

PERANCANGAN SISTEM KEAMANAN JARINGAN BERBASIS VLAN, FIREWALL, DAN PORT SECURITY MENGGUNAKAN MIKROTIK CISCO

Sendy Kurniawan¹, Ade Setiawan²

Universitas Bina Sarana Informatika

e-mail: sendy.2k18@gmail.com, ade.dtx@bsi.ac.id²

Abstrak - Kemajuan teknologi informasi membuat jaringan komputer menjadi kebutuhan utama dalam mendukung komunikasi dan pertukaran data di berbagai perusahaan, termasuk PT Jasa Raharja Putera. Namun, tanpa adanya sistem keamanan yang memadai, jaringan berisiko tinggi terhadap serangan internal maupun eksternal. Penelitian ini bertujuan untuk merancang sistem keamanan jaringan dengan mengimplementasikan Firewall, Port Security, dan VLAN guna meningkatkan perlindungan jaringan pada Kantor Pemasaran PT Jasa Raharja Putera. Metode penelitian yang digunakan meliputi observasi lapangan, wawancara, studi pustaka, serta simulasi jaringan menggunakan perangkat lunak GNS3. Rancangan sistem melibatkan penggunaan Router Mikrotik untuk fungsi routing dan firewall, Switch Cisco manageable sebagai pengatur segmentasi VLAN serta Port Security, dan konfigurasi Access Point di setiap lantai. Firewall berbasis Layer 7 Protocol diterapkan untuk membatasi akses ke situs yang tidak relevan pada VLAN karyawan, sementara komputer pimpinan kantor memperoleh akses penuh melalui filter berbasis MAC Address. Hasil simulasi menunjukkan bahwa desain jaringan yang diajukan mampu meningkatkan keamanan melalui isolasi trafik antar VLAN, pencegahan akses perangkat ilegal, serta pemfilteran lalu lintas internet. Dengan demikian, rancangan ini dapat dijadikan referensi praktis dalam membangun infrastruktur jaringan yang lebih aman dan terstruktur di lingkungan kantor.

Kata Kunci: Keamanan Jaringan, VLAN, Firewall, Port Security, Mikrotik, Cisco

Abstract - The rapid development of information technology has made computer Networks a vital component for communication and data exchange in organizations, including PT Jasa Raharja Putera. However, Networks without proper Security mechanisms are highly vulnerable to both internal and external threats. This study aims to design a Network Security system by implementing Firewall, Port Security, and VLAN to enhance Network protection at the Marketing Office of PT Jasa Raharja Putera. The research methodology consists of field observations, interviews, literature review, and Network simulation using GNS3 software. The proposed design utilizes a Mikrotik Router for routing and firewall functions, Cisco manageable switches for VLAN segmentation and Port Security, and Access Point configurations on each floor. A Layer 7 Protocol-based firewall is applied to restrict non-productive website access within the employee VLAN, while the head office computer is granted full access through MAC Address filtering. The simulation results indicate that the proposed design improves Network Security by isolating traffic between VLANs, preventing unauthorized devices, and filtering internet traffic. Therefore, this design can serve as a practical reference for developing secure and structured Network infrastructures in similar office environments.

Keywords: Network Security, VLAN, Firewall, Port Security, Mikrotik, Cisco.

LATAR BELAKANG MASALAH

Perkembangan teknologi informasi menuntut perusahaan untuk mengoptimalkan infrastruktur jaringan komputer sebagai sarana utama komunikasi dan pertukaran data. Ketergantungan terhadap jaringan membuat aspek keamanan menjadi semakin krusial, mengingat ancaman internal maupun eksternal dapat mengganggu kelancaran operasional dan menimbulkan kerugian signifikan Eben et al. (2024). PT Jasa Raharja Putera, sebagai perusahaan asuransi umum nasional, menghadapi kondisi jaringan yang masih sederhana di kantor pemasarannya di Jakarta Utara. Infrastruktur yang ada hanya menggunakan modem router ONT dan switch *unmanageable* tanpa dukungan sistem keamanan terstruktur. Seluruh perangkat berada dalam satu segmen jaringan, tanpa segmentasi VLAN, *firewall*, maupun *Port Security*. Kondisi ini membuka celah terhadap ancaman seperti penyalahgunaan akses, perangkat asing yang masuk ke jaringan, hingga kebocoran data.

Permasalahan utama yang dihadapi adalah ketiadaan sistem keamanan jaringan yang terstruktur. Tidak adanya segmentasi membuat perangkat internal dan eksternal bercampur, sementara akses internet tidak produktif seperti media sosial tidak dapat dikendalikan. Selain itu, penggunaan switch *unmanageable* tidak memungkinkan penerapan *Port Security* untuk membatasi perangkat asing. Hal ini menunjukkan perlunya perancangan

sistem keamanan jaringan yang dapat menjawab kebutuhan perlindungan data sekaligus mendukung produktivitas kerja.

Berbagai penelitian sebelumnya menunjukkan efektivitas teknologi VLAN, *firewall*, dan *Port Security* dalam meningkatkan keamanan jaringan. Rahman et al. (2020) menekankan bahwa VLAN mampu mencegah akses tidak sah dengan segmentasi trafik yang lebih terstruktur. Azharuddin et al. (2024) membuktikan bahwa *Port Security* dengan *Sticky MAC Address* dapat membatasi perangkat yang terhubung ke switch sehingga mencegah intrusi dari perangkat asing. Sementara itu, Ramadhani et al. (2025) menunjukkan bahwa *firewall* berbasis *Layer 7 Protocol* pada Mikrotik mampu memfilter situs tidak produktif dan menjaga efisiensi jaringan.

Berdasarkan temuan tersebut, penelitian ini mengusulkan solusi berupa perancangan sistem keamanan jaringan berbasis *Firewall*, *Port Security*, dan VLAN menggunakan perangkat Mikrotik dan Cisco. Router Mikrotik difungsikan sebagai DHCP server, *routing* antar VLAN, serta *firewall Layer 7* untuk memblokir akses media sosial pada VLAN karyawan. Switch Cisco *manageable* dikonfigurasi untuk *Port Security* dengan MAC Address *Sticky* serta segmentasi VLAN, yaitu VLAN 10 untuk karyawan dan VLAN 20 untuk tamu. Access Point dipisahkan per VLAN untuk memastikan isolasi trafik. Inovasi lain dalam penelitian ini adalah pemberian akses penuh kepada kepala kantor melalui filter MAC Address, sehingga

tetap memiliki fleksibilitas tanpa mengorbankan keamanan jaringan.

