

Perancangan Infrastruktur Smart Campus Berbasis Open Source melalui Integrasi Manajemen Jaringan, Keamanan Jaringan, dan Monitoring pada Ubuntu Server

Ugan Suganda¹, Nurul Qamariyah², Rachman Hadi³

^{1,2,3} Politeknik Istikom Bina Citra Informatika

e-mail : sugandaugan7@gmail.com¹, ririnskom@gmail.com²,
hadi.rachman@istikombci.ac.id³

Abstrak

Perkembangan transformasi digital di lingkungan pendidikan mendorong institusi untuk membangun infrastruktur Smart Campus yang mampu menyediakan layanan jaringan secara terintegrasi, aman, dan mudah dikelola. Namun, implementasi infrastruktur pada banyak institusi umumnya masih dilakukan secara parsial sehingga manajemen jaringan, keamanan jaringan, dan sistem monitoring belum terintegrasi dalam satu platform. Penelitian ini bertujuan merancang dan mengimplementasikan infrastruktur Smart Campus berbasis *Open Source* melalui integrasi manajemen jaringan, keamanan jaringan, dan monitoring pada Ubuntu Server. Penelitian menggunakan metode Design Science Research (DSR) yang meliputi identifikasi kebutuhan, perancangan infrastruktur, implementasi layanan, pengujian, dan evaluasi sistem. Infrastruktur yang dibangun mengintegrasikan DNS Server, DHCP Server, Apache Web Server, Nginx sebagai Reverse Proxy dan Load Balancer, WireGuard VPN, HTTPS, Firewall UFW, serta sistem monitoring menggunakan Prometheus dan Grafana. Hasil implementasi menunjukkan bahwa seluruh layanan dapat berjalan secara terintegrasi dan berfungsi sesuai kebutuhan. Sistem monitoring mampu menampilkan kondisi server secara *real-time*, sementara mekanisme keamanan jaringan berhasil meningkatkan perlindungan terhadap layanan yang diimplementasikan. Penelitian ini menghasilkan model infrastruktur Smart Campus berbasis *Open Source* yang dapat dijadikan referensi bagi institusi pendidikan dalam membangun layanan jaringan yang terintegrasi, aman, dan mudah dikelola.

Kata kunci: *Smart Campus, Open Source, Manajemen Jaringan, Keamanan Jaringan, Monitoring, Ubuntu Server.*

Abstract

The rapid growth of digital transformation in higher education has encouraged institutions to develop Smart Campus infrastructures capable of providing integrated, secure, and manageable network services. However, infrastructure implementation in many institutions is still carried out partially, resulting in disconnected network management, security, and monitoring systems. This study aims to design and implement an Open Source-based Smart Campus infrastructure through the integration of network management, network security, and monitoring on Ubuntu Server. The study employed the Design Science Research (DSR) method, consisting of requirement identification, infrastructure design, service implementation, testing, and system evaluation. The proposed infrastructure integrates DNS Server, DHCP Server, Apache Web Server, Nginx as a Reverse Proxy and Load Balancer, WireGuard VPN, HTTPS, UFW Firewall, and monitoring services using Prometheus and Grafana. The implementation results demonstrate that all services operate successfully in an integrated environment and perform according to the defined requirements. The monitoring system provides real-time server performance visualization, while the implemented security mechanisms improve service protection. This research contributes an Open Source-based Smart Campus infrastructure model that can serve as a practical reference for educational institutions in developing integrated, secure, and manageable network infrastructures.

Keywords : *Smart Campus, Open Source, Network Management, Network Security, Monitoring, Ubuntu Server.*

PENDAHULUAN

Transformasi digital telah menjadi salah satu faktor utama dalam meningkatkan kualitas layanan di lingkungan pendidikan tinggi. Konsep Smart Campus berkembang sebagai pendekatan yang mengintegrasikan teknologi informasi dan komunikasi untuk mendukung proses akademik, administrasi, serta pengelolaan infrastruktur secara efektif dan efisien. Implementasi Smart Campus tidak hanya memanfaatkan teknologi Internet of Things (IoT), tetapi juga memerlukan infrastruktur jaringan yang mampu menyediakan layanan secara andal, aman, mudah dikembangkan, dan mudah dikelola. Infrastruktur tersebut menjadi fondasi bagi berbagai layanan digital yang saling terhubung sehingga mampu meningkatkan kualitas pelayanan kepada sivitas akademika (Domínguez-Bolaño *et al.*, 2024; Barroso *et al.*, 2023; Fortes *et al.*, 2021).

