JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 14 No. 2, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v14i2.9258

ANALISIS KEAMANAN SERVER DENGAN METODE NEXT-GENERATION FIREWALL FILTERING DAN SINGLE PACKET AUTHORIZATION MENGGUNAKAN PFSENSE DAN FWKNOP

Muhammad Faiz Alimuddin[1*], L.M. Fid Aksara[2], Rizal Adi Saputra[3]

[1,2,3]Universitas Halu Oleo; Jln. H.E.A Mokodompit No. 8 Kampus Baru UHO Bumi Tridharma Anduonohu; 0401-3194163

Keywords:
Next-Generation Firewall Filtering, *Single Packet Authorization*, *Server*, *Penetration Testing*, Serangan Siber.

Corespondent Email:
faisalimudin16@gmail.com

Abstrak. Laporan dari Awanpintar.id tahun 2025 menempatkan Indonesia sebagai negara dengan tingkat ancaman siber tertinggi di Asia Tenggara melalui serangan seperti network scanning, denial of service (DoS/DDoS), dan attempted administrator privilege gain, penelitian ini difokuskan pada penguatan keamanan server. Solusi yang diusulkan adalah implementasi Next-Generation Firewall (NGFW) dengan metode filtering yang dikombinasikan dengan Single Packet Authorization (SPA) sebagai mekanisme pertahanan berlapis untuk melindungi sumber daya sistem. Efektivitas sistem diuji menggunakan metode Penetration Testing yang mensimulasikan berbagai serangan siber umum, meliputi SSH attack, brute force, port scanning, DoS, dan DDoS. Hasil pengujian menunjukkan bahwa integrasi NGFW dan SPA mampu menghalau seluruh serangan yang masuk ke server dengan tingkat akurasi mencapai 100%. Dengan demikian, sistem ini terbukti efektif dalam menjaga stabilitas kinerja server dari berbagai gangguan siber modern yang berpotensi merusak..

Abstract. *According to the 2025 Awanpintar.id report, Indonesia is positioned as one of the countries with the highest cyber threat levels in Southeast Asia, dominated by attacks such as network scanning, denial of service (DoS/DDoS), and attempted administrator privilege gain. This research focuses on strengthening server security through the implementation of a Next-Generation Firewall (NGFW) with filtering methods combined with Single Packet Authorization (SPA) as a layered defense mechanism. The effectiveness of the system was evaluated using Penetration Testing, simulating various common cyber attacks including SSH attacks, brute force, port scanning, DoS, and DDoS. The test results demonstrate that the integration of NGFW and SPA successfully mitigated all incoming attacks with a 100% accuracy rate. Consequently, this system is proven effective in maintaining server stability against modern, potentially destructive cyber disruptions.*

1. PENDAHULUAN

Server merupakan komponen utama dalam suatu infrastruktur jaringan karena berperan sebagai pusat penyimpanan, pengelolaan, dan distribusi data maupun layanan digital. *Server* menyimpan informasi penting dan sensitif yang menjadi target potensial serangan *cyber*. Oleh karena itu, *server* harus dirancang dengan memperhatikan aspek keamanan jaringan yang kuat agar mampu menjaga kerahasiaan, integritas, dan ketersediaan data.

Laporan dari awanpintar.id, sepanjang tahun 2025 Indonesia masih menjadi salah satu negara dengan tingkat ancaman siber tertinggi di kawasan Asia Tenggara. Serangan siber yang terjadi meliputi berbagai jenis, seperti *network scaning*, *attempted administrator privilege gain, denial of service*, hingga serangan *distributed denial of service* (DDoS). Salah satu serangan DDoS terbesar 2025 terjadi kepada situs tempo.co setelah merilis liputan khusus tentang judi online dengan tujuan melumpuhkan akses publik. Pada tahun yang sama unit manajemen teknologi informasi Telkom University juga secara resmi melaporkan adanya anomali trafik yang ekstrem di jaringan mereka serta serangan brute-force otomatis yang menyasar port layanan sensitif.

Melihat besarnya ancaman yang ada, diperlukan solusi keamanan jaringan yang mampu memberikan perlindungan lebih mendalam terhadap *server*. Salah satu teknologi yang memiliki peran penting dalam pertahanan jaringan adalah *firewall*. *Firewall* berfungsi untuk memantau, menyaring, dan mengontrol lalu lintas jaringan berdasarkan aturan tertentu. *Firewall* memungkinkan *administrator* dapat mencegah akses tidak sah, memblokir aktivitas mencurigakan, serta menjaga *server* dari berbagai ancaman eksternal.