Dengan pendekatan ini, penelitian diharapkan dapat memberikan nilai tambah berupa rancangan jaringan yang lebih aman, terstruktur, dan adaptif terhadap kebutuhan perusahaan. Kontribusi utama penelitian ini adalah penerapan kombinasi *firewall Layer 7*, *Port Security*, dan segmentasi VLAN secara terpadu dalam simulasi GNS3 untuk studi kasus kantor pemasaran PT Jasa Raharja Putera. Hasil penelitian ini dapat dijadikan acuan bagi perusahaan lain yang memiliki kondisi jaringan sederhana untuk meningkatkan keamanan tanpa harus melakukan investasi perangkat yang berlebihan.

METODE PENELITIAN

Penelitian ini dilakukan dengan pendekatan eksperimen simulasi jaringan menggunakan aplikasi GNS3 untuk merancang sistem keamanan jaringan berbasis *Firewall*, *Port Security*, dan VLAN pada Kantor Pemasaran PT Jasa Raharja Putera. Metode ini dipilih karena memungkinkan perancangan, implementasi, serta pengujian sistem jaringan dilakukan dalam lingkungan *virtual* sebelum diterapkan pada kondisi nyata.

1. Metode Pengumpulan Data

a. Observasi

Observasi dilakukan secara langsung di Kantor Pemasaran PT Jasa Raharja Putera untuk mempelajari kondisi jaringan yang ada. Hasil observasi menunjukkan bahwa jaringan masih sederhana, hanya terdiri dari modem

router ONT dan switch *unmanageable* tanpa segmentasi VLAN, *firewall*, maupun *Port Security*.

b. Wawancara

Wawancara dilakukan dengan pihak kepala kantor untuk memperoleh informasi mengenai permasalahan yang dihadapi, kebutuhan keamanan jaringan, serta harapan terhadap sistem yang dirancang.

c. Studi Pustaka

Studi pustaka dilakukan dengan meninjau literatur dan penelitian terdahulu mengenai *Firewall*, VLAN, *Port Security*, *Switch Cisco*, Mikrotik RouterOS, serta simulasi jaringan GNS3 sebagai referensi untuk mendukung desain dan implementasi penelitian ini.

2. Metode Pengembangan Jaringan

Penelitian ini menggunakan model prototyping jaringan yang dilakukan melalui tahapan berikut:

a. Analisis Kebutuhan Jaringan

Mengidentifikasi kelemahan jaringan berjalan, seperti tidak adanya VLAN, *Port Security*, maupun *firewall*

b. Perancangan Topologi Usulan

Menambahkan Router Mikrotik sebagai *core router* dan *firewall*, Switch Cisco *manageable* untuk VLAN dan *Port Security*, serta Access Point dengan dua SSID (VLAN 10 untuk karyawan dan VLAN 20 untuk tamu).

c. Implementasi Simulasi di GNS3

Meliputi konfigurasi VLAN dan *trunking*, *Port Security* dengan MAC *Sticky*, *firewall* berbasis *Layer 7 Protocol* pada Mikrotik, serta uji

komunikasi intra-VLAN dan antar-VLAN.

d. Pengujian Jaringan

Dilakukan untuk memastikan bahwa VLAN dapat memisahkan trafik jaringan, *Port Security* dapat membatasi perangkat asing, *firewall* dapat memblokir situs tertentu, serta komputer kepala kantor tetap mendapat akses penuh.

e. Evaluasi dan Dokumentasi

Mengevaluasi hasil simulasi dan mendokumentasikan konfigurasi, tangkapan layar topologi, serta hasil pengujian untuk menjadi acuan perancangan jaringan yang lebih aman dan terstruktur.

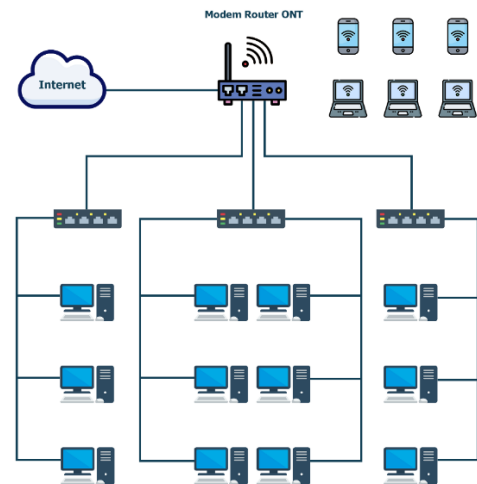
HASIL DAN PEMBAHASAN

Dalam penelitian ini, penulis merancang sistem keamanan jaringan di Kantor Pemasaran PT Jasa Raharja Putera dengan mengimplementasikan *Virtual LAN (VLAN)*, *Firewall Layer 7 Protocol*, serta *Port Security*. Perancangan dilakukan melalui simulasi pada perangkat lunak GNS3, menggunakan Router Mikrotik, *Switch Manageable Cisco*, dan *Access Point*. Hasil rancangan ini kemudian diuji untuk memastikan efektivitas segmentasi jaringan, pembatasan perangkat ilegal, serta pemfilteran akses internet.

1. Analisis Jaringan Berjalan

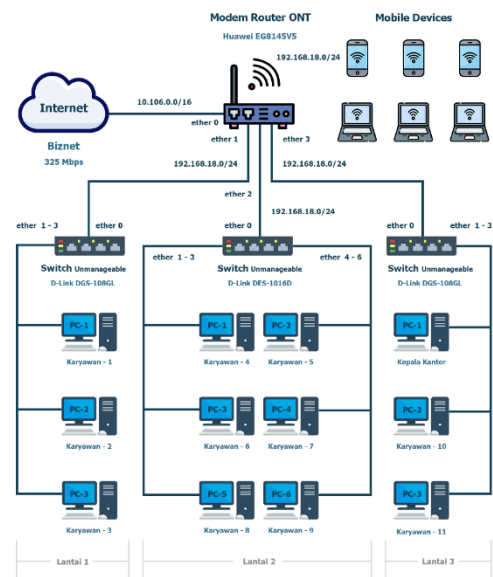
Hasil observasi menunjukkan bahwa jaringan eksisting masih menggunakan modem router ONT Huawei EG8145V5 sebagai *gateway* utama dan *switch unmanageable* di setiap lantai. Semua perangkat berada pada satu segmen jaringan (subnet 192.168.18.0/24) tanpa

adanya segmentasi VLAN maupun pembatasan akses.



Gambar I. 1 Topologi Jaringan Berjalan Kantor Pemasaran PT Jasa Raharja Putera

Sumber: Hasil Observasi dan Desain Penulis



Gambar I. 2 Skema Jaringan Berjalan Kantor Pemasaran PT Jasa Raharja Putera

Sumber: Hasil Observasi dan Desain Penulis

Kondisi ini menyebabkan beberapa kelemahan, di antaranya:

- Tidak adanya pemisahan jaringan antara perangkat karyawan dan tamu.
- Seluruh *port switch* dapat diakses oleh perangkat asing karena tidak diterapkan *Port Security*.
- Akses internet tidak terkontrol, sehingga karyawan dapat membuka situs yang tidak relevan dengan pekerjaan.

