p–ISSN: 2723 - 6609 e-ISSN: 2745-5254
Vol. 5, No. 10, October 2024 http://jist.publikasiindonesia.id/

Implementation Strategy Analysis of Network Security using dalo RADIUS and Pi-hole DNS Server to enhance Computer Network Security, Case Study: XYZ as a Fintech Company

Andika Davi Yudhistira[1], Ruki Harwahyu[2*]
Universitas Indonesia, Indonesia
Email: andika.davi@ui.ac.id[1], ruki.h@ui.ac.id[2*]

*Correspondence

Keywords: RADIUS server; daloradius; pi-hole DNS server.

ABSTRACT

According to the annual report by the National Encryption Agency in 2023, Indonesia had the highest number of cyber-attack sources, with over 1 million attacks, which has increased quite rapidly compared to the last 3 years. Several online media platforms have reported incidents of this nature over the past three years. Among the 10 institutions implicated in the present incident, it has been confirmed that 6 of them are Fintech institutions. The incident's factors are various, including the user's lack of awareness who accessed an unofficial website outside the company's production website. This act ultimately proved to be detrimental to the company. Therefore, this study highlights the importance of RADIUS (Remote Authentication Dial-In User Service) as a comprehensive security tool that contributes to mitigating unauthorized access and strengthening network defenses against emerging threats. This research focuses on XYZ, a Fintech Company, using it as a case study. The main discussion in this paper focuses on utilizing the daloRADIUS server to resolve authorization concerns regarding network security. Pi-hole DNS Server is also used in this research to block access to illegal sites such as pornography and online gambling. The results of this research are proof of the success of a combination of daloRADIUS server components, RADIUS router, and Pi-hole DNS Server in blocking users who are detected accessing illegal sites and are also observed regarding the use of daloRADIUS Server resources in a usage range ranging from 10 active users to 300 active users.

Introduction

Currently, several online news platforms in Indonesia often broadcast news related to network security issues. Cases related to cyber security will increase significantly in 2023 (Indonesia, 2023). When this cyber security case attacks an organization or agency, it will certainly be detrimental to a civil society with digital assets entrusted to the agency,

for example, in a company engaged in Finance and Technology (Fintech). If an organization or agency tasked with managing digital assets, such as a financial technology company, is deemed unreliable, it can undeniably have a deleterious effect on civil society. According to the annual report by the National Encryption Agency in 2023, Indonesia had the highest number of cyber-attack sources, with over 147 million attacks, which has increased quite rapidly compared to the last 3 years. Several online media platforms have reported incidents of this nature over the past three years (Wardhono et al., 2023). Fintech companies have a high potential for attacks in terms of information security. In a Fintech Company, a lot of Sensitive Data (PII) is the main target for a hacker. They start from the full name, telephone number, and address to the names of the customer's parents. If the data falls into the hands of a hacker, then that is when the data is pressed to have leaked. Which in the end will be detrimental to the customer himself because his data has been misused. Not only companies engaged in Fintech, but other agencies also engaged in the same field such as insurance agencies, public health agencies, Freeport, and Startup Companies, all of which store sensitive personal data and information belonging to the public (Charnade, 2022).

Based on the number of cyber security cases in Indonesia, it is evident that many agencies are unaware of their security vulnerabilities. Unfortunately, these types of incidents seem to repeat themselves across different agencies in similar ways, from phishing attacks to ransomware and data breaches. Human error contributes to these issues, which can create security loopholes. (Edbert & Putra, 2023) Hackers often target humans since they're the weakest element of vulnerability in the security chain and prone to mistakes. A hacker can use various methods to access a victim's computer system by anticipating their behavior. The most common way is to send a phishing email that contains a link or an application installer with a .apk extension. When the link is clicked, it gives the hacker unauthorized access to the victim's computer, and eventually, they can gain access to the whole company network.

The presence of security vulnerabilities in a network can potentially lead to data leaks and network attacks by malware. These vulnerabilities often stem from user ignorance, such as when users download files from advertisements found on unofficial or even illegal websites, including pornographic sites. To address this issue, the Ministry of Communication and Information in Indonesia has introduced the Constitution of the Minister of Communication and Information Number 19 of 2014, which outlines measures for dealing with negatively charged internet sites. (Ramdhan et al., 2024). According to Chapter 1 Article 1 of the regulation, negative content can be blocked. This includes pornography, which is mentioned in Chapter 3 Article 4 paragraph 1 point as a form of negative content. This regulation serves as the basis for closing any security loopholes that may pose a threat to network security, particularly for Fintech Companies. One effective measure is to block access to pornographic content, as it is known to contain numerous vulnerabilities that can compromise network security.

