Jurnal Software Engineering and Information System (SEIS)

https://ejurnal.umri.ac.id/index.php/SEIS/index

e-ISSN: 2809-0950

PENERAPAN TEKNOLOGI REVERSE PROXY MENGGUNAKAN NGINX PADA INFRASTRUKTUR DIGITAL PEMERINTAH KOTA PEKANBARU

Dedy Yasriady[1*)], Asep Marzuki[2)], Afifah Cahayani Adha[3)], Sisi Hendriani[4])
[1,2,3,4]S1 Informatika, Teknologi Kreatif dan Ekonomi, Universitas Awal Bros Pekanbaru
email: [1]yasriady@gmail.com, [2]kangasep.net@gmail.com, [3]afifah@univawalbros.ac.id
*Corresponding Author

Abstract

The rapid growth of web-based public services in local government has increased the complexity of managing web traffic, security, SSL certificates, and server administration across numerous subdomains. Without centralized management, these conditions can reduce operational efficiency and increase security risks. This study aims to evaluate the implementation of NGINX as a web gateway and reverse proxy within the digital infrastructure of the Pekanbaru City Government. A case study approach was employed through system design, implementation, and performance evaluation in a production environment managing the primary domain pekanbaru.go.id and approximately 170 subdomains. Data were collected from NGINX access logs, system monitoring using Grafana and Prometheus, and performance benchmarking using ApacheBench. The results show that the implementation of NGINX successfully centralized SSL certificate management, logging, and traffic routing through a single entry point, simplifying the administration of more than 170 subdomains while requiring only one public IP address. Benchmark testing indicates that although the average throughput of NGINX (163.07 requests/s) was slightly lower than the Apache backend (171.62 requests/s), NGINX demonstrated more stable performance with a significantly lower longest request time (2087 ms compared to 4039 ms) and no failed requests. These findings demonstrate that NGINX is an effective solution for improving operational efficiency, centralized security management, and service stability in government web infrastructures.

Keywords: *NGINX, reverse proxy, web gateway, e-government, web server, performance evaluation*

Abstrak

Perkembangan layanan publik berbasis web di lingkungan pemerintahan menyebabkan meningkatnya kompleksitas dalam pengelolaan trafik, keamanan, sertifikat SSL, dan administrasi server pada banyak subdomain. Pengelolaan yang dilakukan secara terpisah berpotensi menurunkan efisiensi operasional serta meningkatkan risiko keamanan. Penelitian ini bertujuan mengevaluasi implementasi NGINX sebagai web gateway dan reverse proxy pada infrastruktur digital Pemerintah Kota Pekanbaru. Metode yang digunakan adalah studi kasus melalui tahapan perancangan, implementasi, dan evaluasi sistem pada lingkungan produksi yang mengelola domain utama pekanbaru.go.id beserta sekitar 170 subdomain. Data diperoleh melalui analisis log akses NGINX, pemantauan sistem menggunakan Grafana dan Prometheus, serta pengujian performa menggunakan ApacheBench. Hasil penelitian menunjukkan bahwa implementasi NGINX berhasil memusatkan pengelolaan sertifikat SSL, pencatatan log, dan pengaturan lalu lintas melalui satu titik masuk (single entry point), sehingga mempermudah administrasi lebih dari 170 subdomain dengan hanya menggunakan satu alamat IP publik. Hasil pengujian menunjukkan bahwa meskipun throughput rata-rata NGINX (163,07 request/detik) sedikit lebih rendah dibandingkan Apache (171,62 request/detik), NGINX memberikan performa yang lebih stabil dengan nilai longest request yang lebih rendah (2087 ms dibandingkan 4039 ms) serta tidak ditemukan failed request. Temuan ini menunjukkan bahwa implementasi NGINX efektif dalam meningkatkan efisiensi pengelolaan infrastruktur, memperkuat keamanan terpusat, dan menjaga stabilitas layanan web pada lingkungan pemerintahan.

Keywords: NGINX, reverse proxy, web gateway, e-government, server web, evaluasi kinerja.

PENDAHULUAN

Kemajuan teknologi informasi mendorong instansi pemerintahan untuk terus bertransformasi menuju sistem digital yang terintegrasi, cepat, dan aman. Transformasi digital dan sistem informasi terintegrasi meningkatkan efisiensi, akurasi, dan transparansi pelayanan publik di sektor pemerintahan pusat, mendukung urgensi sistem digital yang cepat dan terintegrasi (Savitri & MT, 2024). Pemerintah daerah, sebagai garda terdepan dalam pelayanan publik, dituntut untuk menyediakan layanan berbasis web yang dapat diakses dengan mudah oleh masyarakat. Hal ini mencakup portal informasi, sistem administrasi internal, hingga berbagai aplikasi layanan elektronik *e-government*. Pemerintah harus menyediakan pelayanan publik yang efektif dan efisien melalui teknologi informasi berbasis web, sebagai respons terhadap kebutuhan fundamental masyarakat saat ini (Nurnawati et al., 2024).

