International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 15, No. 7, July, 2025, pp. 1493-1500
Journal homepage: http://iieta.org/journals/ijsse

Application of RPZ-Based DNS Filtering in Educational Network Security

Aries Maesya*, Victor Ilyas Sugara, Azi Heris Saputra

Department of Computer Science, Faculty of Mathematics and Natural Sciences, Pakuan University, Bogor 16143, Indonesia

Corresponding Author Email: a.maesya@unpak.ac.id

https://doi.org/10.18280/ijsse.150716

Received: 15 April 2025
Revised: 20 May 2025
Accepted: 28 June 2025
Available online: 31 July 2025

Keywords:
RPZ, DNS filtering, DNS filtering efficiency, network security, educational networks

ABSTRACT

This study examines the implementation of the Response Policy Zone (RPZ) method for Domain Name System (DNS) filtering at Pakuan University, aiming to improve the efficiency and accuracy of blocking harmful content, including pornography and misinformation. RPZ enables predefined rules to control DNS responses to known malicious domains. Although RPZ has been widely adopted in various environments, its application within the Positive DNS Filtering Slave Trust framework at Pakuan University remains underutilized. This research adopts the Network Development Life Cycle (NDLC) methodology, which includes analysis, design, simulation, implementation, monitoring, and management. The effectiveness of the implementation was assessed through a questionnaire distributed to 362 respondents, consisting of 253 students, 48 lecturers, and 61 administrative staff. The Likert scale analysis revealed that 82.32% of respondents rated the system as "very effective." These findings demonstrate that the RPZ-based DNS filtering system significantly improves network security within educational environments.

1. INTRODUCTION

Although the Response Policy Zone (RPZ) method has been widely implemented in various environments, its application to Positive DNS Slave Trust filtering at Pakuan University remains underutilized. Therefore, this study investigates the implementation of the RPZ method in DNS filtering at Pakuan University, focusing specifically on the concept of Positive DNS Filtering Slave Trust and its potential to enhance efficiency and accuracy in managing harmful online content.

Related to this issue, several researchers have conducted studies on DNS filtering using the RPZ method [1]. For instance, Muhlison and Kusnawi [2] explored RPZ-based DNS filtering to reduce client exposure to harmful content using router-based configurations. Similarly, another study [3] utilized Mikrotik Routerboard-based filtering to restrict access to harmful content through Open DNS. While these approaches have shown practical value, they tend to rely on localized, manual configurations and offer limited synchronization capabilities. In contrast, this study presents a novel application of the RPZ method in an educational environment by integrating it with the Positive DNS Slave Trust system, which the Indonesian Ministry of Communication and Information authorizes. This centralized integration allows automated policy updates, improved scalability, and better consistency in DNS filtering. The proposed approach offers significant improvements over traditional methods, particularly in large-scale institutional networks, such as universities. The case study at Pakuan University aims to demonstrate how this architecture can enhance both the efficiency and accuracy of DNS filtering in real-world academic settings [4].

Previous research has also identified several limitations in existing systems [5]. For instance, Recursive DNS software typically acts only as a temporary DNS cache, making it less suitable for long-term policy enforcement. Such constraints make development and scalability difficult, especially in environments where content filtering must be consistent and continuously updated. Implementing the Positive DNS Trust system through RPZ at Pakuan University addresses these limitations by offering a more robust and scalable DNS filtering mechanism.

This case study aims to provide a deeper understanding of how implementing a DNS server with the RPZ method operating as a Slave of the Positive DNS Trust maintained by the Ministry of Communication and Information of the Republic of Indonesia can help Pakuan University block unwanted and harmful content effectively.

2. LITERATURE REVIEW

2.1 DNS

DNS is a hierarchical and distributed naming system that translates human-readable domain names into numerical IP addresses, which are required for locating and identifying devices on the Internet or local networks [6]. It serves as the backbone of the modern Internet, enabling seamless access to websites, applications, and services through domain names rather than complex IP addresses.

DNS serves as a critical component of the Internet infrastructure, operating as a globally distributed database that resolves queries based on the TCP/IP protocol. Through this mechanism, DNS allows users to access network resources by mapping hostnames to IP addresses and vice versa [7]. The performance and security of DNS directly influence the reliability and safety of online communications, making DNS management a crucial aspect of network administration [8].

Furthermore, advancements in DNS technologies such as DNS over HTTPS (DoH) and DNSSEC have introduced additional layers of privacy and authentication to counter threats like spoofing and cache poisoning, thereby enhancing trust in Internet usage [9].

2.2 Berkeley Internet Name Domain

The Berkeley Internet Name Domain (BIND9) is one of the most widely adopted DNS server software systems globally. It is recognized for its flexibility, extensibility, and reliability in managing domain name resolution tasks. BIND9 offers a comprehensive set of features for configuring authoritative and recursive DNS servers, including support for *Split DNS*, zone transfers, access control lists (ACLs), and dynamic updates. BIND9 (version 9) is designed to be cross-platform and is compatible with various operating systems, including Linux, UNIX, and Windows. It supports an extensive range of DNS record types, including A, AAAA, CNAME, MX, NS, SOA, and others, which are essential for mapping domain names to services and ensuring DNS reliability. Recent studies, such as the study [10], highlight the continued relevance of BIND9 in educational and enterprise networks due to its configurability and ability to integrate with advanced security extensions, including Response Policy Zone (RPZ) and DNSSEC. These capabilities make it a preferred choice for institutions aiming to implement robust and customizable DNS infrastructures [11].