Every organization has its own set of policies and procedures regarding employee access to the Internet network. These access rights policies aim to safeguard the network's

security and information from potential cyber-attacks. The IT Support and Security Engineer division oversees this issue, from identifying each division's IP address to determining their access rights. The engineer also needs to create a list of permitted and prohibited websites to minimize the risk of unauthorized access and potential hacking of network and server devices.

A computer network can overcome security issues by implementing a Remote Authentication Dial-In User Service (RADIUS) Server component. To ensure the security of the office and internet network, we use a Two-factor authentication (2FA) method for login. Only authorized employees with a username and password can access the network while unauthorized users are blocked. In addition, we have a DNS Server that filters websites to prevent access to non-production sites. This filtering reduces the risk of accessing or downloading something from an unofficial website, which can create vulnerabilities in the network. To address potential network vulnerabilities, we can take multiple measures to ensure safety. One such measure is to implement filters on the network access side to restrict access to certain websites, such as adult or gambling sites, or other malicious websites. This is important as the impact of a virus spreading from an employee's computer can be detrimental to the company. (AlBenJasim et al., 2023).

In our submitted research, we emphasize several significant advantages and contributions. Not only does daloRADIUS provide secure authentication and authorization access, but our study also presents a strategic approach for securing access to restricted sites, including those of a pornographic nature, by coordinating RADIUS routers, daloRADIUS servers, and DNS servers. Thus, our research aims to implement a strategic analysis of network security using daloRADIUS to enhance computer network security.

In addition, the remaining sections of the paper will be organized as follows: Chapter 2 will delve into prior theories and research that uphold the concept under investigation. Chapter 3 will outline the research methodology and contributions to this study. Finally, Chapter 4 will present the research's conclusive findings.

In this study, the RADIUS Server technology used by the author is daloRADIUS. daloRADIUS is an advanced web platform for managing Hotspots and general-purpose ISP deployments using the RADIUS protocol (Estrada-Jiménez et al., 2017). It is equipped with rich user management, graphical reporting, and accounting, and integrates with Google Maps for geo-locating (GIS). Written in PHP and JavaScript, daloRADIUS uses a database abstraction layer. It can support many database structures, including MySQL, PostgreSQL, SQLite, MsSQL, and many others.

The daloRADIUS solution utilizes a FreeRADIUS deployment with a backend database server, offering a variety of features including ACLs and GoogleMaps integration for enhanced hotspot/access point visualization. While it can theoretically manage any radius server, it is specifically designed for FreeRADIUS and its database structure. Additionally, version 0.9-3 introduced an application-wide database abstraction layer based on PHP's PEAR: DB package, providing support for various database servers. DNS Server III also plays a role in this robust system.

Method

Proposed Implementation

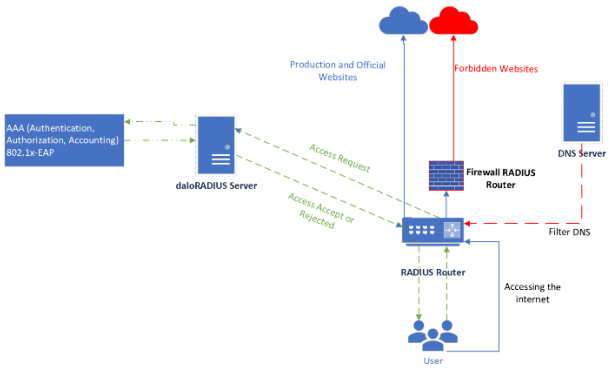

Figure 1 Proposed Implementation

Figure 1 is the network topology that will be analyzed in this study. In this research topology, the author uses a RADIUS router and 2 servers consisting of DNS Server and RADIUS Server, and one client host PC. The initial stage of this test involves conducting an experiment where a user attempts to connect to a Computer Network to gain access to the internet. This study aims to apply security to the network by optimizing the RADIUS Server, where the authentication method the user wants to access the network will first face the two-factor authentication (2FA) process. In addition, in this study, we also implemented security on the DNS Server side as the second layer of security after this RADIUS Server. Based on our analysis, we propose that the implementation of RADIUS (Remote Authentication Dial-In User Service) and DNS (Domain Name System) Servers can significantly enhance the security of a network. We hypothesize that these two layers of security can provide better protection against unauthorized access and data breaches compared to a network without such technology.

