

Implementation of Firewall and Internet Bandwidth Management for Civil Servants at the BKPSDM of Central Sumba Regency

Didi Napoleon Umbu Tara Dima^{1*}, Pingky Alfa Ray Leo Lede²

^{1,2,3} Sumba Informatics Engineering Study Program Wira Wacana Christian University
didhyut38@gmail.com^{1*}

Abstrak

Advancements in information technology require government agencies to maintain secure and stable computer network infrastructures to support operational efficiency. The BKPSDM (Personnel and Human Resources Development Agency) of Central Sumba Regency relies heavily on internet connectivity to manage State Civil Apparatus (ASN) personnel data. However, staff survey results indicate that current internet quality is suboptimal, characterized by frequent slowness and instability caused by the use of bandwidth for non-productive activities, specifically accessing entertainment platforms like YouTube and TikTok. Furthermore, the office WiFi network is vulnerable to unauthorized access, posing a threat to the confidentiality of ASN data. This study aims to implement a network security and bandwidth management system using MikroTik Routerboard devices, grounded in Government Regulation (PP) Number 94 concerning Civil Servant Discipline. The research methodology encompasses network analysis, topology design, implementation, and testing. Implementation results demonstrate that TLS Host-based firewall rules successfully blocked all access to YouTube and TikTok within the ASN work segment. Bandwidth management utilizing the "Simple Queue" feature with a hierarchical method effectively segregated data traffic between the ASN segment and the Public WiFi segment. Quality of Service (QoS) testing revealed significant improvements in network performance: average latency dropped from 185 ms to 32 ms, packet loss decreased from 8.4% to 0.12%, and throughput stabilized at 34.1 Mbps within the ASN segment. This study confirms that integrating firewall capabilities and bandwidth management can optimize data security, stabilize internet connections, and support the enforcement of ASN working-hour discipline at the BKPSDM of Central Sumba Regency.

Keywords: Network Security, Firewall, Bandwidth Management, NDLC, MikroTik.

1. Introduction

Technological advancements require government agencies, such as the BKPSDM of Central Sumba Regency, to maintain a secure and stable computer network to support the management of Civil Servant (ASN) data [1]. However, staff survey results indicate that current internet quality is suboptimal due to frequent slow and unstable connections issues exacerbated by bandwidth consumption for non-work activities like social media (YouTube and TikTok). Although no official circular has been issued, restricting such access is strongly grounded in Government Regulation (PP) Number 94 concerning Civil Servant Discipline, which aims to optimize work productivity. Furthermore, the office WiFi network is considered vulnerable to unauthorized access, posing a threat to the security of confidential ASN data. To address these security concerns and bandwidth distribution imbalances, implementing a firewall to block non-productive sites and employing bandwidth management are essential [2]. Consequently, this research was conducted to enhance network security and internet stability at the BKPSDM of Central Sumba Regency, under the title "Implementation of Network Security and ASN Internet Access Restriction Using Firewalls and Bandwidth Management at the BKPSDM of Central Sumba Regency."

2. Literary Studies

2.1. Computer Networks

A computer network is a collection of two or more computers and supporting equipment interconnected with one another. Computer networks enable users to communicate, share data, and access hardware and software collaboratively within an integrated system. Based on their geographical scope, computer networks are classified into three main types: Local Area Network (LAN), which covers a small area such as an office building; Metropolitan Area Network (MAN), which covers an area within a single city; and Wide Area Network (WAN), which covers a vast area extending across countries [3]

2.2. Firewall

A firewall is a network security system that monitors, filters, and controls data traffic entering or leaving a network based on security rules established by the network administrator [4]. It serves as the first line of defense in protecting the network against external threats and misuse by internal users. Firewalls operate by inspecting every data packet traversing the network and determining whether to allow or deny it based on pre-configured rules. In this study, the firewall is configured using the Layer 7 Protocol feature available on MikroTik routers. Layer 7 Protocol is a filtering method that operates at the application layer of the OSI model, enabling it to identify and block specific applications or websites such as TikTok, YouTube, Instagram, and Facebook based on their data traffic patterns [5]. To enhance blocking effectiveness, administrators can implement firewall rules to restrict the use of specific VPNs employed to bypass internet access policies.