Dalam implementasi transformasi digital tersebut, instansi pemerintahan menghadapi tantangan kompleks terkait keamanan dan efisiensi sistem. Transformasi digital instansi pemerintahan tidak hanya berfokus pada integrasi dan efisiensi, tetapi juga menuntut penerapan praktik keamanan mutakhir. Studi global terbaru mengungkapkan bahwa banyak layanan publik pemerintah di seluruh dunia belum memenuhi standar protokol komunikasi yang aman dan rantai sertifikat digital yang terpercaya, sehingga mengekspos data sensitif dan layanan terhadap ancaman siber (Silva et al., 2024). Aspek keamanan lain yang perlu diperhatikan adalah peran reverse proxy sebagai titik kontrol terpusat dalam mitigasi serangan Distributed Denial of Service (DDoS). Penelitian oleh (Pardosi, 2024) menunjukkan bahwa penerapan NGINX Reverse Proxy sebagai lapisan penyaring trafik mampu memfilter lalu lintas yang mencurigakan sebelum mencapai server internal. Hasil pengujian pada serangan Layer 3 dan Layer 4 memperlihatkan bahwa pendekatan ini secara efektif mengurangi dampak serangan DDoS sekaligus meningkatkan ketersediaan layanan. Banyaknya aplikasi yang tersebar di berbagai subdomain sering kali menimbulkan tantangan dalam hal pengelolaan trafik, keamanan, dan efisiensi sistem, sehingga menggarisbawahi urgensi pemerintah daerah untuk membangun sistem reverse proxy yang tidak hanya menyederhanakan manajemen trafik, tetapi juga memperkuat keamanan komunikasi secara menyeluruh.

Pemerintah Kota Pekanbaru telah mengembangkan berbagai layanan berbasis web yang terintegrasi dengan domain utama pekanbaru.go.id dan subdomain turunannya. Namun, pengelolaan trafik dan akses dari berbagai sumber masih menghadapi kendala, seperti tidak meratanya beban jaringan, potensi serangan siber, serta kerumitan dalam manajemen sertifikat SSL dan konfigurasi server individu. Kondisi ini mendorong perlunya sebuah solusi terpusat yang mampu menyederhanakan manajemen, meningkatkan keamanan, dan sekaligus memberikan skalabilitas tinggi terhadap pertumbuhan layanan. Meskipun teknologi *reverse proxy* telah banyak diterapkan dalam berbagai sistem jaringan modern, penelitian yang secara khusus membahas implementasi NGINX sebagai *reverse proxy* dalam konteks *e-government* di Indonesia, khususnya dengan pendekatan langsung pada sistem produksi pemerintahan daerah, masih relatif terbatas. Hal ini menunjukkan adanya gap penelitian yang perlu dijembatani melalui studi berbasis implementasi nyata seperti yang dilakukan dalam penelitian ini.

Salah satu solusi yang diusulkan adalah penerapan NGINX sebagai *web gateway* sekaligus *reverse proxy*. NGINX dikenal sebagai perangkat lunak open-source yang ringan, cepat, dan dapat dikonfigurasi untuk berbagai kebutuhan, seperti load balancing, caching, SSL termination, dan penyaringan akses. Dengan memusatkan seluruh trafik HTTP/HTTPS ke satu pintu masuk melalui NGINX, sistem dapat dikelola dengan lebih efisien, sekaligus menyediakan kontrol yang lebih baik terhadap keamanan dan kinerja layanan.

Berbagai penelitian sebelumnya telah menunjukkan efektivitas implementasi reverse proxy dalam meningkatkan efisiensi pengelolaan server dan memberikan lapisan keamanan tambahan. Praktik implementasi reverse proxy dengan NGINX di lingkungan pemerintahan telah terbukti efektif dalam mengurangi kebutuhan alamat IP publik secara signifikan. Penelitian di lingkungan data center menunjukkan bahwa satu alamat IPv4 publik dapat digunakan untuk melayani banyak server internal, sekaligus menyembunyikan keberadaan server asal dari pemindaian eksternal—mengurangi potensi serangan langsung ke aplikasi internal (Sandy Bukhari & Iqbal, 2024). Efek ini sangat relevan untuk kondisi Pemerintah Kota Pekanbaru, di mana pengelolaan alamat IP dan pencegahan serangan eksternal adalah tantangan utama. Implementasi *reverse proxy* memudahkan integrasi sistem monitoring dan pencegahan serangan, karena seluruh trafik dapat dikendalikan dari satu titik masuk, menyembunyikan informasi sensitif seperti port dan IP internal dari pemindaian eksternal seperti NMAP (Pebrianto, 2024).

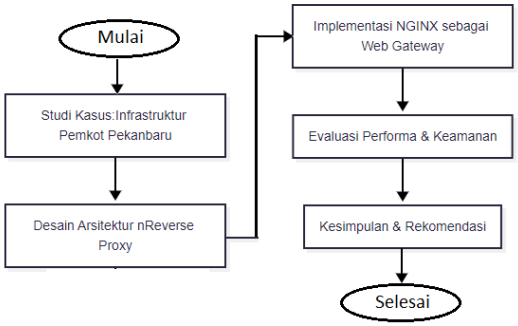
Reverse proxy caching mampu menyeimbangkan beban pada beberapa server *back-end* dan menyediakan caching untuk server *back-end* yang lamban terutama pada web server Apache (Azi et al., 2023). Dalam sebuah penelitian mengenai CDN yang memanfaatkan NGINX, waktu respons

