International Journal of Communication Networks and Information Security
2024, 16(2), 6659
ISSN: 2073-607X,2076-0930
https://https://ijcnis.org/ **Research Article**

Comparative Analysis of Traditional and Modern Proxy Solutions in Cyber Security

Attila Máté Kovacs [1*]

[1] PhD. Candidate, Doctoral School on Safety and Security Sciences, University of Obuda, Budapest, Hungary

***Corresponding Author:** Kovacs.attilamate@uni-obuda.hu

Citation: A. M. Kovacs, "Comparative analysis of traditional and modern proxy solutions in cyber security," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 16, no. 2, pp. 19-32, Aug. 2024.

ARTICLE INFO

Received: 12 May 2024
Accepted: 03 Aug 2024

ABSTRACT

This paper presents a broad comparative analysis of traditional and modern proxy solutions in cyber security landscape. This paper is highlighting the effectiveness, applications, and impact of these proxies in different cyber security environments. Through an extensive literature review, this paper explores the evolution of proxy technologies. A thorough evolution is presented here from basic content filtering and caching tools to sophisticated security techniques. And how these security solutions are integrated with advanced features. These features are deep packet inspection (DPI), real-time threat intelligence, and encryption management of traffic. The quantitative and qualitative data from the University of Maryland CISSM Cyber Attacks Database is used to analyze trends, frequency, and financial impacts for different organizations. This analysis is identifying a major increase in proxy-related attacks and highlighting importance of strong proxy solutions required to handle these growing sophisticated attacks. We investigate different case studies, like high profile breaches at OKX, i2VPN, and the 911[.]re. This investigation is showing real-world applications and consequences of proxy attacks. These case studies provide a qualitative input to our understanding. Also, these case studies are highlighting specific methodologies and mitigation strategies being used by the hackers to breach cyber security solutions. Our findings are showing that modern proxy solutions are considerably outperforming the traditional proxies in different parameters of cyber security. Like security effectiveness, scalability, and adaptability are the main parameters where modern proxy solutions are more proactive and more secure as compare to the tradition proxy solutions. This paper determines different lessons learned and recommendations for enhancing security of organizations. This paper concludes by emphasizing the need for continuous monitoring, comprehensive incident response plans, and employee training.

Keywords: Proxy, Cyber Attack, Vulnerability, Breach, Secure Web Gateway.

INTRODUCTION

The overall paradigm of cyber security is changing with the passage of time and in this evolving scenario of cyber security the proxy solutions are playing vital role to safeguard digital environments. The proxies are acting as mediators between users and the internet. The proxies are providing privacy, filtering, and security enhancements to protect sensitive data and to maintain the privacy of the internet users. With the passage of time the nature, working and functionality of proxy solutions have advanced considerably. The proxies are changing from traditional, static systems to more sophisticated and dynamic solutions that empower the cutting-edge technologies.

Background and Importance

The traditional proxy solutions like forward proxies and reverse proxies are being used from many years. These traditional proxy solutions are utilized to control internet access, cache content, and to balance the loads in network traffic. Most of the traditional proxy solutions are being operated on the network layer. Different services are offered on network layer such as IP masking and basic filtering of web content [1]. These traditional proxy systems were very effective in their time, but these traditional proxies often struggle to work effectively in complex and high-speed demands of modern cyber threats. Also, diverse network environments are not being protected by the traditional proxy systems.

The modern proxy solutions are secure enough in response to the growing complexity of networks and scale of cyber threats. The modern proxy solutions are supporting cloud-based proxies and these cloud-based proxies offer scalability and flexibility. The modern proxies are providing secure web gateways and these gateways are useful enough to integrate advanced threat detection capabilities. The AI based proxies are intelligent enough to provide threat analysis in real time [2]. These modern solutions are designed to mitigate the limitations and drawbacks of traditional proxies. Because these modern proxies are offering enhanced security features and improved performance. That is why, different network configurations are adopting modern proxies and also these are helpful enough to fulfil the needs of end users.

The main objective of this paper is to conduct a comparative analysis of traditional and modern proxy solutions in the field of cyber security. The evaluation of these both types of proxies on the basis of their effectiveness, applications, and performance in various settings is the focus of this paper. This paper is going to provide a detailed understanding of how these solutions operate in different scenarios. Different strengths and weaknesses are going to be evaluated to identify possible issues in both systems. This comparison is going to help out the cyber security professionals and organizations to make informed and accurate decisions during the selection process of the proxy solutions. Also, this paper can help the professional to find out the best proxy solution according to their needs and security requirements.

