Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI) **e-ISSN 2830-3954**
Volume: 5, Nomor: 2, Mei 2026: 180-190 **p-ISSN 2830-6031**
https://jurnal.unity-academy.sch.id/index.php/jirsi/index

Hardening Keamanan Server eOffice Apache dengan TLS 1.3 dan Fail2ban

A Security Hardening Approach for Apache-Based eOffice Servers Using TLS 1.3 and Fail2ban

Parulian*[1], Baringin Sianipar[2], Danny Sihombing[3]
[123]Program Studi Informatika, Universitas HKBP Nommensen
Email: [1]liansirait@uhn.ac.id, [2]danny@uhn.ac.id, [3]baringin.sianipar@uhn.ac.id

Abstrak

Keamanan layanan digital kampus semakin krusial seiring meningkatnya intensitas serangan otomatis seperti brute force, scanning, dan eksploitasi file upload yang menargetkan sistem administrasi berbasis web. Server eOffice Universitas HKBP Nommensen sebagai pusat dokumentasi dan surat-menyurat kampus juga menghadapi ancaman tersebut. Penelitian ini bertujuan untuk meningkatkan keamanan server melalui penerapan strategi hardening berbasis defense-in-depth pada Apache 2.4. Metodologi yang digunakan meliputi aktivasi TLS 1.3 untuk komunikasi terenkripsi modern, penerapan Security Headers sesuai standar OWASP, isolasi direktori untuk membatasi eksekusi file berbahaya, serta implementasi Fail2ban sebagai Intrusion Prevention System (IPS) berbasis log dengan pendekatan multi-jail. Evaluasi dilakukan menggunakan SSL Labs, SecurityHeaders.com, dan analisis log serangan. Hasil penelitian menunjukkan peningkatan signifikan, ditandai dengan peningkatan grade SSL dari B menjadi A+ serta peningkatan nilai Security Headers menjadi Grade A. Selain itu, sistem IPS yang diterapkan terbukti efektif dalam mendeteksi dan memitigasi serangan otomatis secara real-time. Kesimpulannya, kombinasi Apache hardening, konfigurasi TLS modern, dan IPS berbasis log mampu meningkatkan ketahanan layanan eOffice secara signifikan serta dapat direplikasi oleh institusi lain dengan sumber daya terbatas.

Kata kunci: *Keamanan Web; Apache Hardening; TLS 1.3; Security Headers; Fail2ban; IPS*

Abstract

The security of campus digital services has become increasingly critical due to the rising intensity of automated attacks such as brute-force attempts, vulnerability scanning, and file upload exploitation targeting web-based administrative systems. The eOffice server of Universitas HKBP Nommensen, which serves as the central platform for document management and official correspondence, is also exposed to such threats. This study aims to enhance server security by implementing a defense-in-depth hardening strategy on Apache 2.4. The methodology includes the activation of TLS 1.3 for modern encrypted communication, the implementation of OWASP-compliant security headers, directory isolation to restrict malicious file execution, and the deployment of Fail2ban as a log-based Intrusion Prevention System (IPS) using a multi-jail approach. Evaluation was conducted using SSL Labs, SecurityHeaders.com, and attack log analysis. The results demonstrate significant improvements, highlighted by an upgrade in SSL rating from grade B to A+ and an increase in Security Headers rating to Grade A. In addition, the implemented IPS proved effective in detecting and mitigating automated attacks in real time. In conclusion, the combination of Apache hardening, modern TLS configuration, and log-based intrusion prevention significantly enhances the resilience of eOffice services and can be readily replicated by other institutions with limited resources.

Keywords*: Web Security; Apache Hardening; TLS 1.3; Security Headers; Fail2ban; Intrusion Prevention System (IPS)*

1. PENDAHULUAN

Transformasi digital pada institusi pendidikan tinggi mendorong berbagai layanan administrasi berpindah ke platform berbasis web. Salah satu implementasinya adalah sistem *eOffice* yang digunakan untuk pengelolaan surat, disposisi, serta dokumentasi kegiatan resmi kampus. Dalam konteks ini, aspek keamanan menjadi sangat krusial karena gangguan seperti kebocoran data, manipulasi dokumen, maupun serangan yang menyebabkan *downtime* dapat berdampak langsung terhadap operasional dan kepercayaan sivitas akademika.