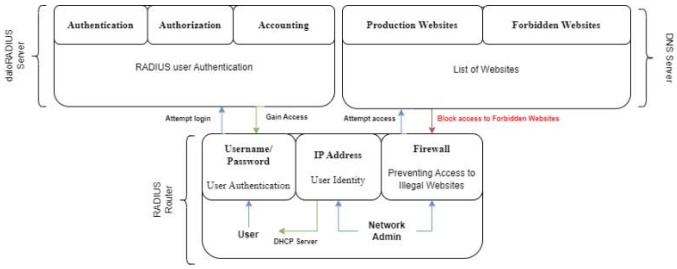

Figure 2 Main topics in this research

Attached is Figure 2, which is the main topic discussed in this study. For the record, the RADIUS Server will execute three essential steps in the computer security system framework, which include authentication, authorization, and accounting. Once the user has completed three stages successfully, they will be assigned an IP address and provided

access to the internet. However, it is important to note that website filtering must be implemented on the DNS Server side.

How Strategy Implementation Works

This research is made possible through the seamless integration and synchronization of the RADIUS Router, daloRADIUS Server, and DNS Server. The RADIUS router serves as a crucial network device responsible for storing IP address configurations, firewall filter rules, and directing IP address configurations to the DNS Server. Additionally, the 802.1X protocol plays a significant role in the authentication process on the RADIUS Server. The 802.1X-EAP authentication takes place between the authentication server and the station, with the access point acting as the mediator. Ultimately, the station is authenticated by the authentication server. (Peoni, 2014).

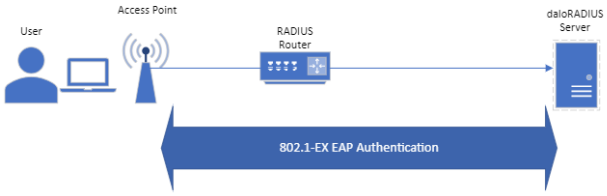

Figure 3 802.1-EX EAP Authentication

The authentication process in this study involves the user accessing the daloRADIUS Server using WiFi as the media. The Topology strategy implementation, as illustrated in Figure 3.1, Figure 3.2, and Figure 3.3 highlights the various stages of this authentication process, which primarily takes place within the User, Router RADIUS, and daloRADIUS Server sections. Once the user receives an authentication response, they are granted access rights in the form of authorization to access the internet network.

daloRADIUS Strategy Orchestration

The daloRADIUS server is a critical component that will be thoroughly examined in this study, specifically in Figure 3.4 This powerful tool serves as a two-factor authentication system, granting secure access to the internet network for authorized users.

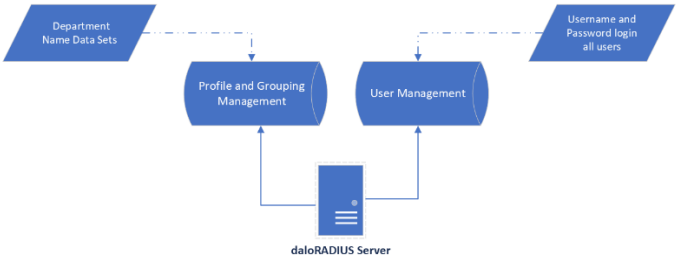

Figure 4 daloRADIUS Orchestration

DaloRADIUS contributes to the utilization of simple access security methods in authentication verification methods. We apply it to the case study of XYZ company as a

company in the field of Fintech according to existing needs. By using a virtual RADIUS server, we leverage these resources to make a significant contribution in terms of strengthening the security of authentication and authorization access on a corporate network. In Figures 3.5 to 3.9 attached are several displays on important components of the daloRADIUS Server used in this research.