2.3 RPZ

RPZ is a mechanism that empowers DNS server administrators to define custom policies for permitting or blocking specific domain queries. It functions by rewriting DNS responses based on preconfigured rules, thereby allowing administrators to filter both harmful and permitted content dynamically [12].

RPZ is typically deployed within recursive DNS servers and has become a standard in DNS-based content filtering. It allows institutions to maintain blocklists or allowlists of domains, enabling them to selectively control internet access at the DNS level [7]. RPZ enhances the scalability and automation of DNS filtering systems by enabling centralized control with policy updates that can be pushed in real time. Without RPZ, DNS servers would resolve all requests indiscriminately, potentially allowing users to access malicious or inappropriate websites. The integration of RPZ provides an effective and efficient means to implement content governance and cybersecurity policies within network infrastructures, particularly in educational and organizational environments [11, 13, 14].

2.4 Trust positif

"Trust Positif" is an initiative launched by the Ministry of Communication and Information Technology of the Republic of Indonesia (Kominfo RI) in 2021 to foster a safer, more positive, and responsible digital environment. The initiative operates by managing a centralized blocklist of domains containing harmful content, such as pornography, violence, gambling, and misinformation. These domains are distributed to participating institutions through DNS synchronization mechanisms, particularly using the Response Policy Zone (RPZ) method.

The implementation of *Trust Positif* [15] via RPZ significantly enhances network security infrastructure in educational environments by enabling real-time blocking of malicious websites. Moreover, the initiative aligns with national policies on digital literacy and internet governance, supporting institutions in complying with state-mandated content regulation frameworks [16]. Initiated in 2021, this movement aims to:

1. Improve digital literacy in society.
2. Counter harmful content on the internet.
3. Encourage responsible internet use.

2.5 Local Area Network

A Local Area Network (LAN) is a type of computer network that interconnects devices within a limited geographic area, such as a classroom, office building, campus, or internet café. LANs are widely used in organizational and educational environments to facilitate resource sharing, file transfers, and internal communication. High data transfer rates, low latency, and centralized management are typically the characteristics of LANs. Their design and efficiency are heavily influenced by network topology, including star, bus, ring, and mesh configurations [17]. Selecting the appropriate topology is crucial to ensuring optimal network performance, minimizing downtime, and enhancing scalability. Modern LAN implementations also integrate security protocols, VLAN configurations, and wireless access points to accommodate flexible and secure connectivity, particularly in academic and enterprise settings.

2.6 *Ping*

The *ping* command is a fundamental network diagnostic tool developed in 1983 by Mike Muuss. It was designed to test the reachability of a host on an Internet Protocol (IP) network and to measure round-trip time for messages sent from the originating host to a destination device. By sending ICMP (Internet Control Message Protocol) echo request packets and receiving echo replies, *ping* helps determine whether a networked device is online and how long it takes to communicate with it. It is commonly used by system administrators and network engineers to troubleshoot connectivity issues and to assess network latency or packet loss. One typical response from the *ping* command, “Destination Host Unreachable,” indicates that the host, IP address, or route is currently inaccessible or does not exist in the routing table. As emphasized [11], tools like *ping* remain essential in diagnosing basic network failures even in advanced enterprise or cloud-based infrastructures [18].

2.7 Nslookup

Name Server Lookup (Nslookup) is a command-line utility used to query the Domain Name System (DNS) for information related to domain names and IP addresses. It is commonly used by system administrators, network engineers, and cybersecurity analysts to troubleshoot DNS resolution issues and verify DNS configurations [11, 19]. The tool allows users to perform the following operations:

1. Look up the IP address of a domain name.
2. Retrieve the domain name from an IP address.
3. Access additional DNS record information, such as MX and CNAME records.

2.8 Likert scale

The Likert Scale is a psychometric scale commonly used in questionnaires and is the most widely used scale in survey research. It includes two types of questions: positive questions to assess positive interest and negative questions to assess negative interest. Positive statements are scored 4, 3, 2, 1, while negative ones are scored in reverse: 1, 2, 3, 4. Response options typically include "strongly agree", "agree", "disagree", and "strongly disagree" [20].

3. RESEARCH METHODS

This study employs the Network Development Life Cycle (NDLC) methodology, which comprises six stages: Analysis, Design, Simulation, Implementation, Monitoring, and Management [7]. The Network Development Life Cycle (NDLC) method is illustrated in Figure 1.

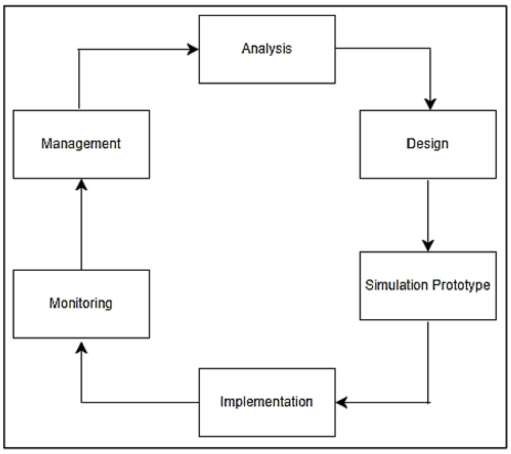


Figure 1. The NDLC (Network Development Life Cycle)

Each stage is described in detail as follows:

3.1 Analysis stage

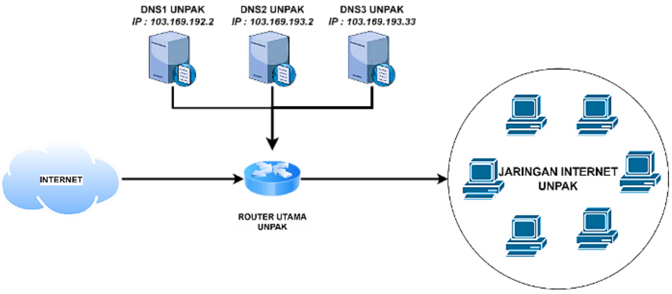
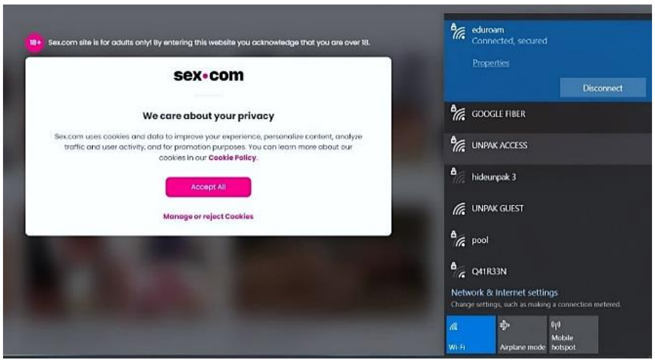


Figure 2. Current network topology

The analysis began by identifying the existing DNS system at Pakuan University's inability to filter harmful content effectively. Network vulnerabilities and the absence of a synchronized filtering mechanism with external trusted sources were documented. The current network topology is illustrated in Figure 2.

Unpak DNS cannot yet filter harmful content spread on UNPAK's Internet, as shown in Figure 3.


18+ Sex.com site is for adults only! By entering this website you acknowledge that you are over 18.

We care about your privacy

Sex.com uses cookies and data to improve your experience, personalize content, analyze traffic and user activity, and for promotion purposes. You can learn more about our cookies in our Cookie Policy.

Network & Internet settings
Change settings, such as making a connection metered.

Figure 3. Access to pornographic content

3.2 Design stage

During the design phase, filtering rules were defined based on domain classifications categorized by the Ministry of Communication and Information (Kominfo). These rules included domains related to pornography, gambling, hoaxes, and other harmful content. The design also included configuring zone transfer settings to enable synchronization between the Pakuan University DNS server and the Positive DNS Trust maintained by Kominfo.

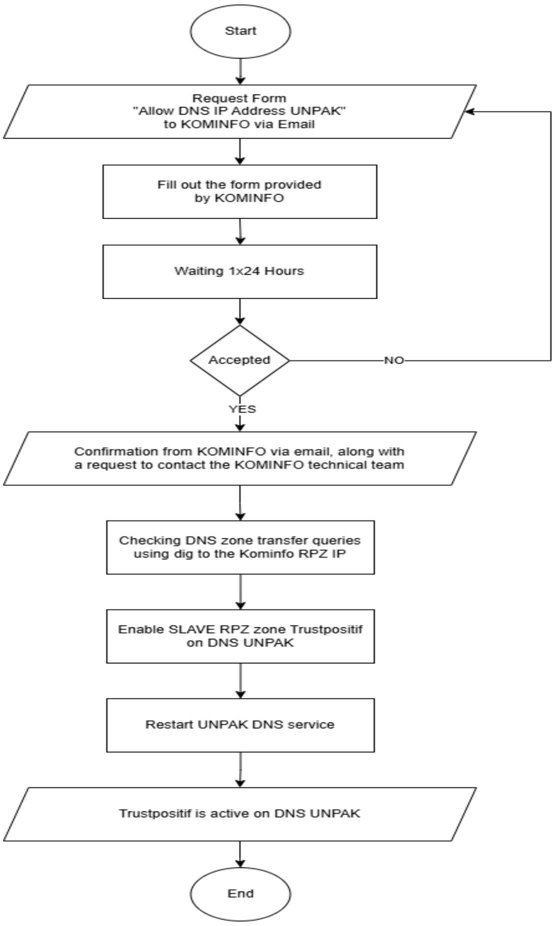

Start
Request Form "Allow DNS IP Address UNPAK" to KOMINFO via Email
Fill out the form provided by KOMINFO
Waiting 1x24 Hours
Accepted
NO
YES
Confirmation from KOMINFO via email, along with a request to contact the KOMINFO technical team
Checking DNS zone transfer queries using dig to the Kominfo RPZ IP
Enable SLAVE RPZ zone Trustpositif on DNS UNPAK
Restart UNPAK DNS service
Trustpositif is active on DNS UNPAK
End

Figure 4. Flowchart synchronization with DNS UNPAK

A detailed synchronization plan was developed, involving steps such as sending IP allowlisting requests to Kominfo, configuring zone files using BIND9 on the Ubuntu DNS server, and defining RPZ zones (e.g., trustpositifkominfo and blocklist.rpz). This ensured automated replication of trusted domains and manual addition of institution-specific blocklists. The Synchronization Flowchart with UNPAK DNS is shown in Figure 4.

Figure 4 explains how the synchronization process of the positive DNS Trust of the Republic of Indonesia Ministry of Communication and Informatics with the UNPAK DNS, starting from making a request form to allow the IP address of the Pakuan University DNS to the positive DNS Trust of the Republic of Indonesia Ministry of Communication and Informatics via email, which will then reply to and a link will be sent to the Form for the RPZ Kominfo connection request to be filled in according to the required data.

Figure 5 illustrates how the DNS server, utilizing the Response Policy Zone (RPZ) method, operates on the Pakuan University internet network as a filter for harmful content. This occurs when internet users at Pakuan University enter a URL in their browser to access a particular site.