Seiring berkembangnya teknik serangan siber dibuatlah *Next-Generation Firewall* (NGFW) yang merupakan pengembangan dari *firewall* tradisional yang tidak hanya berfungsi untuk memfilter lalu lintas jaringan, tetapi juga memiliki kemampuan analisis keamanan yang lebih mendalam. Teknologi ini mendukung *Deep Packet Inspection* (DPI), *application awareness*, serta integrasi dengan sistem *Intrusion Prevention System* (IPS) untuk mendeteksi dan mencegah ancaman tingkat lanjut seperti *zero-day attacks* dan *malware* tersembunyi. Melalui tambahan fitur *sandboxing* dan *real-time threat intelligence feeds*, NGFW mampu memberikan perlindungan menyeluruh terhadap ancaman siber yang tidak dapat dideteksi oleh *firewall* tradisional.

Selain penggunaan NGFW, salah satu pendekatan keamanan jaringan yang efektif untuk melindungi akses terhadap *server* adalah *Single Packet Authorization* (SPA). SPA merupakan mekanisme autentikasi yang menggunakan satu paket terenkripsi untuk memberikan otorisasi akses terhadap layanan atau *port* tertentu pada *server*. Melalui metode SPA, seluruh *port* tetap berada dalam kondisi tersembunyi (*stealth mode*) hingga menerima permintaan autentikasi yang valid dari klien yang sah. Pendekatan ini mampu secara signifikan mengurangi potensi serangan seperti *port scanning*, *brute force*, maupun *unauthorized access*, karena hanya pengguna yang telah terautentikasi yang dapat memicu pembukaan *port*. Penelitian terbaru menunjukkan bahwa SPA berperan penting dalam arsitektur keamanan berbasis *zero trust* karena kemampuannya menyembunyikan jejak layanan dan meminimalkan permukaan serangan jaringan.

Implementasi pfSense sebagai platform *firewall open-source* berbasis FreeBSD mendukung penerapan NGFW dengan berbagai fitur canggih seperti *filtering rules*, *intrusion detection*, *traffic shaping*, dan *VPN*. Sementara itu, fwknop (*Firewall Knock Operator*) digunakan untuk mengimplementasikan sistem SPA secara efisien, memungkinkan komunikasi yang aman antara klien dan *server* dengan otentikasi berbasis enkripsi yang kuat.

Berdasarkan uraian tersebut, penting untuk dilakukan penelitian mengenai penerapan *Next-Generation Firewall* (NGFW) *Filtering* dan *Single Packet Authorization* (SPA) dalam meningkatkan keamanan *server*. Dengan kombinasi *tools* pfSense dan fwknop, diharapkan sistem keamanan yang dirancang mampu menahan berbagai jenis serangan siber modern serta menjaga stabilitas dan integritas *server.*

2. TINJAUAN PUSTAKA

2.1 Server

Server merupakan sistem komputer yang berfungsi menyediakan berbagai layanan dalam suatu jaringan, didukung oleh prosesor yang dapat diskalakan, kapasitas RAM besar, serta sistem operasi dan perangkat lunak administratif untuk mengelola client, akses jaringan, dan sumber daya [1]. Secara umum, server bertanggung jawab menangani permintaan dan memberikan tanggapan kepada client, menyediakan sumber daya jaringan, mengatur lalu lintas data, mengelola izin akses, serta memberikan perlindungan melalui firewall dan anti-malware[2].

2.2 Next-Generation Firewall

Next-Generation Firewall (NGFW) merupakan pengembangan dari firewall tradisional yang tidak hanya memfilter lalu lintas jaringan pada lapisan network dan transport, tetapi juga menganalisis hingga lapisan aplikasi melalui teknologi Deep Packet Inspection (DPI) [3]. Dengan kemampuan ini, NGFW dapat mengenali aplikasi, protokol, serta pola komunikasi berbahaya, termasuk serangan lanjutan seperti zero-day exploit, malware tersembunyi, dan aktivitas command and control (C2). NGFW terintegrasi dengan Intrusion Prevention System (IPS) dan Intrusion Detection System (IDS) untuk mendeteksi serta memblokir ancaman secara otomatis, serta mendukung application awareness and control guna menerapkan kebijakan keamanan berbasis aplikasi[4].