Keberhasilan implementasi Smart Campus sangat dipengaruhi oleh kemampuan infrastruktur jaringan dalam menyediakan berbagai layanan yang terintegrasi. Layanan seperti Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Web Server, Mail Server, serta layanan aplikasi harus mampu bekerja secara terpadu agar menjamin ketersediaan sistem dan kemudahan administrasi jaringan. Selain itu, penerapan Reverse Proxy dan Load Balancer diperlukan untuk meningkatkan ketersediaan layanan, mendistribusikan beban akses pengguna, serta mendukung skalabilitas ketika jumlah pengguna terus meningkat (Savu-Jivanov *et al.*, 2026; Ahmed & Al-Hamadani, 2021).

Selain aspek manajemen jaringan, keamanan infrastruktur menjadi perhatian penting dalam implementasi Smart Campus. Ancaman berupa akses tidak sah, eksploitasi kerentanan layanan, serangan siber, maupun kebocoran data menuntut adanya mekanisme perlindungan yang memadai. Beberapa pendekatan yang umum diterapkan meliputi penggunaan Firewall, Virtual Private Network (VPN), Hypertext Transfer Protocol Secure (HTTPS), serta konsep Zero Trust Architecture untuk meningkatkan keamanan komunikasi dan pengendalian akses terhadap layanan jaringan (Zheng *et al.*, 2021; Purwanto & Kurniawan, 2026).

Di sisi lain, pengelolaan infrastruktur jaringan memerlukan sistem monitoring yang mampu memberikan informasi kondisi server dan jaringan secara real-time. Monitoring terhadap penggunaan prosesor, memori, media penyimpanan, lalu lintas jaringan, serta status layanan menjadi bagian penting dalam menjaga ketersediaan sistem. Prometheus dan Grafana merupakan perangkat lunak *open source* yang banyak digunakan untuk mengumpulkan metrik, melakukan visualisasi data, dan membantu administrator dalam mendeteksi gangguan sejak dini sehingga proses pemeliharaan dapat dilakukan secara lebih efektif (Lubis *et al.*, 2024; Hakim & Setiawan, 2024; Kaur *et al.*, 2021).

Berbagai penelitian telah mengkaji implementasi Smart Campus, keamanan jaringan, maupun monitoring infrastruktur. Domínguez-Bolaño *et al.* (2024) mengembangkan platform Smart Campus berbasis IoT dengan memanfaatkan Home Assistant, InfluxDB, dan Grafana. Zheng *et al.* (2021) mengevaluasi tingkat keamanan jaringan pada beberapa universitas melalui identifikasi aset dan analisis kerentanan. Savu-Jivanov *et al.* (2026) mengembangkan laboratorium virtual yang mengintegrasikan teknologi networking, cybersecurity, reverse proxy, dan load balancer. Sementara itu, beberapa penelitian lain berfokus pada implementasi monitoring menggunakan Prometheus dan Grafana untuk meningkatkan visibilitas performa jaringan dan server (Lubis *et al.*, 2024; Hakim & Setiawan, 2024; Kaur *et al.*, 2021). Meskipun demikian, sebagian besar penelitian tersebut masih membahas setiap komponen secara terpisah sehingga belum menghasilkan model infrastruktur Smart Campus yang mengintegrasikan manajemen jaringan, keamanan jaringan, dan monitoring dalam satu lingkungan yang utuh.

Berdasarkan kondisi tersebut, penelitian ini mengusulkan perancangan infrastruktur Smart Campus berbasis Open Source melalui integrasi manajemen jaringan, keamanan jaringan, dan monitoring pada Ubuntu Server. Infrastruktur yang dikembangkan mengintegrasikan layanan DNS Server, DHCP Server, Apache Web Server, Nginx sebagai

Reverse Proxy dan Load Balancer, WireGuard VPN, HTTPS, Firewall UFW, serta sistem monitoring menggunakan Prometheus dan Grafana. Integrasi seluruh layanan tersebut diharapkan mampu menghasilkan model infrastruktur yang lebih komprehensif, aman, mudah dikelola, dan dapat dijadikan referensi implementasi Smart Campus pada institusi pendidikan.

METODE PENELITIAN

Penelitian ini menggunakan metode Design Science Research (DSR) yang berfokus pada perancangan, implementasi, dan evaluasi infrastruktur Smart Campus berbasis *Open Source*. Metode ini dipilih karena mampu menghasilkan solusi berupa integrasi layanan manajemen jaringan, keamanan jaringan, dan monitoring yang dapat diterapkan secara nyata pada lingkungan institusi pendidikan.