This paper is structured to address the comparative analysis of proxy solutions. After the introduction part of this paper the Literature review section will provide an overview of existing research on both traditional and modern proxy solutions. This part is going to highlight development in both type of proxies. Also, the types, applications, and effectiveness of both proxy solutions will be elaborated in literature review. The Methodology section is going to outline the research design, data collection methods, and basic criteria being used for the comparison of traditional and modern proxy systems. The next is the case studies section and this section will examine and illustrate the real-world examples, practical applications and performance of these proxy solutions. While the discussion section will evaluate and interpret the results discussed in the literature review and presented in the case studies. That's why this discussion section will provide a detailed analysis of the advantages and disadvantages of each type of proxy solution. At the end, the conclusion part will summarize the key results, findings, and offer recommendations for organizations to select a system according to the requirements. The conclusion section will also suggest areas for future research.

The internet security issues are increasing with the passage of time and cyber threats become increasingly sophisticated. That's why, the requirements of robust and adaptive security measures are growing [3]. This paper is comparing the traditional and modern proxy solutions. This paper is contributing for the academic understanding of these technologies and also provides practical perceptions to improve cyber security practices. Different business and security organizations can benefit from this analysis, because they can select best suitable proxy solutions according to their requirements. In this way, the organizations can enhance their overall security posture and resilience against cyber-attacks.

LITERATURE REVIEW

This literature review is going to provide an in-depth analysis of traditional proxy and modern proxy solutions in cyber security. This literature review is examining the articles of different scholars, different technical reports, and industry publications. The aim of this section is to highlight the development, applications, effectiveness, and comparative aspects of traditional and modern proxy solutions. The review is organized to include traditional proxy solutions at the initial stage, then followed by modern proxy solutions, and ended up with a comparative analysis.

Traditional Proxy Solutions

From the early days of internet, the traditional proxy solutions are working as a foundation of network security and management. These proxies mostly function at the network layer [4]. These proxies are categorized into three different types like forward proxies, reverse proxies, and transparent proxies.

Forward Proxies

Forward proxies act as a bridge between the client and the internet. They are used for anonymizing, access control over external resources and caching to optimize the network traffic. Pour et al. [1] and Yeh [4]: Forward proxies are exemplary for handling network traffic in further detail. It also gives a level of security as it hides user IP addresses. However, these two research solutions above also reveal scalability and performance limitations in the network. These proxies could be more effective, especially against high traffic volumes.

Reverse Proxies

The Reverse Proxy works between an internet and internal servers. Therefore, all these carriers and ISPs offer products such as load balancers, caches & web application firewalls via proxies. Reverse proxies are most effective in shielding internal servers from global internet traffic, as Kim and Lee [5] reported. The protection is this addressing and thus minimizing the possibilities of attacks. The research also notes the importance of reverse proxies for spreading client request load across a server farm. This role helps in improving web service performance and reliability. However, reverse proxies are big concerns because if they're not managed properly, they can be single failures [2].

Transparent Proxies

Transparent proxies are to intercept client requests without any configuration done on the client side. Abrahams et al. [6] stated that transparent proxies are very helpful when the user interaction involvement is minimal. Now, with the ease of deployment via such proxies, bear in mind that the fact they intercept means privacy and ethical considerations should follow. The key is that these proxies are brought up without any request to be configured. Should the users not be able to know whether they are using a proxy and steer some privacy or ethical concerns.

Effectiveness and Limitations of Traditional Proxies

The research by Kavya and Rengarajan [7] indicates that traditional proxy solutions are more effective in basic network security tasks. Like IP masking and access control are the main features of traditional proxies. However, the study highlights significant limitations, and these limitations are given below.

- Scalability: The traditional proxies often struggle to handle the increasing volume of traffic. And also, it is quite difficult for traditional proxies to handle the complexity of modern internet traffic.

- Security: These proxies provide basic security measures but these proxies are not equipped to deal with sophisticated cyber threats of modern internet.

- Performance: The caching can improve the performance, but high traffic volumes can lead to the bottlenecks. These bottlenecks can introduce different security attacks like denial-of-service attack etc.

Modern Proxy Solutions

The overall paradigm of cyber security is revolutionizing, that's why the modern proxy solutions have emerged with latest security features. Modern proxies are incorporating advanced technologies to address the limitations of traditional proxies. These modern solutions consist of cloud-based proxies, secure web gateways, and AI-driven proxies.