2.3 Next-Generation Firewall Filtering

Next-Generation Firewall (NGFW) filtering merupakan metode penyaringan lalu lintas jaringan yang bekerja dengan memeriksa setiap paket data yang melintasi batas jaringan dan menentukan apakah paket tersebut diteruskan atau diblokir berdasarkan aturan yang telah ditetapkan [5]. Proses ini dimulai dengan analisis header paket yang memuat informasi seperti alamat IP sumber dan tujuan, nomor port, protokol, serta atribut jaringan lainnya, yang kemudian menjadi dasar pengambilan keputusan. Dalam implementasinya, NGFW filtering dapat diterapkan berdasarkan berbagai kriteria, seperti alamat IP, port, protokol, jenis paket (TCP, UDP, ICMP), autentikasi pengguna, perilaku trafik (misalnya anomali handshake), frekuensi koneksi dalam periode tertentu, hingga pola serangan tertentu seperti flood atau fragmentasi tidak wajar [6].

2.4 Single Packet Authorization

Single Packet Authorization (SPA) merupakan metode keamanan jaringan yang melindungi layanan server dengan menyembunyikan port dari akses tidak sah melalui pengiriman satu paket terenkripsi sebagai proses pra-autentikasi, sehingga lebih efisien dibandingkan port knocking dan efektif mengurangi risiko port scanning maupun brute force [7]. SPA dikembangkan sebagai penyempurnaan dengan mengintegrasikan konsep Advanced Network-Hiding Access Control (AHAC), yang memanfaatkan enkripsi untuk memastikan hanya pengguna dengan kunci autentikasi valid yang dapat membuka akses layanan tersembunyi [8].

2.5 Penetration Testing

Penetration Testing merupakan metode evaluasi keamanan sistem komputer atau server dengan mensimulasikan serangan siber secara terkontrol untuk mengidentifikasi dan mengeksploitasi potensi kerentanan [9]. Pengujian ini dilakukan oleh pentester guna menilai sejauh mana celah keamanan dapat dimanfaatkan oleh pihak tidak berwenang, sehingga hasilnya dapat digunakan sebagai dasar perbaikan dan penguatan sistem. Secara umum, tahapan penetration testing meliputi information gathering untuk mengumpulkan informasi target, vulnerability assessment untuk mengidentifikasi kelemahan, exploitation untuk membuktikan tingkat eksploitasi kerentanan, serta reporting yang memuat temuan, tingkat risiko, dampak, dan rekomendasi mitigasi guna mencegah serangan di masa mendatang[10].

2.6 Pfsense

Pfsense merupakan sistem operasi open-source berbasis FreeBSD yang dikembangkan untuk fungsi firewall dan router, dengan fleksibilitas tinggi dalam mengelola lalu lintas jaringan serta memberikan perlindungan terhadap berbagai ancaman siber[11]. Platform ini dapat dijalankan pada perangkat keras standar maupun mesin virtual, sehingga menjadi solusi keamanan yang efisien dan hemat biaya. pfSense menyediakan fitur seperti stateful packet inspection, Network Address Translation (NAT), Virtual Private Network (VPN), dan traffic shaping, serta antarmuka berbasis web yang memudahkan konfigurasi dan manajemen kebijakan keamanan [12].

2.7 Fwknop

Fwknop (FireWall KNock OPerator) merupakan aplikasi open-source yang dirancang untuk mengimplementasikan metode Single Packet Authorization (SPA) dalam sistem keamanan jaringan, dengan mekanisme pengiriman satu paket terenkripsi sebagai syarat pembukaan akses ke port yang dilindungi sehingga seluruh port tetap berada dalam mode

tersembunyi (stealth) hingga otorisasi sah diterima [13]. Fwknop bekerja dalam dua mode, yaitu client untuk menghasilkan dan mengirim paket SPA terenkripsi (menggunakan AES atau HMAC), serta server (fwknopd) yang memverifikasi paket dan secara otomatis menambahkan aturan sementara pada firewall seperti iptables atau pfSense bagi sumber terautentikasi.

2.8 Iptables

Iptables merupakan program pada sistem operasi Linux yang digunakan untuk mengelola aturan firewall guna mengontrol lalu lintas jaringan masuk dan keluar sesuai kebijakan keamanan server [14]. Iptables bekerja menggunakan struktur tabel yang terdiri dari chains (INPUT, OUTPUT, dan FORWARD) serta rules yang menentukan tindakan terhadap paket berdasarkan kriteria tertentu. Melalui mekanisme ini, administrator dapat memblokir alamat IP mencurigakan, membatasi bandwidth, serta menerapkan Network Address Translation (NAT), sehingga iptables menjadi komponen penting dalam pengamanan jaringan berbasis Linux [15].