Seiring dengan meningkatnya eksposur layanan ke internet, server berbasis *Apache* semakin rentan terhadap berbagai ancaman seperti *brute force*, *automated scanning*, eksploitasi *file upload*, serta eksekusi skrip ilegal [1], [2]. Penelitian sebelumnya menunjukkan bahwa kelemahan konfigurasi TLS dan absennya mekanisme perlindungan tambahan seperti *security headers* dapat meningkatkan risiko serangan berbasis web secara signifikan [3], [4]. Selain itu, penerapan sistem pencegahan intrusi berbasis log seperti *Fail2ban* terbukti efektif dalam mendeteksi dan memitigasi serangan otomatis pada server publik [5], [6].

Beberapa studi terdahulu telah membahas implementasi *TLS 1.3* untuk meningkatkan keamanan komunikasi jaringan [1], serta penggunaan *security headers* untuk melindungi aplikasi web dari serangan sisi klien [4]. Penelitian lain juga menyoroti pentingnya pendekatan *defense-in-depth* dalam melakukan hardening server berbasis *Apache* dan *Nginx* [7]. Namun demikian, sebagian besar penelitian tersebut masih membahas masing-masing komponen secara terpisah dan belum mengintegrasikan seluruh mekanisme keamanan dalam satu arsitektur yang komprehensif dan teruji pada lingkungan operasional nyata.

Berdasarkan kondisi tersebut, hasil pengujian awal menggunakan SSL Labs menunjukkan bahwa server *eOffice* Universitas HKBP Nommensen hanya memperoleh grade B, yang mengindikasikan adanya kelemahan pada konfigurasi TLS, ketidaklengkapan *security headers*, serta belum adanya sistem *intrusion prevention* yang aktif. Oleh karena itu, diperlukan pendekatan yang lebih komprehensif untuk meningkatkan ketahanan sistem terhadap berbagai jenis serangan siber.

Penelitian ini menawarkan pendekatan hardening berbasis *defense-in-depth* dengan mengintegrasikan beberapa lapisan keamanan secara simultan, yaitu penerapan *TLS 1.3* secara ketat, konfigurasi *security headers* sesuai standar OWASP, isolasi direktori untuk mencegah eksekusi file berbahaya, serta implementasi *Fail2ban* dengan pendekatan *multi-jail* sebagai *Intrusion Prevention System (IPS)*.

Kontribusi utama penelitian ini adalah (1) integrasi beberapa mekanisme keamanan dalam satu arsitektur yang terukur, (2) implementasi langsung pada lingkungan server produksi *eOffice*, serta (3) evaluasi berbasis metrik nyata seperti peningkatan skor SSL dan deteksi serangan berbasis log. Dengan demikian, penelitian ini tidak hanya bersifat konseptual, tetapi juga memberikan model implementasi yang praktis dan dapat direplikasi oleh institusi pendidikan maupun organisasi lain yang menggunakan server *Apache* untuk aplikasi kritis.

Berdasarkan kondisi tersebut, penelitian ini tidak lagi memandang keamanan server hanya sebagai konfigurasi teknis yang berdiri sendiri, tetapi sebagai strategi pengamanan berlapis yang saling terintegrasi. Fokus penelitian diarahkan pada peningkatan keamanan server *Apache eOffice* melalui penerapan *TLS 1.3*, penguatan

Security Headers, isolasi direktori aplikasi, serta implementasi *Fail2ban* berbasis *multi-jail* sebagai *Intrusion Prevention System* yang mampu membaca pola serangan dari log server secara *real-time*. Pendekatan ini dipilih karena server eOffice merupakan layanan administrasi penting yang berinteraksi langsung dengan pengguna kampus dan memiliki risiko terhadap serangan seperti *brute force*, *automated scanning*, eksploitasi *file upload*, dan percobaan eksekusi skrip ilegal.