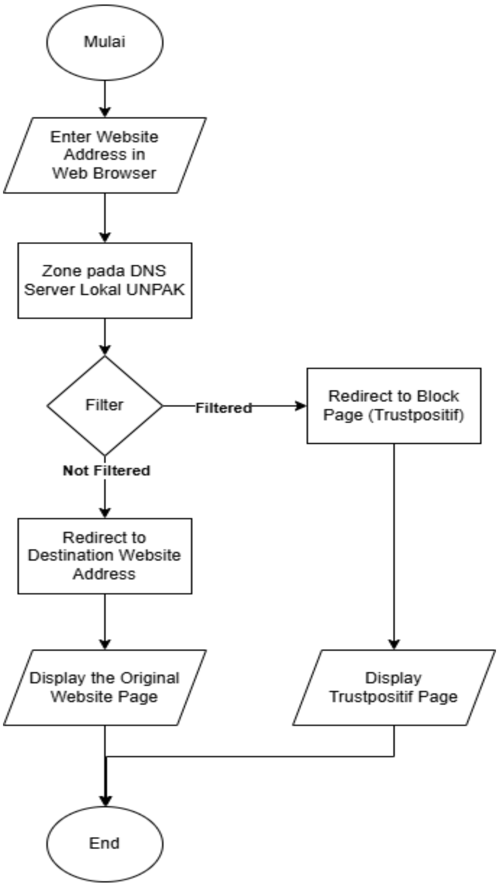

Mulai
Enter Website Address in Web Browser
Zone pada DNS Server Lokal UNPAK
Filter
Filtered
Redirect to Block Page (Trustpositif)
Not Filtered
Redirect to Destination Website Address
Display the Original Website Page
Display Trustpositif Page
End

Figure 5. DNS filtering flowchart with RPZ method

The Pakuan University DNS server becomes a positive trust Master DNS for filtering using the RPZ method. This method begins by activating the Positive Trust Zone Master on the Pakuan University DNS server and then populating the list of domains that the Pakuan University DNS will block (Figure 6).

Figure 7 explains how to report domains containing harmful content to the positive trust of the Indonesian Ministry of Communication and Information so that they can block them via the aduankonten.ID website. It starts by registering an account to access the aduankonten. Visit the ID website page, verify the registered account by checking the registered email, and then log in to the Aduankonten—ID website to report the domain that will be blocked.

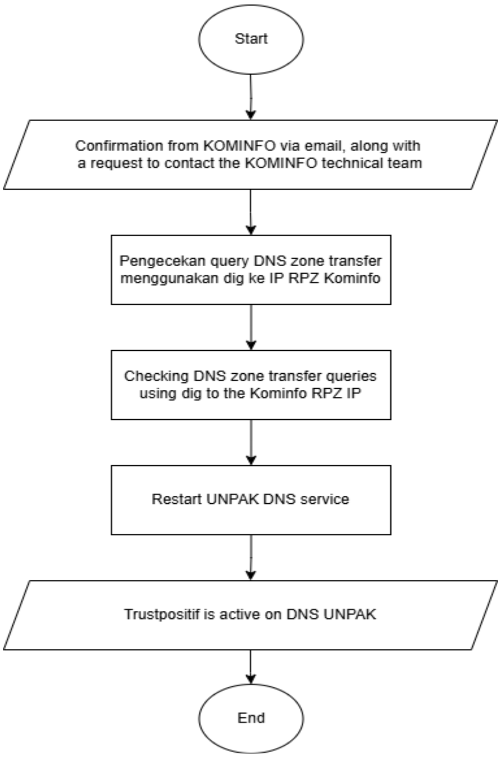

Start
Confirmation from KOMINFO via email, along with a request to contact the KOMINFO technical team
Pengecekan query DNS zone transfer menggunakan dig ke IP RPZ Kominfo
Checking DNS zone transfer queries using dig to the Kominfo RPZ IP
Restart UNPAK DNS service
Trustpositif is active on DNS UNPAK
End

Figure 6. Positive master trust flowchart in DNS UNPAK

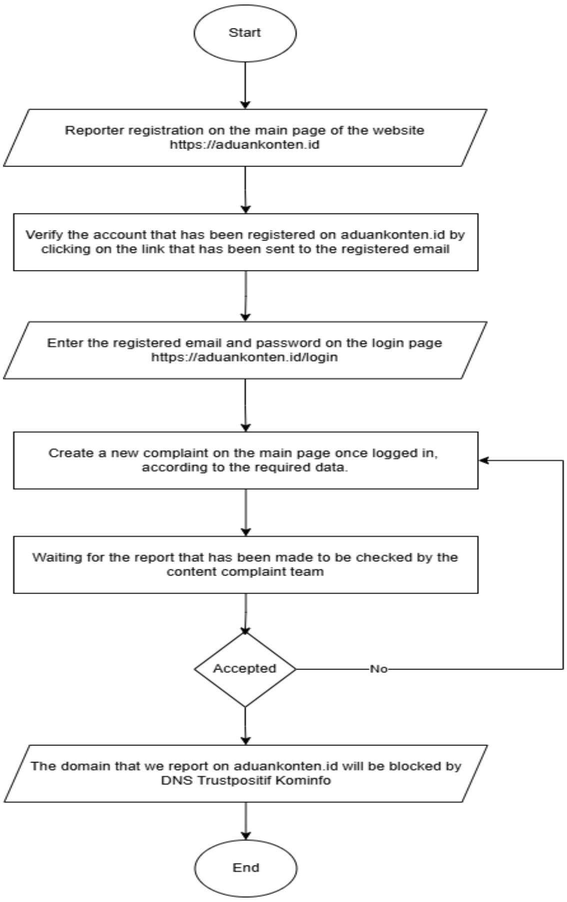
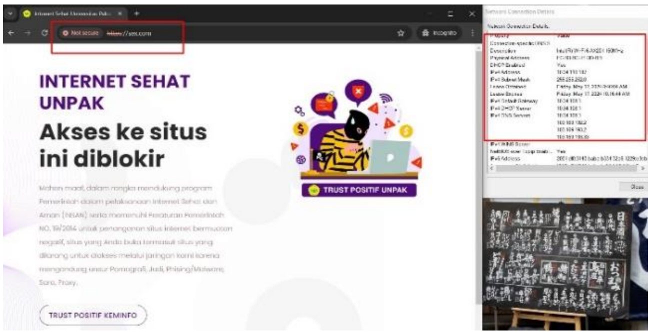