Cloud-Based Proxies

Cloud-based proxies are based on the scalability and flexibility of cloud computing to offer better performance and security to the internet users. According to Couretas [8], the cloud-based proxies can dynamically scale the resources to handle fluctuating traffic loads. This feature can really reduce the bottleneck issues for heavy traffic. These proxies also incorporate advanced security features, because these proxy work as a real time threat detection tool. The automatic updates are making these proxies stronger against different modern cyber security threats.

Secure Web Gateways (SWGs)

The Secure web gateways are comprehensive security solutions to provide reliable cyber security. These solutions are providing advance threat protection, data loss prevention, and secure access to the internet. Studies by Obi et al. [3] are highlighting the effectiveness of SWGs in cyber security paradigm. Like blocking malicious websites, enforcing security policies, and monitoring web traffic for suspicious activities are the main features of SWGs. Obi et al. [3] stated that unlike traditional proxies, the SWGs offer secure control to monitor user activities and helpful to integrate with other security solutions. For example, the SIEM (Security Information and Event Management) systems are providing a complete security approach [2].

AI-Driven Proxies

Proxy solutions now use Artificial intelligence (AI) and machine learning (ML). This is because the intelligence behind AI and ML goes far enough actually to improve what proxies can do [9]. AI-driven proxies, for instance, can sift through huge volumes of data in real time and pinpoint new threats. This real-time analysis by AI can also help in real-time response to threats. These are proxies that can detect developing attack patterns. The application will then press on them so that they can handle these; Zero-day vulnerabilities and deadly cyber-attacks can be countered using these proxies. Another advantage emphasized by Da Cunha Costa Caldas [10] returned to the AI routine that requires less manual work when configuring and updating. It can help make the proxy solution more efficient and responsive overall.

Effectiveness and Limitations of Modern Proxies

Traditional proxies have many limitations; modern proxy solutions overcome them. Modern proxies' good features and how they scale better provide more security for our network. Research by Obour et al. [11] provides advantages of modern proxies.

- Scalability: The cloud-based proxies can easily manage many users without any performance degradation.

- Security: Advanced security features, such as real-time threat detection, AI-driven analysis and integration with other tools. In the modern world of cyber security, this feature can serve to defend against advanced threats with strong protection.

- Performance: Modern proxies run on cloud infrastructure with intelligent caching; hence, they offer good performance and low latency support.

Nevertheless, modern proxies are not 100% ideal either since there have been problems that these proxies have already encountered. The study by Yeh [4] lists the challenges as follows:

- Cost: Modern proxies tend to be rich in features and capabilities, making it near-impossible to get an affordable option. Incorporating a high-cost level can work as an obstruction from smaller organizations.

- Complexity: Integrating, controlling and managing the modern proxy solutions can be difficult. You need expertise and knowledgeable professionals to work with such proxies.

- Privacy Concerns: AI-based proxies require extensive data analysis, which can result in privacy concerns. Especially in the regions which have more stringent data protection rules and regulations [9].

Comparative Analysis

In the comparative analysis of traditional vs modern proxy solutions, these two differ in terms of their characteristics and applications and regarding how efficient they are. First, traditional proxies are quite straightforward and work well for basic network security duties. However, these proxies have been getting tough to cater to modern intricate cyber security threats. Modern proxies are still feature-filled for security and compliance while also bringing massive scaling benefits (including simple performance proxying) [11]. These characteristics of modern proxies make them more mind-blowing in meeting some recent cyber security needs.

Security Effectiveness

Traditional proxies do not support advanced threat detection and response capabilities. Only modern proxies have these capabilities. Cloud-based proxies, secure web gateways and AI-driven Proxies are all effective in real-time threat detection [7]. Security policies and advanced response mechanisms are present in modern proxies [9]. This is why you can now use modern proxies to see through, directly monitor and maintain the security standard of the Internet.

Performance and Scalability

The traditional proxies can increase performance via caching and load balancing. But these proxies are facing real issues with so much traffic. The high traffic can provide significant challenges. Furthermore, more traditional proxies need help with the complexity of network environments. Modern proxies like [2] can handle network traffic with a big load. Another great advantage of modern proxies is their aligned performance, which enables you to avoid being held up on picking the right options, and thus, they can adapt to, e.g., cloud settings quite easily. With the help of Modern Proxies, traffic can be routed via an optimized route, such as reducing network latency and saving resources for better use in other activities.

