

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



**MODUL LATIH SISTEM KEAMANAN JARINGAN FTTH DAN
MANAGEMENT IP**

“Modul Latih Sistem Keamanan Jaringan FTTH”

TUGAS AKHIR

**POLITEKNIK
NEGERI
JAKARTA**

Sujatmiko Jarwoto

2303332004

PROGRAM STUDI TELEKOMUNIKASI

JURUSAN TEKNIK ELEKTRO

POLITEKNIK NEGERI JAKARTA

2026



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



**MODUL LATIH SISTEM KEAMANAN JARINGAN FTTH DAN
MANAGEMENT IP**

“Modul Latih Sistem Keamanan Jaringan FTTH”

TUGAS AKHIR

**POLITEKNIK
NEGERI
JAKARTA**

Sujatmiko Jarwoto

2303332004

PROGRAM STUDI TELEKOMUNIKASI

JURUSAN TEKNIK ELEKTRO

POLITEKNIK NEGERI JAKARTA

2026



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

HALAMAN PERNYATAAN ORISINALITAS

Tugas Akhir ini adalah hasil karya saya sendiri dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar

Nama : Sujatmiko Jarwoto

NIM : 2303332004

Tanda Tangan :

Tanggal : 01-07-2026





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

**LEMBAR PENGESAHAN
TUGAS AKHIR**

Tugas Akhir diajukan oleh :

Nama : Sujatmiko Jarwoto
NIM : 2303332004
Program Studi : D3-Teknik Telekomunikasi
Judul Tugas Akhir : Modul Latih Sistem Keamanan Jaringan Dan
Management IP
Sub Judul Tugas Akhir : Modul Latih Sistem Keamanan Jaringan FTTH

Telah diuji oleh tim penguji dalam Sidang Tugas Akhir pada Selasa 30 Juni 2026
dan dinyatakan **LULUS**.

Pembimbing : Ir. Sri Danaryani, M.T,
NIP : 196305031991032001

()

**POLITEKNIK
NEGERI
JAKARTA**

Depok, 25 Juli 2026

Disahkan oleh

Ketua Jurusan Teknik Elektro



Dr., Murie Dwiyaniti, S.T., M.T
NIP. 197803312003122002



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmatnya, penulis dapat menyelesaikan tugas akhir ini. Penulisan tugas akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar diploma tiga politeknik. Tugas akhir ini berisi tentang Modul Latih Sistem Kemanan FTTH. Penulis menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan tugas akhir ini sangatlah sulit bagi penulis untuk menyelesaikan tugas akhir ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Ir.Sri Danaryani, M.T selaku dosen pembimbing atas bimbingan dan arahnya selama proses tugas akhir.
2. Seluruh dosen dan staff pengajar Jurusan Teknik Elektro PNJ, khususnya Program Studi Telekomunikasi.
3. Orang tua dan keluarga atas doa serta dukungan moril dan materiil.
4. Citra Amelia, rekan sekelompok atas kerja sama dan kontribusinya dalam proyek dan laporan.
5. Teman-teman atas semangat dan bantuan yang diberikan selama penyusunan tugas akhir.

Penulis menyadari bahwa laporan ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun demi perbaikan dan penyempurnaan di masa mendatang.

Depok, 1 Juli 2025

Penulis

Sujatmiko Jarwoto



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

MODUL LATIH SISTEM KEAMANAN JARINGAN FTTH DAN MANAGEMENT IP

“Modul Latih Sistem Keamanan Jaringan FTTH”