Tahapan penelitian diawali dengan identifikasi kebutuhan berdasarkan studi literatur dan analisis layanan yang dibutuhkan pada lingkungan Smart Campus. Selanjutnya dilakukan perancangan topologi jaringan dan arsitektur sistem yang mengintegrasikan DNS Server, DHCP Server, Apache Web Server, Nginx sebagai Reverse Proxy dan Load Balancer, WireGuard VPN, HTTPS, Firewall UFW, serta sistem monitoring menggunakan Prometheus dan Grafana. Seluruh layanan diimplementasikan pada sistem operasi Ubuntu Server sebagai platform utama.

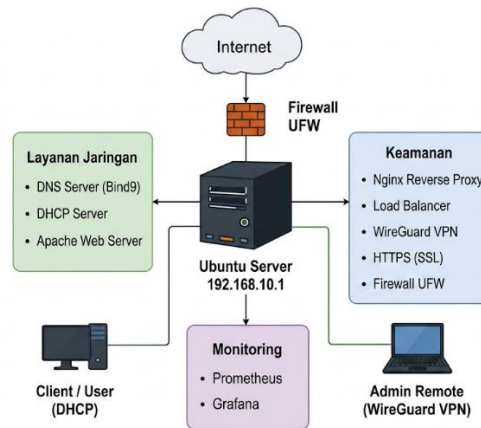
Setelah proses implementasi selesai, dilakukan pengujian fungsional terhadap setiap layanan untuk memastikan seluruh komponen berjalan sesuai dengan kebutuhan sistem. Evaluasi dilakukan melalui pengamatan terhadap keberhasilan konfigurasi layanan, akses jaringan, mekanisme keamanan, serta hasil monitoring menggunakan Prometheus dan Grafana. Alur tahapan penelitian ditunjukkan pada Gambar 1.



Gambar 1. Tahapan Penelitian

HASIL DAN PEMBAHASAN

Pada penelitian ini berhasil dibangun infrastruktur Smart Campus berbasis Open Source pada sistem operasi Ubuntu Server melalui integrasi layanan manajemen jaringan, keamanan jaringan, dan monitoring server. Implementasi dilakukan secara bertahap sesuai rancangan yang telah disusun pada tahap metode penelitian. Infrastruktur yang dibangun mengintegrasikan layanan DNS Server, DHCP Server, Apache Web Server, Nginx sebagai Reverse Proxy dan Load Balancer, WireGuard VPN, HTTPS, Firewall UFW, serta sistem monitoring menggunakan Prometheus dan Grafana. Seluruh layanan dikonfigurasi agar mampu bekerja secara terintegrasi sehingga mendukung kebutuhan operasional Smart Campus.



Gambar 2. Topologi Infrastruktur Smart Campus

Gambar 2 menunjukkan arsitektur infrastruktur Smart Campus yang dikembangkan pada penelitian ini. Ubuntu Server berfungsi sebagai pusat layanan yang mengintegrasikan layanan DNS, DHCP, Apache Web Server, Reverse Proxy, Load Balancer, WireGuard VPN, HTTPS, Firewall UFW, serta sistem monitoring menggunakan Prometheus dan Grafana. Infrastruktur tersebut memungkinkan pengguna mengakses layanan melalui jaringan lokal maupun melalui koneksi VPN sehingga meningkatkan fleksibilitas dan keamanan akses terhadap layanan Smart Campus.

Implementasi Layanan Jaringan

```
root@ubuntu:~
GNU nano 6.2 /etc/bind/named.conf.local

// Zona Forward
zone "smartcampus.local" {
    type master;
    file "/etc/bind/db.smartcampus.local";
};

// Zona Reverse
zone "10.192.168.in-addr.arpp" {
    type master;
    file "/etc/bind/db.192.168.10";
};

^G Help ^Q Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^J Paste ^_ Justify
```

Gambar 3. Konfigurasi DNS Server

Layanan DNS Server diimplementasikan menggunakan Bind9 untuk melakukan resolusi nama domain pada lingkungan Smart Campus. Konfigurasi meliputi pembuatan *forward zone* dan *reverse zone* sehingga setiap perangkat dapat diakses menggunakan nama domain yang telah ditentukan. Implementasi DNS mempermudah pengelolaan layanan dibandingkan penggunaan alamat IP secara langsung.

```
root@client:~#  
root@client:~# nslookup www.smartcampus.local  
Server:      192.168.10.1  
Address:     192.168.10.1#53  
  
Name:   www.smartcampus.local  
Address: 192.168.10.1  
  
root@client:~# nslookup mail.smartcampus.local  
Server:      192.168.10.1  
Address:     192.168.10.1#53  
  
Name:   mail.smartcampus.local  
Address: 192.168.10.1  
  
root@client:~#
```

