BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi saat ini semakin pesat membawa dampak positif dalam berbagai sektor kehidupan saat ini, tetapi juga diiringi oleh meningkatnya ancaman keamanan siber. Salah satu ancaman utamanya yaitu Ransomware, sebuah jenis malware yang mengancam data korban dan meminta tebusan untuk memulihkan akses. Sebagai contoh, serangan malware seperti Ransomware telah berkembang menjadi ancaman yang semakin sering terjadi dan berdampak besar pada berbagai sektor industri[1].

Menggunakan perangkat lunak keamanan yang kuat, seperti antivirus dan firewall, untuk mendeteksi dan mencegah serangan ransomware. Untuk mendeteksi serangan ransomware dengan lebih baik, pertimbangkan untuk menggunakan produk keamanan tambahan, seperti sistem deteksi intrusi atau pemantauan perilaku[2]. Di dalam kasus ini penulis ingin membuktikan perangkat lunak keamanan yang kuat, seperti antivirus dan firewall dengan snort untuk mencegah Ransomware. Menggunakan perangkat lunak keamanan yang kuat, seperti antivirus dan firewall, untuk mendeteksi dan mencegah serangan Ransomware.

PfSense adalah Firewall *open-source* yang dilengkapi dengan antarmuka berbasis web yang intuitif serta beragam fitur, termasuk pengaturan rute, VPN, dan QoS[3]. Dalam pfSense yang *open-source* di dalamnya di pasangkan juga snort untuk IDS/IPS terhadap ransomware.

Antivirus Avast merupakan antivirus yang relatif lebih efisien dibandingkan dengan antivirus lain yang diuji karena memiliki rata-rata penggunaan CPU dan memory yang rendah, tingkat deteksi yang cukup tinggi, dan waktu scan yang cepat[4].

Meskipun kedua solusi ini dirancang untuk melindungi sistem dari ancaman seperti Crypto Ransomware, perbedaan dalam pendekatan, metode deteksi, dan cakupan perlindungan menimbulkan pertanyaan tentang efektivitas masing-

masing. Oleh karena itu,penelitian ini bertujuan untuk menganalisis dan membandingkan efektivitas pfSense dengan IDS/IPS dan Avast Antivirus dalam mencegah ransomware. Dengan pengujian dan simulasi nyata, hasil dari penelitian ini diharapkan dapat memberikan panduan yang jelas bagi pengguna dalam memilih atau mengintegrasikan solusi keamanan siber yang optimal.

1.2 Rumusan Masalah

1. Bagaimana efektivitas pfSense dengan Snort IDS/IPS dibandingkan dengan Antivirus Avast dalam mencegah serangan Crypto Ransomware?
2. Apa kelebihan dan kekurangan dari pfSense dengan IDS/IPS dibandingkan dengan Antivirus Avast dalam mencegah Crypto Ransomware?

1.3 Batasan Masalah

1. Penelitian dilakukan pada lingkungan jaringan yang disimulasikan menggunakan perangkat virtual seperti VirtualBox.
2. Penelitian hanya difokuskan pada ancaman Crypto Ransomware dan tidak mencakup jenis malware lainnya.
3. Firewall yang digunakan adalah pfSense versi terbaru dengan fitur IDS/IPS yang di padukan dengan snort.
4. Antivirus yang digunakan adalah Avast versi gratis dengan pengaturan *Ransomware Shield*.
5. Penelitian hanya mencakup aspek efektivitas deteksi, pencegahan, kelebihan dan kekurangan sistem.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitiannya adalah menghasilkan :

1. Menganalisis efektivitas pfSense dengan Snort IDS/IPS dan Antivirus Avast dalam mendeteksi dan mencegah serangan Crypto Ransomware
2. Membandingkan kelebihan dan kekurangan dari kedua solusi keamanan ini dalam konteks pencegahan ransomware.

1.5 Manfaat Penelitian

1. Manfaat Teoritis :
   a. Menambah wawasan ilmiah tentang peran dan efektivitas teknologi keamanan jaringan (pfSense dengan IDS/IPS) dan perangkat keamanan endpoint (Antivirus Avast) dalam mencegah Ransomware.
   b. Memberikan edukasi tentang pentingnya keamanan siber, terutama dalam menghadapi ancaman ransomware.
2. Manfaat Praktisi :
   a. Membantu praktisi memahami efektivitas kombinasi solusi keamanan jaringan dan endpoint.
   b. Memberikan gambaran nyata tentang kelebihan dan kekurangan penggunaan pfSense dengan IDS/IPS serta Antivirus Avast dalam menangani ancaman Ransomware.

1.6 Sistematika Penulisan

BAB I Menjelaskan tentang pendahuluan laporan yang meliputi latar belakang, rumusan masalah, tujuan, batasan masalah dan sistematika penulisan.

BAB II Menjelaskan tentang tinjauan pustaka yang mendukung pemahaman penulis untuk melaksanakan penelitian yang berkaitan dengan penerapan Firewall dan Antivirus dalam mencegah serangan ransomware.

BAB III Menjelaskan tentang metodologi penelitian, tahapan penelitian (flowchart).

BAB IV Menjelaskan tentang perbandingan antara Firewall dengan Antivirus dari segi pengolahan data dan analisis yang di hasilkan.

BAB V Menjelaskan tentang kesimpulan dan saran penulis.