ABSTRAK

Keamanan jaringan Fiber To The Home (FTTH) merupakan aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan layanan jaringan. Penelitian ini bertujuan merancang dan membangun modul latih sistem keamanan jaringan FTTH berbasis Router MikroTik dengan menerapkan Virtual Private Network (VPN), autentikasi One-Time Password (OTP), firewall, notifikasi keamanan berbasis email, serta pemblokiran otomatis terhadap serangan *brute force*. Metode penelitian meliputi studi literatur, perancangan, implementasi, dan pengujian. Hasil penelitian menunjukkan bahwa seluruh mekanisme keamanan berhasil diimplementasikan sesuai rancangan. VPN mampu mengamankan akses WebFig, OTP memverifikasi pengguna, notifikasi email berhasil mengirimkan informasi aktivitas login, dan firewall memblokir percobaan login berulang. Pengujian Quality of Service (QoS) menghasilkan throughput 4075 bit/s, delay 0,193 ms, jitter 0,057 ms, dan packet loss 0%. Berdasarkan standar TIPHON, parameter delay, jitter, dan packet loss termasuk kategori Sangat Baik. Modul latih ini layak digunakan sebagai media praktikum keamanan jaringan FTTH.

Kata kunci: *Fiber To The Home (FTTH)*, Router MikroTik, *Virtual Private Network (VPN)*, *One-Time Password (OTP)*, *Firewall*, Notifikasi Keamanan.

Training Module on FTTH Network Security Systems and IP Management



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

“FTTH Network Security Systems Training Module”

ABSTRACT

Fiber To The Home (FTTH) network security is a crucial aspect of maintaining the confidentiality, integrity, and availability of network services. This research aims to design and build an FTTH network security training module based on MikroTik routers, incorporating Virtual Private Network (VPN) technology, One-Time Password (OTP) authentication, firewalls, email-based security notifications, and automatic blocking of brute-force attacks. The research methodology encompasses literature review, design, implementation, and testing. The results demonstrate that all security mechanisms were successfully implemented according to the design. The VPN effectively secured WebFig access, OTP successfully verified users, email notifications reliably transmitted login activity information, and the firewall successfully blocked repeated login attempts. Quality of Service (QoS) testing yielded a throughput of 4075 bit/s, a delay of 0.193 ms, jitter of 0.057 ms, and 0% packet loss. Based on TIPHON standards, the delay, jitter, and packet loss parameters fall into the "Very Good" category. This training module is suitable for use as a practical learning tool for FTTH network security.

Keywords: *Fiber To The Home (FTTH), MikroTik Router, Virtual Private Network (VPN), One-Time Password (OTP), Firewall, Security Notification.*



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun

tanpa izin Politeknik Negeri Jakarta

Daftar Isi

HALAMAN SAMPUL	i
HALAMAN JUDUL.....	ii
HALAMAN PERNYATAAN ORISINALITAS	iii
LEMBAR PENGESAHAN.....	iv
TUGAS AKHIR.....	iv
KATA PENGANTAR	v
ABSTRAK.....	vi
Daftar Isi.....	viii
Daftar Gambar	x
Daftar Table.....	xii
BAB I	1
PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah.....	2
1.3. Tujuan	2
1.4. Luaran.....	2
BAB II.....	3
TINJAUAN PUSTAKA.....	3
2.1. Fiber To The Home (FTTH).....	3
2.2. Virtual Private Network (VPN)	3
2.3. Oracle Virtualbox.....	4
2.5. Web Remote Management (WebFig).....	5
2.6. Linux Ubuntu	6
2.7. Python	6
2.8. Domain	7
2.9. Ip Brute Force	8
2.10. Firewall.....	8
BAB III	11
PERANCANGAN DAN REALISASI.....	11
3.1 Rancangan Sistem Secara Kelesuruhan.....	11
3.2 Cara Kerja Sistem Secara Keseluruhan	11
3.3 Realisasi Sistem Secara Keseluruhan.....	13
3.4.1 Cara Kerja Sistem Notifikasi Login Pada Mikrotik	16
3.4.2 Diagram Blok Kerja Notifikasi Login Pada Mikrotik	17
3.4.3 Perancangan Sistem Notifikasi Login	18
3.4.4 Rancangan Sistem Pemblokiran IP	27
3.4.5 Cara Kerja Pemblokiran IP	27
3.4.6 Diagram Blok Cara kerja sistem pemblokiran IP	28
3.4.7 Rancangan Sistem Pemblokiran IP	29
3.5 Perancangan Sistem Remote Mikrotik.....	33
3.5.1 Cara Kerja Sistem Remote web mikrotik.....	33
3.5.2 Diagram Blok Kerja Sistem Remote web mikrotik	34