berkurang hingga 50% di semua lokasi, berkisar antara 450 ms hingga 600 ms. Pengurangan ini disebabkan oleh caching yang memungkinkan konten diambil dari server CDN terdekat, mengurangi latensi (Darujati & Al Azam, 2023). Selain keunggulan performa dalam menangani permintaan dari banyak klien secara bersamaan, NGINX juga memberikan fleksibilitas arsitektur melalui kemampuannya sebagai reverse proxy server yang bertindak sebagai perantara antara klien dan server backend. Pendekatan ini memungkinkan NGINX berfungsi sebagai pintu gerbang utama yang menerima permintaan HTTP dari web client dan menentukan server *backend* yang akan menangani permintaan tersebut, sekaligus meningkatkan keamanan dengan melindungi server asli dari serangan langsung seperti DDoS dan memudahkan penerapan kebijakan keamanan seperti otentikasi dan otorisasi pengguna (Satrya Bhayangkara & Miftahul Ashari, 2024). Dengan demikian akan diperoleh fleksibilitas operasional melalui kemampuan sebagai gateway satu pintu untuk layanan, *load balancer*, *SSL termination*, dan *cache*. Pendekatan ini menyederhanakan konfigurasi sertifikat TLS/SSL dan memudahkan pembaruan keamanan, alih-alih menangani sertifikat pada masing-masing layanan secara terpisah. Dengan demikian, solusi berbasis NGINX secara central terpusat menyediakan skalabilitas operasional dan pengamanan yang konsisten terhadap pertumbuhan layanan *e-government* kota yang dikelola.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengevaluasi efektivitas penerapan NGINX sebagai *web gateway* dan *reverse proxy* pada infrastruktur jaringan Pemerintah Kota Pekanbaru. Metode yang digunakan adalah studi kasus melalui perancangan, implementasi, dan evaluasi sistem *reverse proxy* berbasis NGINX yang mengelola domain pekanbaru.go.id dan seluruh subdomainnya. Hasil dari penelitian ini diharapkan dapat menjadi referensi praktis bagi instansi pemerintahan lainnya yang ingin menerapkan pendekatan serupa dalam upaya digitalisasi layanan publik yang terpusat dan aman. Hipotesis yang diajukan dalam penelitian ini adalah bahwa penggunaan NGINX sebagai *reverse proxy* terpusat dapat secara signifikan meningkatkan efisiensi, keamanan, dan kinerja sistem layanan berbasis web di lingkungan pemerintahan.

METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan studi kasus terhadap infrastruktur jaringan Pemerintah Kota Pekanbaru, dengan fokus pada implementasi NGINX sebagai reverse proxy dan web gateway yang mengelola domain utama pekanbaru.go.id beserta seluruh subdomain di bawahnya. Pendekatan studi kasus dipilih karena penelitian dilakukan pada lingkungan operasional yang nyata sehingga memungkinkan evaluasi langsung terhadap efektivitas implementasi teknologi yang diterapkan. Pendekatan ini memberikan gambaran menyeluruh mengenai proses perancangan, implementasi, serta evaluasi performa dan keamanan sistem dalam kondisi operasional sebenarnya. Secara umum, tahapan penelitian yang dilakukan ditunjukkan pada Gambar 1.



Gambar 1. Metodologi Penelitian

Tahapan penelitian terdiri atas lima tahap utama sebagai berikut:

1. Studi Kasus Infrastruktur

Tahap pertama dilakukan melalui observasi terhadap infrastruktur jaringan Pemerintah Kota Pekanbaru yang melayani domain utama pekanbaru.go.id beserta seluruh subdomain-nya. Pada tahap ini dilakukan identifikasi kondisi eksisting, arsitektur layanan, mekanisme pengelolaan trafik, pengelolaan sertifikat SSL, serta berbagai permasalahan yang dihadapi dalam operasional sistem.

2. Perancangan Arsitektur

Berdasarkan hasil identifikasi kebutuhan, dirancang arsitektur *reverse proxy* menggunakan NGINX sebagai *single entry point*. Perancangan meliputi mekanisme *SSL termination*, *URL routing*, *reverse proxy*, pengelolaan sertifikat digital, pencatatan log (*logging*), serta integrasi dengan sistem monitoring dan keamanan.

3. Implementasi Sistem

Tahap implementasi dilakukan dengan mengonfigurasi NGINX sebagai *reverse proxy* pada lingkungan produksi. Implementasi meliputi konfigurasi *virtual host*, pengalihan trafik menuju server *backend*, penerapan sertifikat SSL, pencatatan log akses, serta integrasi dengan sistem monitoring dan mekanisme keamanan.

4. Evaluasi Sistem

Tahap evaluasi dilakukan untuk mengetahui efektivitas implementasi NGINX terhadap performa, kemudahan pengelolaan, dan keamanan sistem. Evaluasi dilakukan melalui pengujian performa menggunakan Apache Benchmark (AB), pemantauan sistem menggunakan Grafana dan Prometheus, analisis log akses NGINX, serta observasi terhadap kestabilan layanan selama periode pengujian.

5. Analisis dan Kesimpulan

Data hasil pengujian dianalisis secara kuantitatif dan kualitatif untuk mengevaluasi efektivitas penerapan NGINX sebagai *reverse proxy*. Hasil analisis kemudian digunakan sebagai dasar dalam penyusunan kesimpulan dan rekomendasi pengembangan sistem pada penelitian selanjutnya.