Start
Reporter registration on the main page of the website https://aduankonten.id
Verify the account that has been registered on aduankonten.id by clicking on the link that has been sent to the registered email
Enter the registered email and password on the login page https://aduankonten.id/login
Create a new complaint on the main page once logged in, according to the required data.
Waiting for the report that has been made to be checked by the content complaint team
Accepted
No
The domain that we report on aduankonten.id will be blocked by DNS Trustpositif Kominfo
End

Figure 7. Flowchart of domains to be blocked via content complaints

3.3 Simulation stage

Before full deployment, a controlled simulation was conducted on the university's LAN at the Information and Communication Technology Center (PUTIK). This stage tested the effectiveness of rule enforcement and ensured stability in a limited environment (Figure 8).



Not secure https://sex.com

INTERNET SEHAT UNPAK

Akses ke situs ini diblokir

Mohon maaf, dalam rangka mendukung program Pemerintah dalam pelaksanaan Internet Sehat dan Aman (INSAN) serta memenuhi Peraturan Pemerintah NO. 19/2014 untuk penanganan situs internet bermuatan negatif, situs yang Anda buka termasuk situs yang dilarang untuk diakses melalui jaringan kami karena mengandung unsur Pornografi, Judi, Phising/Malware, Sara, Proxy.

Figure 8. Negative content testing on the network at PUTIK

3.4 Implementation stage

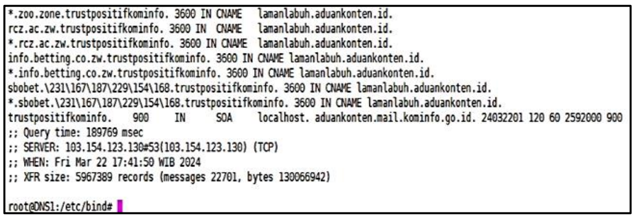
After a successful simulation, the RPZ-based DNS configuration was deployed across the university-wide network. The DNS server was synchronized with the central Kominfo trust zone, and zone transfers were monitored to verify consistent updates.

3.4.1 Checking Kominfo's positive DNS trust query

After contacting the technical team of the Indonesian Ministry of Communication and Information, you will be asked to perform a DNS zone transfer query check on the Indonesian Ministry of Communication and Information's positive trust DNS server, whether it has been successfully synchronized with the Pakuan University DNS server, by entering the following command:

# dig AXFR @103.154.123.130 trustpositifkominfo +noidnout

The above command is executed on the DNS Server of Pakuan University, which uses the Ubuntu Server 22.04 LTS operating system with the DNS server application BIND9. If it is successfully synchronized with the Kominfo positive DNS Trust, information will appear as in Figure 9.



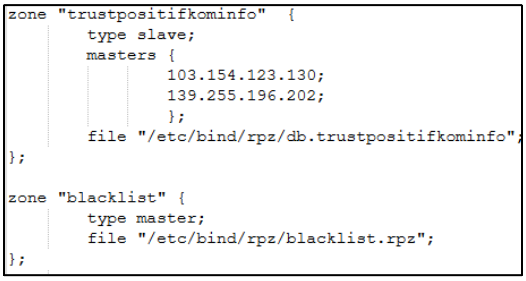
```
*.zoo.zone.trustpositifkominfo. 3600 IN CNAME   lamanlabuh.aduankonten.id.
rcz.ac.zw.trustpositifkominfo. 3600 IN  CNAME   lamanlabuh.aduankonten.id.
*.rcz.ac.zw.trustpositifkominfo. 3600 IN CNAME  lamanlabuh.aduankonten.id.
info.betting.co.zw.trustpositifkominfo. 3600 IN CNAME lamanlabuh.aduankonten.id.
*.info.betting.co.zw.trustpositifkominfo. 3600 IN CNAME lamanlabuh.aduankonten.id.
sbobet.\231\167\187\229\154\168.trustpositifkominfo. 3600 IN CNAME lamanlabuh.aduankonten.id.
*.sbobet.\231\167\187\229\154\168.trustpositifkominfo. 3600 IN CNAME lamanlabuh.aduankonten.id.
trustpositifkominfo.    900     IN      SOA     localhost. aduankonten.mail.kominfo.go.id. 24032201 120 60 2592000 900
;; Query time: 189769 msec
;; SERVER: 103.154.123.130#53(103.154.123.130) (TCP)
;; WHEN: Fri Mar 22 17:41:50 WIB 2024
;; XFR size: 5967389 records (messages 22701, bytes 130066942)

root@DNS1:/etc/bind#
```

Figure 9. UNPAK DNS server synchronization process

In Figure 9 above, you can see that when you execute the command # dig AXFR @103.154.123.130 trustpositifkominfo +noidnout on the Pakuan University DNS server, a display will appear indicating that the Kominfo positive trust DNS server and the Pakuan University DNS server have been successfully synchronized.