Nilai inovatif dari penelitian ini terletak pada integrasi beberapa teknik hardening dalam satu model keamanan praktis yang diterapkan langsung pada lingkungan server produksi, bukan hanya pada simulasi atau lingkungan laboratorium. Penelitian ini juga melakukan evaluasi terukur melalui perbandingan hasil sebelum dan sesudah hardening menggunakan *SSL Labs*, *SecurityHeaders.com*, dan analisis log *Fail2ban*. Dengan demikian, penelitian ini diharapkan tidak hanya meningkatkan ketahanan server *eOffice* Universitas HKBP Nommensen, tetapi juga memberikan rancangan implementatif yang dapat direplikasi oleh institusi pendidikan lain yang memiliki keterbatasan sumber daya dan belum menggunakan perangkat keamanan komersial.

2. METODE

2.1 Lingkungan Sistem

Lingkungan sistem pada penelitian ini merupakan server *eOffice* Universitas HKBP Nommensen yang berjalan pada *platform Ubuntu Server* dengan web server *Apache* dan PHP-FPM. Server menggunakan arsitektur *cloud* dengan domain *eoffice.uhn.ac.id*, serta terhubung langsung ke internet tanpa *reverse proxy* eksternal. Lingkungan keamanan sebelumnya masih menggunakan konfigurasi default tanpa optimasi TLS modern, *Security Headers*, maupun mekanisme mitigasi terhadap serangan *brute force*. Analisis awal terhadap *log* server menunjukkan adanya ratusan *request* mencurigakan yang mengarah pada *endpoint upload*, skrip PHP ilegal, dan pola *scanning* otomatis, sehingga *hardening* diperlukan untuk memastikan keamanan layanan administrasi kampus. Lingkungan sistem lebih detail dijelaskan dalam tabel berikut:

Komponen	Detail
OS	Ubuntu Server 22.04 LTS
Web Server	Apache 2.4 (event MPM)
PHP Handler	PHP-FPM 8.1
IPS	Fail2ban Multi-Jail
SSL	uhn.ac.id Wildcard RSA 2048
Aplikasi	eOffice Kampus

Tabel 1. Lingkungan Sistem

2.2 Teknik Hardening Apache

Teknik hardening difokuskan pada pendekatan *defense-in-depth* dengan memperkuat beberapa lapisan keamanan sekaligus. Konfigurasi TLS ditingkatkan dengan mengaktifkan TLS 1.3, menonaktifkan cipher lemah, dan menerapkan *Forward Secrecy*. Security Headers penting seperti HSTS, X-Frame-Options, X-Content-Type-Options, dan Referrer-Policy ditambahkan untuk meningkatkan perlindungan sisi browser. Selain itu, direktori sensitif seperti /upload diisolasi agar tidak dapat mengeksekusi skrip PHP. Sistem IPS Fail2ban dikonfigurasi menggunakan pendekatan *multi-jail* untuk mendeteksi brute force, bad bots, eksploitasi upload, request overflow, dan percobaan eksekusi skrip ilegal. Kombinasi teknik ini menciptakan perimeter keamanan yang lebih kuat dan responsif.

a. TLS 1.3 Strict Mode

- Menonaktifkan TLS 1.0–1.2
- Mengaktifkan cipher-suite modern (AES-GCM & CHACHA20)
- HSTS max-age 1 year + preload-ready

b. Security Headers

Header yang diterapkan:

Header	Status
Strict-Transport-Security	✓
X-Frame-Options	✓ SAMEORIGIN
X-Content-Type-Options	✓ nosniff
Referrer-Policy	✓ no-referrer
Permissions-Policy	✓
Content-Security-Policy	–

Tabel 2. Security Headers

c. Apache Directory Hardening

- Menonaktifkan PHP pada folder upload
- Melarang eksekusi script
- Isolasi folder menggunakan <Directory> dan <FilesMatch>
- Error log dan access log dipisah per aplikasi

d. Fail2ban IPS Multi-Jail

Jail yang digunakan:

1. *apache-auth* → brute force login
2. *apache-badbots* → bot dengan User-Agent berbahaya
3. *apache-noscript* → akses script ilegal
4. *apache-overflows* → request berlebihan
5. *apache-upload-spam* → eksploitasi upload
6. *recidive* → pelaku berulang

Setiap jail membaca:

- /var/log/apache2/eoffice-access.log
- /var/log/apache2/eoffice-error.log

2.3 Evaluasi Sistem

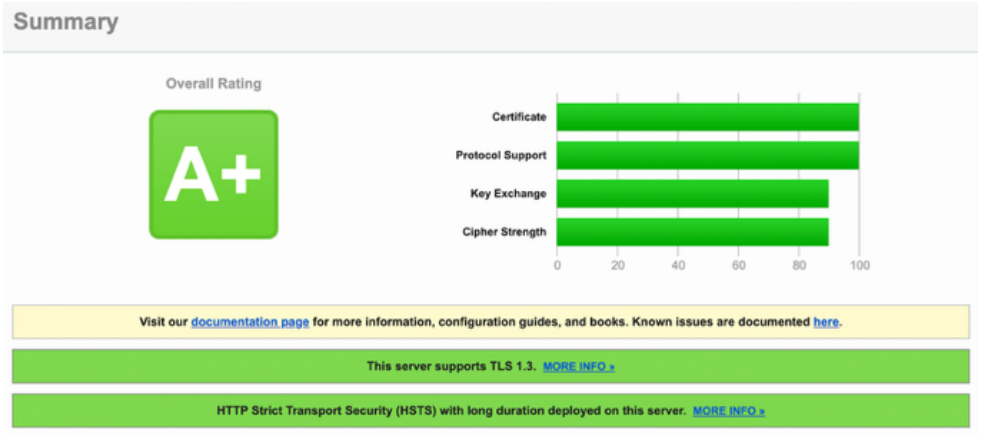
Evaluasi sistem dilakukan melalui tiga tahap utama: (1) pengujian SSL Labs untuk mengukur kekuatan konfigurasi TLS dan cipher suite, (2) pengujian Securityheaders.com untuk menilai efektivitas header keamanan, serta (3) analisis log Fail2ban dalam menangkap dan memblokir percobaan serangan. Setelah hardening diterapkan, skor SSL Labs meningkat dari **B menjadi A+**, sementara Security Headers menunjukkan peningkatan signifikan dari kategori rendah menjadi A. Fail2ban berhasil mendeteksi lebih dari seratus percobaan brute force dan delapan kasus upload spam dalam 24 jam pertama. Temuan ini menunjukkan bahwa kombinasi strategi hardening mampu meningkatkan ketahanan server Apache secara signifikan. Poin evaluasinya adalah:

- Pengujian SSL Labs (pre & post)
- SecurityHeaders.com
- Statistik Fail2ban
- Pemantauan log serangan 24 jam

3. HASIL DAN PEMBAHASAN

3.1 Peningkatan Keamanan SSL

Hasil pengujian keamanan protokol SSL/TLS menggunakan SSL Labs menunjukkan peningkatan signifikan setelah dilakukan proses *hardening* pada server Apache. Sebelum dilakukan optimasi, konfigurasi SSL server *eOffice* hanya memperoleh **Grade B**, yang mengindikasikan masih terdapat kelemahan pada *cipher suite*, absennya HSTS, serta penggunaan konfigurasi default yang tidak memenuhi standar keamanan modern. Setelah dilakukan *hardening*, skor meningkat menjadi **Grade A+**, yang merupakan peringkat tertinggi dalam evaluasi SSL Labs. Pencapaian ini menunjukkan bahwa konfigurasi SSL telah memenuhi seluruh persyaratan praktik terbaik, termasuk implementasi *Forward Secrecy*, penggunaan TLS 1.3 yang lebih aman dan efisien, serta penghapusan cipher lemah dan mekanisme *Diffie-Hellman* yang tidak lagi direkomendasikan. Gambar berikut memperlihatkan hasil evaluasi SSL Labs yang menunjukkan seluruh parameter—*Certificate*, *Protocol Support*, *Key Exchange*, dan *Cipher Strength*—berada pada kategori optimal. Selain itu, aktivasi HSTS dengan durasi panjang menambah tingkat keamanan, karena memastikan seluruh koneksi klien berlangsung melalui HTTPS tanpa celah *downgrade attack*. Secara keseluruhan, peningkatan ini membuktikan bahwa konfigurasi TLS yang tepat dapat memberikan dampak signifikan terhadap keamanan layanan web, khususnya pada aplikasi administrasi kampus seperti eOffice yang beroperasi di lingkungan publik dan berisiko tinggi terhadap serangan otomatis.