First login to the daloRADIUS Server

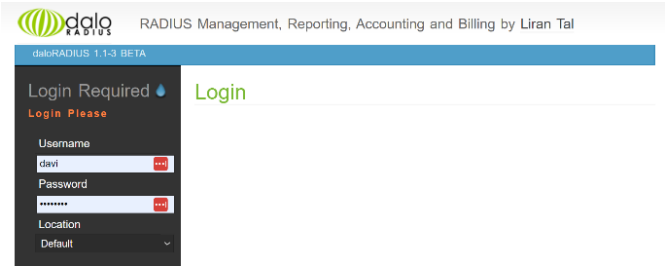

Figure 5 First login page daloRADIUS

The section at hand serves as the first page when accessing the daloRADIUS server. It functions as a login page, facilitating IT administrators to effectively execute daloRADIUS server management.

1. After Login Display

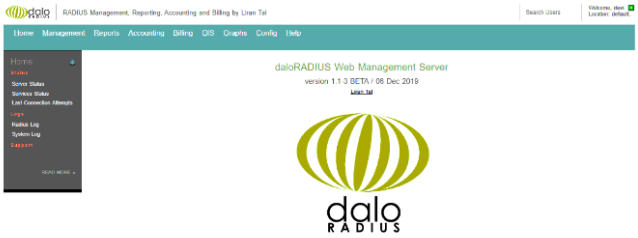

Figure 6 After login page daloRADIUS

This section is related to a website page accessible only to IT administrators who have successfully logged into the daloRADIUS web server. For the present research, the daloRADIUS server version 1.1.3 BETA was utilized.

1. Profile Management

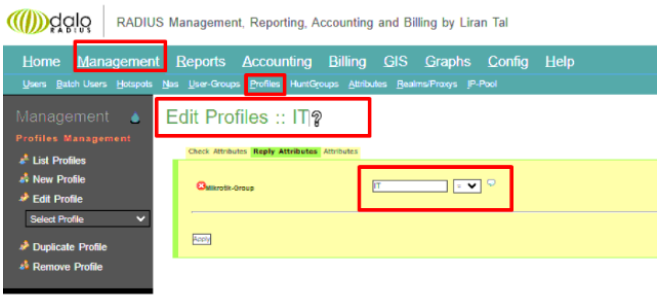

Figure 7 Profile Management daloRADIUS

The Profile Management section is utilized to gather user Profiles or Groupings that will subsequently be granted access privileges for login and authentication, thereby classifying them as authorized users. As exemplified in Figure 3.7, one of the Grouping Profiles created pertains to the IT department.

2. User Management

Figure 8 User Management daloRADIUS

The User Management section is a repository of information containing data for all users who are granted access rights. This section records the username and password parameters of prospective users. As illustrated in Figure 3.8, one of the usernames, "davi-IT," has been successfully registered in the daloRADIUS server.

3. Grouping Management

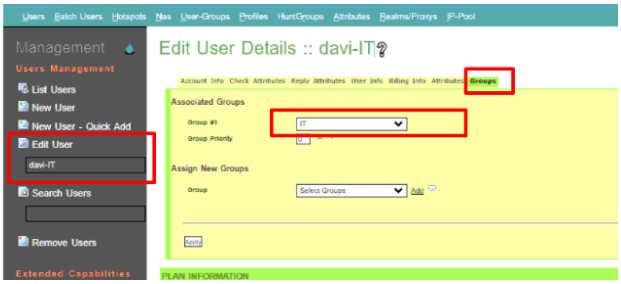

Figure 9 Grouping Management daloRADIUS

The Grouping Management section encompasses crucial data about divisional Grouping within an organization. It serves as a pivotal element in grouping IP Addresses. Each grouping division is designated a unique IP address, allowing IT administrators to efficiently ascertain access rights for each division. To determine the access rights of these divisions will later proceed to the Pi-hole DNS Server section, which is included in the test discussion in this study.

Pi-hole DNS Server

As shown in Figure 3.10 This study also involves the use of DNS Servers to compile a list of websites that have been deemed inappropriate by network administrators. The list mainly includes websites that fall under the category of prohibited sites, with a significant emphasis on pornographic websites. The rationale behind this categorization is that such websites are deemed to contain content that violates the principles of healthy internet use.

Moreover, these websites harbor a significant amount of malware and malicious viruses that can cause significant information security breaches.