Sistem yang dikembangkan mengintegrasikan NGINX sebagai *reverse proxy* utama yang menangani seluruh trafik HTTP/HTTPS dari domain dan subdomain. Fungsi utama NGINX dalam penelitian ini meliputi:

1. *SSL termination* dan manajemen sertifikat digital;
2. URL routing dan pengalihan (*redirect/rewrite*);
3. *Logging* dan *monitoring* trafik web secara *real-time*;

Implementasi dilakukan pada infrastruktur nyata yang telah berjalan, terdiri atas:

1. Server virtual berbasis Linux (Ubuntu 20.04);
2. Hypervisor Proxmox untuk virtualisasi;
3. Beberapa aplikasi layanan web (portal informasi resmi, sistem kepegawaian, layanan publik, aplikasi internal, dsb);
4. Sistem DNS yang terintegrasi dengan *reverse proxy;*

Dalam hal pengumpulan data dilakukan melalui beberapa metode:

1. Log server NGINX;
2. Monitoring sistem menggunakan tools seperti Grafana dan Prometheus;
3. *Benchmark* performa dengan *ApacheBench* dan curl untuk mengukur latensi dan throughput;
4. Observasi langsung terhadap kestabilan dan downtime sistem selama periode tertentu;

Data yang dihasilkan oleh NGINX (access.log) dapat digunakan untuk untuk berbagai keperluan analisis. Terdapat studi yang menggunakan log Nginx untuk analisis keamanan serangan *brute force* melalui metodologi *digital forensic*. Penelitian dimaksud membangun *dashboard* monitoring berbasis log Nginx untuk mendeteksi aktivitas login administrator yang mencurigakan (*brute force attack*). Dengan analisis log yang dilakukan secara kuantitatif, penelitian tersebut berhasil mengidentifikasi *metadata* serangan dan lokasi dari aktivitas penyerang (Pradana Aji et al., 2023). Selain itu, penelitian mengenai analisis web server access log juga menunjukkan bahwa berkas access log dapat dimanfaatkan sebagai sumber data utama untuk menganalisis pola akses pengguna, alamat IP, halaman yang paling sering dikunjungi, serta karakteristik perilaku pengunjung melalui proses web usage mining dan clustering. Analisis tersebut membuktikan bahwa data log server mampu memberikan informasi yang komprehensif mengenai aktivitas pengguna sebagai dasar pengambilan keputusan dalam pengelolaan layanan web (Dixit & Sharma, 2023) Dalam suatu secara eksplisit menggunakan Grafana untuk visualisasi monitoring performa NGINX dalam konteks skala otomatis (auto-scaling). Dibahas mengenai keunggulan alerting Grafana dibandingkan Prometheus Alert Manager. Ini menegaskan pemanfaatan Grafana dalam konteks monitoring metrik dan alert NGINX (Darmawan, 2023). Dalam suatu penelitian dengan judul "Analisis Perbandingan Performa Web Server Apache, Nginx, Dan Litespeed Studi Kasus Implementasi Di VPS", pengujian performa dilakukan menggunakan alat seperti Apache Benchmark (ab) atau JMeter untuk mengevaluasi parameter teknis seperti waktu respons, throughput, latensi, dan penggunaan sumber daya seperti CPU, dan RAM (Perdana & Prihanto, 2025). Ini memberikan gambaran jelas penggunaan ApacheBench dalam mengukur *throughput* dan latency pada web server berbasis HTTP.

Dalam penelitian yang dilakukan ini, efektivitas sistem dinilai berdasarkan beberapa indikator berikut:

1. Kemudahan manajemen konfigurasi, ditinjau dari perbandingan antara pendekatan terpusat dan terpisah dalam instalasi dan pengelolaan sertifikat SSL pada masing-masing layanan.
2. Rata-rata waktu respons sistem sebelum dan sesudah implementasi NGINX, yang diukur menggunakan Apache Benchmark sebagai alat uji performa.
3. Efisiensi manajemen log akses, ditinjau dari kemampuan sistem dalam mengonsolidasikan file log dari seluruh domain dan subdomain ke dalam satu titik pemantauan.
4. Stabilitas layanan, yang diukur melalui tingkat downtime dan error rate selama periode pengamatan operasional sistem.

5. Efektivitas mekanisme penyaringan keamanan terpusat, meliputi pemblokiran alamat IP mencurigakan, penerapan rate limiting, serta integrasi dengan modul proteksi seperti Fail2Ban dan ModSecurity sebagai Web Application Firewall (WAF).

Data kuantitatif dianalisis secara komparatif untuk menunjukkan peningkatan performa dan efisiensi sistem. Sedangkan data kualitatif dianalisis untuk mendukung interpretasi hasil serta mengidentifikasi potensi tantangan dan pengembangan lebih lanjut.

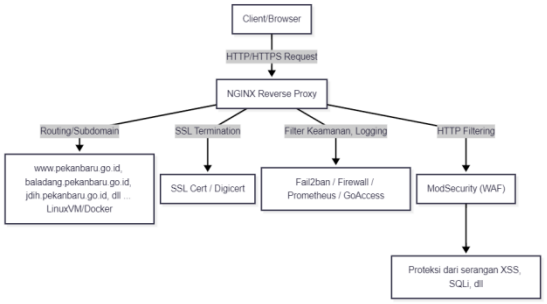
Dalam pelaksanaan dan implementasi sistem secara aktual, spesifikasi yang digunakan dapat dilihat pada table 1.

