p-ISSN: 2301-6949
e-ISSN : 2715-5064

Integrasi Firewall Untuk Meningkatkan Keamanan Akses Ssh Pada Ubuntu Server 20.04

Zaenal Mutaqin Subekti[1*)], Kikim Mukiman[2], Ramdani[3], H.S. Sulistyowati[4], Muhamad Dedi Suryadi[5], Iwan Jaya[6]
[145]Program Studi Teknik Informatika, Fakultas Teknologi Informasi dan Digital, Universitas Bani Saleh, Bekasi
[23]Program Studi Teknik Komputer, Fakultas Teknologi Informasi dan Digital, Universitas Bani Saleh, Bekasi
[6]Program Studi Komputerisasi Akuntansi, Fakultas Teknologi Informasi dan Digital, Universitas Bani Saleh, Bekasi
[123456]Jln. M Hasibuan No 68, Kota Bekasi, 50272, Indonesia
email: [1]zaenalms@ubs.ac.id, [2]kikim@ubs.ac.id, [3]ramdani@ubs.ac.id, [4]sulis@ubs.ac.id, [5]kangdedi@gmail.com, [6]iwan@ubs.ac.id

Abstract **−− Network access security on servers is a crucial issue in the digital era. One of the vulnerable points is the Secure Shell (SSH) service, which if not properly configured, can be a vulnerability. This study aims to design an SSH access security system on Ubuntu Server 20.04 through firewall integration using Uncomplicated Firewall (UFW). The methodology used is experimental with a needs analysis approach, system design, configuration implementation, and testing to conduct security analysis. The test results show that selective use of firewalls for IP and ports can significantly reduce the potential for illegal access. This study concludes that firewall integration provides significant reinforcement to SSH service security and is worthy of being adopted as a standard practice in server management.**

Abstrak Keamanan akses jaringan pada server merupakan isu krusial di era digital. Salah satu titik rawan adalah layanan Secure Shell (SSH), yang jika tidak dikonfigurasi dengan tepat, dapat menjadi celah serangan. Penelitian ini bertujuan untuk merancang sistem keamanan akses SSH pada Ubuntu Server 20.04 melalui integrasi firewall menggunakan Uncomplicated Firewall (UFW). Metodologi yang digunakan adalah eksperimental dengan pendekatan analisi kebutuhan, design sistem, implementasi konfigurasi, dan pengujian untuk melakukan analisis keamanan. Hasil pengujian menunjukkan bahwa penggunaan firewall secara selektif untuk IP dan port dapat secara signifikan mengurangi potensi akses ilegal. Studi ini menyimpulkan bahwa integrasi firewall memberikan penguatan signifikan terhadap keamanan layanan SSH dan layak diadopsi sebagai praktik standar dalam pengelolaan server.

Kata Kunci **– firewall, ssh, security, ubuntu.**

I.PENDAHULUAN

Keamanan sistem informasi menjadi aspek yang sangat krusial dalam era digital, khususnya dalam pengelolaan server berbasis Linux seperti Ubuntu Server 20.04. Salah satu titik paling rawan dalam sistem jaringan adalah akses Secure Shell (SSH), yang merupakan protokol utama untuk mengelola server secara jarak jauh. Meskipun SSH menawarkan komunikasi terenkripsi[1], port SSH yang terbuka secara default sering menjadi target empuk bagi serangan brute force dan scanning otomatis yang dilakukan oleh pihak tidak bertanggung jawab. Oleh karena itu, diperlukan langkah pengamanan tambahan untuk memitigasi potensi celah yang ada, salah satunya melalui integrasi firewall.

Firewall berfungsi sebagai gerbang kontrol terhadap lalu lintas jaringan yang masuk maupun keluar, dan mampu menyaring koneksi berdasarkan aturan yang telah ditentukan. Pada Ubuntu Server 20.04, Uncomplicated Firewall (UFW) menjadi solusi firewall[2][3] yang sederhana namun efektif untuk mengelola aturan jaringan. Dengan mengatur akses SSH hanya untuk alamat IP tertentu, mengubah port default SSH, serta memblokir permintaan mencurigakan, administrator dapat meningkatkan tingkat proteksi server[4] secara signifikan.

