

BAB V PENUTUP

5.1 Kesimpulan

Berdasarkan dari hasil penelitian ini. Penelitian ini memperoleh Konfigurasi perlindungan maksimal jaringan yang dicapai melalui penerapan tiga lapisankeamanan secara bertingkat pada router pfsense :

1. Segmentasi antarmuka jaringan menjadi WAN, LAN, OPT1 untuk membatasi lateral movement antar segmen
2. Penerapan firewall rules berbasis least privilege dan penerapan prinsip default deny pada setiap interface.
3. Integrasi IDS snort dengan fitur block offenders yang mengubah dari deteksi aktif menjadi sistem pencegahan aktif (IPS). Kombinasi ke tiga lapisan mampu mengisolasi jaringan internal dari ancaman external sepenuhnya.

Sistem IDS snort yang terintegrasi pada pfSense berhasil menanggulangi seluruh jenis ancaman yang di uji secara otomatis : *Port Scanning (Nmap)*, *SYN flood* dan *ICMP flood (Hping3)*, *UDP Flood (Loic)*, dan *Brute Force SSH (Hydra)*, setelah deteksi, IP penyerang secara otomatis dimasukan ke Alert Snort dan Block Table sehingga seluruh koneksi dari IP tersebut di putus tanpa menunggu layanan jaringan internal

Secara keseluruhan, integrasi pfSense dan Snort terbukti mampu mengoptimalkan keamanan jaringan secara terpusat, adaptif, dan responsif terhadap ancaman pada lingkungan jaringan skala kecil hingga menengah.

5.2 Saran

Sebagai bahan pertimbangan peneliti memberikan beberapa saran untuk nantinya dijadikan pengembangan pada penelitian selanjutnya.

1. Peneliti berikutnya dapat melakukan pengujian pada skala jaringan yang lebih besar dengan jumlah client dan trafik yang lebih tinggi untuk mengetahui performa sistem keamanan secara lebih mendalam.

2. Pengembangan sistem keamanan dapat ditingkatkan dengan menambahkan mekanisme keamanan lain seperti VPN, Web Application Firewall (WAF), Multi-Factor Authentication (MFA), dan SIEM (Security Information and Event Management).
3. Rules pada fitur IDS Snort perlu diperbaharui secara berkala agar sistem mampu mendeteksi pola serangan terbaru dan meminimalkan false positif dan false negatif.
4. Monitoring jaringan sebaiknya diintegrasikan dengan sistem notifikasi otomatis seperti email alert atau Telegram bot agar administrator dapat merespons ancaman keamanan secara lebih cepat.