3. METODE PENELITIAN

Penelitian ini merupakan penelitian terapan dengan pendekatan kuantitatif yang berfokus pada analisis dan implementasi mekanisme keamanan server menggunakan metode Next-Generation Firewall (NGFW) Filtering dan Single Packet Authorization (SPA). Penelitian bertujuan untuk mengukur tingkat efektivitas penerapan kebijakan keamanan dalam melindungi layanan server dari ancaman seperti port scanning dan brute force. Implementasi dilakukan menggunakan pfSense sebagai platform firewall untuk menerapkan filtering berbasis aturan (IP, port, protokol, dan pola trafik), serta fwknop sebagai mekanisme SPA untuk menyembunyikan port layanan melalui otorisasi paket terenkripsi. Pendekatan ini dipilih karena mampu meningkatkan perlindungan akses secara preventif tanpa membuka layanan secara langsung ke publik, sehingga dapat mengurangi attack surface dan risiko eksploitasi.

Tahapan penelitian dilakukan secara sistematis menggunakan kerangka kerja Security Policy Development Life Cycle (SPDLC) agar proses perancangan dan implementasi keamanan berjalan terstruktur dan terukur. Adapun tahapan penelitian meliputi:

3.1. Analysis

Pada tahap ini dilakukan pengumpulan dan studi literatur terkait metode Next-Generation Firewall (NGFW) Filtering dan Single Packet Authorization (SPA) sebagai dasar teoritis penelitian. Selanjutnya, dilakukan pengkajian terhadap berbagai jenis serangan siber populer yang berbahaya, seperti port scanning dan brute force, beserta mekanisme mitigasinya melalui penerapan NGFW filtering dan SPA guna memperkuat keamanan server.

3.2. Design

Pada tahap ini dilakukan perancangan sistem yang meliputi pembuatan flowchart algoritma serta flowchart keseluruhan arsitektur firewall yang dibangun. Selain itu, dilakukan analisis kebutuhan sistem yang mencakup kebutuhan fungsional, spesifikasi perangkat keras (hardware), serta perangkat lunak (software) yang diperlukan untuk mendukung implementasi Next-Generation Firewall (NGFW) Filtering dan Single Packet Authorization (SPA) agar dapat berjalan secara optimal.

3.3. Implementation

Pada tahap ini dibuat simulasi server menggunakan Ubuntu Server yang dijalankan melalui VirtualBox sebagai lingkungan pengujian. Selanjutnya dilakukan konfigurasi rule keamanan berdasarkan metode Next-Generation Firewall (NGFW) filtering menggunakan pfSense serta penerapan Single Packet Authorization (SPA) menggunakan fwknop untuk membatasi dan menyembunyikan akses layanan pada server.

3.4. Enforcement

Pada tahap ini dilakukan pengujian terhadap sistem keamanan yang telah dirancang menggunakan metode penetration testing. Simulasi serangan dilancarkan pada server Ubuntu Server yang telah dikonfigurasi sebelumnya, dengan memanfaatkan Kali Linux sebagai mesin penyerang untuk menguji ketahanan sistem terhadap berbagai skenario serangan.

3.5. Enchantment

Pada tahap ini dilakukan perbaikan dan mitigasi terhadap kerentanan yang ditemukan selama proses penyerangan dan pengujian sistem. Tindakan yang dilakukan meliputi penyesuaian konfigurasi firewall, pembaruan aturan filtering, penguatan mekanisme autentikasi, serta penutupan celah akses yang masih terbuka. Selain itu, dilakukan evaluasi ulang terhadap kebijakan keamanan yang diterapkan guna memastikan setiap potensi risiko telah diminimalkan.

4. HASIL DAN PEMBAHASAN

Sistem keamanan server yang telah dibangun menggunakan metode Next-Generation Firewall Filtering dan Single Packet Authorization diuji melalui simulasi pengujian dalam dua skenario, yaitu simulasi tanpa menggunakan firewall dan simulasi dengan menerapkan firewall. Pengujian tersebut dilakukan terhadap lima jenis serangan yang berbeda untuk melihat perbandingan tingkat keamanan sistem sebelum dan sesudah penerapan mekanisme proteksi.