Tabel 1. Spesifikasi Server

Komponen	Spesifikasi
Hostname	nginx.pekanbaru.go.id
Sistem Operasi	20.04.6 LTS (Focal Fossa)
CPU	16 vCPU (Intel Xeon Gold)
RAM	16 GB
Storage	32 GB
Koneksi Jaringan	500 Mbps
Versi NGINX	nginx/1.18.0
Hypervisor	Proxmox VE 5.x

Berikut adalah konfigurasi yang diaplikasikan pada NGINX:

```
server {
   listen 443 ssl;
   server_name www.pekanbaru.go.id;
   access_log /var/log/nginx/acces.log;
   error_log /var/log/nginx/error.log;
   ssl_certificate
/etc/ssl/certs/star_pekanbaru_go_id.pem;
   ssl_certificate_key
/etc/ssl/private/star_pekanbaru_go_id.key;
   ssl_trusted_certificate /etc/ssl/certs/DigiCertCA.crt;
   location / {
      proxy_pass https://10.11.15.26;
      proxy_set_header Host $host;
      client_max_body_size 0;
      proxy_set_header X-Real-Ip $remote_addr;
      proxy_set_header X-Forwarded-For
$proxy_add_x_forwarded_for;
      proxy_set_header REMOTE_ADDR
$remote_addr;
   }
}
```



Gambar 2. Diagram Implementasi NGINX

Penjelasan dari gambar diagram implementasi adalah sebagai berikut:

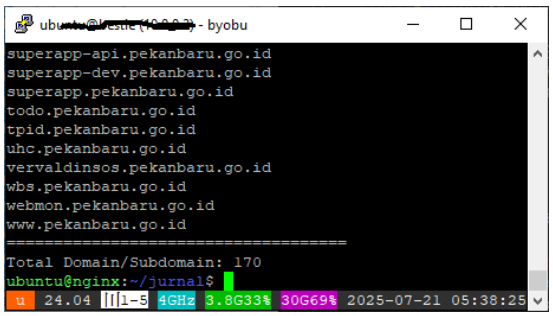
1. NGINX bertindak sebagai *reverse proxy* pusat untuk semua subdomain;
2. Lalu lintas HTTPS diterminasi di NGINX dan diarahkan ke *backend service*;
3. Manajemen sertifikat SSL yang diterbitkan oleh Digicert;
4. Monitoring & logging dilakukan melalui tools seperti GoAccess, Grafana atau Prometheus;
5. Keamanan diperkuat melalui Fail2ban dan firewall, yang memblokir akses mencurigakan.
6. ModSecurity digunakan sebagai Web Application Firewall (WAF) untuk mendeteksi dan memblokir serangan berbasis aplikasi seperti SQL Injection, XSS, dan request tidak sah lainnya.

Penelitian ini dilakukan secara langsung di lingkungan nyata, berdasarkan implementasi sistem yang telah dibangun dan dijalankan oleh penulis sendiri pada infrastruktur jaringan Pemerintah Kota Pekanbaru. Sistem *reverse proxy* berbasis NGINX yang dibahas dalam studi ini merupakan bagian integral dari operasional harian layanan publik berbasis web, termasuk domain utama pekanbaru.go.id dan berbagai subdomain turunannya. Untuk menjaga kerahasiaan sistem serta mencegah potensi penyalahgunaan informasi, seluruh data sensitif yang ditampilkan dalam dokumen ini telah disesuaikan. Beberapa elemen seperti alamat IP, nama domain internal, kredensial, dan konfigurasi keamanan tertentu telah dianonimkan atau dimodifikasi tanpa mengubah substansi teknis dan konteks fungsional sistem. Penyesuaian ini dilakukan sebagai bagian dari upaya perlindungan terhadap celah keamanan aktual yang dapat dieksploitasi oleh pihak tidak bertanggung jawab. Dengan demikian, meskipun penelitian ini didasarkan pada kondisi dan sistem yang benar-benar digunakan di lapangan, publikasi ini tetap memperhatikan prinsip-prinsip keamanan informasi

dan etika dalam penyebaran data infrastruktur kritikal.

HASIL DAN PEMBAHASAN

Gambar 3 berupa hasil tangkapan layar berikut menyajikan visualisasi jumlah subdomain yang dikelola dan dilayani oleh sistem NGINX sebagai *web gateway*.



Gambar 3. Subdomain yang menggunakan NGINX

Berdasarkan data hasil implementasi, tercatat bahwa sistem *reverse proxy* berbasis NGINX yang diterapkan dalam infrastruktur Pemerintah Kota Pekanbaru telah melayani sekitar 170 subdomain. Jumlah ini menunjukkan skala kompleksitas layanan web yang cukup tinggi, di mana masing-masing subdomain mewakili aplikasi, layanan, atau unit kerja tertentu dalam sistem pemerintahan elektronik. Jika sistem ini tidak menggunakan pendekatan sentralisasi melalui NGINX sebagai *web gateway*, maka pengelolaan konfigurasi keamanan, khususnya sertifikat SSL (*Secure Socket Layer*), akan menjadi sangat rumit dan tidak efisien. Hal ini disebabkan karena setiap *subdomain* yang berada di server *backend* harus dikonfigurasi secara manual satu per satu, baik dari sisi instalasi sertifikat, perpanjangan masa berlaku, maupun pembaruan kunci enkripsi. Proses tersebut tentunya akan menyita waktu, meningkatkan risiko kesalahan konfigurasi, serta menyulitkan proses audit keamanan.

Lebih lanjut, penggunaan NGINX sebagai reverse proxy juga memberikan manfaat signifikan dalam hal efisiensi pemanfaatan sumber daya jaringan, terutama pada penggunaan alamat IP publik. Seluruh subdomain yang tersebar di berbagai server *backend* kini cukup dilayani melalui satu IP publik saja, sehingga menghemat kebutuhan IP dan menyederhanakan konfigurasi NAT (*Network Address Translation*) di perangkat jaringan. Pendekatan ini juga berdampak positif terhadap manajemen trafik, karena seluruh permintaan HTTP/HTTPS diarahkan dan dikendalikan dari satu titik pusat yang lebih mudah diawasi dan diamankan.