Cost Efficiency

The traditional proxies are cheaper than the latest ones. However, these are not secure for performance, which is a requirement from the proxy servers. So, ultimately, the users could be in a position of security problems and cyber-attacks. Falling cheap is falling deep [8]. The cost of the newer proxies is higher and can compensate for this with better performance, a lower chance of getting hacked, and less maintenance.

Ease of Deployment and Management

Traditional proxies are comparatively easy to deploy and manage, especially in small and medium size networks. On the other hand, the modern proxies are offering greater capabilities, but these are more complex to integrate. The cloud-based proxies and managed security services are helpful to mitigate these challenges. Because cloud-based proxies are offering simplified deployment and management options to facilitate the professionals [6].

From the literature review, it could be inferred that traditional proxy solutions have contributed significantly to network security. However, in this latest information technology world, their limitations have become obstacles to tackling various modern cyber security threats. The new proxy solutions provide more advanced security features and scalability [10] in Recognition of the Modern Internet Security Framework, which demands great performance improvements for a proxy in modern times. Hence, the organizations must carefully consider their specific needs, resources, and threat mitigation requirements while specific proxy solution.

METHODOLOGY

This methodology section presents the proposed approach to perform research on traditional and modern proxy solutions for comparative analysis in cyber security. This chapter covers research design, data collection and analysis methods. This section also defined the steps taken to check the validity and reliability of the collected findings through interviews. The current research has been designed to use mixed investigation methodologies by incorporating both qualitative and quantitative investigations. It was looking for — a complete comparison of the efficacy, consistency and appropriateness of existing introductions with proprietary ones given individual cyber security needs.

Qualitative Component

The qualitative part of this research approach includes an extensive literature review and case study analysis. This extends to the practical applications of proxy solutions and the historical development behind these proxy suitors. This research methodology also includes the development of a framework for proxies, with a detailed analysis of each proxy.

Quantitative Component

This part of the research methodology concerns gathering and examining numerical data. Both proxies ' performance measurement, security effectiveness and scalability should be derived from analyzed data. Some of this data is based on statistical analysis, and real-world implementation metrics provide some.

Data Collection Methods

The literature review is the main data collection method and it is based on different academic papers, technical reports and other publications. Different case studies are also selected to identify different features and challenges of both proxy solutions. A deep analysis of these case studies is helpful to identify how different proxy solutions are implemented in different organizational contexts. These case studies were sources from academic publications and from industry reports. Another source of data collection is “University of Maryland CISSM Cyber Attacks Database”, this database consists of different types of proxy attacks recorded. The following detailed information is available on the cyber events stored in the database:

- Threat actor type (nation or state, hacktivist, criminal)
- Attack type (exploitative, disruptive, mixed)
- Target details (industry, country of impact)
- End effects and outcomes of the attacks

The cyber-attacks related to the both proxies are retrieved from this database to analyze the impact, weaknesses, and type of compromised proxy, targeted industry and targeted organizations related data is presented. All these methods are going to be used in this research to collect data related to the traditional and modern proxies. The data collected from these sources must be analyzed on the basis of different parameters. Like date of the attack, type of attack, type and nature of proxy compromised in the result of attack, identified weaknesses and vulnerabilities.

RESULTS AND DISCUSSION

Case Studies

Case Study 1: OKX - Decentralized Exchange Hack

- Date: December 12, 2023
- Actor: Undetermined
- Actor Type: Criminal
- Organization: OKX
- Industry: Finance and Insurance
- Motive: Financial
- Event Type: Exploitive
- Event Subtype: Exploitation of Application Server [12]

The decentralized exchange OKX was working quite perfectly, but suddenly a hacking attack exploit the vulnerabilities in the application server of the exchange. In this attack the attackers managed to redirect transactions of the user through a malicious proxy. This attack enables them to draw off funds during the exchange procedure. This attack identified different weaknesses in the server security. And also identified the need for improved proxy protection mechanisms [12].

This attack on OKX decentralized exchange is a significant event in the world of block chain technology. The decentralized finance (DeFi) platforms are growing in popularity, that's why these platforms are main targets for sophisticated cyber-attacks. This case study is going to investigate the methods used by the attackers. The impact of this attack on the platform and on users is going to be discussed.

