

BAB V PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian, pengujian, serta analisis yang telah dilakukan pada bab-bab sebelumnya mengenai implementasi *Cloud SIEM Wazuh* pada *pfSense*, maka dapat ditarik kesimpulan sebagai berikut:

10. Keberhasilan Integrasi Infrastruktur Hybrid:

Penelitian ini telah berhasil mengintegrasikan *pfSense* di jaringan lokal dengan *Wazuh Manager* yang berada di *Cloud VPS*. Sistem mampu melakukan pengiriman *log* secara *real-time* dan melakukan analisis terpusat meskipun terdapat perbedaan lokasi infrastruktur.

11. Peningkatan Kecepatan Respon Mitigasi:

Penggunaan fitur *Active Response* terbukti secara signifikan meningkatkan efektivitas keamanan. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi dan melakukan mitigasi otomatis dalam waktu rata-rata **2,2 detik**. Hal ini menunjukkan peningkatan efisiensi sebesar **78%** dibandingkan dengan sistem standar *pfSense* (Skenario A) yang membutuhkan waktu di atas 10 detik.

12. Akurasi Deteksi Ancaman Kritis:

Implementasi *ruleset* dengan ambang batas Level 10 (Rule ID 5760) terbukti akurat dalam mengidentifikasi serangan *brute force*. Sistem mampu membedakan antara insiden keamanan kritis dengan kesalahan *login* biasa, sehingga tindakan pemblokiran (*firewall-drop*) hanya dilakukan pada aktivitas yang benar-benar mengancam integritas jaringan.

13. Resiliensi Sistem Keamanan:

Pengujian membuktikan bahwa mesin analisis pada *Cloud VPS* tetap bekerja secara mandiri untuk memberikan perintah mitigasi meskipun terdapat kendala pada akses visual Dashboard (GUI). Hal ini menunjukkan bahwa fungsi proteksi sistem tetap berjalan optimal selama layanan pusat analisis aktif.

5.2 Saran

Berdasarkan proses pengerjaan dan kendala yang ditemukan selama penelitian, peneliti memberikan beberapa saran untuk pengembangan lebih lanjut:

5. **Implementasi Jalur VPN Site-to-Site:** Untuk mengatasi kendala eksekusi mitigasi balik akibat limitasi jaringan (Double NAT/ISP), disarankan untuk menggunakan jalur VPN antara pfSense lokal dan Cloud VPS guna memastikan komunikasi instruksi *Active Response* lebih stabil dan langsung.
6. **Optimasi Monitoring Visual:** Perlu dilakukan peninjauan ulang terhadap konfigurasi *Security Group* atau penggunaan *Reverse Proxy* pada Cloud VPS untuk mempermudah akses administrator ke Dashboard Wazuh tanpa terkendala oleh kebijakan jaringan ISP tertentu.
7. **Pengembangan Ruleset Multidimensi:** Penelitian selanjutnya dapat dikembangkan dengan menambahkan aturan (*custom rules*) untuk jenis serangan lain seperti *Port Scanning* atau *DDoS Attack* guna memperluas cakupan proteksi SIEM pada infrastruktur pfSense.