2.3. Bandwidth Management

Bandwidth refers to the capability or capacity of an Ethernet cable to facilitate a specific volume of data packet traffic, typically measured in Mbps or Kbps. Bandwidth management is a method used to regulate the allocation of bandwidth to each client on a network, aiming to ensure equitable bandwidth usage among users [6]. Without effective bandwidth management, one or more users could excessively consume network capacity, resulting in slow and unstable internet connections for other users.

2.3. MikroTik

MikroTik is network hardware utilizing RouterOS an operating system based on open-source UNIX which enables a standard computer to function as a router, firewall, bridge, hotspot, proxy server, and more, even with modest hardware specifications [7]. MikroTik is widely adopted by both government agencies and private organizations due to its affordability, comprehensive feature set, and ease of network configuration and management. RouterOS offers a full suite of networking capabilities, including firewall filtering, bandwidth management via Simple Queue, routing, VPN, hotspot functionality, and various other network security features. In this study, MikroTik serves as the primary device for configuring a Layer 7 Protocol firewall and implementing Simple Queue bandwidth management at the BKPSDM of Central Sumba Regency.

3. Research Method

3.1. Research Location and Time

3.1.1. Research Location

This research was conducted at the Personnel and Human Resources Development Agency (BKPSDM) of Central Sumba Regency, East Nusa Tenggara Province. The BKPSDM office is located within the Central Sumba Regency Government Office Complex in Katiku Tana District, Waibakul. The selection of this location was based on the fact that the agency faces tangible issues regarding internet network performance specifically slow and unstable connections, uncontrolled internet usage by civil servants (ASN), and a weak network security system. The physical condition of the BKPSDM office, which served as the research site, is shown in Figure 3.1 below.



Fig. 1: Central Sumba Regency BKPSDM Office Building

3.1.2. Research Period

This research was conducted at the Personnel and Human Resources Development Agency (BKPSDM) of Central Sumba Regency, East Nusa Tenggara Province. The location was selected due to identified issues regarding network security and uncontrolled internet usage within the agency; consequently, this research aims to provide solutions that can be directly implemented. The research is scheduled to span approximately three months, encompassing the stages of initial observation, planning, system implementation, testing, and results evaluation. A detailed schedule of the research activities is presented in the following table.

Table 1: Research Implementation Schedule

Activity	Month 1 Week 1	Month 1 Week 2-3	Month 1 Week 4	Month 2 Weeks 1-2	Month 2 Week 3-4	Month 3
Observation and Data Collection	✓					
Design and Planning						
Prototype Simulation		✓				

Implementation	✓	✓		
Monitoring and Testing			✓	
Evaluation and Reporting				✓

3.2. Method of collecting data

Data collection for this study employed a mixed-method approach, integrating direct technical observation of the network infrastructure with the distribution of structured questionnaires to civil service staff (ASN) at the BKPSDM of Central Sumba Regency. The questionnaires utilized a Likert scale to assess user perceptions regarding internet service quality (Quality of Service) and the current level of network security.

Based on the results of the staff questionnaires, three key issues were identified that serve as the primary justification for this study:

1. Complaints Regarding Slow and Unstable Internet Connections

The majority of respondents (78%) reported that the office internet connection frequently suffers from sluggish speeds and sudden instability during active working hours (08:00–14:00 WITA). This directly impacts work productivity, as staff often experience delays when accessing and uploading documents to the civil servant (ASN) information system.

2. Bandwidth Drain Due to Non-Productive Usage

Survey results confirm irregular bandwidth usage. A total of 65% of respondents admitted to freely using the office WiFi during working hours to access high-bandwidth entertainment and social media platforms (such as YouTube and TikTok). The absence of access restrictions was identified as the primary cause of bandwidth starvation a competition for capacity that disadvantages other users performing administrative tasks.