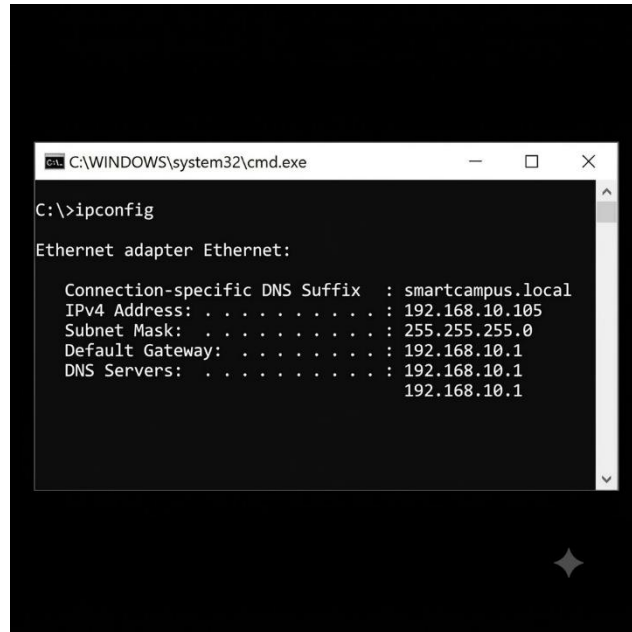
Gambar 4: Pengujian DNS (nslookup)

Pengujian dilakukan menggunakan perintah nslookup untuk memastikan layanan DNS berjalan sesuai konfigurasi. Hasil pengujian menunjukkan bahwa domain berhasil diterjemahkan menjadi alamat IP server dengan benar sehingga proses resolusi nama dapat dilakukan tanpa kendala.

```
root@lubuntu: ~  
GNU nano 6.2 /etc/dhcp/dhcpd.conf  
  
subnet 192.168.10.0 network 192.168.255.0 {  
    range 192.168.10.100 192.168.10.200;  
    option routers 192.168.10.1;  
    option domain-name-servers 192.168.10.1;  
    option domain-name "smartcampus.local";  
    optialet-lease-time 100;  
    max-lease-time 7200;  
}  
  
# Interface  
INJTERFACESv4 "ens33"  
  
^G Help  ^W Write Out  ^W Where Is  ^K Cut  ^T Execute  
^X Exit  ^R Read File  ^\ Replace  ^J Paste  ^J Justify
```

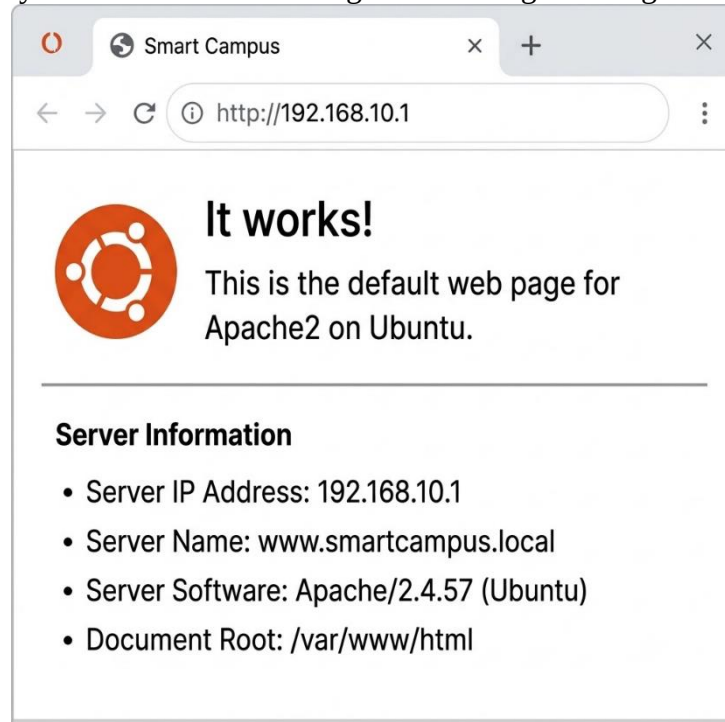
Gambar 5: Konfigurasi DHCP (dhcpd.conf)

DHCP Server dikonfigurasi menggunakan ISC DHCP Server untuk mendistribusikan alamat IP secara otomatis kepada perangkat klien. Konfigurasi meliputi rentang alamat IP, gateway, DNS server, dan masa aktif alamat IP (*lease time*). Implementasi DHCP mengurangi proses konfigurasi manual sehingga pengelolaan jaringan menjadi lebih efisien.