Manfaat strategis lain dari penerapan NGINX sebagai *web gateway* dan *reverse proxy* dalam sistem ini adalah kemampuannya dalam mengonsolidasikan log akses dari seluruh subdomain yang dilayani. *Log* yang dihasilkan oleh NGINX tidak hanya mencatat permintaan terhadap domain utama, tetapi juga semua aktivitas yang terjadi pada ratusan subdomain lainnya dalam satu berkas log yang terpusat. Konsolidasi ini memberikan keuntungan signifikan dalam hal pemantauan, audit, dan analisis lalu lintas jaringan secara menyeluruh.

Sebagai contoh, data log yang ditampilkan mencerminkan keberagaman sumber permintaan, termasuk dari mesin pencari seperti Googlebot dan Amazonbot, crawler sosial media seperti Facebook meta-externalagent, serta aktivitas yang mencurigakan seperti permintaan terhadap file ilegal (misalnya, __MACOSX.rar atau www.zip). Semua ini dapat terpantau secara *real-time* melalui satu titik sentral, tanpa memerlukan akses ke setiap server backend secara individual.

Konsolidasi log ini memberikan efisiensi dalam manajemen sistem, karena tidak lagi diperlukan prosedur pencatatan terpisah untuk masing-masing server aplikasi. Selain itu, analisis forensik pasca insiden keamanan dapat dilakukan secara lebih cepat dan akurat, karena semua data lalu lintas tersedia secara komprehensif di satu lokasi. Keunggulan ini menjadikan NGINX tidak hanya sebagai komponen pengatur lalu lintas jaringan, tetapi juga sebagai alat strategis dalam memperkuat postur keamanan siber serta mendukung pengambilan keputusan berbasis data secara efektif di lingkungan pemerintahan.

Selanjutnya, untuk mengevaluasi kinerja layanan web yang dijalankan melalui NGINX sebagai reverse proxy, dilakukan pengujian berbasis tool Apache Benchmark (AB). Pengujian dilakukan terhadap dua endpoint yang merepresentasikan sistem: satu melalui NGINX (port 443) sebagai web gateway, dan satu lagi langsung ke Apache backend server (port 10443) tanpa perantara reverse proxy. Perintah pengujian dilakukan dengan parameter -n 1000 -c 10 -k, yang berarti setiap pengujian menjalankan 1000 permintaan secara berurutan dengan 10 permintaan paralel secara konkuren, dan menggunakan koneksi keep-alive untuk mensimulasikan trafik riil.

```
ab -n 1000 -c 10 -k
https://www.pekanbaru.go.id/coba.txt
ab -n 1000 -c 10 -k
https://www.pekanbaru.go.id:10443/coba.txt
```

Data yang diperlihatkan pada tabel 2 berikut menyajikan hasil pengujian rata-rata dari 10 iterasi:

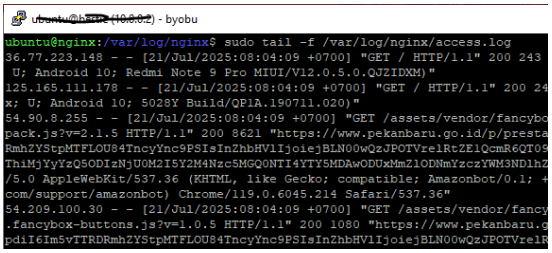
Tabel 2. Metrik perbandingan Nginx dan Apache

Metrik	Apache	NGINX
Requests per second (avg)	171.62 req/sec	163.07 req/sec
Time per request (avg)	58.30 ms	61.29 ms
Transfer rate (avg)	222.01 KB/sec	212.92 KB/sec
Longest request (maks)	4039 ms	2087 ms
Failed requests	0	0

Secara umum, hasil *benchmark* menunjukkan bahwa meskipun Apache sedikit lebih unggul dari sisi *throughput* rata-rata (requests per second), NGINX menunjukkan performa yang lebih stabil dan konsisten antar iterasi. Puncak performa NGINX tercatat pada iterasi kelima dengan *throughput* sebesar 193.78 req/sec, sedangkan waktu respon rata-rata per permintaan berkisar antara 55 hingga 65 milidetik, yang mencerminkan kestabilan sistem dalam menangani beban kerja secara simultan.

Meskipun rata-rata throughput Apache sedikit lebih tinggi dibandingkan NGINX, hasil pengujian juga mencatat bahwa nilai *longest request* pada NGINX lebih rendah dibandingkan Apache (2087 ms vs. 4039 ms). Metrik ini bukan merupakan indikator utama performa, namun dapat memberikan gambaran tambahan terkait kestabilan respons dalam kondisi beban tertentu. Temuan ini mengindikasikan bahwa dalam skenario tertentu, NGINX cenderung menghasilkan waktu tunggu ekstrem yang lebih terkendali, meskipun perbandingan ini perlu ditafsirkan secara hati-hati dan tidak dapat dijadikan satu-satunya acuan untuk menyimpulkan keandalan sistem secara keseluruhan.

Selain peningkatan performa, penerapan NGINX sebagai *reverse proxy* juga memberikan dampak strategis dalam hal efisiensi arsitektur dan penguatan aspek keamanan sistem. Dengan pendekatan terpusat, seluruh lalu lintas HTTP/HTTPS dikonsolidasikan melalui satu titik masuk, sehingga memungkinkan penerapan kebijakan keamanan yang seragam, terstandarisasi, dan mudah diaudit. Hal ini menyederhanakan pengelolaan sistem secara menyeluruh, baik dari sisi operasional maupun teknis.