4.1 Pengujian Tanpa Firewall

1. Pengujian SSH Attack dan Brute Force Attack

Pengujian SSH Attack dan Bruteforce Attack dilakukan dengan menggunakan modul /auxiliary/scanner/ssh/ssh_login pada tool msfconsole di Kali Linux. Ketika modul telah digunakan, selanjutnya mengisi informasi yang dibutuhkan seperti IP dan port SSH target, serta file wordlist.txt yang berisi daftar kombinasi karakter dalam membentuk username dan password. Penyerang harus terlebih dahulu mengisi requirements seperti IP, port target dan file dictionary untuk username dan passwords. Setelah itu penyerang memilih mode serangan biasa ataupun verbose.

Setelah requirements telah diisi, selanjutnya ialah menjalankan modul. Ketika proses running modul selesai, akan menampilkan hasil berupa percobaan username dan password SSH, bahkan dapat melakukan remote pada server target.

Gambar 1 menunjukkan penyerang menemukan sessions yang terbuka dan dapat melakukan remote terhadap server. Dampaknya penyerang dapat mengeksploitasi server.

```
msf auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.1.10:22 - Starting bruteforce
[+] 192.168.1.10:22 - Success: 'lswazuh:wazuhls' 'uid=1000(lswazuh) gid=1000(lswazuh) groups=1000
u Sep 18 15:26:59 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux '
[!] No active DB -- Credential data will not be saved!
[*] SSH session 1 opened (192.168.1.9:46013 → 192.168.1.10:22) at 2025-10-06 12:53:07 +0700
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  1         shell linux  SSH root @   192.168.1.9:46013 → 192.168.1.10:22 (192.168.1.10)

msf auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

whoami
lswazuh
pwd
/home/lswazuh
```

Gambar 1 Hasil Pengujian SSH Attack dan Brute Force Attack

2. Pengujian Port Scanning Attack

Pengujian Port Scanning Attack ialah salah satu simulasi information gathering. Tujuan dari simulasi serangan ini yaitu mengumpulkan informasi target yang dibutuhkan. Informasi yang dikumpulkan dalam port scanning attack berupa port yang terbuka dan jenis layanan aplikasi yang digunakan.

Gambar 2 menunjukkan hasil scanning terhadap server yang menampilkan port dan layanan yang terbuka serta versi layanan yang digunakan. Umumnya, dari informasi yang yang telah diperoleh, dapat digunakan sebagai serangan. Karena melalui ip dan port target, penyerang dapat memetakan jenis serangan yang cocok, serta versi layanan dapat digunakan untuk mencari log vulnerability.

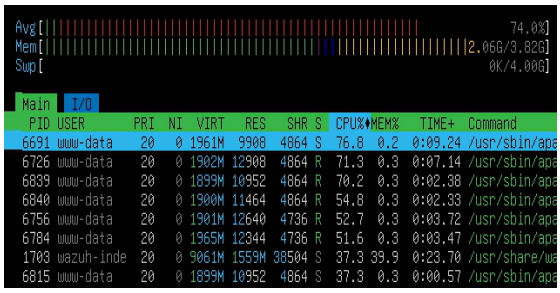
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -sS 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-06 10:32 WIB
Nmap scan report for 192.168.1.10
Host is up (0.0026s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
MAC Address: 08:00:27:91:4D:CE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.57 seconds