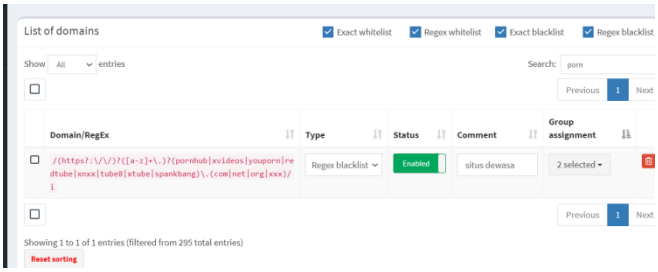

Figure 10 List of Prohibited Websites

This study features a flow chart, displayed in the next section, that outlines the testing process. Initially, the user's internet access will be evaluated through the daloRADIUS Server to determine if they can log in successfully. Once the user has gained internet access via the daloRADIUS Server, website access will be tested to confirm whether the Pi-hole DNS Server effectively filters websites.

Results and Discussion

The research results that we propose this time compare whether daloRADIUS can overcome access security problems in the internet network more simply compared to using RADIUS Server in other studies. In this chapter, we will explain the Flow of daloRADUIUS in securing a network and the role of DNS servers and firewalls in the RADIUS Router in blocking access for users who access negative content. Coupled with the method of blocking user access rights when the user is detected by the Router if accessing negative content that can endanger security on the network.

Flow Chart of RADIUS Testing

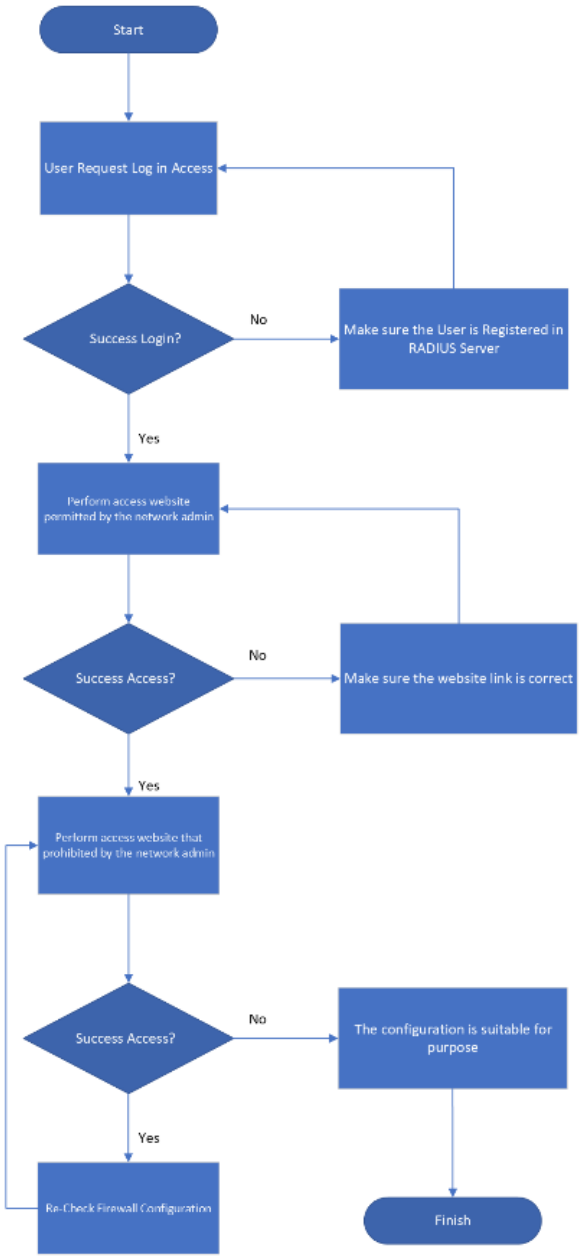

Figure 11 Flowchart of Testing

The flowchart attached to Figure 11 represents the testing stage conducted in this study. It begins with testing the login to access network rights and proceeds to testing access to restricted sites.

Scenario 1. Attempting to access allowed websites

As shown in Figure 12, access was granted to the authorized website https://ojk.go.id/id/Default.aspx while internet access remained unblocked for users. The purpose of this scenario was to evaluate the difference in user access between legal and illegal websites.