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB IV	64
Pembahasan	64
4.1 Pengujian Quality Of Service.....	64
4.2 Deskripsi Pengujian	64
4.3 Alat alat yang digunakan.....	65
4.4 Langkah-Langkah Pengujian	65
4.5 Pengujian Web.....	65
4.6 Data Hasil Pengujian Qos Web	69
4.7 Pengujian Sistem Notifikasi	72
4.8 Deskirpsi Pengujian	72
4.9 Langkah Langkah Pengujian.....	73
4.10 Data Hasil Pengujian	73
BAB V	79
Penutup	79
5.1. Kesimpulan	79
5.2. Saran	79
Daftar Pustaka	81
Daftar Riwayat Hidup.....	82
Lampiran.....	83

**POLITEKNIK
NEGERI
JAKARTA**



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

2. Dilarang mengumpukan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Daftar Gambar

Gambar 2. 1 Oracle VirtualBox	4
Gambar 2. 2 CloudFlare Tunnel.....	4
Gambar 2. 3 Tampilan WebFig	5
Gambar 2. 4 Ubuntu.....	6
Gambar 2. 5. Python	6
Gambar 2. 6. Domainesia.....	7
Gambar 2. 7. IP Brute Force	8
Gambar 2. 8. Firewall	8
Gambar 2. 9. Standar Tiphon	9
Gambar 3.1.3. 1. Tampilan Server Sistem remote	14
Gambar 3.1.3. 2. Tampilan Server Sistem autentikasi	14
Gambar 3.2. 1.Flowchart Cara kerja sistem notifikasi.....	17
Gambar 3.2. 2. Diagram Kerja.....	18
Gambar 3.2. 3 Flowchart Pemblokiran IP	28
Gambar 3.2. 4 Diagram Blok kerja sistem pemblokiran IP	29
Gambar 3.2.3. 1 Tampilan Notifikasi Saat Login	19
Gambar 3.2.3. 2 hasil login yang gagal	24
Gambar 3.3. 1 Flowchart Sistem Remote Web Mikrotik.....	34
Gambar 3.3. 2 Diagram Blok Kerja Sistem Remote Mikrotik	35
Gambar 3.3.3. 1 Install Ubuntu Server	37
Gambar 3.3.3. 2 Pembuatan Domain	58
Gambar 3.3.3. 3 Pembuatan akun CloudFlare	59
Gambar 3.3.3. 4 Pendaftaran Domain Di CloudFlare.....	59
Gambar 3.3.3. 5 Autorisasi CloudFlare Dengan Server.....	60
Gambar 3.3.3. 6 Proses Autorisasi.....	61
Gambar 3.3.3. 7 Tampilan Server Remote Web.....	63
Gambar 4.5 1 Tampilan Halaman Login.....	66
Gambar 4.5 2 Pengujian Throughput.....	69
Gambar 4.5 3 Hasil Pengujian Jitter Dan Delay	70
Gambar 4.9. 1 Login Berhasil Dengan Akun Admin.....	74
Gambar 4.9. 2 Login Berhasil Dengan Akun User	74
Gambar 4.9. 3. Hasil Pengujian Remote Web Mikrotik	71
Gambar 4.9. 4 Login Dengan Password Salah Via Winbox	76
Gambar 4.9. 5 Login Dengan Password Salah Via Winbox Device Hp	76
Gambar 4.9. 6 Login Dengan Password Salah Via Winbox Device Laptop Akun Admin	77



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4.9. 7 Login Dengan Password Salah Via Winbox Device Laptop..... 78