3. WiFi Network Security Vulnerabilities

From a security perspective, 82% of respondents consider the current office WiFi security system unreliable and vulnerable to unauthorized access. This is attributed to the use of a shared password without periodic authentication, creating a loophole that allows outsiders in the vicinity of the office to access the BKPSDM network. This situation is deemed to pose a significant risk of potential leaks regarding sensitive ASN (State Civil Apparatus) personnel data.

3.3. Research Flow

This research methodology is systematically designed across four main stages to ensure a focused approach to resolving security and bandwidth management issues at BKPSDM Central Sumba Regency. These stages are illustrated in the following flowchart:

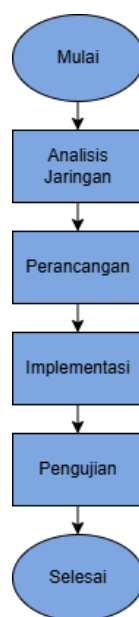


Fig. 2: Research Flow

Description of Research Stages

To clarify the flowchart above, each stage is detailed as follows:

1. Network Analysis Stage (Analysis)

This initial stage focuses on mapping the existing network conditions at BKPSDM. The researcher analyzes available bandwidth capacity, maps user habits via questionnaires, and identifies security vulnerabilities in the office WiFi that have previously caused slow connections due to non-productive usage.

2. Topology & Firewall Rule Design Stage (Design)

In this stage, a new network topology is designed to segregate network segments for civil servants (ASN), public services, and guests. Additionally, firewall rules are formulated (e.g., utilizing Address Lists and Layer 7 Protocols to detect YouTube/TikTok application packets), alongside a fair bandwidth allocation scheme.

3. Implementation Stage (Implementation)

The developed design is subsequently implemented directly on the MikroTik Routerboard at the Central Sumba Regency BKPSDM. This process involves IP address configuration, the creation of packet filtering rules (Filter Rules), and the setup of bandwidth queues to limit download and upload speeds for each user.

4. Testing Stage (Testing)

This is the final stage to validate the system's success. Testing is conducted using two methods: penetration testing (attempting to access restricted sites to verify firewall functionality) and Quality of Service testing (measuring parameters such as delay and throughput during peak loads) to demonstrate that the office internet is now more stable and secure.

3.4. Network Topology

To illustrate the technological infrastructure transition at BKPSDM Central Sumba Regency, the image above presents a visualization of the existing network structure (pre-implementation) alongside the proposed network structure (post-implementation).

1. Analysis of the Existing Topology (Pre-Implementation)

In the existing topology scheme, the internet connection from the Internet Service Provider (ISP) enters via an ISP modem configured in Bridge Mode. Data traffic is forwarded directly to an unmanaged switch hub without any intermediate traffic control device. From the switch hub, the connection is distributed to access points that lack managed security features.

The absence of control functions at this core layer results in several key negative impacts:

- a. **Unfiltered Traffic Bypass:** Data traffic from employee devices (civil servant PCs/laptops) and guest devices (public smartphones) flows directly to the internet without content filtering; consequently, high-bandwidth platforms like YouTube and TikTok can be accessed without restriction during working hours.
- b. **Single Network Segment (Flat Network):** All users reside within the same IP subnet without segmentation, leading to random contention for bandwidth capacity (bandwidth starvation).
- c. **WiFi Security Vulnerability:** The broadcasted wireless signal is open and lacks a periodic authentication system, allowing anyone within range to connect unauthorized and potentially compromise the privacy of civil servant personnel data.

2. Analysis of the Proposed Topology (Post-Implementation)

In the proposed topology scheme, a hardware intervention is implemented by placing a MikroTik Routerboard directly between the ISP modem and the switch hub. This placement establishes the MikroTik device as the primary gateway, as well as the central hub for security (firewall) and capacity allocation (bandwidth management).