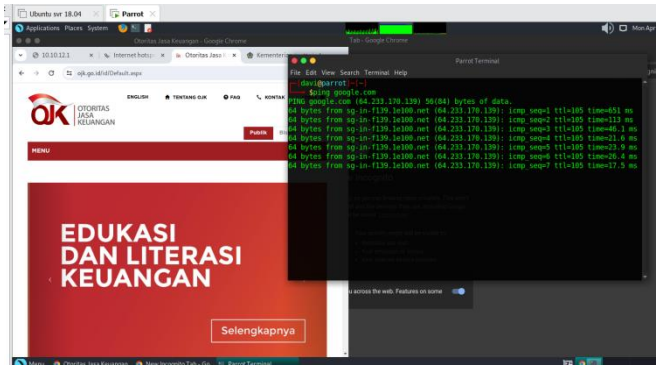

Figure 12 Accessing Allowed Website

Based on the data presented in Table 4.1, it can be concluded that users who access authorized websites like government portals, corporate web pages, and other lawful content can enjoy uninterrupted internet access without facing any connectivity issues or IP blocking.

Table 1 Result of Scenario 1

Scenario 1		
Action	**Access the official site**	**Result**
Internet Access	√	User Gain Internet Access
IP Blocked?	X	IP's User didn't block when accessing Official or Production sites
Users can still log into the Network by RADIUS.	√	Users can log into the network.
Ping google.com	√	Ping on Google results in a reply

This is primarily because the router can identify the accessed website as a legitimate and secure destination belonging to the category of non-hazardous websites. This feature of the router ensures that users can access the websites they need to without any interruptions or restrictions. For instance, government portals are critical information sources for citizens, and corporate web pages are necessary for employees to carry out their duties efficiently. Therefore, it is essential to have unrestricted access to these websites.

Furthermore, the router's ability to identify non-hazardous websites ensures that users do not inadvertently land on websites that may pose a threat to their privacy or data security. This is especially important in today's digital age, where cyber threats are rampant, and malicious websites are always on the prowl. In summary, the router's ability to identify legitimate and secure websites and categorize them as non-hazardous ensures that users have unrestricted internet access without facing any connectivity issues or IP

blocking. This feature is crucial for users who need to access authorized websites like government portals, corporate web pages, and other lawful content without any interruptions.

Scenario 2. Attempting to access prohibited websites

In a recent experiment, researchers were interested in assessing the effectiveness of filter blocking in preventing access to illicit sites by certain IP addresses. The researchers experimented by testing the access of pornhub.com and noted that the results showed that the IP address was promptly blocked by the Firewall on the RADIUS router, which prevented internet access. The primary objective of this experiment was to identify the IP address that was blocked, which is shown in Figures 4.8 and 4.9 This is significant because it facilitates the work of network administrators in monitoring users who attempt to access prohibited sites.

By identifying and blocking the IP addresses of users attempting to access illicit sites, institutions can effectively prevent such access and promote safe and responsible internet use. The experiment also highlights the importance of having a robust Firewall system in place to protect against unauthorized access to sensitive information and prevent the spread of malware.

Overall, this experiment demonstrates the importance of ensuring that proper measures are put in place to protect networks and users from unauthorized access to prohibited sites. It also underscores the role of network administrators in monitoring and enforcing internet usage policies to promote a safe and secure online environment for all users.

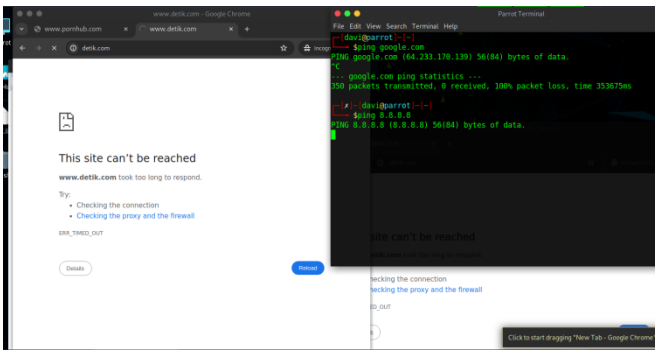

Figure 11 Access website allowed by Admin

According to the information presented in Figure 4.9, it appears that the IP address has been detected and listed in the 'Firewall > Address List' menu. In such a scenario, it is worth noting that the IP in question shall be automatically blocked for network access, thereby rendering it incapable of accessing the internet in any way.

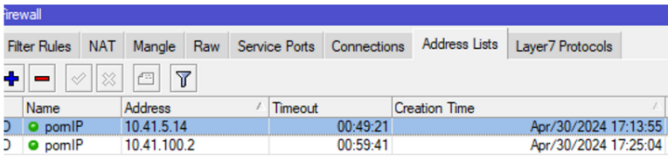

Figure 2 IP addresses detected in RADIUS Router

After analyzing the data presented in Table 2, it can be inferred that Company XYZ has taken appropriate measures to restrict access to unauthorized content, particularly pornography.