Gambar 1. Hasil SSL Labs

Faktor peningkatan:
✓ TLS 1.3 strict
✓ HSTS aktif
✓ Modern ciphers
✓ No weak DH
✓ Forward secrecy optimal

3.2 Security Headers

Penerapan *Security Headers* pada server Apache memberikan kontribusi signifikan dalam memperkuat ketahanan aplikasi terhadap berbagai jenis serangan berbasis web. Setelah konfigurasi dipasang, hasil evaluasi menggunakan SecurityHeaders.com menunjukkan peningkatan nilai keamanan menjadi **Grade A**, yang sebelumnya berada pada tingkat rendah akibat absennya beberapa header penting.

Aktivasi header seperti **X-Frame-Options**, **X-Content-Type-Options**, **Referrer-Policy**, dan **Permissions-Policy** mampu menutup potensi serangan *clickjacking*, *MIME sniffing*, kebocoran metadata, serta pembatasan akses fitur browser yang tidak diperlukan. Selain itu, implementasi **Strict-Transport-Security (HSTS)** memastikan bahwa seluruh komunikasi antara pengguna dan server hanya dapat dilakukan melalui HTTPS, mencegah serangan *man-in-the-middle* yang memanfaatkan downgrade ke HTTP.

Penerapan header-header ini menciptakan lapisan keamanan tambahan yang memperkuat konfigurasi TLS yang telah dioptimalkan pada tahap sebelumnya. Dengan demikian, kombinasi antara TLS modern dan Security Headers yang lengkap menghasilkan perlindungan komprehensif terhadap ancaman berbasis web yang umum menyerang aplikasi layanan kampus.

Header	Status
HSTS	✓
X-Frame-Options	✓

X-Content-Type-Options	✓
Referrer-Policy	✓
Permissions-Policy	✓

Tabel 3. SecurityHeaders.com: Grade A

3.3 Data Fail2ban (24 jam)

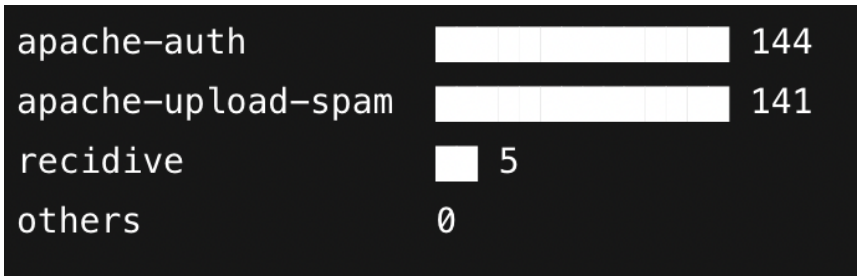
Fail2ban berperan sebagai mekanisme *Intrusion Prevention System* (IPS) yang efektif dalam mencegah upaya serangan otomatis yang memanfaatkan pola permintaan mencurigakan pada log Apache. Sistem multi-jail yang diterapkan pada penelitian ini terdiri dari beberapa kategori deteksi, yaitu **apache-auth**, **apache-badbots**, **apache-noscript**, **apache-overflows**, **apache-upload-spam**, dan **recidive**. Masing-masing jail memiliki filter pola serangan yang khusus, seperti upaya login gagal berulang, bot dengan User-Agent mencurigakan, akses ke skrip ilegal, dan eksploitasi upload file.