The changes in data distribution flow following implementation are as follows:

- a. **Implementation of Firewall Rules:** All data traffic passing through the forwarding chain is strictly filtered. The RouterBoard detects and automatically blocks HTTPS handshake packets destined for TikTok and YouTube servers across all user devices within the BKPSDM environment.
- b. **SSID Segmentation via Managed Access Points:** Access Points are configured to broadcast separate SSIDs (wireless network segmentation). The network is divided into two logical paths: the ASN LAN segment (for official operational use) and the Public WiFi segment (for general public/guest use).
- c. **Hierarchical Bandwidth Management:** The MikroTik device manages data rate (bandwidth) allocation fairly. Users on the ASN LAN segment receive guaranteed priority bandwidth (Limit At) to ensure smooth access to the personnel information system, while users on the Public WiFi segment are subject to a maximum speed cap (Max Limit) to prevent interference with office operations.

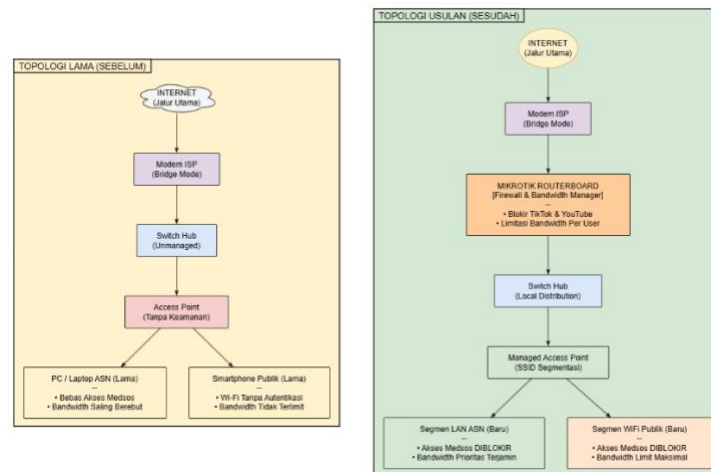


Fig. 3: Analysis of the Proposed Topology

4. Results and Discussion

4.1. Security System Configuration (Firewall)

The implementation of network security and internet access restrictions on the MikroTik Routerboard at BKPSDM Central Sumba Regency utilizes Filter Rules, advanced data packet inspection via Layer 7 Protocols, and TLS Host-based content grouping (to block HTTPS-encrypted traffic for YouTube and TikTok).

The following are the command lines (CLI scripts) implemented on the MikroTik device:

1. Block YouTube and TikTok access using TLS Host & Content

Access restriction is achieved by identifying the TLS domain name (host) when an ASN device attempts an HTTPS encryption handshake with the entertainment platform's servers.

```
# DEFINISI ATURAN BLOKIR YOUTUBE

/ip firewall filter
add chain=forward action=drop protocol=tcp dst-port=443 tls-host=*youtube.com* \
comment="Blokir Akses YouTube via HTTPS (ASN)"
add chain=forward action=drop protocol=tcp dst-port=443 tls-host=*googlevideo.com* \
comment="Blokir Stream Video YouTube"
add chain=forward action=drop content="youtube.com" \
comment="Blokir Konten HTTP YouTube"

# DEFINISI ATURAN BLOKIR TIKTOK
|
add chain=forward action=drop protocol=tcp dst-port=443 tls-host=*tiktok.com* \
comment="Blokir Akses Web TikTok"
add chain=forward action=drop protocol=tcp dst-port=443 tls-host=*byteoversea.com* \
comment="Blokir Server Konten Video TikTok (Aplikasi)"
add chain=forward action=drop content="tiktok.com" \
comment="Blokir Konten HTTP TikTok"
```

Fig. 4: Code to block access to YouTube and TikTok

2. Securing the Internal Network Against Unauthorized Access

To secure the router and restrict unauthorized access to management systems (such as Winbox and Webfig) from external users or public Wi-Fi, the following filtering rule policies are implemented:

```
# PROTEKSI ROUTER & PENGAMANAN LAYANAN MIKROTIK
|
# Membuat daftar alamat IP (Address List) khusus untuk admin/staf IT
/ip firewall address-list
add address=192.168.10.2-192.168.10.5 list=IP_Admin_BKPSDM

# Aturan menyaring akses ke Router (Chain Input)
/ip firewall filter
add chain=input action=accept src-address-list=IP_Admin_BKPSDM \
comment="Izinkan akses konfigurasi hanya untuk IP Admin"
add chain=input action=drop protocol=tcp dst-port=21,22,23,80,8291 \
comment="Blokir semua akses Winbox/Webfig/SSH dari luar IP Admin"

# Menahan serangan brute-force pada port Winbox (8291)
add chain=input action=drop protocol=tcp dst-port=8291 connection-state=new \
src-address-list=Blacklist_Attack comment="Blokir IP Penyerang"
```

