BAB 1

PENDAHULUAN

1.1 Latar Belakang

Di era digitalisasi yang semakin berkembang, teknologi informasi dalam berbagai aspek kehidupan tidak dapat dihindari. Universitas Bina Darma yang bermotto Standar Internasional dan Berbasis Teknologi Sistem Informasi, merupakan entitas yang sangat tergantung pada infrastruktur IT untuk mendukung proses pembelajaran, penelitian, dan administrasi. Namun, semakin berkembangnya teknologi juga membawa risiko yang semakin kompleks terhadap keamanan informasi. Ancaman keamanan seperti malware, serangan DDoS, dan penetrasi hacker menjadi ancaman yang nyata dan berpotensi merusak integritas jaringan dan ketersediaan data serta layanan.

Dalam konteks Universitas Bina Darma, keamanan informasi menjadi krusial karena melibatkan data sensitif seperti informasi pribadi mahasiswa dan pegawai, data akademik, serta sistem administrasi universitas. Salah satu pendekatan utama dalam melindungi sistem informasi dari ancaman tersebut adalah dengan penggunaan teknologi firewall. Firewall tradisional sudah umum diterapkan untuk membatasi akses jaringan berdasarkan aturan tertentu, namun demikian, semakin berkembangnya teknik serangan mengharuskan pengembangan solusi keamanan yang lebih maju.

Dikutip dari *Gartner (2024)* Next Generation Portal Web muncul sebagai evolusi dari firewall tradisional dengan menawarkan kemampuan yang lebih canggih, termasuk integrasi dengan teknologi Intrusion Prevention System (IPS). IPS memungkinkan firewall untuk melakukan deteksi dan pencegahan terhadap serangan yang lebih kompleks dan lebih canggih, termasuk serangan yang menggunakan pola serangan yang tidak biasa atau *zero-day attacks*.

Namun demikian, Rancang bangun Next Generation Portal Web dengan IPS tidak selalu mudah dilakukan karena memiliki tantangan tersendiri. Beberapa faktor yang perlu dipertimbangkan antara lain adalah kompleksitas konfigurasi, biaya implementasi dan operasional, serta kebutuhan akan pemeliharaan yang terus-menerus. Oleh karena itu, penelitian ini bertujuan untuk mengeksplorasi Next Generation Portal Web dengan metode IPS khususnya untuk server Portal Web di Universitas Bina Darma.

Dengan memfokuskan penelitian pada Rancang Bangun Next Generation Portal Web berbasis IPS, diharapkan dapat meningkatkan pemahaman dan penerapan teknologi keamanan informasi yang lebih efektif dan adaptif di lingkungan akademik. Maka dari itu penulis akan melakukan penelitian yang berjudul **"Rancang Bangun Next Generation Portal Web Di Universitas Bina Darma".**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan diatas rumusan masalah dalam penelitian ini adalah untuk memperbarui firewall dan melindungi dari ancaman-ancaman baru?

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

a. Difokuskan pada firewall Next Generation pada Portal Web sebagai solusi utama untuk meningkatkan keamanan sever, khususnya di lingkungan Universitas Bina Darma.

b. Rancang Bangun Next Generation Portal Web akan secara khusus mengintegrasikan teknologi IPS, yang bertujuan untuk mendeteksi port jaringan komputer khususnya di Universitas Bina Darma dan mencegah serangan jaringan secara aktif dengan mengidentifikasi pola serangan yang tidak biasa dan tanda-tanda intrusi.

c. Penggunaan Next Generation Firewall dengan Metode IPS untuk meningkatkan keamanan server portal web di Universitas Bina Darma. Hal ini mencakup perlindungan terhadap akses tidak sah, pencurian data, dan serangan-serangan yang dapat mempengaruhi integritas serta ketersediaan layanan web universitas.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah merancang keamanan menggunakan firewall next Generation dengan metode IPS yang bertujuan untuk mengetahui penyerangan jalur jaringan pada Server Portal Web di Universitas Bina Darma.

1.5 Manfaat Penelitian

a. Manfaat terhadap penulis yaitu akan memberikan pengalaman berharga bagi penulis dalam merancang, dan mengevaluasi teknologi keamanan informasi yang kompleks seperti Next Generation Portal Web dengan teknologi Intrusion Prevention System (IPS). Hal ini akan meningkatkan pemahaman teknis dan metodologis penulis dalam bidang keamanan informasi.
b. Manfaat terhadap universitas bina darma yaitu mengurangi risiko terhadap serangan yang dapat mengganggu ketersediaan layanan, universitas akan dapat memberikan layanan yang lebih stabil dan dapat diandalkan kepada seluruh komunitas akademiknya, termasuk mahasiswa, staf, dan dosen.
c. Manfaat terhadap dunia akademis yaitu untuk memberikan masukan berharga bagi pengembangan teknologi keamanan informasi, khususnya dalam konteks penggunaan Next Generation Portal Web dengan IPS. Temuan dan metodologi yang dikembangkan dapat digunakan sebagai referensi bagi institusi pendidikan lainnya untuk meningkatkan keamanan informasi mereka.