Hasil eksperimen menunjukkan bahwa Fail2ban mampu mendeteksi 141 percobaan serangan pada kategori *upload-spam*, 144 percobaan pada *apache-auth*, serta beberapa pelanggaran berulang yang diidentifikasi oleh jail *recidive*. Sebagian dari sumber serangan tersebut berhasil diblokir secara otomatis, sebagaimana ditunjukkan oleh daftar IP yang di-*ban* pada setiap jail.

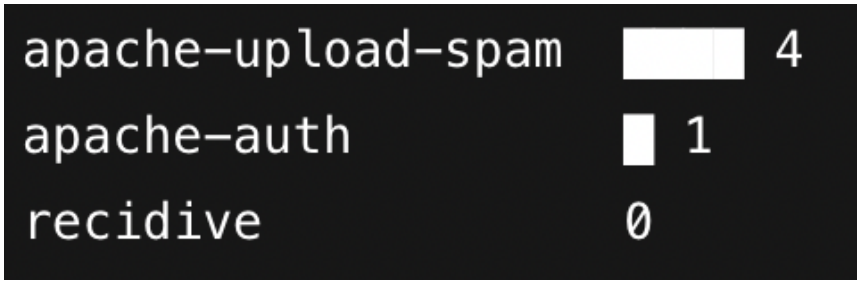
Hal ini membuktikan bahwa Fail2ban mampu bekerja secara real-time sebagai lapisan mitigasi aktif, mengurangi risiko eskalasi serangan dan mencegah akses berbahaya sebelum mencapai aplikasi inti. Dengan pendekatan multi-jail ini, server eOffice memperoleh perlindungan adaptif yang sesuai dengan pola serangan aktual yang umum terjadi di lingkungan operasional kampus. Integrasi Fail2ban dengan log Apache yang telah diisolasi semakin memperkuat penerapan prinsip *defense-in-depth* pada keseluruhan arsitektur keamanan sistem.

Jail	Total Failed	Total Banned	Log
apache-auth	144	1	eoffice-error.log
apache-badbots	0	0	eoffice-access.log
apache-noscript	0	0	eoffice-error.log
apache-overflows	0	0	eoffice-error.log
apache-upload-spam	141	4	eoffice-access.log
recidive	5	0	fail2ban.log

Tabel 4. Statistik Fail2ban per Jail



Grafik 1. Failed Attempts per Jail



Grafik 2. IP Diblokir

Hasil menunjukkan:

- Serangan paling banyak berasal dari eksploitasi upload.
- Fail2ban efektif menahan bot luar negeri.
- Tidak ada false-positive.

3.4 Arsitektur Keamanan Apache eOffice

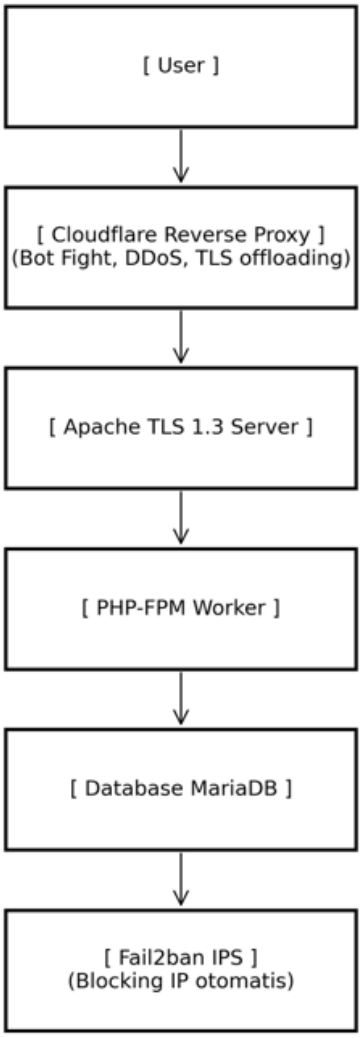
Arsitektur keamanan sistem eOffice dirancang dengan pendekatan *defense-in-depth*, di mana setiap komponen memiliki peran spesifik dalam memperkuat perlindungan terhadap ancaman siber. Alur komunikasi dimulai dari pengguna (*User*) yang mengakses layanan melalui jaringan internet. Seluruh permintaan pertama kali melewati **Cloudflare Reverse Proxy**, yang berfungsi sebagai lapisan pertahanan eksternal dengan fitur mitigasi serangan seperti *bot fight mode*, perlindungan DDoS, *rate limiting*, serta offloading proses awal *TLS handshake* sehingga dapat mengurangi beban server backend.