Gambar 6: Pengujian DHCP (Klien Mendapat IP)

Hasil pengujian menunjukkan bahwa perangkat klien berhasil memperoleh alamat IP, subnet mask, gateway, dan DNS server secara otomatis dari DHCP Server. Hal ini menunjukkan bahwa layanan DHCP telah berfungsi sesuai dengan konfigurasi yang dirancang.



Gambar 7: Apache Web Server

Apache berhasil diimplementasikan sebagai web server utama untuk menyediakan layanan web pada lingkungan Smart Campus. Hasil pengujian menunjukkan bahwa halaman web dapat diakses melalui browser tanpa mengalami kendala, sehingga layanan web telah berfungsi dengan baik.



```
root@ubuntu: ~
GNU nano 6.2 /etc/nginx/sites-available/reverse-proxy

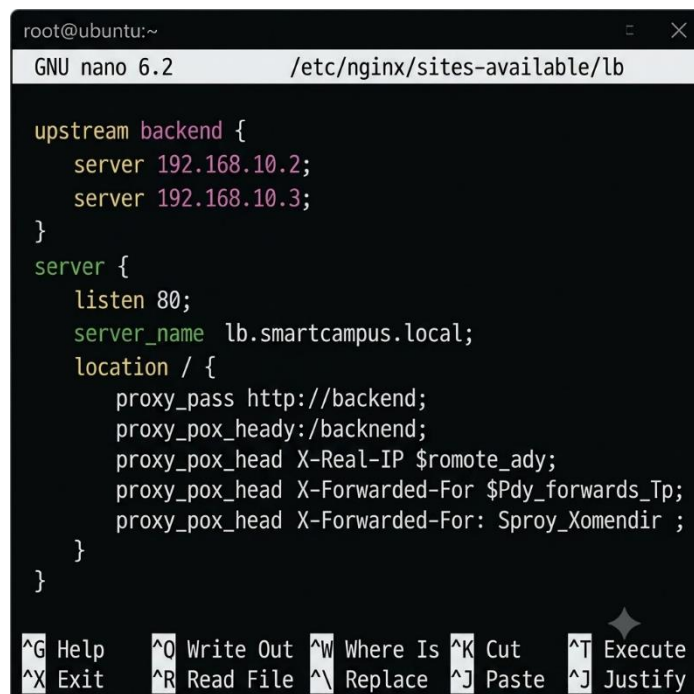
server {
    listen 80;
    server_name www.smartcampus.local;

    location / {
        proxy_pass http://127.0.0.1:8080;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_al,_forwarded:by;
        proxy_set_header X-Forwarded-Proxy-$osname;
    }
}
```

Help Write Out Where Is Cut Execute
Exit Read File Replace Paste Justify

Gambar 8: Nginx Reverse Proxy

Nginx dikonfigurasi sebagai Reverse Proxy untuk meneruskan permintaan dari pengguna menuju layanan Apache Web Server. Penerapan Reverse Proxy meningkatkan fleksibilitas pengelolaan layanan web serta mempermudah penerapan HTTPS dan Load Balancer pada tahap berikutnya.



```
root@ubuntu:~
GNU nano 6.2 /etc/nginx/sites-available/lb

upstream backend {
    server 192.168.10.2;
    server 192.168.10.3;
}

server {
    listen 80;
    server_name lb.smartcampus.local;
    location / {
        proxy_pass http://backend;
        proxy_pox_heady:/backend;
        proxy_pox_head X-Real-IP $romote_ady;
        proxy_pox_head X-Forwarded-For $Pdy_forwards_Tp;
        proxy_pox_head X-Forwarded-For: Sproy_Xomendir ;
    }
}
```

Help Write Out Where Is Cut Execute
Exit Read File Replace Paste Justify

Gambar 9: Load Balancer (Nginx)

Konfigurasi Load Balancer dilakukan menggunakan fitur upstream pada Nginx. Mekanisme ini memungkinkan distribusi permintaan pengguna menuju beberapa backend