┌──(root㉿kali)-[/home/kali]
└─#
```

Gambar 2 Hasil Pengujian Port Scanning Attack

3. Pengujian Denial of Service Attack

Pengujian Denial of Service Attack dilakukan dengan menggunakan tools apache benchmark melalui sebuah perintah looping otomatis. metode ini membombardir server dengan permintaan HTTP (port 80) dalam jumlah yang sangat besar, yaitu 1.000.000 request dengan 2.000 koneksi serentak pada setiap iterasinya sehingga kinerja RAM dan CPU meningkat. Kinerja RAM dan CPU yang meningkat dapat menurunkan kinerja server.

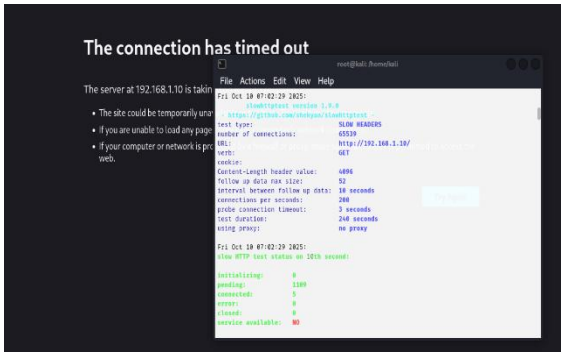
Gambar 3 merupakan pengujian Denial of Service 1.000.000 request dengan 2.000 koneksi serentak. Akibat dari serangan ini, penggunaan CPU yang semula 0,1% lalu meningkat drastis menjadi 74%.



Gambar 3 Hasil Pengujian DoS

4. Pengujian Distributed Denial of Service Attack

Pengujian Distributed Denial of Service Attack dilakukan dengan menggunakan tools slowhttp. Serangan ini mengirimkan header berupa GET atau POST dalam jumlah yang besar. Akibatnya server kehabisan resource dan web server tidak dapat diakses. Gambar 4 menunjukkan pengujian DDoS dengan mengirimkan 65.000 header dan hasilnya server down.

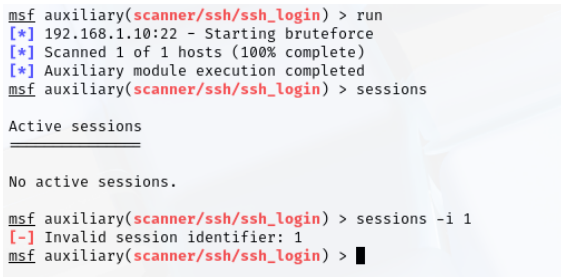


Gambar 4 Hasil Pengujian DDoS

4.2 Pengujian Menggunakan Firewall

1. Pengujian SSH Attack dan Brute Force Attack

Gambar 5 menunjukkan hasil pengujian SSH Attack dan Brute Force Attack pada server yang dilindungi oleh metode single packet authorization. Hasilnya, metode single packet authorization dapat mengamankan server dengan menolak semua permintaan masuk ke layanan SSH, kecuali pengguna yang berhasil mengirimkan spa key yang valid.



Gambar 1 Hasil Pengujian SSH Attack dan Brute Force Attack

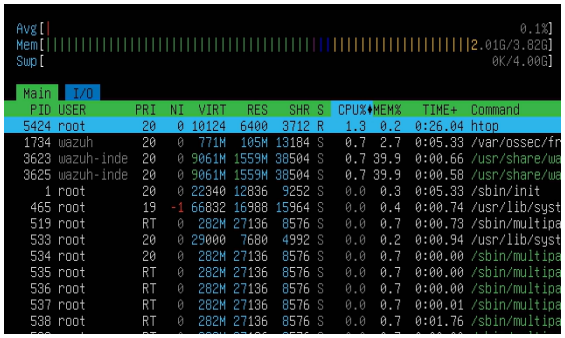
2. Pengujian Port Scanning Attack

Gambar 6 menunjukkan hasil pengujian port scanning attack pada server yang dilindungi oleh metode single packet authorization. Hasilnya, penyerang tidak mendapatkan informasi mengenai port sensitif server.

Gambar 6 Hasil Pengujian Port Scanning Attack

3. Pengujian Denial of Service Attack

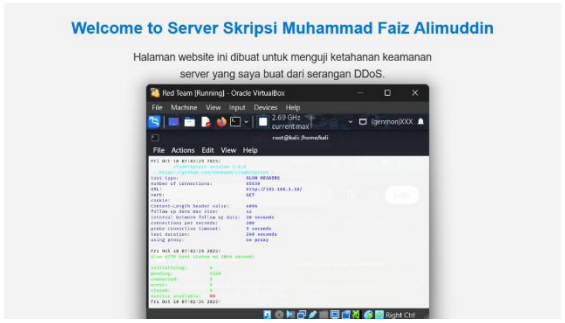
Gambar 7 menunjukkan metode *next-generation firewall filtering* dapat menekan efek dari serangan *denial of service*. Efek serangan semula pemakaian CPU meningkat hingga 75% dan dapat ditekan total hingga tetap 0.1%.



Gambar 7 Hasil Pengujian DoS

4. Pengujian Distributed Denial of Service Attack

Gambar 8 menunjukkan hasil pengujian DDoS dengan mengirimkan 65.000 header pada server yang dilindungi metode *next-generation firewall filtering*. Hasilnya, layanan web server masih dapat berfungsi normal.



Gambar 8 Hasil Pengujian DDoS

4.3 Hasil Pengujian

Berdasarkan serangkaian pengujian yang telah di lakukan pada server dapat disimpulkan bahwa konfigurasi firewall dengan menggunakan metode next-generation firewall filtering dan single packet authorization dapat menghalau serangan. Pada serangan SSH Attack dan Brute Force yang memfokuskan serangan pada port SSH, kemudian melancarkan serangan melalui teknik Brute Force yang mencoba masuk server dengan percobaan berulang dengan memanfaatkan kombinasi pada dictionary. Namun serangan tersebut dapat dihalau firewall, karena port SSH diamankan oleh metode single packet authorization. Sehingga ketika penyerang tidak memasukan SPA key yang valid, maka penyerang tidak akan bisa melacak dan masuk ke port SSH.