Penelitian ini bertujuan untuk mengkaji bagaimana integrasi firewall dapat diterapkan secara optimal untuk mengamankan akses SSH pada Ubuntu Server 20.04. Langkah ini tidak hanya bertujuan untuk mencegah akses ilegal, tetapi juga mendukung praktik keamanan berlapis yang menjadi standar dalam pengelolaan infrastruktur Teknologi Informasi yang andal..

*) **penulis korespondensi**: Zaenal Mutaqin Subekti
Email: zaenalms@ubs.ac.id

II.PENELITIAN YANG TERKAIT

Implementasi Firewall Pada Protokol SSH Linux Ubuntu Menggunakan Iptables[5] oleh Tamsir Ariyadi, M. Rizky Pohan , M. Khairul Hadi, Ahmad Anwar Widod Jurnal ini membahas penggunaan iptables sebagai firewall untuk meningkatkan keamanan sistem SSH pada Linux Ubuntu[6]. Dijelaskan bagaimana aturan firewall dapat membatasi akses yang tidak diinginkan dan melindungi sistem dari serangan seperti brute force dan man-in-the-middle.

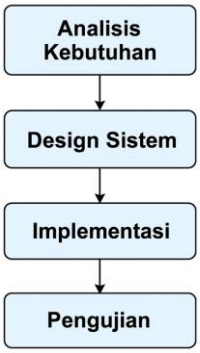
Firewall Sistem Keamanan Jaringan[7] Menggunakan Firewall dengan Metode Port Blocking dan Firewall Filtering[8] oleh Dwiki Wicaksono dan Dwiki Wicaksono jurnal tersebut menjelaskan Firewall merupakan bagian penting dalam suatu keamanan jaringan dimana akses lalu lintas internet banyak digunakan dalam dunia pendidikan maupun pekerjaan. Dalam hal ini firewall sangat diperlukan untuk mengatur akses lalu lintas internet agar melindungi sistem dari ancaman dan serangan. Penelitian ini membahas tentang sistem keamanan jaringan menggunakan firewall dengan metode port blocking dan firewall filtering. Penelitian ini menggunakan router Mikrotik dan aplikasi Winbox untuk meremote router untuk membuat rule firewall yang berisi

blocking port komunikasi dan pembatasan akses internet[9] menggunakan web proxy dengan memblock situs http dan https dalam suatu jaringan. Hasil penelitian ini diuji menggunakan aplikasi Nmap Zenmap untuk melihat sisa port komunikasi yang terbuka dan menggunakan browser untuk mengakses web situs yang dialihkan dan di block. Dengan memaksimalkan dan mengoptimalkan kinerja firewall sebuah jaringan internet akan lebih aman dan meminimalisir ancaman serangan dari luar

Model Keamanan Jaringan Menggunakan Firewall Port Blocking[10] oleh Sartomo, Wiwin Sulistyo jurnal ini menjelaskan Keamanan merupakan unsur yang sangat penting pada jaringan komputer. Hal ini dilakukan dalam upaya memberikan perlindungan pada jaringan komputer untuk mencegah ancamanancaman baik dari internal maupun eksternal dalam upaya mencegah pengambilan data secara paksa (tidak sah). Sistem keamanan jaringan perlu dibangun untuk mengontrol akses pada aset-aset yang penting, salah satunya data, sehingga hak akses setiap komputer maupun user perlu diatur. Metode port blocking menjadi salah satu teknik yang dapat digunakan dalam mengatur akses dari user maupun komputer. Port blocking dapat digunakan untuk mengatur hak akses jaringan pada setiap port LAN (Local Area Network). Secara spesifik pengaturan port yang berbeda dengan metode default atau static port security, port security dynamic learning dan sticky port security dapat dilakukan. Hal ini sangat berguna untuk menghalangi akses dari pihak satu ke pihak lain untuk mencegah terjadinya pencurian data dari orang tidak dikenal maupun yang dikenal. Dari pengujian yang dilakukan diketahui bahwa penerapan firewall security port dapat melakukan aksi block pada koneksi jaringan tersebut ketika terjadi perpindahan hak akses.