1.6 Penelitian Terdahulu

1. Dalam penelitian yang berjudul "Keamanan jaringan Vlan dan VoIP menggunakan Metode IPS" (Satra & Fattah, 2021) Penulis telah mencapai beberapa kesimpulan yaitu pengujian implementasi firewall untuk keamanan jaringan VLAN dan VoIP. Pengujian firewall menunjukkan bahwa sistem memiliki kemampuan untuk memblokir pengguna yang tidak terdaftar dalam router. Diharapkan bahwa ini akan membantu mengamankan jalur komunikasi antar user. Berdasarkan temuan di atas, penulis dapat memberikan rekomendasi tentang cara melakukan pengembangan sistem yang lebih baik. Dengan demikian, penelitian ini dapat digunakan sebagai referensi untuk penelitian selanjutnya yang berkaitan dengan meningkatkan keamanan sistem seperti pengawasan intrusi, sistem perlindungan, dan lain-lain. sistem dapat menggabungkan area Metropolitan Area Network (MAN) atau Wide Area Network (WAN).
2. Dalam penelitian yang berjudul "Perancangan Keamanan Jaringan Next-Generation Firewall Menggunakan Router Fortinet Pada Pt. Alodokter Teknologi Solusi" (Dwi Setiawan, Ridwansyah, 2023) Penulis telah mencapai beberapa kesimpulan dari diskusi dan penelitian yang telah dilakukan, termasuk bahwa fitur Next-Generation Firewall yang diaktifkan pada router Fortinet dapat membantu menjaga keamanan jaringan internet, melindungi jaringan dari serangan siber dari pihak ketiga, membatasi akses internal yang dapat menyebabkan

serangan atau efek negatif pada pengguna interpersonal, dan melacak trafik di berbagai platform jaringan. Fitur Intrusion Prevention System (IPS) dapat membantu secara aktif memasukkan lalu lintas yang mencurigakan ke daftar hitam. Untuk meningkatkan keamanan jaringan, fitur Web Filtering dan Control Application yang sudah digunakan secara default harus digunakan sebaik mungkin. Dengan Next-Generation Firewall, pengguna internal tidak dapat mengakses hal-hal yang tidak diizinkan. Ini juga memungkinkan mereka untuk memantau trafik yang digunakan dan menangkal serangan siber dari pihak ketiga.

3. Dalam penelitian yang berjudul "Implementasi Web Application Firewall Dalam Mencegah Serangan SQL Injection Pada Website"(Bangkit Wiguna et al., 2020) Pengujian dan analisis Web Application Firewall menunjukkan bahwa menggunakan mod keamanan akan memperpanjang waktu load website karena sistem keamanan pada Sebelum dikirim ke website, WAF akan memeriksa semua masuk. Dengan demikian, akan membutuhkan waktu bagi pengguna untuk menerima halaman web yang diminta oleh server. Loading time (ms) OWASP WAF dan Mod Security WAF berbeda, tetapi load time HTTP biasanya tidak mempengaruhi kinerja web. Hasil uji coba serangan menunjukkan bahwa penggunaan Web Application Firewall dapat mengurangi serangan SQL Injection. Hal ini disebabkan oleh fakta bahwa alat mod keamanan ini akan memungkinkan sistem untuk membatasi kemampuan penyerang untuk menerapkan SQL

Injection dalam sebuah website. Dengan demikian, hasil pengujian menunjukkan bahwa penyerang tidak dapat mengakses informasi apa pun yang ada di situs web karena celah yang terbuka di sistem keamanan ini telah ditutup.

4. Dalam penelitian yang berjudul "Analisis Dan Perancangan Private Cloud Storage Menggunakan Metode Pengamanan Ids (Intrusion Detection System) Dan Ips(Intrusion Prevention System) (Studi Kasus: Diskominfo Kota Padang Panjang) (Meiditra, 2023)Metode IPS mendeteksi penyusup melalui analisis lalu lintas real-time.

   Ini dapat mendeteksi berbagai jenis serangan masuk. Selain itu, fitur Snort dapat membantu administrator sistem dan jaringan dengan memberikan peringatan. kita atas penyusup yang mungkin mengancam keamanan. Metode IPS dapat mencegah serangan port scanning yang dilakukan oleh pencuri terhadap server cloud computing dengan mengaktifkan fitur firewall dan mengkonfigurasikannya dengan iptables. IPS berfungsi seperti firewall, mengizinkan atau menghalang paket data kepada beberapa komponen, seperti mesin deteksi, scanner layanan, dan pengatur lalu lintas. Shaper menggabungkan metode firewall dan intrusion detection system (IDS) dengan baik. Serangan ke jaringan lokal dapat dicegah dengan teknologi ini. memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor saat seragan teridentifikasi.