Pada serangan Port Scanning, nmap mengirimkan sejumlah paket kepada server target. Lalu jika paket tersebut direspon oleh server target, maka nmap dapat mengetahui host dan service yang aktif. Namun serangan tersebut dapat dihalau firewall menggunakan metode single packet authorization, karena firewall tidak akan membuka port dan informasi tentang port tersebut jika SPA key yang valid belum di terima.

Pada serangan Denial of Service, apache benchmark mengirimkan banyak 1.000.000 request dengan 2.000 koneksi serentak melalui sebuah perintah looping otomatis, sehingga kinerja CPU meningkat drastis. Namun serangan tersebut dapat dihalau firewall menggunakan metode next-generation firewall filtering, karena firewall memfilter paket yang masuk.

Pada serangan Distributed Denial of Service, slowhhtp mengirimkan banyak header GET dan POST, sehingga server kehabisan resource dan layanan web server tidak dapat berjalan dengan baik. Namun serangan tersebut dapat dihalau firewall, karena firewall memfilter paket yang masuk.

4.4 Pengujian Akurasi Firewall

Dalam menguji akurasi firewall menggunakan True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN). TP ialah serangan yang berhasil dihentikan oleh firewall. FN ialah serangan yang lolos dalam firewall. FP ialah aktivitas normal yang dianggap serangan. TN ialah aktivitas normal yang tidak dianggap serangan.

Berikut ialah rekap dari nilai TP, TN, FP, dan FN setelah dilakukan pengujian sebanyak 50 kali.

Tabel 1 Tabel Nilai TP, TN, FP, FN dalam menghitung akurasi

Jenis Serangan	TP	FP	TN	FN
SSH Attack	50	0	50	0
Brute Force Attack	50	0	50	0
Port Scanning	50	0	50	0
Denial of Service	50	0	50	0
Distributed Denial of Service	50	0	50	0

Berikut ialah rumus dalam menghitung akurasi tiap - tiap serangan, yaitu:

$$\text{Akurasi} = \frac{TP + TN}{TP + TN + FP + FN} \times 100\%$$

Berikut ialah nilai akurasi dari pengujian SSH Attacks yang telah dilakukan, yaitu:

$$\text{SSH Attack} = \frac{50 + 50}{50 + 50 + 0 + 0} \times 100\% = 100\%$$

Berikut ialah nilai akurasi dari pengujian Brute Force Attack yang telah dilakukan, yaitu:

$$\text{Brute Force} = \frac{50 + 50}{50 + 50 + 0 + 0} \times 100\% = 100\%$$

Berikut ialah nilai akurasi dari pengujian Port Scanning Attack yang telah dilakukan, yaitu:

$$\text{Port Scanning} = \frac{50 + 50}{50 + 50 + 0 + 0} \times 100\% = 100\%$$

Berikut ialah nilai akurasi dari pengujian Denial of Service Attack yang telah dilakukan, yaitu:

$$DoS\ attack = \frac{50 + 50}{50 + 50 + 0 + 0} \times 100\% = 100\%$$

Berikut ialah nilai akurasi dari pengujian Distributed Denial of Service Attack yang telah dilakukan, yaitu:

$$DDoS\ attack = \frac{50 + 50}{50 + 50 + 0 + 0} \times 100\% = 100\%$$

Selanjutnya, menghitung rata - rata akurasi dari tiap serangan dengan menggunakan rumus berikut, yaitu:

$$\frac{\text{jumlah akurasi per serangan}}{\text{Jumlah serangan}}$$

$$\frac{100\% + 100\% + 100\% + 100\% + 100\%}{5} = 100\%$$

Sehingga dari pengujian penetration testing yang telah dilakukan untuk menguji kinerja firewall, didapatkan nilai akurasi 100%.

5. KESIMPULAN