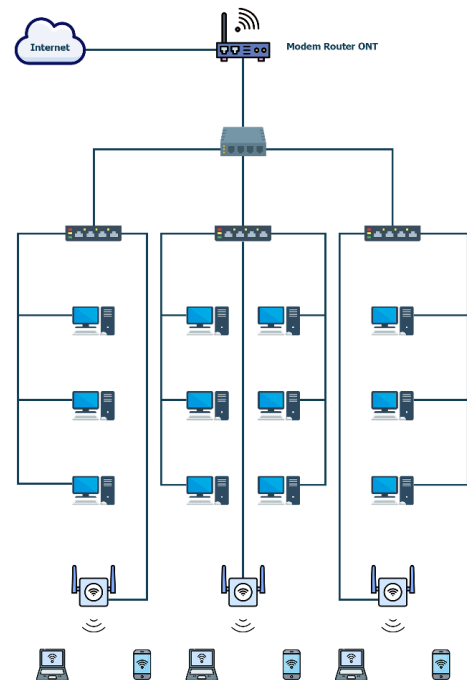
Permasalahan ini mengindikasikan perlunya perancangan ulang dengan menambahkan perangkat yang mendukung konfigurasi keamanan jaringan.

2. Rancangan Jaringan Usulan

Rancangan jaringan usulan masih menggunakan topologi star dengan tambahan *Router Mikrotik*, *Switch Cisco* manageable pada setiap lantai, serta *Access Point* yang dipisahkan sesuai VLAN. *Router Mikrotik* berfungsi sebagai *DHCP server*, routing antar VLAN, serta *firewall* berbasis *Layer 7*. *Switch Cisco* digunakan untuk segmentasi VLAN dan penerapan *Port Security*.

Berikut adalah tampilan gambar dari Topologi dan Skema Jaringan Usulan pada Kantor Pemasaran PT Jasa Raharja Putera :

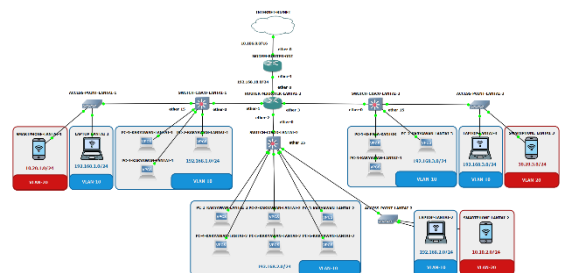
2.1. Topologi Jaringan Usulan :



Gambar II. 1 Topologi Jaringan Usulan Kantor Pemasaran PT Jasa Raharja Putera

Sumber: Hasil Observasi dan Desain Penulis

2.2. Skema Jaringan Usulan :



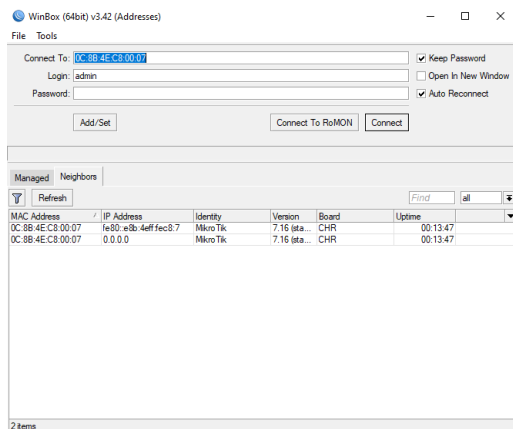
Gambar II. 2 Skema Jaringan Usulan Kantor Pemasaran PT Jasa Raharja Putera

Sumber: Hasil Observasi dan Desain Penulis

Dalam implementasi simulasi pada GNS3, langkah-langkah konfigurasi dilakukan sebagai berikut:

a. Konfigurasi Router Mikrotik

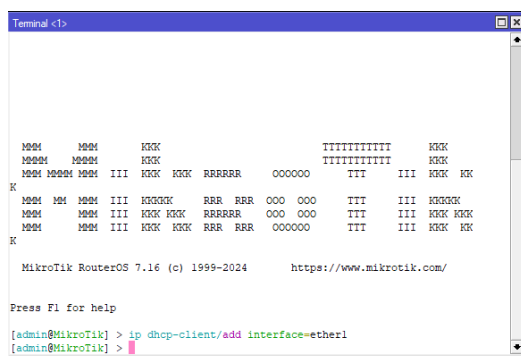
1. Buka aplikasi Winbox dan login menggunakan MAC Address atau IP Address.



Gambar II. 3 Tampilan Login Aplikasi Winbox

Sumber: Hasil Dokumentasi Penulis

2. Periksa koneksi internet router di DHCP Client; jika IP terdeteksi dan status "bound", router sudah terhubung. Jika kosong, router belum dapat IP. Berikut langkah konfigurasi di Terminal Winbox :



Gambar II. 4 Langkah ke-2 Konfigurasi Awal Perangkat Router Mikrotik.

Sumber: Hasil Dokumentasi Penulis

3. Tambahkan Interface VLAN pada setiap port yang terhubung ke switch. Berikut

langkah konfigurasi di Terminal Winbox :



Gambar II. 5 Langkah ke-3 Konfigurasi Awal Perangkat Router Mikrotik

Sumber: Hasil Dokumentasi Penulis

4. Kelompokkan setiap Interface VLAN ke dalam satu daftar melalui menu Interface List. Berikut langkah konfigurasi di Terminal Winbox :



Gambar II. 6 Langkah ke-4 Konfigurasi Awal Perangkat Router Mikrotik

Sumber: Hasil Dokumentasi Penulis

5. Nonaktifkan port Mikrotik yang tidak digunakan untuk meningkatkan keamanan. Berikut langkah konfigurasi di Terminal Winbox :

```

Terminal <1>

MikroTik RouterOS 7.16 (c) 1999-2024      https://www.mikrotik.com/

Press F1 for help

[admin@MikroTik] > interface/disable ether5
[admin@MikroTik] > interface/disable ether6
[admin@MikroTik] > interface/disable ether7
[admin@MikroTik] > interface/disable ether8
[admin@MikroTik] >

```

Gambar II. 7 Langkah ke-5 Konfigurasi Awal Perangkat Router Mikrotik.