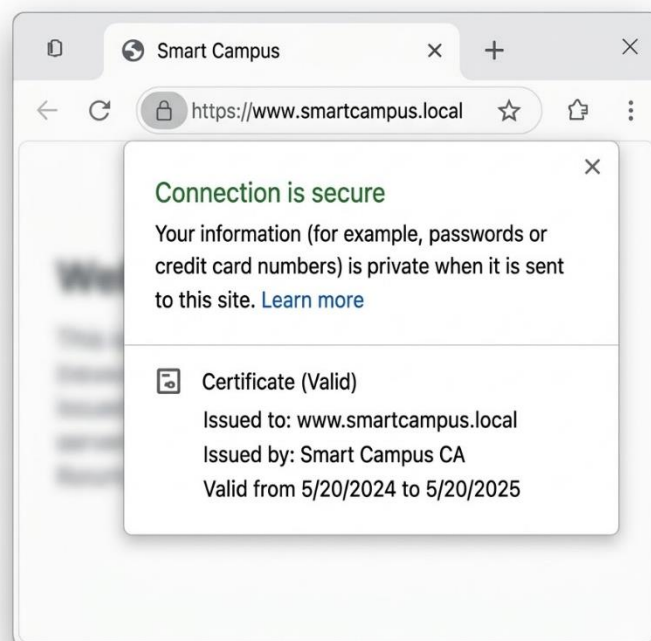
server sehingga meningkatkan ketersediaan layanan dan mendukung skalabilitas sistem ketika jumlah pengguna meningkat.

Implementasi Keamanan Jaringan

```
root@ubuntu: ~  
root@ubuntu:~# wg  
  
interface: wg0  
  public key: 2hBc.....y2p=  
  private key: (hidden)  
  listening port: 51820  
  
peer: 5Hdk.....d9A=  
  
peer: 5Hdk.....d9A=  
  endpoint: 203.0.113.1:51820  
  allowed ips: 10.8.0.2/32  
  latest handshake: 1 minute, 8 seconds ago  
  transfer: 12.45 KiB received, 3.21 KiB sent  
}
```

Gambar 10. Konfigurasi WireGuard VPN

WireGuard VPN diimplementasikan sebagai mekanisme akses aman bagi administrator dari luar jaringan lokal. Hasil pengujian menunjukkan bahwa koneksi VPN berhasil dibangun dan perangkat administrator dapat mengakses layanan server melalui jalur komunikasi yang terenkripsi.



Gambar 11. Konfigurasi HTTPS

Keamanan komunikasi web ditingkatkan melalui penerapan sertifikat SSL/TLS sehingga layanan web dapat diakses menggunakan protokol HTTPS. Hasil implementasi menunjukkan bahwa browser mengenali sertifikat sebagai koneksi yang aman sehingga komunikasi antara pengguna dan server berlangsung secara terenkripsi.

```

root@ubuntu:~$ sudo ufw status verbose
Status: active

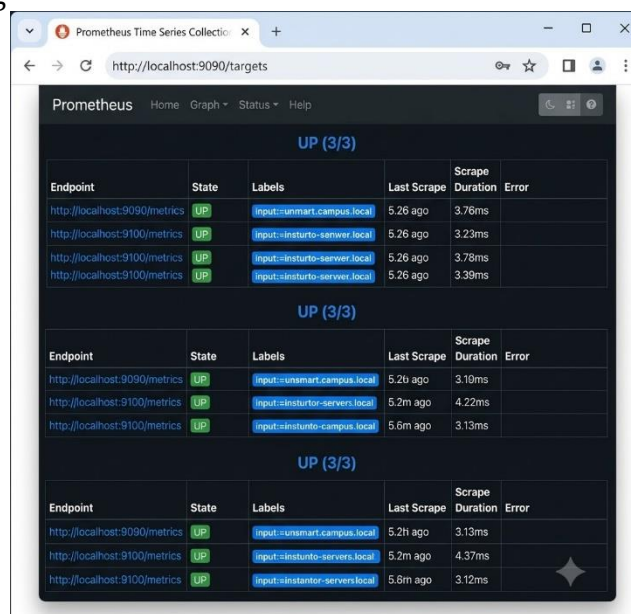
To Action From
--
22/tcp ALLOW IN Anywhere
80/tcp ALLOW IN Anywhere
443/tcp ALLOW IN Anywhere
51820/udp ALLOW IN Anywhere
51820/udp (v6) ALLOW IN Anywhere
22/tcp (v6) ALLOW IN Anywhere (v6)
80/tcp (v6) ALLOW IN Anywhere (v6)
443/tcp (v6) ALLOW IN Anywhere (v6)
51820/udp (v6) ALLOW IN Anywhere (v6)