Gambar 4. File access.log

Gambar 4 memperlihatkan hasil penyimpanan log yang berada di satu tempat. Sentralisasi ini memperkuat kemampuan dalam melakukan pemantauan dan analisis trafik secara *real-time*. Administrator jaringan dapat dengan lebih mudah mengidentifikasi pola lalu lintas, mengklasifikasikan jenis agen pengguna (user-agent), serta mendeteksi aktivitas anomali atau potensi ancaman keamanan, seperti *bot scraping*, pemindaian port ilegal (*unauthorized port probing*), maupun upaya eksploitasi lainnya. Untuk mendukung analisis lalu lintas secara cepat dan informatif, sistem ini dapat diintegrasikan dengan GoAccess sebagai alat visualisasi ringan berbasis terminal atau web dashboard yang menyajikan statistik log akses secara interaktif dan *real-time*. Selain itu, penerapan *Security Information and Event Management (SIEM)* berbasis Wazuh dapat dilakukan guna memperluas cakupan monitoring dengan kemampuan korelasi log, deteksi anomali, dan notifikasi insiden keamanan yang lebih terstruktur. Integrasi dengan sistem pemantauan seperti Grafana dan Prometheus memungkinkan visualisasi performa dan kesehatan sistem secara komprehensif, serta memfasilitasi deteksi dini terhadap serangan atau gangguan layanan. Di sisi lain, kolaborasi dengan modul keamanan seperti Fail2ban memberikan lapisan proteksi tambahan dengan kemampuannya memblokir otomatis alamat IP yang menunjukkan pola akses mencurigakan.

Dari perspektif manajemen TI, sistem berbasis NGINX ini juga menyederhanakan proses pemeliharaan. Sebelumnya, pengelolaan server web dilakukan secara terpisah untuk masing-masing subdomain, yang membutuhkan konfigurasi individual dan pemantauan terpisah. Dengan pendekatan terpusat, tim teknis kini dapat memfokuskan pengelolaan pada satu sistem pusat, mengurangi beban kerja, risiko konfigurasi inkonsisten, serta waktu tanggap terhadap insiden.

Hasil implementasi ini menunjukkan bahwa NGINX tidak hanya efektif sebagai *reverse proxy* dari sisi teknis dan performa, tetapi juga membuka peluang pengembangan sistem lebih lanjut. Beberapa potensi pengembangan ke depan meliputi integrasi dengan Web Application Firewall (WAF) seperti *ModSecurity*, penerapan caching sisi edge

untuk akselerasi konten, dan replikasi arsitektur ini pada sistem layanan digital lainnya di tingkat daerah maupun nasional.

SIMPULAN

Penelitian ini bertujuan untuk mengevaluasi efektivitas penerapan NGINX sebagai web gateway dan reverse proxy pada infrastruktur jaringan Pemerintah Kota Pekanbaru. Berdasarkan hasil implementasi dan evaluasi sistem, dapat disimpulkan bahwa tujuan penelitian telah tercapai. Implementasi NGINX terbukti mampu menyediakan mekanisme pengelolaan layanan web yang lebih terpusat melalui satu titik masuk (single entry point) sehingga mempermudah administrasi lebih dari 170 subdomain yang digunakan pada lingkungan Pemerintah Kota Pekanbaru. Sentralisasi tersebut menyederhanakan konfigurasi layanan, pengelolaan sertifikat SSL, serta pemantauan lalu lintas jaringan secara terintegrasi.

Hasil pengujian menggunakan Apache Benchmark menunjukkan bahwa keberadaan NGINX sebagai reverse proxy tidak memberikan penurunan performa yang signifikan terhadap layanan web. Meskipun nilai throughput rata-rata sedikit berada di bawah Apache, NGINX memperlihatkan respons yang lebih stabil dengan nilai longest request yang lebih rendah. Temuan ini menunjukkan bahwa NGINX layak diterapkan sebagai lapisan gateway pada lingkungan produksi yang mengutamakan stabilitas, kemudahan pengelolaan, dan konsistensi layanan.

Selain aspek performa, penerapan NGINX juga meningkatkan efektivitas pengelolaan infrastruktur melalui konsolidasi log akses, sentralisasi kebijakan keamanan, efisiensi penggunaan alamat IP publik, serta kemudahan integrasi dengan berbagai mekanisme keamanan dan sistem monitoring. Dengan demikian, implementasi reverse proxy berbasis NGINX tidak hanya memberikan manfaat teknis, tetapi juga mendukung tata kelola infrastruktur digital pemerintahan yang lebih efisien, aman, dan mudah dikembangkan.

SARAN

Penelitian ini masih berfokus pada implementasi dan evaluasi reverse proxy pada satu lingkungan operasional Pemerintah Kota Pekanbaru sehingga ruang lingkup pengujiannya masih terbatas. Oleh karena itu, penelitian selanjutnya disarankan untuk melakukan evaluasi pada lingkungan yang lebih beragam, baik dari sisi jumlah layanan, karakteristik trafik, maupun skenario beban yang lebih tinggi agar diperoleh gambaran performa yang lebih komprehensif.

Selain itu, pengembangan penelitian dapat diarahkan pada integrasi NGINX dengan teknologi keamanan dan observabilitas yang lebih maju, seperti Web Application Firewall (ModSecurity), Security Information and Event Management (SIEM), analisis log berbasis kecerdasan buatan (AI-based anomaly detection), serta implementasi high availability dan load balancing untuk meningkatkan keandalan layanan pemerintah yang bersifat kritikal.