Sumber: Hasil Dokumentasi Penulis

6. Berikan IP Address pada setiap Interface VLAN sesuai skema jaringan melalui menu Addresses. Berikut langkah konfigurasi di Terminal Winbox:

```

Terminal <1>

MikroTik RouterOS 7.16 (c) 1999-2024      https://www.mikrotik.com/

Press F1 for help

[admin@MikroTik] > ip address/add address=192.168.1.1/24 interface=VLAN-10-Lantai-1
[admin@MikroTik] > ip address/add address=192.168.2.1/24 interface=VLAN-10-Lantai-2
[admin@MikroTik] > ip address/add address=192.168.3.1/24 interface=VLAN-10-Lantai-3
[admin@MikroTik] > ip address/add address=10.20.1.1/24 interface=VLAN-20-Lantai-1
[admin@MikroTik] > ip address/add address=10.20.2.1/24 interface=VLAN-20-Lantai-2
[admin@MikroTik] > ip address/add address=10.20.3.1/24 interface=VLAN-20-Lantai-3
[admin@MikroTik] >

```

Gambar II. 8 Langkah ke-6 Konfigurasi Awal Perangkat Router Mikrotik

Sumber: Hasil Dokumentasi Penulis

7. Tambahkan DHCP Server pada setiap Interface VLAN agar perangkat di jaringan VLAN mendapat IP. Berikut langkah konfigurasi di Terminal Winbox :

```

Terminal <1>

MikroTik RouterOS 7.16 (c) 1999-2024      https://www.mikrotik.com/

Press F1 for help

[admin@MikroTik] > ip dhcp-server/setup
Select interface to run DHCP server on

dhcp server interface: VLAN-10-Lantai-1
Select network for DHCP addresses

dhcp address space: 192.168.1.0/24
Select gateway for given network

gateway for dhcp network: 192.168.1.1
Select pool of ip addresses given out by DHCP server

addresses to give out: 192.168.1.2-192.168.1.254
Select DNS servers

dns servers: 192.168.15.1
Select lease time

lease time: 1800
[admin@MikroTik] >

```

Gambar II. 9 Langkah ke-7 Konfigurasi Awal Perangkat Router Mikrotik

Sumber: Hasil Dokumentasi Penulis

8. Konfigurasi koneksi internet untuk jaringan VLAN melalui menu IP > Firewall > NAT. Berikut langkah konfigurasi di Terminal Winbox:

```

Terminal <1>

MikroTik RouterOS 7.16 (c) 1999-2024      https://www.mikrotik.com/

Press F1 for help

[admin@MikroTik] > ip firewall/nat add chain=srcnat out-interface=ether1 action=masquerade
[admin@MikroTik] >

```

Gambar II. 10 Langkah ke-8 Konfigurasi Awal Perangkat Router Mikrotik

Sumber: Hasil Dokumentasi Penulis

b. Konfigurasi Firewall Layer 7 Protocol (Router Mikrotik)

1. Buka menu Firewall > Layer 7 Protocol, lalu tambahkan aturan baru dengan Name (misal: Blokir-Situs) dan Regexp `^.*(facebook|instagram|tiktok|twitter|youtube).*`. Berikut langkah konfigurasi di Terminal Winbox :

```

Terminal <1>

MikroTik RouterOS 7.16 (c) 1999-2024      https://www.mikrotik.com/

Press F1 for help

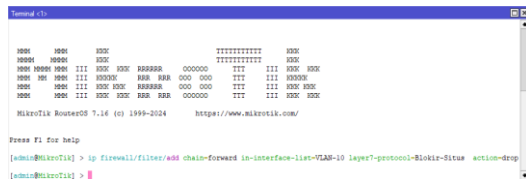
[admin@MikroTik] > ip firewall/layer7-protocol/add name=Blokir-Situs regexp="^.*(facebook|instagram|tiktok|twitter|youtube).*"
[admin@MikroTik] >

```

Gambar II. 11 Langkah ke-1 Konfigurasi Firewall Layer 7 Protocol

Sumber: Hasil Dokumentasi Penulis

2. Masuk ke *tab Filter Rules*, tambahkan aturan dengan *Chain=forward*, *in-Interface-list=VLAN-10*, *Layer 7 Protocol=Blokir-Situs*, dan *Action=Drop*. Berikut langkah konfigurasi di Terminal Winbox :



```

Mikrotik RouterOS 7.16 (c) 1999-2024      https://www.mikrotik.com/

Press F1 for help

[admin@Mikrotik] > ip firewall/filter/add chain=forward in-interface-list=VLAN-10 layer7-protocol=Blokir-Situs action=drop
[admin@Mikrotik] >

```

Gambar II. 12 Langkah ke-2 Konfigurasi Firewall Layer 7 Protocol

Sumber: Hasil Dokumentasi Penulis

3. Berikan akses penuh ke situs yang diblokir di VLAN 10 untuk komputer tertentu dengan menambahkan aturan di *Filter Rules*: (Misalkan), *Chain=forward*, *Layer 7 Protocol=Blokir-Situs*, *Src. MAC Address=00:50:79:66:68:05*, *Action=accept*. Berikut langkah konfigurasi di Terminal Winbox :



```

Mikrotik RouterOS 7.16 (c) 1999-2024      https://www.mikrotik.com/

Press F1 for help

[admin@Mikrotik] > ip firewall/filter/add chain=forward src-mac-address=00:50:79:66:68:05 layer7-protocol=Blokir-Situs action=accept
[admin@Mikrotik] >

```

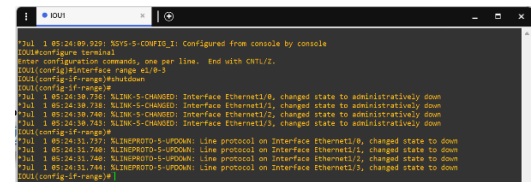
Gambar II. 13 Langkah ke-3 Konfigurasi Firewall Layer 7 Protocol

Sumber: Hasil Dokumentasi Penulis

c. Konfigurasi Switch Cisco

1. Buka aplikasi GNS3 dan project skema jaringan, lalu *double klik* switch Cisco IOU L2 untuk masuk ke Solar PuTTY.
2. Matikan port yang tidak digunakan pada switch untuk mengamankan

jaringan dari akses tidak sah, Berikut langkah konfigurasi menggunakan Solar PuTTY :



```

IOU1 1 85:24:09:920: IOSV-5-CWF10-1 Configured from console by console
IOU1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IOU1(config)#interface range e1-2
IOU1(config-if-range)#shutdown
IOU1(config-if-range)#
IOU1 1 85:24:19:726: VLNW-5-CHANGED: Interface Ethernet1/0, changed state to administratively down
IOU1 1 85:24:19:726: VLNW-5-CHANGED: Interface Ethernet1/0, changed state to administratively down
IOU1 1 85:24:19:748: VLNW-5-CHANGED: Interface Ethernet1/2, changed state to administratively down
IOU1 1 85:24:19:748: VLNW-5-CHANGED: Interface Ethernet1/2, changed state to administratively down
IOU1 1 85:24:19:748: VLNW-5-CHANGED: Interface Ethernet1/3, changed state to administratively down
IOU1(config-if-range)#
IOU1 1 85:24:11:777: VLNWPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
IOU1 1 85:24:11:748: VLNWPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/1, changed state to down
IOU1 1 85:24:11:748: VLNWPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/2, changed state to down
IOU1 1 85:24:11:748: VLNWPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/3, changed state to down
IOU1(config-if-range)#

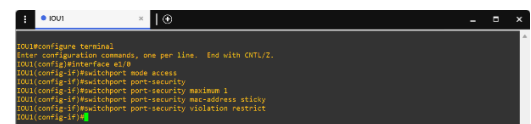
```