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Daftar Table

Table 1. Hasil Pengujian Web	68
Table 2. Hasil Pengujian QoS Web	70
Table 3. Hasil Pengujian Througput Via Web	71
Table 4. Hasil Perbandingan QoS dengan Standar TIPHON	72
Table 5. Hasil Pengujian keamanan	75
Table 6. Hasil Pengujian Notifikasi Gagal	78





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB I

PENDAHULUAN

1.1.Latar Belakang

Perkembangan teknologi telekomunikasi berbasis serat optik telah mendorong meningkatnya penggunaan jaringan *Fiber To The Home* (FTTH) sebagai media penyedia layanan internet berkecepatan tinggi. Selain menawarkan kapasitas bandwidth yang besar dan koneksi yang stabil, implementasi jaringan FTTH juga memerlukan sistem keamanan yang memadai untuk melindungi perangkat jaringan dari berbagai ancaman, seperti akses tanpa izin, penyalahgunaan hak akses, dan serangan *brute force* [1]. Keamanan jaringan menjadi aspek penting karena setiap perangkat yang terhubung ke jaringan berpotensi menjadi sasaran serangan siber apabila tidak dilengkapi dengan mekanisme pengamanan yang sesuai [2]. Salah satu perangkat yang banyak digunakan dalam implementasi jaringan FTTH adalah Router MikroTik karena menyediakan berbagai fitur keamanan, seperti *virtual private network* (VPN), *firewall*, sistem *logging*, dan otomasi melalui *script* [3]. Pemanfaatan fitur-fitur tersebut memungkinkan administrator mengamankan akses administrasi jaringan, membatasi akses pengguna yang tidak berwenang, serta melakukan pemantauan terhadap aktivitas yang terjadi pada jaringan secara lebih efektif [3].

Namun, dalam proses pembelajaran, implementasi keamanan jaringan FTTH masih didominasi oleh penyampaian materi secara teoretis sehingga mahasiswa belum memperoleh pengalaman dalam melakukan konfigurasi, pengujian, dan analisis mekanisme keamanan secara langsung [4]. Selain itu, ketersediaan media praktikum yang membahas penerapan keamanan jaringan FTTH masih terbatas sehingga pemahaman mahasiswa terhadap implementasi keamanan di lingkungan nyata belum optimal [4]. Kondisi tersebut menyebabkan mahasiswa lebih memahami konsep dibandingkan penerapannya dalam menghadapi permasalahan keamanan jaringan.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana merancang dan membangun modul latih sistem keamanan jaringan Fiber To The Home (FTTH) menggunakan Router MikroTik sebagai media praktikum?
2. Bagaimana mengimplementasikan sistem keamanan akses jarak jauh pada Router MikroTik menggunakan Virtual Private Network (VPN) dan autentikasi One-Time Password (OTP)?
3. Bagaimana mengimplementasikan sistem notifikasi keamanan pada Router MikroTik untuk mendeteksi aktivitas login berhasil, login gagal, dan percobaan akses berulang (*brute force*)?
4. Bagaimana hasil pengujian fungsional modul latih sistem keamanan jaringan FTTH yang telah dirancang?

1.3. Tujuan

Berdasarkan rumusan masalah yang telah dirumuskan, maka tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Merancang modul latih keamanan jaringan FTTH berbasis Router MikroTik.
2. Menerapkan keamanan akses jarak jauh menggunakan VPN dengan autentikasi OTP. Menguji keandalan modul latih dalam mendeteksi dan memitigasi percobaan akses ilegal (*brute force*) melalui penerapan firewall dan sistem notifikasi keamanan pada Router MikroTik.

1.4. Luaran

Adapun luaran dari tugas akhir ini sebagai berikut.