The attack on OKX was precisely planned and executed quite accurately. The attackers identified the vulnerabilities in the protocols of smart contract. The attackers manipulate the price oracle and this manipulation allowed the attackers to create buying and selling opportunities. That's why, they buy assets at artificially low prices and sell them at high prices.

To avoid detection of this attack, the attackers routed their transactions through multiple proxy servers. This technique masked their original IP addresses and geographic locations. This proxy server tactic complicates the efforts of security team to trace the source and location of the malicious activities. The use of proxies was helpful for the attackers to conduct large trading activities. This attack was executed during a period of high market activity. This high market activity time helped the malicious transactions to mix-up with legitimate transactions.

The attack resulted in the theft of approximately $2.7 million worth of various crypto currencies assets. The use of proxy servers by attackers to exploit the vulnerabilities in the smart contract is a big security challenge [12]. This incident serves as a lesson for the cyber security experts, because proxy servers can be used to hide the location and source of the attack.

Case Study 2: i2VPN - Breach of VPN Service

- Date: June 5, 2023
- Actor: Undetermined
- Actor Type: Criminal
- Organization: i2VPN
- Industry: Management of Companies and Enterprises
- Motive: Undetermined
- Event Type: Exploitive
- Event Subtype: Exploitation of Application Server [12]

The attackers behind this attack also proclaimed that they had penetrated the i2VPN servers. According to the team, all proxy services of i2VPN were tampered with so that any transmitted data was intercepted and decrypted. The breach also exposed the sensitive information and user privacy of i2VPN users. This attack reminds us of the need to harden proxy services used by VPN providers [12].

It was a sophisticated, multi-stage operation that targeted i2VPN. This exploit was created to threaten the VPN service infrastructure, leaking user data. In the second week of April, cyber-criminals managed to enter i2VPN's network with a phishing campaign and started this attack. Various company employees began receiving phishing emails impersonating legitimate internal communications from the group. These phishing emails attract the employees of the company to click different malicious links and finally leading towards a malicious software installation. After obtaining access to the network, the attackers exploited vulnerabilities in i2VPN's server infrastructure. The server infrastructure was using outdated software and also weak proxy configurations allowed the attackers to access key systems of the company. The attackers spent several weeks in the i2VPN's network to infiltrated sensitive data. They access sensitive data like user login credentials, browsing histories, and other personal information [12]. In the last step of this attack, the sensitive data was transferred to the external servers.

The main impact of this attack was on the user privacy. The VPNs are used to ensure online anonymity and are used for secure communications. But this breach undermined these fundamental agreements. The browsing history of the users, their login credentials, and personal information were exposed.

Case Study 3: 911[.]re - Proxy Service Exploitation

- Date: July 28, 2022
- Actor: Undetermined
- Actor Type: Criminal
- Organization: 911[.]re
- Industry: Professional, Scientific, and Technical Services
- Motive: Financial
- Event Type: Exploitive
- Event Subtype: Exploitation of Application Server [12]

The proxy service 911[.]re is working since 2015. This proxy service faced a significant breach in which attackers exploited its application servers. The attackers, therefore, used the proxy network for criminal purposes. It is as if they used this proxy network to steal data from it and used it for unpermitted access on the restricted networks.

The 911[.] used to have a proxy service; the way it worked was just shared the access point into their residential IP addresses network. This way, users could mask their locations and bypass the geographical restrictions networks often place on various online services. In July 2022, however, attackers got the better of its application servers [12].

The attack on 911[.] revealing many security vulnerabilities in the network infrastructure. Using the exploits of these loopholes, attackers had successfully breached inside the application servers. Lastly, this got them to attack more; they changed the proxy network to a fluff house for destructiveness. By using the proxy network of the company, they performed different illegal activities. Like data theft, fraud, and unauthorized access to restricted networks. The proxy servers of the company were not secure enough, because they were using outdated proxy services in the network. This breach enforces the 911[.]re to shut down its operations temporarily. And this shutdown created widespread disruption to its legitimate users.

The main factor in this attack was the limited security measures deployed to protect the application servers. The attackers exploited vulnerabilities in the old proxy server software. Because unpatched software or weak authentication mechanisms allowed the attackers to breach network security parameters. After gaining access to the network, the attackers can control the proxy network [12]. They could use this proxy network to route their malicious traffic.

There are many consequences of this attack, but the potential risks associated with this attack are the usage of third-party proxy services. The third-party proxy services can create security problems for any business organization. Particularly those third-party proxy services that do not follow strict security practices.