Gambar II. 14 Langkah ke-2 Konfigurasi Awal Perangkat Switch Cisco

Sumber: Hasil Dokumentasi Penulis

d. Konfigurasi Port Security (Switch Cisco)

1. Klik dua kali perangkat Switch untuk masuk ke Solar PuTTY.
2. Aktifkan Port Security di switch dengan mengetik perintah *enable*, lalu *configure terminal*, kemudian pilih port yang akan diamankan. Berikut langkah konfigurasi menggunakan Solar PuTTY :



```

IOU1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IOU1(config)#interface e1/0
IOU1(config-if)#switchport mode access
IOU1(config-if)#switchport port-security
IOU1(config-if)#switchport port-security maximum 1
IOU1(config-if)#switchport port-security mac-address sticky
IOU1(config-if)#switchport port-security violation restrict
IOU1(config-if)#

```

Gambar II. 15 Langkah ke-2 Konfigurasi Port Security (Switch Cisco)

Sumber: Hasil Dokumentasi Penulis

e. Konfigurasi VLAN (Switch Cisco)

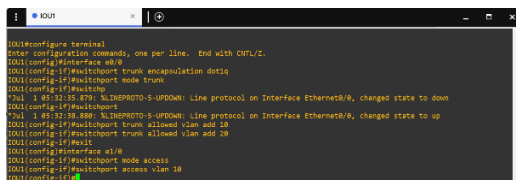
1. Klik dua kali perangkat Switch untuk masuk ke Solar PuTTY.
2. Aktifkan VLAN di switch dengan perintah *enable*, lalu *configure terminal*, kemudian buat VLAN 10 dan VLAN 20 menggunakan perintah yang sesuai. Berikut langkah konfigurasi menggunakan Solar PuTTY :



Gambar II. 16 Langkah ke-2 Konfigurasi VLAN (Switch Cisco)

Sumber: Hasil Dokumentasi Penulis

3. Setelah itu, atur Port 1 dan 16 sebagai VLAN mode Trunk untuk akses VLAN 10 dan 20, serta Port 2–15 sebagai VLAN 10 mode Access menggunakan perintah yang sesuai. Berikut langkah konfigurasi menggunakan Solar PuTTY:



Gambar II. 17 Langkah ke-3 Konfigurasi VLAN (Switch Cisco)

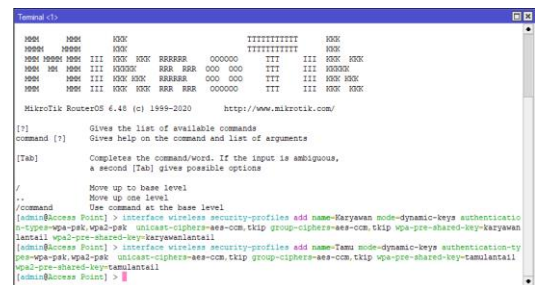
Sumber: Hasil Dokumentasi Penulis

f. Konfigurasi Access Point (Router Mikrotik)

1. Buka menu Wireless, lalu pilih tab Security Profiles.
2. Buat keamanan password WiFi Karyawan dan Tamu dengan klik tanda + di Security Profiles, lalu atur:
 - a. Name: Karyawan atau Tamu
 - b. Mode: dynamic keys
 - c. Authentication Types: centang WPA PSK dan WPA2 PSK
 - d. Unicast Ciphers: centang aes ccm dan tkip
 - e. Group Ciphers: centang aes ccm dan tkip

f. WPA/WPA2 Pre-Shared Key: gunakan format karyawanlantai-(lantai) atau tamulantai-(lantai).

3. Setelah itu, klik Apply dan OK. Berikut langkah konfigurasi di Terminal Winbox :



Gambar II. 18 Langkah ke-3 Konfigurasi Access Point (Router Mikrotik)

Sumber: Hasil Dokumentasi Penulis

4. Jika sudah, buka menu Wireless lalu ke tab WiFi Interfaces.
5. Setelah itu, aktifkan Interface wlan1 untuk WiFi Karyawan.
6. Buat juga Interface wlan2 untuk WiFi Tamu, dengan mengklik tanda +, lalu pilih Virtual.
7. Ubah pengaturan wlan1 dan wlan2 sebagai berikut:
 - a. Mode: ap-bridge
 - b. SSID = Karyawan Lantai (sesuaikan lantai) atau Tamu Lantai (sesuaikan lantai)
 - c. Security Profile = Karyawan atau Tamu
8. Setelah itu, klik Apply dan OK. Berikut langkah konfigurasi di Terminal Winbox :

```

Terminal <2>
MikroTik RouterOS 6.48 (c) 1999-2020 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments
[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@Access Point] > interface wireless set wlan1 mode=ap-bridge ssid="Baryawan Lantai 1" security
-profile=Baryawan disabled=no
[admin@Access Point] > interface wireless add name=wlan2 mode=ap-bridge ssid="Tamu Lantai 1" security
-profile=Tamu master-interface=wlan1 disabled=no
[admin@Access Point] >

```

Gambar II. 19 Langkah ke-8
Konfigurasi Access Point (Router
Mikrotik)

Sumber: Hasil Dokumentasi Penulis

9. Jika sudah, buka menu *Bridge* lalu ke *tab Bridge*.
10. Klik tanda + di menu *Bridge*, lalu atur:
 - a. *Name* = *bridge1*
 - b. Centang *VLAN Filtering* di *tab VLAN*
 - c. Klik *Apply* dan *OK*.
11. Klik *Apply* dan *OK*. Berikut langkah konfigurasi di Terminal Winbox :

```

Terminal <1>
MikroTik RouterOS 6.48 (c) 1999-2020 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments
[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@Access Point] > interface bridge add name=bridge1 vlan-filtering=yes
[admin@Access Point] >

```

Gambar II. 20 Langkah ke-11
Konfigurasi Access Point (Router
Mikrotik)

Sumber: Hasil Dokumentasi Penulis

12. Jika sudah, buka *tab Ports*.
13. Tambahkan tiga aturan baru di *tab Ports* dengan klik tanda +, lalu atur sebagai berikut:

Pertama :
 - a. *Interface* = *ether1*

b. *Bridge* = *bridge1*

c. *PVID* = 1

d. Hapus centang *Hardware Offload*

Kedua :

a. *Interface* = *wlan1*

b. *Bridge* = *bridge1*

c. *PVID* = 10

Ketiga :

a. *Interface* = *wlan2*

b. *Bridge* = *bridge1*

c. *PVID* = 20

14. Klik *Apply* dan *OK*. Berikut langkah konfigurasi di Terminal Winbox :

```

Terminal <1>
MikroTik RouterOS 6.48 (c) 1999-2020 http://www.mikrotik.com/

[?] Gives the list of available commands
command [?] Gives help on the command and list of arguments
[Tab] Completes the command/word. If the input is ambiguous,
a second [Tab] gives possible options

/ Move up to base level
.. Move up one level
/command Use command at the base level
[admin@Access Point] > interface bridge port add interface=ether1 bridge=bridge1 hw=no
[admin@Access Point] > interface bridge port add interface=wlan1 bridge=bridge1 pvid=10
[admin@Access Point] > interface bridge port add interface=wlan2 bridge=bridge1 pvid=20
[admin@Access Point] >

```

Gambar II. 21 Langkah ke-14
Konfigurasi Access Point (Router
Mikrotik)

Sumber: Hasil Dokumentasi Penulis

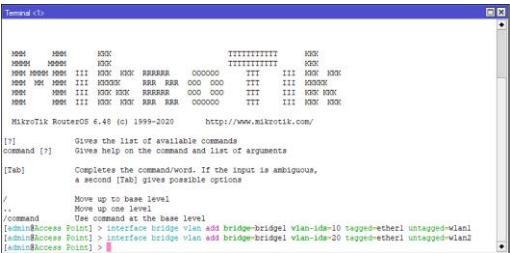
15. Jika sudah, buka *tab VLANs*.
16. Tambahkan dua aturan baru di *tab VLANs* dengan klik tanda +, lalu atur sebagai berikut:

Pertama :
 - a. *Bridge* = *bridge1*
 - b. *VLAN IDs* = 10
 - c. *Tagged* = *ether1*
 - d. *Untagged* = *wlan1*

Kedua :

- a. Bridge = bridge1
- b. VLAN IDs = 20
- c. Tagged = ether1
- d. Untagged = wlan2

17. Setelah itu, klik Apply dan OK. Berikut langkah konfigurasi di Terminal Winbox :



Gambar II. 22 Langkah ke-17 Konfigurasi Access Point (Router Mikrotik)

Sumber: Hasil Dokumentasi Penulis

3. Manajemen Jaringan

Manajemen jaringan diatur melalui konfigurasi alamat IP pada masing-masing VLAN.

Tabel III. 1 Tabel IP Address Kantor Pemasaran PT Jasa Raharja Putera

Perangkat	Interface	VLAN	IP Address
Modem Router ONT	Ether 1 - (ISP)	-	10.106.0.0/16
Modem Router ONT	Ether 2 - (Ether 1, Router Mikrotik Lantai 2)	-	192.168.18.0/24
Router Mikrotik Lantai 2	Ether 1 – (Ether 2, Modem	-	10.106.0.0/16

	Router ONT)		
Router Mikrotik Lantai 2	Ether 2 – (Ether 0, Switch Cisco Lantai 1)	10	192.168.1.0/24
Router Mikrotik Lantai 2	Ether 2 – (Ether 0, Switch Cisco Lantai 1)	20	10.20.1.0/24
Router Mikrotik Lantai 2	Ether 3 – (Ether 0, Switch Cisco Lantai 2)	10	192.168.2.0/24
Router Mikrotik Lantai 2	Ether 3 – (Ether 0, Switch Cisco Lantai 2)	20	10.20.2.0/24
Router Mikrotik Lantai 2	Ether 4 – (Ether 0, Switch Cisco Lantai 3)	10	192.168.3.0/24
Router Mikrotik Lantai 2	Ether 4 – (Ether 0, Switch Cisco Lantai 3)	20	10.20.3.0/24

Sumber : Hasil Dokumentasi Penulis

Implementasi VLAN pada switch dilakukan dengan mode access untuk perangkat end-user dan trunk untuk koneksi antar switch maupun ke router.

Tabel III. 2 Tabel VLAN Kantor
Pemasaran PT Jasa Raharja Putera

Perangkat	Interface	VLAN
Switch Lantai 1	Ethernet 0/1	Mode Trunk – Trunk Allowed VLAN 10 dan VLAN 20
Switch Lantai 1	Ethernet 0/2 – Ethernet 3/2	Mode Access – Access VLAN 10
Switch Lantai 1	Ethernet 3/3	Mode Trunk – Trunk Allowed VLAN 10 dan VLAN 20
Switch Lantai 2	Ethernet 0/1	Mode Trunk – Trunk Allowed VLAN 10 dan VLAN 20
Switch Lantai 2	Ethernet 0/2 - Ethernet 3/2	Mode Access – Access VLAN 10
Switch Lantai 2	Ethernet 3/3	Mode Trunk – Trunk Allowed VLAN 10 dan VLAN 20
Switch Lantai 3	Ethernet 0/1	Mode Trunk – Trunk Allowed VLAN 10 dan VLAN 20
Switch Lantai 3	Ethernet 0/2 – Ethernet 3/2	Mode Access – Access VLAN 10

Switch Lantai 3	Ethernet 3/3	Mode Trunk – Trunk Allowed VLAN 10 dan VLAN 20
-----------------	--------------	--

Sumber : Hasil Dokumentasi Penulis

Untuk menghindari akses ilegal, Port Security diaktifkan dengan metode MAC Address Sticky yang membatasi hanya satu perangkat sah per port.

Tabel III. 3 Tabel *Port Security* Kantor Pemasaran PT Jasa Raharja Putera

Perangkat	Interface	Port Security
Switch Lantai 1	Ethernet 0/2 - Ethernet 3/2	MAC Address Sticky – Violation Restrict
Switch Lantai 2	Ethernet 0/2 - Ethernet 3/2	MAC Address Sticky – Violation Restrict
Switch Lantai 3	Ethernet 0/2 - Ethernet 3/2	MAC Address Sticky – Violation Restrict

Sumber : Hasil Dokumentasi Penulis

Sementara itu, *firewall Layer 7* pada Mikrotik memblokir situs tidak produktif seperti Facebook, Instagram, TikTok, Twitter, dan YouTube untuk VLAN 10. Namun, komputer kepala kantor tetap mendapat akses penuh melalui *filter MAC Address*.