Table 2

Result of Scenario 2

Scenario 2		
Action	**Access the prohibited site.**	**Result**
Internet Access	X	User can't Gain Internet Access
IP Blocked?	√	IP's User was blocked when accessing prohibited websites.
Users can still log into the Network by RADIUS	X	Users can't log into the network
Ping google.com	X	Pinging Google results in a timeout

The issue of unauthorized access to sensitive content is a growing concern for many companies, and it is no surprise that Company XYZ has taken the initiative to protect its users from such threats. The implementation of an automated firewall that blocks the IP address of the device being used in case of any attempt to access unauthorized content is a great step in ensuring the safety of the company's users. It is important to note that unauthorized websites pose a significant risk to users, as they may display harmful advertisements or links that can contain malware capable of compromising the users' devices and networks. In addition, the potential harm that pornography can cause to individuals, especially minors, cannot be ignored. Therefore, it is laudable that Company XYZ has taken appropriate measures to restrict access to such content.

Unfortunately, not many users are aware of these potential threats, and this highlights the need for stringent security measures to prevent any possible data breaches. The fact that Company XYZ has put in place such measures shows its commitment to ensuring the privacy and safety of its users. Other companies need to follow in the footsteps of Company XYZ and implement similar measures to protect their users from any potential harm. It is also essential for users to be educated on the potential risks of unauthorized content and how to protect themselves from such threats. By doing so, we can all work together to create a safer and more secure online environment for everyone.

Monitoring Resource untuk Router RADIUS

Table 3
Resources Router Usage

Quantity User	CPU Load
10	1%
50	2%
100	5%
200	6%
300	10%

Attached in Table 3, are the resources of the RADIUS router CPU. It can be concluded that each user connected to the internet does not take up too much burden on the RADIUS router so that the router's performance and user connectivity are not disturbed. Testing was carried out starting from 10 connected users to 100 users. When there are 10 users, the CPU load only reaches 1%, which is considered low router resource usage. When 50 users are connected to the internet, the CPU load only increases by 1 point to 2% and in this condition, it is still in the low CPU usage category. Up to 300 users connected to the internet, the CPU has only reached 10% and this figure is still within the low CPU usage limit, namely still below 50%.

Comparison of Research on Similar Topics

In our submitted research, we emphasize numerous advantages as a significant contribution and novelty. daloRADIUS not only ensures secure authentication and authorization access but our study also presents a strategic approach for securing access to restricted sites, particularly those of a pornographic nature, by coordinating RADIUS routers, daloRADIUS servers, and DNS servers. Therefore, our research aims to implement a strategic analysis of network security using daloRADIUS to enhance computer network security.

Table 4
Research Comparison
(√ Covered || X Not Covered)

Compared with Previous	Network Security Implementation	Network Security Implementation with DNS Implementation	Illegal Websites Filter
	√	X	X	X
	√	X	X	√
	√	√	√	X
	√	X	√	X
	√	√	X	X
This Work	√	√	√	√

By comparing it with previous studies, the research we propose has several advantages and new contributions. Attached to Table 4.3 is a comparison between the research we conducted and previous research. In the research that we submitted this time, we observed advantages in several aspects, especially in the filtering of negative content.

In the following reference paper (Mulyaningsih, 2016) This paper discusses cybersecurity challenges in the FinTech industry and regulations in Bahrain. The paper concludes that Bahrain has made significant progress in addressing cybersecurity challenges within the FinTech sector. Almost like the research case study that we submitted, however, in the paper, no contributing factor explains access security from the user side and filter content. The following reference paper (Musyafak & Handayani, 2017) Explores the privacy threats associated with online advertising and approaches to protecting user privacy. This paper implements effective strategies to protect user privacy, but in this paper, there has been no discussion and contribution to the security of access to the internet network as we carried out. In reference paper (Palamà et al., 2023) It discusses attacks and vulnerabilities associated with Enterprise Wi-Fi networks and evaluates user security awareness through credential theft attack experiments. However, in the following reference paper, there is no discussion about content filters in terms of user access to negative content. The following reference paper discusses various aspects of network security, such as access control, intrusion detection, and data protection, which are specifically customized to the context of educational institutions that utilize virtualization technology. In the paper, unfortunately, no technology utilizes security-related features with RADIUS and also filters content against negative sites. In reference paper, this paper discusses the design and implementation of campus network security systems based on RADIUS and AAA with the main focus being to improve campus network security by using the RADIUS protocol for authentication and access management. However, this paper has not discussed the security of user access filters against accessing negative content.