3.4.2 Activating positive trust zone and blocklist

Successful synchronization between the Kominfo positive trust DNS server and the Pakuan University DNS server has been achieved. The next step is to activate the positive trust RPZ zone and Blacklist on the Pakuan University DNS server to store negative content data on the UNPAK DNS Server.



```
zone "trustpositifkominfo"  {
        type slave;
        masters {
                103.154.123.130;
                139.255.196.202;
                };
        file "/etc/bind/rpz/db.trustpositifkominfo";
};

zone "blacklist" {
        type master;
        file "/etc/bind/rpz/blacklist.rpz";
};
```

Figure 10. Adding zones to the UNPAK DNS server

In Figure 10, to add a positive trust zone and a Blacklist zone to the Pakuan University DNS server in the BIND9 application, you can add a script to the /etc/bind/named.conf.local file as in Figure 10 by creating a positive trust zone with the slave type whose master destination is the IP address of the Kominfo positive trust controller DNS server, namely 103.154.123.130 and 139.255.196.202, with the file destination to store a copy of the positive trust domain from the Kominfo DNS server in /etc/bind/rpz/db.trustpositifkominfo and the Blacklist zone with the master type with the file destination to store the domain to be blocked in /etc/bind/rpz/blocklist.rpz.

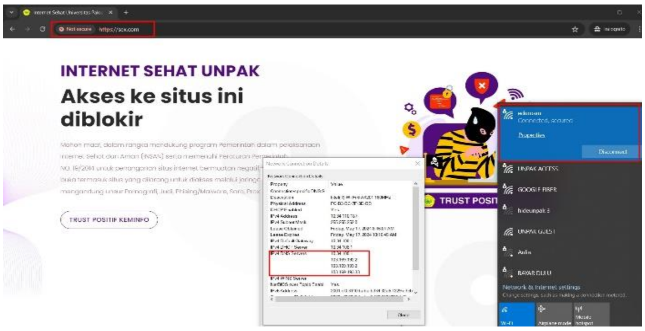
3.5 Monitoring and management

The system was continuously monitored to track blocking accuracy and synchronization reliability. DNS logs and access reports were analyzed, and a feedback loop was established to refine filtering rules and address any access anomalies. The management plan includes regular audits and the potential integration of DNS over HTTPS (DoH) for enhanced security.

This detailed NDLC-based methodology ensures a structured and secure approach to implementing RPZ in an educational environment.

4. DISCUSSION OF RESULTS

Implementation of the Response Policy Zone (RPZ) Method on DNS Filtering Slave Trust Positif KOMINFO RI based on the analysis and configuration described in Chapter 4. To check pornographic content, see Figure 11.



Not secure https://sex.com

INTERNET SEHAT UNPAK

Akses ke situs ini diblokir

Mohon maaf, dalam rangka mendukung program Pemerintah dalam pelaksanaan Internet Sehat dan Aman (INSAN) serta memenuhi Peraturan Pemerintah NO. 19/2014 untuk penanganan situs internet bermuatan negatif, situs yang Anda buka termasuk situs yang dilarang untuk diakses melalui jaringan kami karena mengandung unsur Pornografi, Judi, Phising/Malware, Sara, Proxy.

Figure 11. DNS RPZ pornography content check

4.1 Validation test

A total of 362 respondents participated in the validation survey, including 253 students (69.9%), 48 lecturers (13.3%), and 61 administrative staff (16.8%). The evaluation used a Likert scale ranging from 1 (Very Ineffective) to 5 (Very Effective).

The questionnaire results were processed using Likert scale calculations. Scores were made on a scale of 1 to 5. For calculations using the Likert scale, see Table 1.

Table 1. Questionnaire results

Answer	Score	Maximum Score (Score × Number of Respondents)
VE: Very Effective	5	133
QE: Quite Effective	4	150
E: Effective	3	71
LE: Less Effective	2	4
VI: Very Ineffective	1	4

Formula: T x Pn

T = Total number of respondents who chose

Pn = Select the Likert score number

1. 1. Very Effective Respondents (5 Score): 133 * 5 = 665
2. Respondents are Quite Effective (4 Scores): 150 * 4 = 600
3. 3. Effective Respondent (3 Score): 71 * 3 = 213
4. Less Effective Respondents (2 Scores): 4 * 2 = 8
5. 5. Respondents are Very Ineffective (1 Score): 4 * 1 = 4
6. All results are added up, total score = 1.490

Assessment interval

1. Index 0% - 19.99% : Very Ineffective
2. Index 20% - 39.99% : Less Effective
3. Index 40% - 59.99%: Effective
4. Index 60% - 79.99%: Quite Effective
5. Index 80% - 100% : Very Effective

Interpretation of calculation scores

To obtain the interpretation result value, you must first know the highest score (x) and the lowest score (y) for the assessment item using the following formula :

Y: Highest Likert Score * Number of Respondents

X: Lowest Likert Score * Number of Respondents

“Very Effective “ = 5 * 362 = 1,810

“Very Ineffective “ = 1 * 362 = 362

Index Formula % = Total Score / Y * 100

Index Formula % = $\frac{1490}{1810}$ * 100 = 82.32%

The questionnaire, using a Likert scale calculation, obtained a result of 82.32%, indicating that the assessment interval fell within the Very Effective index in filtering harmful content on the Internet at Pakuan University. Based on the percentage of questionnaires that had participated in filling out as many as 362 responses, consisting of students, lecturers, and employees, as shown in Figure 12.