Fig. 5: Internal Network Security Code from Unauthorized Access

4.2 Bandwidth Management (QoS) Configuration

In this study, bandwidth management is implemented using the Simple Queue method on MikroTik RouterOS. The bandwidth allocation policy is designed hierarchically (utilizing the Parent-Child Queue concept) to strictly separate access rights for Civil Servants (ASN) from those for Public Services (Public WiFi). The total dedicated bandwidth subscribed to from the ISP by BKPSDM Central Sumba Regency is 50 Mbps. The proposed bandwidth capacity allocations are defined in the following table:

Table 2. Bandwidth capacity allocation

User Category	Target Limit (IP Subnet)	Maximum Limit (Max Limit - Upload/Download)	Guaranteed Bandwidth (Committed Rate – Upload/Download)	Traffic Priority
Parent Queue	192.168.0.0/16	50 Mbps / 50 Mbps	50 Mbps / 50 Mbps	-
Civil Servant Segment (Wired & Secure WiFi)	192.168.10.0/24	35 Mbps / 35 Mbps	20 Mbps / 20 Mbps	1 (Highest)
Service Segment / Public WiFi	192.168.20.0/24	15 Mbps / 15 Mbps	5 Mbps / 5 Mbps	8 (Lowest)

Skip Perintah CLI MikroTik untuk Queue:

```
# KONFIGURASI QUEUE TREE / SIMPLE QUEUE HIERARKIS

/queue simple
add name="Total_Bandwidth" target=192.168.0.0/16 max-limit=50M/50M \
comment="Parent Limit Total ISP"

add name="Segmen_ASN" target=192.168.10.0/24 parent="Total_Bandwidth" \
limit-at=20M/20M max-limit=35M/35M priority=1/1 \
comment="Alokasi Prioritas Utama ASN"

add name="Segmen_Publik" target=192.168.20.0/24 parent="Total_Bandwidth" \
limit-at=5M/5M max-limit=15M/15M priority=8/8 \
comment="Alokasi Terlimit WiFi Publik"
```

Fig. 6: MikroTik CLI Command Script for Queue

4.3 Analysis of Security Testing Results (Firewall)

Testing was conducted using a direct client-side testing method to evaluate the effectiveness of port filtering rules and the blocking of social media domains (YouTube & TikTok).

Table 3. Security Testing Results (Firewall)

Test Scenario Parameters	Conditions Before the Firewall Was Implemented	Conditions After the Firewall Is Implemented	Status Uji
Access YouTube Web & App	It opens smoothly, and the video resolution automatically selects Full HD (1080p).	Connection failed (timeout); the application status remains stuck on loading.	Succeed
Access TikTok Web & App	FYP video content plays smoothly without any interruptions (buffering).	Connection refused (Connection reset); the video failed to load data.	Succeed
Port Scanning & Vulnerability Scanning	The Winbox (8291) and Webfig (80) ports appear open from anywhere..	The Winbox and Webfig ports appear as Filtered/Closed when accessed from outside the Admin IP.	Succeed
Brute Force Attack Simulation (SSH/Winbox)	The router is receiving thousands of login requests that are driving CPU usage up to 90%.	The attacker's IP is immediately blacklisted after three failed attempts; CPU usage remains stable at <15%.	Succeed

Analysis: The implementation of TLS Host Filtering for HTTPS successfully intercepted the cryptographic key negotiation (handshake) process between user devices and TikTok and YouTube servers. This demonstrates that security measures not only protect infrastructure but also safeguard the productivity of civil servants during working hours.