III.METODE PENELITIAN

Metode penelitian menggunakan empat tahap yaitu, Analisa kebutuhan, design system, implementasi dan pengujian, seperti terlihat pada gambar dibawah ini.



Gbr. 1 Metode Penelitian.

A. *Analisa Kebutuhan*

Analisis kebutuhan bertujuan untuk mengidentifikasi perangkat keras dan perangkat lunak yang diperlukan dalam pembangunan sistem keamanan akses SSH dengan integrasi firewall. Proses ini penting untuk memastikan bahwa lingkungan pengujian memiliki spesifikasi minimum yang mendukung pelaksanaan seluruh tahapan implementasi dan pengujian.

1. Kebutuhan perangkat keras

Server : Ubuntu Server 20.04 LTS
Spesifikasi minimum:

- CPU Dual-core 2.0 GHz
- RAM 2 GB
- Penyimpanan 20 GB HDD/SSD
- Konektivitas jaringan aktif

Client Komputer:

- Digunakan untuk mengakses server dan melakukan simulasi serangan
- OS bebas (Linux/Windows)
- Koneksi jaringan yang sama dengan server (LAN atau via router/NAT)

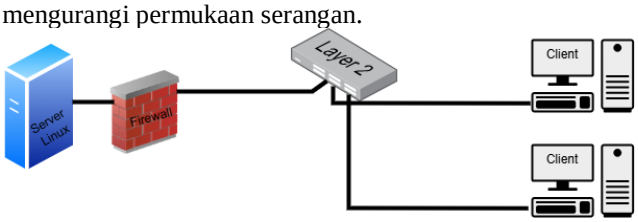
2. Kebutuhan Perangkat Lunak

- OpenSSH Server
- Uncomplicated Firewall (UFW)
- Hydra (Security Tool)
- Log Monitoring Tool

Analisis kebutuhan ini menjadi fondasi dalam tahap perancangan dan implementasi sistem. Kesesuaian spesifikasi dan ketersediaan perangkat akan mempengaruhi efektivitas pengujian serta validitas dari hasil yang diperoleh dalam penelitian ini.

B. *Design Sistem*

Desain sistem dalam penelitian ini bertujuan untuk menggambarkan arsitektur keamanan jaringan pada server Ubuntu dengan mengintegrasikan firewall sebagai mekanisme utama perlindungan layanan SSH. Sistem dirancang dengan pendekatan whitelist IP dan pengubahan port default untuk mengurangi permukaan serangan.



Gbr. 2 Topologi sistem

C. *Implementasi*

Berikut ini adalah bagian Implementasi dari sistem keamanan akses SSH pada Ubuntu Server 22.04 melalui integrasi firewall, disusun secara rinci, sesuai alur: instalasi, konfigurasi SSH, pengamanan firewall.

Update system linux

```
root@zms-ti4ap:/home/zms# apt-get update
```

Gbr. 3 update sistem

Instalasi open ssh server

```
root@zms-ti4ap:/home/zms# apt-get install openssh-server
```

Gbr. 4 install ssh

Verifikasi status ssh

```
zms@zms-ti4ap:~$ sudo su
[sudo] password for zms:
root@zms-ti4ap:/home/zms# service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2025-05-02 01:25:45 UTC; 1min 43s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 744 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 810 (sshd)
      Tasks: 1 (limit: 2254)
     Memory: 5.4M
     CGroup: /system.slice/ssh.service
             └─810 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
```

Gbr. 5 verifikasi status ssh

Konfigurasi SSH untuk Keamanan

```
root@zms-ti4ap:/home/zms# nano /etc/ssh/sshd_config
```

Gbr. 6 Konfigurasi SSH

Ubah port default, contoh menjadi 2345

```
  GNU nano 4.8                                    /etc/ssh/sshd_config
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

Port 2345
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Gbr. 7 ubah port default

Nonaktifkan login root