Berdasarkan hasil penelitian, implementasi Next-Generation Firewall Filtering dan Single Packet Authorization (SPA) menggunakan pfSense dan fwknop terbukti efektif dalam melindungi server dari berbagai simulasi serangan seperti port scanning, brute force, SSH attack, DoS, dan DDoS, karena mampu menutup celah layanan terbuka dan memfilter trafik berbahaya. Namun demikian, pada skenario serangan DDoS berskala sangat besar (Tbps), sistem tetap memiliki keterbatasan akibat saturasi bandwidth dan kelelahan perangkat keras, sehingga firewall dapat mengalami down meskipun metode filtering berjalan dengan baik. Dengan demikian, perlindungan terhadap serangan volumetrik ekstrem memerlukan pendekatan defense in depth yang melibatkan mitigasi di tingkat upstream atau layanan berbasis cloud.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada pihak-pihak terkait yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Z. Husen and M. S. Surbakti, *Membangun server dan jaringan komputer dengan Linux Ubuntu*. Syiah Kuala University Press, 2020.

[2] M. F. Ardiansyah, T. M. Diansyah, and R. Liza, 'Penggunaan Set top box Bekas untuk Dimanfaatkan sebagai Cloud Server', *Blend Sains Jurnal Teknik*, vol. 1, no. 2, pp. 88–96, 2022.

[3] B. Sugiantoro, 'Pemanfaatan Hasil Report Next-Generation Firewall Sebagai Security Awareness', *Cyber Security dan Forensik Digital*, 2019.

[4] U. Patel, 'The role of next-generation firewalls in modern network security: a comprehensive analysis', *International Journal of Advanced Research in Engineering and Technology (IJARET)*, vol. 15, no. 4, pp. 135–154, 2024.

[5] J. Heino, A. Hakkala, and S. Virtanen, 'Study of methods for endpoint aware inspection in a next generation firewall', *Cybersecurity*, vol. 5, no. 1, p. 25, 2022.

[6] A. DORIA, 'Identification of cyber attacks using Next Generation protection tools: NGFW, NG-SIEM, AI and Machine Learning', 2022.
[7] M. Xu, J. Guo, H. Yuan, and X. Yang, 'Zero-Trust security authentication based on SPA and endogenous security architecture', *Electronics (Basel).*, vol. 12, no. 4, p. 782, 2023.
[8] H. Muhammad, I. W. A. Arimbawa, and A. H. Jatmika, 'Analisis Perbandingan Sistem Autentikasi Port Knocking dan Single Packet Authorization pada Server Raspbian', *Jurnal Informatika dan Rekayasa Elektronik*, vol. 2, no. 1, pp. 28–37, 2019.
[9] D. A. Pribadi and W. Winarti, 'EVALUASI KEAMANAN SISTEM INFORMASI KEUANGAN SEKOLAH PAUD BERBASIS LARAVEL FILAMENT 3 MENGGUNAKAN PENETRATION TESTING', *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 14, no. 1, 2026.
[10] M. Fadhli, 'Comprehensive Analysis of Penetration Testing Frameworks and Tools: Trends', *Challenges, and Opportunities*, vol. 4, pp. 15–22, 2024.
[11] P. E. Firewall, 'Hotspot Network Security System From Brute Force Attack Using Pfsense External Firewall (Case Study of Wifi-Ku. Net Hotspot) Sistem Keamanan Jaringan Hotspot Dari Serangan Brute Force Menggunakan Firewall Eksternal Pfsense'.
[12] K. C. Patel and P. Sharma, 'A Review paper on pfsense-an Open source firewall introducing with different capabilities & customization', *IJARIIE*, vol. 3, pp. 2395–4396, 2017.
[13] S. S. Brar, 'Additional Security Mechanism in Single Packet Authorization', 2021.
[14] Y. M. Abdussyakur, A. Z. Mardiansyah, and A. H. Jatmika, 'Optimasi port knocking dan honeypot menggunakan IPTables sebagai keamanan jaringan pada server', *Jurnal Teknologi Informasi, Komputer, dan Aplikasinya (JTIKA)*, vol. 3, no. 2, pp. 35–45, 2021.
[15] D. Desmira, 'Sistem Keamanan Operasi Linux Ubuntu Iptables Sebagai Firewall Di Dinas Pendidikan Kabupaten Serang', *Jurnal Khatulistiwa Informatika*, vol. 9, no. 1, 2021.