The overall effectiveness score reached 82.32%, placing the system in the "Very Effective" category. However, when analyzing feedback across different user groups, distinct variations emerged:

•Administrative staff provided the most consistent positive feedback, with over 85% rating the system as very effective. This group likely benefited the most from reduced exposure to harmful websites during their daily operations.

•Lecturers showed a slightly lower effectiveness rating, with around 78% selecting "Very Effective". Some of their written feedback indicated that occasional access delays may have affected their browsing experience.

•Students, while still rating the system positively, showed the widest range of responses. Approximately 76% rated the system as very effective, while a minority (about 10%) expressed concern over blocked access to non-malicious sites, indicating the need for fine-tuning the filtering list.

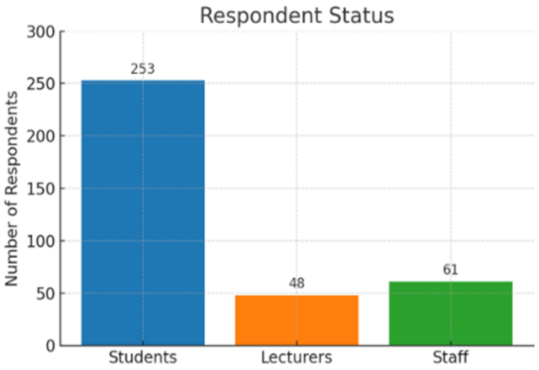


Figure 12. Percentage chart of respondent status

These group-based insights suggest that the RPZ method is highly effective for institutional control and administration; however, improvements can still be made to serve academic and learning needs better. Tailoring access policies by user role and allowing request-based allowlist options may further improve user satisfaction and system performance.

4.2 Harmful content resolve time test

Negative content resolution time testing to test DNS resolution time for harmful content that has just been added to smartphone devices, laptops, and PCs within the Pakuan University network. DNS Server is a key part of the internet infrastructure that converts domain names to their associated IP Addresses. Harmful content refers to domains that Pakuan University DNS blocks. Pakuan University's network uses special software. As presented in Table 2.

Despite its advantages, implementing RPZ-based DNS filtering in complex network environments presents several limitations. Key challenges identified in this study include:

Scalability in high-traffic networks: As the number of DNS queries increases, the DNS server may experience delays or performance degradation if not properly optimized or distributed. This can be problematic in environments with thousands of concurrent users.

Synchronization dependency: The reliability of the filtering system heavily depends on successful and timely synchronization with the central Positive DNS Trust server. Network outages or delayed updates from the authoritative server may affect real-time effectiveness.

Overblocking and false positives: In some cases, non-malicious domains may be blocked due to outdated or overly broad filtering rules. This could impact teaching, research, or administrative tasks that require access to specific online resources.

Lack of user-level customization: The current system applies uniform filtering policies to all user types, which may not be ideal for a diverse academic community. Different user roles (e.g., students, faculty, staff) have varying needs and permissions.

Table 2. Device resolution time testing

Data Collection	Holiday			Working Days		
	Smartphone	Laptop	Computer	Smartphone	Laptop	Computer
Capture Time (Minutes)	30	30	30	30	30	30
DNS Average Time Response (ms)	9	3	2	11	5	3
New Content Resolve Time (Minutes)	4	2	1	6	3	1

Table 3. Comparison of firewall Mode and RPZ

Aspect	Mikrotik Firewall	RPZ DNS Server
Block Type	IP & Domain-based	Domain-based
Implementation Location	On the router (network level)	On the DNS server (DNS level)
Traffic Affected	All passing traffic	DNS traffic only
Management Flexibility	Manual	Dynamic, via RPZ
Implementation Difficulty	Requires firewall expertise	Easier, DNS-based
Scalability	Limited by router performance	Scalable with server upgrades
Filtering System	Redirects to an IP address	Redirects to a specific CNAME record

To overcome these limitations and enhance the system's effectiveness, the following improvements are proposed:

Implement DNS load balancing or clustering: To handle high query volumes, the institution could adopt a distributed DNS infrastructure using round-robin DNS or load-balanced agent servers.

To overcome these limitations and enhance the system's effectiveness, the following improvements are proposed:

Implement DNS load balancing or clustering: To handle high query volumes, the institution could adopt a distributed DNS infrastructure using round-robin DNS or load-balanced agent servers.

Establish redundant synchronization nodes: Setting up local caching and secondary synchronization servers can reduce dependency on a single upstream DNS and ensure continuous operation during outages.

Introduce a user-role-based filtering system: Customize DNS policies based on user categories to provide more appropriate access levels while maintaining security and compliance.

Develop a request-based allowlist mechanism: Allow users to request access to specific domains that are blocked but necessary for legitimate academic purposes, subject to administrative approval.

Periodic review and refinement of blocklists: Regularly audit and update the RPZ rules to eliminate false positives and adapt to evolving content threats.

By addressing these limitations, the RPZ implementation at Pakuan University can become more resilient, responsive, and tailored to the dynamic needs of the educational environment.

Using a DNS Server, the Response Policy Zone (RPZ) method is more effective and dynamic than a Firewall on a Mikrotik Router. As presented in Table 3.

5. CONCLUSION

Based on the study's results, which employed a Likert scale questionnaire, 82.32% of the 362 respondents—comprising students, lecturers, and administrative staff—rated the system as "Very Effective." Specifically, the respondents included 253 students, 48 lecturers, and 61 staff members. The analysis of the questionnaire responses revealed that the majority of participants had a positive evaluation of the DNS filtering implementation. The interpretation of the Likert scale scores indicates that the system effectively filters harmful internet content within the Pakuan University network environment. Furthermore, testing the resolution time for newly blocked content revealed that desktop computers consistently exhibited the fastest DNS resolution performance, followed by laptops and smartphones. These findings confirm the effectiveness and practicality of the RPZ-based DNS filtering system in enhancing network security and content governance in an educational setting.