```
# Authentication:
PermitRootLogin no
```

Gbr. 8 konfigurasi Nonaktifkan login root

Simpan konfigurasi, ctrl x, ketik y dan enter.
Restart SSH untuk penerapan perubahan

```
root@zms-ti4ap:/home/zms# service ssh restart
```

Gbr. 9 restart service ssh

Konfigurasi Firewall Menggunakan UFW
Aktifkan UFW jika belum aktif

```
root@zms-ti4ap:/home/zms# ufw enable
```

Gbr. 10 aktivasi firewall pada linux

Izinkan koneksi SSH dari IP tertentu saja

```
root@zms-ti4ap:/home/zms# ufw allow from 192.168.100.9 to any port 2345 proto tcp
```

Gbr. 11 konfigurasi firewall mengizin ip address tertentu

Tolak semua koneksi SSH dari IP lain

```
root@zms-ti4ap:/home/zms# ufw deny 2345/tcp
Rule updated
Rule updated (v6)
```

Gbr. 12 konfigurasi tolak semua port kecuali port tertentu

Lihat status aturan firewall:

```
root@zms-ti4ap:/home/zms# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 2345/tcp                   ALLOW IN    192.168.100.9
```

Gbr. 13 cek konfigurasi ufw yang sedang berjalan

D. Pengujian

Lakukan penujian dari client dengan ip address client 192.168.100.13/24 lakukan pengujian ssh