1. Alat
2. Laporan
3. Artikel ilmiah
4. Jobsheet

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB V

Penutup

5.1. Kesimpulan

1. Modul latihan sistem keamanan jaringan *Fiber To The Home* (FTTH) menggunakan Router MikroTik telah berhasil dirancang dan dibangun sebagai media praktikum mahasiswa. Modul latihan ini mampu mendukung pembelajaran mengenai implementasi keamanan jaringan FTTH melalui konfigurasi Router MikroTik dan integrasinya dengan perangkat pendukung.
2. Sistem keamanan akses jarak jauh (*remote access*) menggunakan *Virtual Private Network* (VPN) dengan autentikasi *One-Time Password* (OTP) berhasil diimplementasikan. Proses autentikasi mampu memverifikasi identitas administrator sebelum memberikan akses ke halaman WebFig Router MikroTik sehingga meningkatkan keamanan dalam pengelolaan perangkat jaringan.
3. Pengujian terhadap sistem keamanan menunjukkan bahwa mekanisme *firewall* dan sistem notifikasi keamanan dapat berfungsi sesuai dengan rancangan. Sistem mampu mengirimkan notifikasi aktivitas login melalui *email*, mendeteksi percobaan akses yang mencurigakan, serta melakukan pemblokiran otomatis terhadap alamat IP yang terindikasi melakukan percobaan *brute force*. Dengan demikian, modul latihan yang dikembangkan dapat digunakan sebagai media praktikum untuk mempelajari implementasi sistem keamanan jaringan FTTH berbasis Router MikroTik.

5.2. Saran

1. Penelitian selanjutnya disarankan untuk mengembangkan modul latihan dengan menambahkan mekanisme keamanan lainnya, seperti Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS), sehingga sistem keamanan jaringan menjadi lebih komprehensif.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2. Pengujian sistem dapat dilakukan pada jaringan FTTH dengan skala yang lebih besar dan jumlah pengguna yang lebih banyak untuk mengetahui performa sistem keamanan dalam kondisi lalu lintas jaringan yang lebih kompleks.
3. Pengujian Quality of Service (QoS) disarankan menggunakan perangkat atau aplikasi pendukung, seperti iPerf3 atau metode pengukuran lainnya, sehingga parameter throughput, delay, jitter, dan packet loss dapat dianalisis secara lebih akurat.
4. Sistem notifikasi dapat dikembangkan dengan menambahkan media pengiriman lain, seperti Telegram, WhatsApp, atau aplikasi pesan instan lainnya, sehingga administrator dapat menerima informasi keamanan secara lebih cepat dan fleksibel.
5. Pengembangan selanjutnya dapat menerapkan metode Multi-Factor Authentication (MFA) selain One-Time Password (OTP), sehingga keamanan akses jarak jauh menuju Router MikroTik dapat semakin ditingkatkan.

**POLITEKNIK
NEGERI
JAKARTA**



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Daftar Pustaka

- D. M. Megananda and A. Prihanto, "Implementasi Penggunaan VLAN pada Jaringan FTTH Wifi Publik di Telaga Sarangan," *Journal of Informatics and Computer Science (JINACS)*, vol. 7, no. 1, pp. 163–166, 2025, doi: 10.26740/jinacs.v7n01.p163-166
- A. Fauzi, F. Firmansyah, and T. A. A. Sandi, "Perancangan Keamanan Router Mikrotik Dari Serangan FTP dan SSH Brute Force," *Jurnal Infortech*, vol. 6, no. 1, 2024.
- Seyhan and J. Triloka, "Implementation of Mikrotik Firewall and QoS for Secure and Efficient Internet Networking," *Jurnal Teknologi Informasi dan Pendidikan*, vol. 18, no. 2, pp. 1097–1109, 2025
- R. Oktiana and L. Widyawati, "Desain dan Implementasi VLAN untuk Manajemen Access User pada Access Point Multi SSID dengan CAPsMAN Berbasis Mikrotik," *Jurnal Teknologi, Kesehatan, dan Sosial*, vol. 1, no. 1, pp. 57–66, 2025.
- M. D. Ipang, S. C. Kumajas, and K. Santa, "Implementasi Sistem Management Bandwidth Menggunakan Metode Per Connection Queue (PCQ) pada Jaringan VLAN Berbasis Mikrotik di SMK Negeri Tana Toraja," *REMIK: Riset dan E-Jurnal Manajemen Informatika Komputer*, vol. 10, no. 2, pp. 630–636, 2026.
- Intan Nuraini, Dahlan, and M. A. Mu'min, "Optimasi Kinerja Trafik Jaringan Internet Menggunakan Quality of Service (QoS) pada Mikrotik RouterOS di Kantor Lurah Sarae Kota Bima," *ARMADA: Jurnal Penelitian Multidisiplin*, vol. 4, no. 4, pp. 301–310, 2026.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Daftar Riwayat Hidup