Tabel III. 4 Tabel *Layer 7 Protocol* Kantor Pemasaran PT Jasa Raharja Putera

Perangkat	Situs Di Blokir	Tujuan	Aksi
Router Mikrotik Lantai 2	Facebook, Instagram,	VLAN 10	Drop

	Twitter, Tiktok, Youtube		
Router Mikrotik Lantai 2	-	VLAN 20	Accept
Router Mikrotik Lantai 2	-	Komputer Kepala Kantor (VLAN 10)	Accept

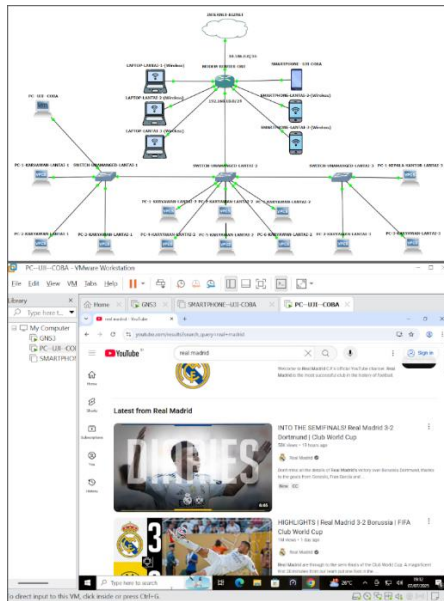
Sumber : Hasil Dokumentasi Penulis

4. Hasil Pengujian

Pengujian dilakukan sebelum dan sesudah penerapan sistem keamanan jaringan. Hasilnya adalah sebagai berikut:

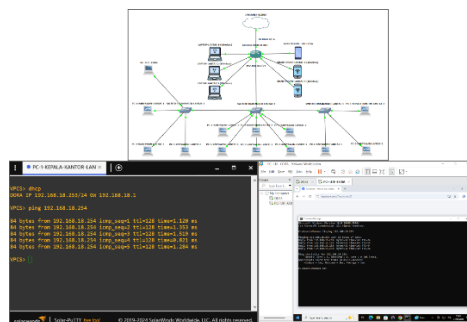
1. Pengujian Awal

Seluruh perangkat masih dapat mengakses situs tanpa *filter*.



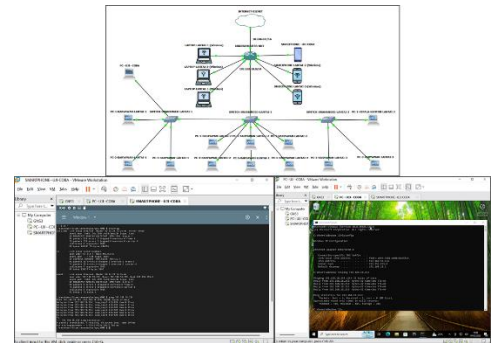
Gambar IV. 1 Tampilan Pengujian Awal Sebelum Menerapkan Layer 7 Protocol

Sumber : Hasil Dokumentasi Penulis
Perangkat asing dapat langsung masuk jaringan melalui port switch.



Gambar IV. 2 Tampilan Pengujian Awal Sebelum Menerapkan Port Security

Sumber : Hasil Dokumentasi Penulis
Tidak ada segmentasi antar perangkat, sehingga semua saling terkoneksi.

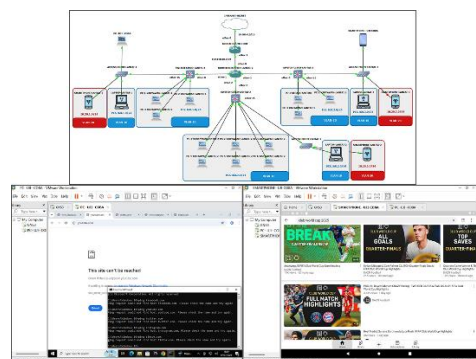


Gambar IV. 3 Tampilan Pengujian Awal Sebelum Menerapkan VLAN

Sumber : Hasil Dokumentasi Penulis

2. Pengujian Akhir

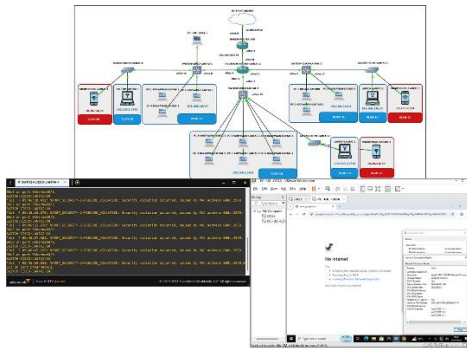
Situs tidak produktif berhasil diblokir pada VLAN 10, ditunjukkan dengan pesan *Error/Timeout* saat diakses.



Gambar IV. 4 Tampilan Pengujian Akhir Setelah Menerapkan Layer 7 Protocol

Sumber : Hasil Dokumentasi Penulis

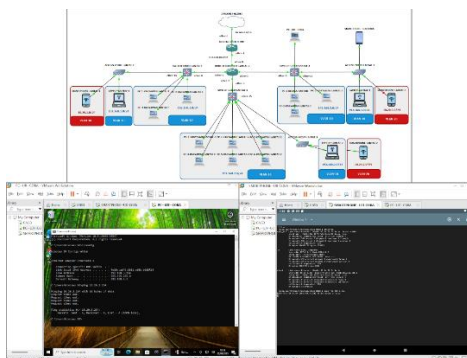
Port Security berhasil mencegah perangkat asing masuk ke jaringan; port otomatis mati jika ada perangkat ilegal.



Gambar IV. 5 Tampilan Pengujian Akhir Setelah Menerapkan Port Security

Sumber : Hasil Dokumentasi Penulis

Segmentasi VLAN berhasil diterapkan; perangkat VLAN 10 tidak dapat terkoneksi ke VLAN 20.



Gambar IV. 6 Tampilan Pengujian Akhir Setelah Menerapkan VLAN

Sumber : Hasil Dokumentasi Penulis

KESIMPULAN

Penelitian ini berhasil menjawab permasalahan yang telah dirumuskan dalam pendahuluan, yaitu merancang sistem keamanan jaringan yang lebih aman dan terstruktur pada Kantor Pemasaran PT Jasa Raharja Putera. Hasil implementasi menunjukkan bahwa penerapan VLAN mampu memisahkan lalu lintas jaringan antara karyawan dan tamu, *Port Security* efektif membatasi perangkat asing yang mencoba

terhubung ke jaringan, serta *firewall Layer 7* dapat memblokir akses terhadap situs tidak produktif tanpa mengganggu kebutuhan akses penuh bagi kepala kantor. Dengan demikian, tujuan penelitian untuk meningkatkan keamanan jaringan internal sekaligus menjaga efisiensi operasional dapat tercapai.