Suggestions can focus on further enhancing the network security system for DNS servers by implementing a dedicated firewall device that prioritizes DNS server protection both from external threats and internal network vulnerabilities at Pakuan University. Securing DNS servers is essential to maintaining internet stability across the university's network.

ACKNOWLEDGMENT

This work was supported by the Center for Information and Communication Technology, Pakuan University (UNPAK).

REFERENCES

[1] Magnusson, J. (2024). Survey and analysis of DNS filtering components. arXiv preprint arXiv:2401.03864. https://doi.org/10.48550/arXiv.2401.03864

[2] Muhlison, S., Kusnawi, K. (2015). Analisa dan implementasi dns server sebagai filtering konten negatif menggunakan metode RPZ (Response Policy Zone) di pt. time excelindo. Jurnal Ilmiah DASI, 16(1), 49-54.

[3] Firmansyah, F., Purnama, R.A. (2019). Filtering domain name server (DNS) untuk Membangun Internet Sehat Menggunakan Routerboard Mikrotik. JUITA: Jurnal Informatika, 7(1): 43-48. https://doi.org/10.30595/juita.v7i1.4164

[4] Kang, A.R., Spaulding, J., Mohaisen, A. (2016). Domain Name System security and privacy: Old problems and new challenges. https://doi.org/10.48550/arXiv.1606.07080

[5] Cheng, Y., Liu, Y., Li, C., Zhang, Z., Li, N., Du, Y. (2022). In-depth evaluation of the impact of national-level DNS filtering on DNS resolvers over space and time. Electronics, 11(8): 1276. https://doi.org/10.3390/electronics11081276

[6] Xiao, G. (2025). Set up Response Policy Zone (RPZ) in BIND resolver on Debian/Ubuntu. https://www.linuxbabe.com/ubuntu/set-up-response-policy-zone-rpz-in-bind-resolver-on-debian-ubuntu.

[7] Ichise, H., Jin, Y., Iida, K. (2022). Policy-based detection and blocking system for abnormal direct outbound DNS queries using RPZ. In Proceedings of International Conference on Future Computer and Communication (ICFCC 2022).

[8] Zhauniarovich, Y., Khalil, I., Yu, T., Dacier, M. (2018). A survey on malicious domains detection through DNS data analysis. ACM Computing Surveys, 51(4): 1-36. https://doi.org/10.1145/3191329

[9] Jawaid, S.A. (2022). Cybersecurity threats to educational institutes: A growing concern for the new era of cybersecurity. International Journal of Data Science & Big Data Analytics, 2(2): 11-17. https://doi.org/10.20944/preprints202211.0128.v1

[10] Zhou, J., Fu, W., Hu, W., Sun, Z., He, T., Zhang, Z. (2024). Challenges and advances in analyzing TLS 1.3-encrypted traffic: A comprehensive survey. Electronics, 13(20): 4000. https://doi.org/10.3390/electronics13204000

[11] Ichise, H., Jin, Y., Iida, K. (2025). RPZ-based mechanism for detecting suspicious direct outbound DNS traffic with adaptive policy updates. IEEE Access. https://doi.org/10.1109/ACCESS.2025.3542234

[12] Jalalzai, M.H., Shahid, W.B., Iqbal, M.M.W. (2015). DNS Security Challenges and Best Practices for Deploying Secure DNS with Digital Signatures. In 2015, the 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 280-285. https://doi.org/10.1109/IBCAST.2015.7058517

[13] Marques, C., Malta, S., Magalhães, J.P. (2021). DNS dataset for malicious domains detection. Data in brief, 38: 107342. https://doi.org/10.1016/j.dib.2021.107342

[14] Salem, A., Elmedany, W. (2023). Defending the core: A comprehensive analysis of DDoS attacks on DNS infrastructure and proactive defense strategies. In 7th IET Smart Cities Symposium (SCS 2023), pp. 439-444. https://doi.org/10.1049/icp.2024.0964

[15] Marques, C., Malta, S., Magalhães, J. (2021). DNS firewall based on machine learning. Future Internet, 13(12): 309. https://doi.org/10.3390/fi13120309

[16] Imana, B., Korolova, A., Heidemann, J. (2021). Institutional privacy risks in sharing DNS data. In Proceedings of the 2021 Applied Networking Research Workshop, pp. 69-75. https://doi.org/10.1145/3472305.3472324

[17] Hafiz, A., Kurnia, I. (2021). Mengembangkan jaringan wireless local area network (WLAN) dan hotspot pada amik dian cipta cendikia (DCC) pringsewu menggunakan router mikrotik. Jurnal Informatika Software dan Network (JISN), 2(1): 15-22.

[18] Tchao, E.T., Ansah, R.Y., Djane, S.D. (2017). Barrier-free internet access: Evaluating the cybersecurity risk posed by the adoption of bring your own devices to e-learning network infrastructure. https://doi.org/10.48550/arXiv.1710.08795

[19] Andersen, M.F. (2022). Detecting malware and cyber attacks using ISP data. Aalborg Universitetsforlag. https://doi.org/10.54337/aau483028127

[20] Jebb, A.T., Ng, V., Tay, L. (2021). A review of key Likert scale development advances: 1995–2019. Frontiers in psychology, 12: 637547. https://doi.org/10.3389/fpsyg.2021.637547