Penelitian berikutnya juga dapat melakukan perbandingan implementasi NGINX dengan solusi reverse proxy lainnya, seperti HAProxy, Traefik, atau Envoy Proxy, menggunakan parameter evaluasi yang lebih lengkap, meliputi performa, skalabilitas, konsumsi sumber daya, kemudahan administrasi, dan tingkat keamanan. Hasil penelitian tersebut diharapkan dapat menjadi acuan dalam penyusunan arsitektur infrastruktur digital pemerintahan yang semakin adaptif terhadap kebutuhan transformasi digital.

TERIMA KASIH

Penulis menyampaikan apresiasi dan rasa terima kasih yang sebesar-besarnya kepada berbagai pihak yang telah memberikan dukungan, baik secara langsung maupun tidak langsung, sehingga penelitian ini dapat terlaksana dengan baik. Ucapan terima kasih khusus ditujukan kepada Kepala Bidang SPBE dan Persandian Dinas Komunikasi Informasi Statistik Persandian Kota Pekanbaru, atas dukungan teknis dan akses infrastruktur jaringan yang diberikan selama proses implementasi sistem. Penulis juga berterima kasih Dekan Fakultas Desain dan Teknologi Universitas Awal Bros Pekanbaru, atas arahan dan dorongan akademik yang sangat berarti selama proses penulisan karya ilmiah ini. Tak lupa, penghargaan yang tulus diberikan kepada Pimpinan dan seluruh Civitas Akademika Universitas Awal Bros Pekanbaru atas suasana akademik yang kondusif, yang telah memberikan ruang kolaborasi, diskusi, dan evaluasi ilmiah terhadap topik yang diangkat dalam penelitian ini.

DAFTAR PUSTAKA

Azi, M. N. A., Arifwidodo, B., & Wahyudi, E. (2023). Analisis Performansi Web Server Saat Menangani Permintaan Client Menggunakan Metode Reserve Proxy Caching dan Varnish. *Journal of Telecommunication, Electronics, and Control Engineering (JTECE)*, *5*(1), 14–21. https://doi.org/10.20895/jtece.v5i1.843

Darmawan, R. T. (2023). Implementasi Grafana untuk Auto-Scaling pada NGINX Web-Server di Lingkungan Docker Container. *Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *7*(7), 3165.

Darujati, C., & Al Azam, M. N. (2023). Membangun Content Delivery Network (CDN)

menggunakan Reverse Proxy dan Caching berbasis Linux. *KERNEL: Jurnal Riset Inovasi Bidang Informatika Dan Pendidikan Informatika*, *4*(2), 146–151. https://doi.org/10.31284/j.kernel.2023.v4i2.7564

Dixit, A., & Sharma, S. (2023). Web server access log pattern analysis using GWO-based clustering. In *J. Integr. Sci. Technol* (Vol. 2023, Number 2).

Nurnawati, O. E., Johanes Mau, F., Guntoro, D., Program,), Rekayasa, S. T., & Pemerintahan,

Pardosi, V. B. A. (2024). Cost-Effective DDoS Mitigation: Leveraging Nginx Reverse Proxy for Enhanced Server Protection. *Jurnal Teknologi Informasi Dan Pendidikan*, *17*(2), 371–382. https://doi.org/10.24036/jtip.v17i2.845

Pebrianto, J. (2024). Perlindungan Port dari Pemindaian NMAP dan Meningkatkan Efisiensi IPv4 dengan MikroTik dan Nginx. *Media Jurnal Informatika*, *16*(1), 54. https://doi.org/10.35194/mji.v16i1.4012

Pradana Aji, R., Prayudi, Y., & Luthfi, A. (2023). Analysis of Brute Force Attack Logs Toward Nginx Web Server on Dashboard Improved Log Logging System Using Forensic Investigation Method. *Jurnal Teknik Informatika (Jutif)*, *4*(1), 39–48. https://doi.org/10.52436/1.jutif.2023.4.1.644

Putra Perdana, G., & Prihanto, A. (2025). Analisis Perbandingan Performa Web Server Apache, Nginx, Dan Litespeed Studi Kasus Implementasi Di VPS. *Journal of Informatics and Computer Science*, *06*.

Sandy Bukhari, A., & Iqbal, M. (2024). Public IP Efficiency and Data Center Security Enhancement with Reverse Proxy Implementation. *Journal of Systems Engineering and Information Technology (JOSEIT)*, *3*(2), 37–42. https://doi.org/10.29207/joseit.v3i2.5948

Satrya Bhayangkara, D., & Miftahul Ashari, W. (2024). Pengaruh Load Balancing Pada Serangan DDoS Menggunakan Nginx. *The Indonesian Journal of Computer Science*, *13*(4), 6275–6287. https://doi.org/10.33022/ijcs.v13i4.4118

Savitri, E., & MT, I. S. (2024). Pengaruh Transformasi Digital dan Sistem Informasi Terintegrasi Terhadap Laporan Kinerja di Kementerian Pertahanan. *Arus Jurnal Sosial Dan Humaniora*, *4*(3), 1804–1811. https://doi.org/10.57250/ajsh.v4i3.759

Silva, J. M., Ribeiro, D., Ramos, L. F., & Fonte, V. (2024). A worldwide overview on the information security posture of online public services. *Proceedings of the Annual Hawaii International Conference on System Sciences*, (January), 1881–1890. https://doi.org/10.24251/hicss.2024.237