```

Gambar 12. Firewall UFW

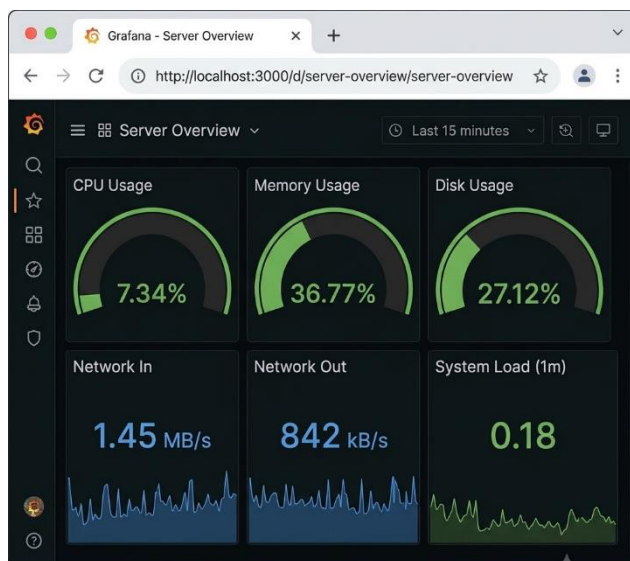
Firewall UFW (Uncomplicated Firewall) digunakan untuk mengendalikan akses terhadap layanan jaringan berdasarkan aturan yang telah ditentukan. Hasil konfigurasi menunjukkan bahwa hanya port yang diperlukan yang diizinkan untuk diakses sehingga meningkatkan keamanan server.

Implementasi Monitoring



Gambar 13. Dashboard Prometheus

Prometheus berhasil diimplementasikan sebagai sistem pengumpul metrik server. Seluruh target monitoring berada pada status UP, yang menunjukkan bahwa proses pengumpulan data berjalan dengan baik dan siap digunakan sebagai sumber informasi monitoring.



Gambar 14. Dashboard Grafana

Grafana digunakan sebagai media visualisasi data yang dikumpulkan oleh Prometheus. Dashboard menampilkan informasi penggunaan CPU, memori, penyimpanan, lalu lintas jaringan, dan beban sistem secara real-time, sehingga administrator dapat memantau kondisi server dengan lebih mudah.

Parameter	Nilai	Keterangan
CPU Usage	7.34 %	Normal
Memory Usage	36.77 %	Normal
Disk Usage	27.12 %	Normal
Network In	1.45 MB/s	Normal
Network Out	842 kB/s	Normal
Load Average (1m)	0.18	Normal
Uptime	2 day, 4 hour	Normal

Gambar 15: Hasil Monitoring CPU RAM Disk

Hasil monitoring menunjukkan bahwa penggunaan sumber daya server masih berada pada kondisi normal. Penggunaan CPU, memori, dan penyimpanan berada pada tingkat yang stabil sehingga seluruh layanan dapat berjalan secara bersamaan tanpa menyebabkan penurunan performa server yang signifikan.

Hasil implementasi menunjukkan bahwa integrasi manajemen jaringan, keamanan jaringan, dan monitoring berbasis Open Source pada Ubuntu Server dapat diterapkan dengan baik untuk mendukung lingkungan Smart Campus. Seluruh layanan utama berhasil diimplementasikan dan saling terintegrasi sesuai dengan rancangan sistem. Implementasi DNS dan DHCP mempermudah pengelolaan jaringan, sedangkan Apache Web Server yang dipadukan dengan Nginx sebagai Reverse Proxy dan Load Balancer meningkatkan fleksibilitas serta ketersediaan layanan. Dari sisi keamanan, WireGuard VPN, HTTPS, dan Firewall UFW memberikan perlindungan terhadap akses dan komunikasi data. Selain itu, Prometheus dan Grafana menyediakan mekanisme monitoring secara real-time yang membantu administrator dalam memantau kondisi server serta mendeteksi potensi gangguan lebih dini. Hasil penelitian ini menunjukkan bahwa pendekatan integrasi berbagai layanan berbasis *Open Source* dapat menjadi alternatif implementasi infrastruktur Smart Campus yang efisien, aman, dan mudah dikelola.

