BAB V
KESIMPULAN

5.1. Kesimpulan

Berdasarkan hasil penelitian yang peneliti lakukan tentang analisi performa keamanan jaringan di PT XYZ terhadap serangan DDoS dan serangan *ransomware*, maka dapat diambil kesimpulan sebagai berikut :

a. Kontrol keamanan terhadap serangan DDoS di PT XYZ sangat perlu diterapkan karena pengaruhnya terhadap infrastruktur IT sangat besar dan akibatnya akan mengganggu operasional bisnis.
b. Penerapan kontrol keamanannya dapat berupa pembatasan koneksi suatu alamat IP pada *firewall* dan penggunaan *rate limiter* pada *reverse proxy* untuk mengurangi pengaruh dari serangan DDoS dengan *flag* SYN, TCP, dan HTTP dengan perubahan rata-rata kenaikan pada *throughput* sebesar 6,67 Mbps, rata-rata nilai pada *jitter* sebesar 2,23 ms, rata-rata persentase penurunan *latency* sebesar 86,67%, rata-rata persentase penurunan *packet loss* sebesar 87%, dan rata-rata persentase penurunan penggunaan CPU pada *firewall* sebesar 49,67%.
c. Penggunaan Suricata sebagai IDS juga dapat dipertimbangkan untuk mendeteksi sumber serangan dan adanya potensi serangan lebih lanjut sekaligus menjadi dokumentasi untuk mencegah terjadinya serangan lebih lanjut.
d. Autentikasi dan *website filtering* yang sudah diterapkan di PT XYZ dengan Squid Proxy terbukti mampu mengurangi potensi ancaman di Head Office.
e. Implementasi dari Squid Proxy tersebut tidak terlalu memengaruhi kecepatan internet di Head Office sehingga tidak mengganggu operasional bisnis.
f. Suricata sebagai IDS juga dapat diimplementasikan untuk memastikan koneksi jaringan yang masuk dan keluar jaringan Head Office untuk

deteksi awal dari adanya aktivitas mencurigakan sekaligus mengurangi potensi ancaman serangan *ransomware*.

g. Mitigasi dan pencegahan terhadap serangan *ransomware* lebih tepat diamankan pada keamanan *endpoint*, yaitu perangkat yang digunakan karyawan seperti antivirus, SIEM, dan XDR.
h. Meskipun keamanan jaringan tidak dapat mencegah serangan *ransomware* seutuhnya, namun keamanan jaringan seperti penerapan autentikasi, *website filtering*, dan IDS dapat mengurangi potensi serangan.

5.2. Saran

Berikut ini adalah saran yang dapat peneliti sampaikan untuk penelitian berikutnya dalam topik ini agar mendapatkan hasil yang lebih baik:

a. Pengujian dapat dilakukan pada *environment* terisolasi di perusahaan agar hasil performa jaringan akan sesuai dengan kondisi aslinya.
b. *Firewall* dengan perangkat keras atau *firewall appliance* seperti Cisco Secure Firewall dan Fortinet Fortigate dapat digunakan agar konfigurasi dapat disesuaikan dengan kondisi perusahaan dan fitur yang dapat digunakan lebih banyak
c. Penerapan antivirus pada *network layer* dapat dipertimbangkan dengan menggunakan *software* berbayar seperti FortiGuard untuk mencegah serangan *ransomware*.
d. Jumlah *botnet* pada serangan DDoS dapat diperbanyak sebanyak 10 perangkat dan protokol yang digunakan bisa lebih beragam seperti UDP dan ICMP.