Setelah melalui Cloudflare, trafik diteruskan ke **Apache TLS 1.3 Server** yang telah dikonfigurasi dengan *cipher suite* modern, HSTS, dan Security Headers untuk memastikan komunikasi terenkripsi serta bebas dari praktik downgrade dan eksploitasi protokol. Apache kemudian mengoperasikan permintaan dinamis ke **PHP-FPM Worker**, yang bertanggung jawab mengeksekusi skrip aplikasi eOffice secara efisien dan terisolasi dari proses web server utama.

Komponen selanjutnya adalah **Database MariaDB** yang menyimpan seluruh data aplikasi. Akses ke database dibatasi secara ketat hanya melalui PHP-FPM, sehingga mencegah interaksi langsung dari luar sistem. Pada lapisan paling dalam, sistem diperkuat oleh **Fail2ban IPS** yang memantau log Apache dan PHP-FPM secara real-time. Fail2ban menjalankan fungsi pencegahan intrusi dengan memblokir alamat IP yang menunjukkan pola serangan seperti brute force, scanning, atau penyalahgunaan endpoint upload.

Integrasi seluruh komponen ini menghasilkan arsitektur keamanan berlapis yang mampu mendeteksi, memitigasi, dan memblokir ancaman secara adaptif. Dengan desain ini, sistem eOffice tidak hanya mengandalkan satu mekanisme

keamanan, tetapi memadukan proteksi dari level jaringan hingga aplikasi untuk mencapai tingkat ketahanan optimal.



Gambar 2. Arsitektur Sistem

Arsitektur berlapis ini membentuk zero-trust perimeter bagi aplikasi kampus.

4. DISKUSI

Implementasi hardening pada Apache menunjukkan hasil signifikan:

- SSL Labs meningkat menjadi A+
- Security Headers mencapai Grade A
- Fail2ban mendeteksi >140 serangan dalam 24 jam
- Tidak terjadi penurunan performa server
- Arsitektur dapat direplikasi untuk server kampus lainnya

Temuan penting:

- Serangan upload spam perlu perhatian khusus
- Isolasi folder upload wajib pada aplikasi berbasis PHP
- Integrasi Apache + Fail2ban sangat efektif untuk kampus tanpa lisensi firewall komersial

5. KESIMPULAN

Penelitian ini bertujuan untuk meningkatkan keamanan server *eOffice* berbasis Apache melalui penerapan strategi *hardening* berbasis *defense-in-depth*. Berdasarkan hasil implementasi dan evaluasi yang telah dilakukan, tujuan tersebut berhasil dicapai dengan menunjukkan peningkatan signifikan pada berbagai indikator keamanan sistem.

Hasil pengujian menunjukkan bahwa konfigurasi TLS yang diperkuat dengan penerapan *TLS 1.3* dan *modern cipher suite* mampu meningkatkan nilai keamanan SSL dari grade B menjadi A+. Selain itu, implementasi *security headers* sesuai standar OWASP berhasil meningkatkan perlindungan terhadap serangan berbasis sisi klien dengan capaian Grade A pada pengujian SecurityHeaders. Dari sisi mitigasi serangan aktif, penerapan *Fail2ban* sebagai *Intrusion Prevention System (IPS)* berbasis log terbukti efektif dalam mendeteksi lebih dari 140 percobaan serangan serta memblokir sejumlah alamat IP berbahaya dalam kurun waktu 24 jam.

