ANALISIS IMPLEMENTASI MODSECURITY DAN NGINX CACHING DI KUBERNETES UNTUK MITIGASI HTTP(S) FLOOD

Pembimbing Ery Setyawan Jullev Atmadji, S.Kom., M.Cs.

Muhammad Ilham
Program Studi Teknik Informatika
Jurusan Teknologi Informasi

ABSTRAK

Serangan *Distributed Denial of Service* (DDoS), khususnya jenis *HTTP(S) Flood*, menjadi ancaman serius bagi ketersediaan layanan web karena kemampuannya dalam menguras sumber daya server. Penelitian ini menganalisis implementasi arsitektur pertahanan ganda (*dual-layer defense*) yang mengombinasikan ModSecurity sebagai *Web Application Firewall* (WAF) dan *Nginx Caching* pada klaster Kubernetes untuk memitigasi serangan tersebut. Pengujian dilakukan menggunakan metode *incremental load testing* dan *stress testing* hingga beban 1.000 *concurrent users* melalui perangkat Apache JMeter. Hasil eksperimen menunjukkan bahwa penerapan mekanisme mitigasi tunggal menyisakan celah kerentanan kritis, seperti manipulasi *cache bypass* atau terjadinya efek *bottleneck* komputasi CPU yang parah pada gerbang *Ingress*. Sebaliknya, penggabungan kedua metode tersebut terbukti secara efektif mampu mengisolasi *Application Pods* dari ancaman kelumpuhan layanan (*downtime*), menjaga konsumsi CPU internal tetap stabil di bawah 25 *millicores*, serta mencapai tingkat pemblokiran serangan yang konsisten sebesar 95,00%. Kendati demikian, ketahanan infrastruktur klaster pada akhirnya dibatasi oleh spesifikasi perangkat keras fisik (2 *core* CPU), yang memicu lonjakan anomali *Context Switches* serta fenomena *CPU throttling* saat menerima tekanan beban ekstrem.

Kata kunci: Kubernetes, ModSecurity, Nginx, Caching, HTTP(S) Flood, DDoS, *Web Application Firewall*, *Nested Virtualization*, Proxmox, Apache JMeter

ANALYSIS OF MODSECURITY AND NGINX CACHING IMPLEMENTATION IN KUBERNETES FOR HTTP(S) FLOOD MITIGATION

Supervisor Ery Setyawan Jullev Atmadji, S.Kom., M.Cs.

Muhammad Ilham
Study Program of Informatics Engineering
Majoring of Information Technology

ABSTRACT

Distributed Denial of Service (DDoS) attacks, particularly HTTP(S) Floods, pose a severe threat to web service availability as they rapidly exhaust server resources. This study analyzes the implementation of a dual-layer defense architecture that combines ModSecurity as a Web Application Firewall (WAF) and Nginx Caching within a Kubernetes cluster to mitigate these attacks. Testing was executed using incremental load and stress testing scenarios with up to 1,000 concurrent users conducted via Apache JMeter. The experimental results demonstrate that deploying a single mitigation mechanism leaves critical vulnerabilities open to cache bypass manipulations and causes severe CPU utilization bottlenecks at the Ingress gateway. In contrast, combining both methods effectively isolates Application Pods against service downtime, maintaining internal CPU consumption consistently below 25 millicores and achieving a stable attack blocking rate of 95.00%. However, the overall cluster resilience remains constrained by the physical hardware limitations (2 CPU cores), triggering elevated context switches and CPU throttling under extreme load pressures.

Keywords: Kubernetes, ModSecurity, Nginx, Caching, HTTP(S) Flood, DDoS, *Web Application Firewall*, *Nested Virtualization*, Proxmox, Apache JMeter