```
C:\Users\DELL>ssh zms@192.168.100.13
```

Gbr. 14 koneksi ssh dari client windows

Berikut hasil pengujian dalam bentuk table

Tabel 1 pengujian koneksi ssh dengan port default (22)

No	Client	Server ssh	Parameter	Keterangan
1	192.168.100.9	192.168.100.13	Koneksi ssh dari client ke server	Berhasil
2	192.168.100.8	192.168.100.13	Koneksi ssh dari client ke server	Berhasil
3	192.168.100.7	192.168.100.13	Koneksi ssh dari client ke server	Berhasil

Pengujian ssh, dengan port ssh diganti menjadi 2345

Tabel 2 pengujian koneksi ssh dengan port custom (2345)

No	Client	Server ssh	Port	Parameter	Keterangan
1	192.168.100.9	192.168.100.13	2345	Koneksi ssh dari client ke server	Berhasil
2	192.168.100.8	192.168.100.13	2345	Koneksi ssh dari client ke server	Berhasil
3	192.168.100.7	192.168.100.13	2345	Koneksi ssh dari client ke server	Berhasil

IV.HASIL DAN PEMBAHASAN

Penelitian ini menguji sistem keamanan SSH dalam dua kondisi: sebelum dan sesudah penerapan firewall menggunakan firewall dan konfigurasi keamanan pada layanan ssh. Uji coba dilakukan pada topologi sederhana yang terdiri dari satu server Ubuntu 20.04, tiga client sebagai pengguna sah.

Skenario tanpa firewall dan hardening ssh, Pada kondisi awal, server masih menggunakan konfigurasi default Sssh, Port 22 terbuka untuk semua IP, Login root masih diizinkan.

Skenario setelah implementasi Firewall dan ssh hardening, Setelah implementasi dilakukan, port ssh diubah menjadi 2345, root login dinonaktifkan, firewall dikonfigurasi untuk hanya menerima koneksi dari ip tertentu (192.168.100.9/24), firewall secara eksplisit menolak koneksi dari ip asing, berikut hasil pengujian nya.

Tabel 3 pengujian koneksi ssh dengan port custom (2345) dan penerapan firewall

No	Client	Server ssh	Port	Parameter Firewall	Keterangan
1	192.168.100.9	192.168.100.13	2345	tolak semua koneksi ssh kecuali 192.168.100.9	Berhasil
2	192.168.100.8	192.168.100.13	2345	tolak semua koneksi ssh kecuali 192.168.100.9	Gagal, Koneksi time out
3	192.168.100.7	192.168.100.13	2345	tolak semua koneksi ssh kecuali 192.168.100.9	Gagal, Koneksi time out

V.KESIMPULAN

Kesimpulan Integrasi firewall menggunakan UFW pada Ubuntu Server 20.04 terbukti efektif dalam menurunkan risiko keamanan pada layanan ssh. Penggunaan metode, whitelist IP address, dan pengubahan port secara signifikan mengurangi peluang keberhasilan serangan. Terlihat dari hasil pengujian ip address tertentu yang dapat masuk ke ubuntu server melalui ssh dan selain ip address yang ditentukan maka gagal, dengan informasi koneksi time out, Studi ini merekomendasikan integrasi firewall sebagai praktik baik dalam keamanan jaringan server.

UCAPAN TERIMA KASIH

Kami mengucapkan rasa syukur dan terima kasih yang sebesar-besarnya kepada Universitas Bani Saleh atas dukungan dan bantuan dana penelitian yang telah diberikan. Bantuan ini memungkinkan kami untuk melaksanakan penelitian dengan lebih optimal, mengembangkan wawasan akademik, serta memberikan kontribusi nyata dalam bidang yang kami teliti.
Kami juga berterima kasih kepada seluruh pihak yang telah membantu, baik dalam bentuk saran, dukungan teknis, maupun motivasi selama proses penelitian ini berlangsung. Semoga hasil dari penelitian ini dapat bermanfaat bagi kemajuan ilmu pengetahuan serta memberikan dampak positif bagi masyarakat..

4 DAFTAR PUSTAKA

[1] D. P. Kuswandono, Z. Mutaqin, U. B. Saleh, and U. B. Saleh, "INTERNET RUMAH DENGAN TEKNOLOGI VPN," vol. 2, no. 1, pp. 73–89, 2024.

[2] muhammad yusuf Imani, N. Rachman, and P. Chorina, "Implementasi Backbone Network Security System," pp. 1–6, 2021.

[3] T. Informatika *et al.*, "Implementasi keamanan jaringan komputer dengan iptables sebagai firewall menggunakan," vol. 10, no. 1, pp. 720–738, 2025.

[4] A. I. Ramdhani, "MENGGUNAKAN EPRINTS DENGAN TEKNOLOGI TUNNELING (STUDI KASUS : UNIVERSITAS BANI SALEH)," vol. 2, no. 1, 2024.

[5] T. Ariyadi, M. Rizky, M. K. Hadi, and A. A. Widodo, "Implementasi Firewall Pada Protokol SSH Linux Ubuntu Menggunakan Iptables," *Semin. Ris. Mahasiswa-Computer Electr. (SERIMA-CE*, vol. 1, no. 1, pp. 170–175, 2023.

[6] Z. M. Subekti *et al.*, "RANCANG BANGUN INFRASTRUKTUR WEB SERVER," vol. 2, no. 1, pp. 144–151, 2024.

[7] K. M. Kim, Z. M. Subekti, M. D. Suryadi, and ..., "Perancangan dan Implementasi Jaringan Virtual Private Network (VPN) Pada PT. XYZ," *J. ICT Inf. ...*, vol. 23, pp. 310–316, 2023, [Online]. Available: https://ejournal.ikmi.ac.id/index.php/jict-ikmi/article/view/81%0Ahttps://ejournal.ikmi.ac.id/index.php/jict-ikmi/article/download/81/74

[8] D. Wicaksono, "Firewall Sistem Keamanan Jaringan Menggunakan Firewall dengan Metode Port Blocking dan Firewall Filtering," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 1380–1392, 2022, doi: 10.35957/jatisi.v9i2.2103.

[9] Z. M. Subekti *et al.*, "IMPLEMENTASI LOCK MAC ADDRESS STUDI KASUS RT / RW," vol. 1, no. 1, 2023.

[10] W. Sulistyo and S. Sartomo, "Model Keamanan Jaringan Menggunakan Firewall Port Blocking," *Krea-TIF J. Tek. Inform.*, vol. 10, no. 1, pp. 10–18, 2022, doi: 10.32832/kreatif.v10i1.6678.

[1]