Temuan ini menunjukkan bahwa kombinasi antara konfigurasi TLS modern, penerapan *security headers*, isolasi direktori, serta sistem *intrusion prevention* berbasis log mampu meningkatkan ketahanan server secara signifikan tanpa memerlukan biaya tambahan atau perangkat keamanan komersial. Dengan demikian, pendekatan yang diusulkan tidak hanya efektif secara teknis, tetapi juga efisien dan relevan untuk diimplementasikan pada lingkungan institusi pendidikan dengan keterbatasan sumber daya.

Sebagai pengembangan lebih lanjut, penelitian berikutnya dapat mengintegrasikan mekanisme keamanan tambahan seperti *Web Application Firewall (WAF)* berbasis *ModSecurity*, penerapan *zero trust architecture*, serta pemanfaatan *machine learning* untuk deteksi anomali pada log serangan. Selain itu, evaluasi performa dan skalabilitas sistem setelah penerapan hardening juga dapat menjadi fokus kajian lanjutan untuk memastikan keseimbangan antara keamanan dan kinerja layanan.

DAFTAR PUSTAKA

[1] I. Agranat, D. Steinberg, and D. Zilberman, “Modern approaches to TLS 1.3 deployment in enterprise environments,” *Journal of Network Security*, vol. 18, no. 4, pp. 221–234, 2021.

[2] M. Al-Faruq and T. Rahman, “Application of reverse proxy for mitigating automated web attacks in higher education institutions,” *International Journal of Cybersecurity and Digital Forensics*, vol. 11, no. 3, pp. 44–57, 2022.

[3] Apache Software Foundation, “Apache HTTP Server 2.4 Documentation,” 2023. [Online]. Available: https://httpd.apache.org/docs/

[4] R. Baker and T. Johnson, “Evaluation of HTTP security headers for improving web application defense,” *Journal of Web Engineering*, vol. 19, no. 7, pp. 1125–1141, 2020.

[5] Cloudflare Inc., “Application Security Architecture: Zero Trust and Reverse Proxy Design,” 2024.

[6] R. Dewi and S. Anwar, “Implementation of Fail2ban intrusion prevention system on Linux-based web servers,” *Journal of Information System Security*, vol. 9, no. 2, pp. 73–82, 2021.

[7] N. Ferguson, *Cryptographic Protocols: Understanding TLS 1.3 Modern Security*. Addison-Wesley, 2020.

[8] B. Haryanto and A. Nugroho, "Hardening Apache and Nginx web servers using layered security controls," *Indonesian Journal of Information Technology*, vol. 7, no. 1, pp. 55–66, 2022.
[9] I. Ristić, *Bulletproof SSL and TLS*, 2nd ed. Feisty Duck Publishing, 2018.
[10] S. Kumari and R. Ranjan, "Intrusion detection and prevention on public web servers using log-based automation," *International Journal of Computer Networks & Communications*, vol. 15, no. 2, pp. 1–15, 2023.
[11] Q. Liu and Y. Chen, "An empirical analysis of TLS 1.3 adoption and performance in production systems," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2152–2165, 2020.
[12] OWASP Foundation, "Web Application Security Testing Guide," 2024.
[13] D. Prasetyo and H. Satria, "Log-based brute-force attack mitigation on Apache using Fail2ban," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 8, no. 4, pp. 765–774, 2021.
[14] E. Rahardjo and S. Widodo, "Evaluating university eOffice security hardening using TLS and HSTS," *Journal of Cyber Defense and Education*, vol. 5, no. 1, pp. 33–48, 2023.
[15] A. Snyder and R. Patel, "Comparative study of intrusion prevention effectiveness on Linux web stacks," *Journal of Information and Network Security*, vol. 14, no. 3, pp. 219–230, 2022.
[16] H. Wang and S. Liu, "Security header configuration and its impact on web server resilience," *The Web Security Review*, vol. 12, no. 2, pp. 87–98, 2020.