Prospek pengembangan dari hasil penelitian ini adalah penerapan langsung pada infrastruktur jaringan nyata, sehingga dapat diuji pada kondisi lingkungan kerja yang lebih kompleks. Selain itu, penelitian lanjutan dapat mengintegrasikan fitur keamanan tambahan seperti *Intrusion Detection System (IDS)*, manajemen *bandwidth*, maupun VPN untuk akses jarak jauh yang aman, sebagaimana direkomendasikan dalam literatur terbaru mengenai keamanan jaringan berbasis *enterprise*.

Dengan adanya penelitian ini, rancangan keamanan jaringan berbasis simulasi GNS3 tidak hanya memberikan solusi praktis untuk kasus PT Jasa Raharja Putera, tetapi juga dapat dijadikan model acuan bagi instansi atau perusahaan lain dengan kondisi serupa dalam membangun sistem jaringan yang aman, efisien, dan adaptif terhadap kebutuhan di masa depan.

REFERENSI

- Assilmi, M. R., Sotyohadi, Soetedjo, A., Elektro, T. S., & Malang, I. (2023). *Magnetika Volume 07 Nomor 2 Tahun 2023* 301.
- Azharuddin, L., Jenih, Sugiarso, T., & Nurhastuti, T. (2024). Perancangan dan Implementasi Sistem Keamanan Jaringan dengan *Port Security*

- Menggunakan Switch CISCO di PT. Citra Solusi Pratama. *Jurnal Teknologi Informasi*, 10(2), 148–150. <https://doi.org/https://doi.org/10.52643/jti.v9i1.3175>
- Dara, Y. C., Hariadi, F., Alfa, P., & Lede, R. L. (2022). Analisis Penerapan Sistem Keamanan Jaringan Menggunakan Metode Dhcp-Snooping Dan Switch-Port-Security (Implementation Analysis of Network Security Systems Using the DHCP Snooping and Switch Port Security Methods) (Vol. 01). <https://doi.org/https://doi.org/10.58300/inovatif-wira-wacana.v1i3.337>
- Eben, E., Mukramin, M., & Abduh, H. (2024). PENGEMBANGAN MANAJEMEN KEAMANAN JARINGAN NIRKABEL (WIFI) MENGGUNAKAN ROUTERBOARD MIKROTIK DAN FIREWALL PADA SMK KRISTEN PALOPO. *Jurnal Informatika dan Teknik Elektro Terapan*, 12(3), 2229–2238. <https://doi.org/10.23960/jitet.v12i3.4716>
- Fardani, A. S. (2020). INSTALASI KABEL FIBER OPTIC DAN PERANGKAT SWITCH UNTUK LAYANAN INTERNET MENGGUNAKAN METODE CWDM OLEH PT. XYZ.
- Hendita, A. K. G. (2021). adminjiac,+3259-Article+Text-11423-1-10-20220228. *Journal of Informatics and Advanced Computing*, 2(2), 58–61. <https://doi.org/https://doi.org/10.35814/jiac.v2i2.3259>
- Irfan, Satra, R., & Fattah, F. (2021). Buletin Sistem Informasi dan Teknologi Islam Keamanan Jaringan VLAN dan VoIP Menggunakan Firewall INFORMASI ARTIKEL ABSTRAK. *Buletin Sistem Informasi dan Teknologi Islam*, 2(1), 27–35. <https://doi.org/https://doi.org/10.33096/busiti.v2i1.720>
- Mananggell, A. V., Mewengkang, A., & Djamen, A. C. (2021). 1124-Article Text-9783-1-10-20211213. *Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, 1(2), 119–131. <https://doi.org/https://doi.org/10.53682/edutik.v1i2.1124>
- Noviriandini, A., Hermanto, Ambarsari, D. A., & Eriawan, D. (2022). ANALISIS MANAGEMENT BANDWIDTH DAN FIREWALL DENGAN ROUTER MIKROTIK PADA PT. BCA MULTIFINANCE. *Jurnal Teknik dan Science*, 1(3), 40–45. <https://doi.org/https://doi.org/10.56127/jts.v1i3.466>
- Rahman, T., Zaini, T. R., & Chrisnawati, G. (2020). PERANCANGAN JARINGAN VIRTUAL LOCAL AREA NETWORK (VLAN) & DHCP PADA PT.NAVICOM INDONESIA BEKASI. *Jurnal Informatika*, 4(1), 36–41. <https://doi.org/http://dx.doi.org/10.31000/jika.v4i1.2366>
- Ramadhan, J. A., Susilo, A., Irawan, Y., & Solehudin, A. (2023). PERANCANGAN APLIKASI PENGELOLAAN PERANGKAT JARINGAN DENGAN PEMROGRAMAN PYTHON BERBASIS WEB (STUDI KASUS: SMKN 3 KOTA BEKASI). In *Jurnal Mahasiswa Teknik Informatika* (Vol. 7, Issue 4). <https://doi.org/https://doi.org/10.36040/jati.v7i4.7188>
- Ramadhani, A., Palasara, N., & Gani, A. (2025). Filtering Firewall dan Manajemen Bandwidth untuk Keamanan Jaringan pada Kelurahan Buaran Indah. *remik*, 9(1), 346–355. <https://doi.org/10.33395/remik.v9i1.14482>
- Rokim, M. N., Nainggolan, E. R., & Tinggi Manajemen Informatika dan Komputer Nusa Mandiri Jakarta, S. (2021). PEMANFAATAN MANAJEMEN JARINGAN

- MENGGUNAKAN VIRTUAL LOCAL AREA NETWORK (VLAN) PADA PT. JANTRA REKA SAKSANAMAS CENGKARENG TIMUR JAKARTA BARAT. In *Jurnal Rekayasa Perangkat Lunak* (Vol. 2, Issue Mei). <https://doi.org/https://doi.org/10.31294/REPUTASI.V2I1.121>
- Sidik, Rahadjeng, I. R., & Fajrin, A. I. (2021). Implementasi Manajemen Bandwidth Menggunakan Simple Queue Dan Filtering Content Pada Pusat Pelatihan Kerja Pengembangan Industri Jakarta Timur. *Jurnal Rekayasa Perangkat Lunak*, 2(1), 26–30. <http://jurnal.bsi.ac.id/index.php/reputasi>
- Sitohang, S., Pangaribuan, H., & Maslan, A. (2023). PELATIHAN MIKROTIK DI SEKOLAH SMK TUNAS MUDA BERKARYA. *Jurnal Pengabdian Kepada Masyarakat*, 2(2), 138–144. <https://jurnal-adaikepri.or.id/index.php/JUPADAI>
- Sutiman, & Gunawan, A. (2021). FIREWALL PORT SECURITY SWITCH UNTUK KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN CISCO ROUTER 1600S PADA PT. TIRTA KENCANA TATA WARNA SUKABUMI. *CONTEN: Computer and Network Technology*, 1(1), 13–22. <http://jurnal.bsi.ac.id/index.php/content>