Sujatmiko Jarwoto Lahir di Kota Jakarta pada tanggal 9 Februari 2005. Memulai Pendidikan formal di SD Negeri kampung bambu 3 pada tahun 2011 hingga lulus pada tahun 2017. Setelah itu melanjutkan Pendidikan ke SMP Islam Al-Hikmah Jakarta dan lulus pada tahun 2020. Kemudian penulis melanjutkan Pendidikan ke SMK Grafika Yayasan Lektor Jakarta dan lulus pada tahun 2023. Setelah lulus dari Sekolah Menengah kejuruan, penulis menempuh pendidikan Jurusan Teknik Elektro, Program

Studi D3 Telekomunikasi, Politeknik Negeri Jakarta sejak tahun 2023. Saat ini, penulis sedang menyelesaikan Tugas Akhir dengan merancang modul latih atau *jobsheet* praktikum terkait keamanan FTTH dan manajemen IP.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran





© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
:global LastLoginTime
:local emailTujuan "jarwotosujatmiko@gmail.com"
:local identity [/system identity get name]

:local logs [/log find where message~"logged in"]

:if ([:len $logs] > 0) do={

  :local lastId [:pick $logs ([:len $logs]-1)]
  :local logTime [/log get $lastId time]
  :local logMsg [/log get $lastId message]

  :if ($LastLoginTime != $logTime) do={

    :set LastLoginTime $logTime

    :local ip ""
    :if ([:find $logMsg "from"] != nil) do={
      :set ip [:pick $logMsg ([:find $logMsg "from"] + 5)
[:len $logMsg]]
    }

    :local user "unknown"
    :if ([:find $logMsg "user"] != nil) do={
      :set user "admin"
    }

    :local subject ("Login Berhasil - " . $identity)

    :local body \
    ("Login Berhasil\r\n\r\n" . \
    "Router : " . $identity . "\r\n" . \
    "User : " . $user . "\r\n" . \
    "IP : " . $ip . "\r\n" . \
    "Waktu : " . $logTime . "\r\n\r\n" . \
    "Detail Log:\r\n" . $logMsg . "\r\n\r\n" . \
    "Sistem Keamanan MikroTik")

    /tool e-mail send \
    to=$emailTujuan \
    subject=$subject \
    body=$body

    :log warning ("LOGIN TERDETEKSI dikirim ke email: " .
$emailTujuan)
  }
}
```



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

```
:local ipBad "Unknown"
:local posFrom [:find $logMsg "from "]
:if ($posFrom != -1) do={
:  set ipBad [:pick $logMsg ($posFrom + 5) [:len $logMsg]]
:  local posVia [:find $ipBad " via"]
:  if ($posVia != -1) do={
:    :set ipBad [:pick $ipBad 0 $posVia]
:  }
}
```

```
:local body \
("Login Berhasil\r\n\r\n" . \
"Router   : " . $identity . "\r\n" . \
"User     : " . $user . "\r\n" . \
"IP       : " . $ip . "\r\n" . \
"Waktu    : " . $logTime . "\r\n\r\n" . \
"Detail Log:\r\n" . $logMsg . "\r\n\r\n" . \
"Sistem Keamanan MikroTik")
```

**POLITEKNIK
NEGERI
JAKARTA**