4.4. Analysis of Bandwidth Stability (QoS) Results

To objectively evaluate network performance before and after bandwidth management optimization, Quality of Service (QoS) parameters were measured based on the ITU-T G.1010 standard using Wireshark software during active working hours (peak load).

Table 4. Comparison of QoS Performance Metrics

QoS Test Parameters	Before Optimization (Without Queuing)	After Optimization (Implementation of Simple Queue)	ITU-T Index Standard	Category
Throughput	9.4 Mbps (Stable for Civil Servants)	34.1 Mbps (Stable for Civil Servants)	> 2.1 Mbps	Very good
Delay / Latency	185 ms	32 ms	< 150 ms	Very good
Packet Loss	8.4%	0.12%	< 1%	Very good

5. Conclusion

Based on the analysis, design, implementation, and testing conducted at the BKPSDM of Central Sumba Regency, it can be concluded that implementing bandwidth allocation management using the Simple Queue method on MikroTik RouterOS significantly improved network quality. This is evidenced by test results showing a drastic reduction in average latency from 185 ms to 32 ms, a decrease in packet loss from 8.4% to 0.12%, and an increase in data traffic stability (throughput), reaching 34.1 Mbps within the Civil Servant (ASN) segment. Furthermore, security effectiveness improved markedly through the application of Firewall Filter Rules and TLS Host-based HTTPS filtering on the MikroTik router, which successfully blocked all access to non-productive entertainment platforms such as YouTube and TikTok for the ASN workforce. These protective measures were reinforced by restricting Winbox and Webfig access to registered administrator IP addresses, thereby minimizing the risk of unauthorized access from outside the network. From a non-technical perspective, these internet traffic restrictions serve as a highly effective tool for enforcing working-hour discipline among employees. The traffic management policy aligns structurally with Government Regulation (PP) Number 94 regarding Civil Servant Discipline. Consequently, the integration of these security systems and access restrictions not only optimizes local network infrastructure performance but also directly supports increased productivity and improved public service quality within the BKPSDM of Central Sumba Regency.

Referensi

- [1] S. Nurul, S. Anggrainy, and S. Aprelyani, "FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI : KEAMANAN INFORMASI , TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM)," vol. 3, no. 5, pp. 564–573, 2022.
- [2] H. Gunawan, "sebuah profil dan jaringan personal yang dapat menghubungkan mereka dengan pengguna kemampuan yang baik dalam melakukan praktik keamanan pada saat menggunakan situs jejaring internet dan memahami arti penting melindungi data pribadi dan atau data kelompok atas nama," vol. 5, no. 1, pp. 1–8, 2021.
- [3] S. A. Imawan and S. Dwiasnati, "Implementasi Pemblokiran Situs Dengan Firewall Layer 7 Protocol Menggunakan Metode Ndlc Pada Router Mikrotik," *Multinetics*, vol. 11, no. 1, pp. 22–34, 2025, doi: 10.32722/multinetics.v11i1.6844.
- [4] F. Prasetyo, E. Putra, A. Hamzah, W. Agel, and R. O. F. Kusuma, "Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking," vol. 5, no. 4, pp. 82–87, 2024, doi: 10.60083/jsisfotek.v5i4.329.
- [5] I. Gunawan *et al.*, "KEAMANAN JARINGAN WLAN DENGAN METODE FIREWALL FILTER ING MENGGUNAKAN MIKROTIK PADA SMP NEGERI 1 DOLOK MERAWAN," vol. 2, no. 3, 2022.
- [6] A. P. Sari, P. M. Aziz, and R. Nasution, "MANAJEMEN BANDWIDTH DENGAN METODE HIERARCHICAL TOKEN BUCKET (HTB) PADA LEMBAGA AMIL ZAKAT NURUL HAYAT TANGERANG," pp. 145–151, 2021.
- [7] J. Barri, "Implementasi Firewall Filtering Menggunakan Mikrotik Pada Jaringan Internet Kantor Camat Lamasi," *SINTA J. Sist. Inf. dan Teknol. Komputasi*, vol. 2, pp. 195–203, 2025.