasi total kerugian mulai dari ratusan juta hingga miliaran US dollar. Cara kerja wannacry sendiri adalah dengan mengenkripsi semua dokumen yang dimiliki korban, sehingga korban tidak dapat mengakses dokumen tersebut dan juga menuntun tebusan kepada korban untuk dapat mengakses dokumen yang dia miliki. Target dari Proyek Akhir ini diharapkan dapat meningkatkan pertahanan sebuah firewall dari serangan malware dan juga membantu dalam mendeteksi dan mencegah serangan malware lebih awal.