The research submitted this time highlights advantages in various aspects, particularly in the filtering of negative content. However, the referenced papers do not adequately address the security of access to the internet network and the filtering of negative content from the user's perspective. This research aims to fill the gap and make a significant contribution to the field.

Conclusion

Based on the research findings, it can be concluded that the daloRADIUS server serves as a web server that enhances network authentication security. Additionally, daloRADIUS facilitates the sharing of IP Grouping across various divisions, thereby granting each division its access rights. This allows for strict access control, ensuring that only authorized personnel can access certain information. Given these benefits, implementing daloRADIUS can be an effective alternative for securing Company XYZ's network, especially since it is a fintech company. As part of our study, we analyzed the IP addresses that accessed prohibited sites, such as pornographic sites. Such sites are considered forbidden due to the potential security loopholes they can create. Pop-up ads on these sites can often be malicious and lead to phishing incidents for unsuspecting users.

The challenge of securing computer systems and networks in companies is increasing due to the sophisticated technology and science of hacking, which makes it difficult for organizations to protect themselves from cyber threats. Moreover, the lack of awareness and knowledge on the part of clients and users adds to this challenge. This move can be particularly relevant for companies that operate globally and are subject to the supervision of various stakeholders, including the government. Therefore, we aim to prevent such issues from arising within the company.

Bibliography

AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2023). Fintech cybersecurity challenges and regulations: Bahrain case study. *Journal of Computer Information Systems*, 1–17.

Charnade, R. S. V. (2022). Urgency Public Data Protection Based on Data Leakage Cases at The Indonesian Child Protection Commission. *Constitutionale*, *3*(1), 77–86.

Edbert, F., & Putra, M. R. S. (2023). Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi pada Perusahaan Pengelola Jasa Keuangan Berbasis IT. *UNES Law Review*, *6*(2), 5966–5977.

Estrada-Jiménez, J., Parra-Arnau, J., Rodríguez-Hoyos, A., & Forné, J. (2017). Online advertising: Analysis of privacy threats and protection approaches. *Computer Communications*, *100*, 32–51.

Indonesia, B. B. C. (2023). BSI Diduga Kena Serangan Siber, Pengamat Sebut Sistem Pertahanan Bank "Tidak Kuat." *Bbc. Com*.

Mulyaningsih, S. S. (2016). *Analisis peraturan menteri komunikasi dan informatika nomor 19 tahun 2014 tentang penanganan situs internet bermuatan negatif sebagai pembatasan hak asasi manusia ditinjau dari ketentuan pasal 28j ayat (2) undang-undang dasar negara republik Indonesia tahun 1945*.

Musyafak, N., & Handayani, M. R. (2017). Implementasi Peraturan Menteri Komunikasi Dan Informatika Nomor 19 Tahun 2014 Dalam Penanganan Situs Internet Bermuatan Negatif (Studi Kasus Pemblokiran terhadap Situs Radikal oleh Kemenkominfo Tahun 2015). *Islamic Communication Journal*, *2*(1), 80–99.

Palamà, I., Amici, A., Bellicini, G., Gringoli, F., Pedretti, F., & Bianchi, G. (2023). Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments. *Computer Communications*, *212*, 129–140.

Peoni, H. (2014). Pengaruh karakteristik individu dan lingkungan kerja terhadap kinerja karyawan (Studi Pada PT. Taspen (Persero) Cabang Manado). *Jurnal Administrasi Bisnis (JAB)*, *3*(001).

Ramdhan, T. W., Florina, I. D., & Permadi, D. (2024). Analisis Framing Pemberitaan Peretasan Pusat Data Nasional (PDN) di Media Online Tempo. Co. *Journal of Education Research*, *5*(3), 3368–3379.

Wardhono, R. D. T. K., Hermawan, D., & Cahyaningtyas, D. (2023). *Dampak Implementasi Transaksi Bilateral Dengan Menggunakan Uang Lokal Terhadap Regulasi Dan Reformasi Kelembagaan Di Sektor Keuangan*.