SIMPULAN DAN SARAN

Penelitian ini berhasil merancang dan mengimplementasikan infrastruktur Smart Campus berbasis Open Source melalui integrasi manajemen jaringan, keamanan jaringan, dan monitoring pada Ubuntu Server. Infrastruktur yang dibangun meliputi DNS Server, DHCP Server, Apache Web Server, Nginx sebagai Reverse Proxy dan Load Balancer, WireGuard VPN, HTTPS, Firewall UFW, serta sistem monitoring menggunakan Prometheus dan Grafana. Hasil implementasi menunjukkan bahwa seluruh layanan dapat berjalan secara terintegrasi dan berfungsi sesuai dengan kebutuhan sistem. Penerapan monitoring memungkinkan administrator memantau kondisi server secara *real-time*, sedangkan implementasi keamanan jaringan mampu meningkatkan perlindungan terhadap layanan yang tersedia.

Penelitian selanjutnya dapat mengembangkan infrastruktur ini dengan menambahkan teknologi containerization seperti Docker atau Kubernetes, mekanisme High Availability (HA), integrasi Identity and Access Management (IAM), serta implementasi Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS) untuk meningkatkan keandalan dan keamanan lingkungan Smart Campus.

DAFTAR PUSTAKA

- Ahmed, A.H. & Al-Hamadani, M.N.A. 2021. Designing a Secure Campus Network and Simulating It Using Cisco Packet Tracer. *Indonesian Journal of Electrical Engineering and Computer Science*. Vol. 23(1): 479–489. <https://doi.org/10.11591/ijeecs.v23.i1.pp479-489>
- Barroso, S., Bustos, P. & Núñez, P. 2023. Towards a Cyber-Physical System for Sustainable and Smart Building: A Use Case for Optimising Water Consumption on a SmartCampus. *Journal of Ambient Intelligence and Humanized Computing*. <https://doi.org/10.1007/s12652-021-03656-1>
- Domínguez-Bolaño, T., Barral, V., Escudero, C.J. & García-Naya, J.A. 2024. An IoT System for a Smart Campus: Challenges and Solutions Illustrated Over Several Real-World Use Cases. *Internet of Things*. Vol. 27: 101099. <https://doi.org/10.1016/j.iot.2024.101099>
- Fortes, S., Hidalgo-Triana, N., Sánchez-la-Chica, J.M., García-Ceballos, M.L., Cantizani-Esteva, J., Pérez-Latorre, A.V., Baena, E., Pineda, A., Barrios-Corpa, J. & García-Marín, A. 2021. Smart Tree: An Architectural, Greening and ICT Multidisciplinary Approach to Smart Campus Environments. *Sensors*. Vol. 21(21): 7202. <https://doi.org/10.3390/s21217202>
- Hakim, A.R. & Setiawan, M.A. 2024. Resilience and Robustness Analysis of Enterprise Network with Edge Sensors. *Indonesian Journal of Computer Science*. Vol. 13(5). <https://doi.org/10.33022/ijcs.v13i5.4415>

- Kaur, D., Mohammed, B. & Kiran, M. 2021. NetGraf: A Collaborative Network Monitoring Stack for Network Experimental Testbeds. *arXiv*. <https://doi.org/10.48550/arXiv.2105.10326>
- Lubis, A., Giffari, M.A. & Wahyuni, S. 2024. Enhancing Network Performance Visibility with Grafana and Prometheus: A Case Study at P.T. Nata Digital Solution. *Proceeding of International Conference on Artificial Intelligence, Navigation, Engineering, and Aviation Technology (ICANEAT)*.
- Purwanto, J. & Kurniawan, S.D. 2026. Implementation of Zero Trust Architecture on Local Server Management in Educational Institutions. *Journal of Strategic and Global Studies*. Vol. 9(1). <https://doi.org/10.7454/jsjgs.v9i1.1195>
- Savu-Jivanov, A., Stolojescu-Crisan, C., Gal, J. & Ancuti, C. 2026. Integrated Virtual Laboratory for Networking, Cybersecurity, and Automation Education with Enhanced Scalability. *Frontiers in Education*. Vol. 11. <https://doi.org/10.3389/feduc.2026.1708228>
- Zheng, R., Ma, H., Wang, Q., Fu, J. & Jiang, Z. 2021. Assessing the Security of Campus Networks: The Case of Seven Universities. *Sensors*. Vol. 21(1): 306. <https://doi.org/10.3390/s21010306>