To mitigate this type of attack in future, the 911[.]re had to conduct a comprehensive review of its security infrastructure. In this review, the need to patch the vulnerabilities that were exploited during this attack. And also, they need to implement stronger authentication and access controls. The incident also highlighted the importance of regular security audits and penetration testing. Because it is helpful to identify weaknesses and to mitigate potential vulnerabilities in the network before these vulnerabilities can be exploited by the attackers.

On the other hand, this breach leaves a lesson for the whole proxy service industry. After this attack, the other third-party proxy service providers must reconsider their security controls. And also, they need to implement more robust measures to protect their networks. Also, this incident raised awareness among users related to the risks of using proxy services.

Discussion

This section is going to evaluate and synthesize findings from the literature review and from detailed case studies. Also, the qualitative and quantitative analyses from the University of Maryland CISSM Cyber Attacks Database is going to be discussed. The main objective is to evaluate the efficiency and effectiveness of traditional and modern proxy solutions being used in cyber security industry [12]. Different trends in proxy-related attacks are observed to identify reliable proxy solution. And a meaningful conclusion is sketched related to the developing landscape of cyber security threats.

Literature Review Insights

The literature review explained the evolution of proxy solutions from traditional to modern solutions. The web proxies and forward proxies are presented as traditional solutions and cloud-based proxies and secure web gateways are presented a modern solution. The traditional proxies primarily served to cache content and to filter traffic. That's why, providing a basic level of security and improved network performance. However, modern proxies are equipped with advanced features to protect from cyber-attacks [7]. Like these features are deep packet inspection (DPI), real-time threat intelligence, and robust encryption methods. All these features are good enough to protect from sophisticated cyber threats.

On the other hand, several studies underlined the limitations of traditional proxies. These traditional proxies are vulnerable to advanced evasion techniques. And also providing limited scope to handle encrypted traffic. While, modern proxies offer improved capabilities to protect systems from all latest cyber threats. These modern proxies are offering improved visibility into encrypted traffic to filer the insecure traffic. These proxies are providing better user authentication mechanisms and integration with large security frameworks [11]. For example, the Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE) frameworks are working with modern proxies.

Quantitative Analysis from CISSM Database

An inclusive analysis of the CISSM Cyber Attacks Database is provided with complete quantitative analysis on the frequency of proxy related attacks and their impact on different industries. Out of the 13,408 documented cyber incidents, there is a big percentage of cyber security attacks where proxy servers are involved. Approximately 10% attacks are proxy server related attacks in this database.

Prevalence of Proxy Attacks: The attacks related to proxy have shown a rising trend from last decade. And it is indicating that that attackers are increasingly influencing the proxies to hide their locations. They are also using proxies to bypass traditional security measures. Particularly, the proxy server-based attacks are increased by 20% in the last five years. This figure is reflecting their growing role in the cyber security toolkits [12].

Attack Vectors and Methods: The data is showing that phishing campaigns were the most common methods being used for initial access. And after accessing the network, attackers are frequently using compromised proxy servers to redirect malicious traffic. In this way, they can infiltrate data and they can avoid detection.

Impact on Organizations: The analysis indicated that organizations targeted through proxy-related attacks are facing big financial and moral losses. The database is showing that organizations are facing an average loss of $3 million per incident [12]. This loss includes costs related to downtime of the system, data breaches, and mitigation efforts.

Qualitative Analysis from Case Studies

The case studies are presenting a qualitative aspect of the proxy related attacks. To understand the proxy-related cyber incidents, a detailed analysis of attacks on different organizations like OKX, i2VPN, and 911[.]re is presented.

OKX - Decentralized Exchange Hack: This case study is stating that how attackers are using proxy servers to hide their identities. And how they can conduct a sophisticated attack on a decentralized exchange. This security breach managed to theft large amount of cryptocurrency assets. And this attack highlighted the vulnerabilities within the decentralized financial systems [12].

i2VPN - Breach of VPN Service: The i2VPN case study demonstrated that how attackers used proxy servers for phishing attack. After entering the network, they managed to access secure data of the company. This breach compromised the privacy of the users and goodwill of the company was also compromised. Also, this case study highlighted the importance of strong security measures for the VPN services.

911[.]re - Proxy Service Exploitation: The attack on 911[.]re demonstrated big impact of compromised proxy servers. The attackers used vulnerability in the proxy services of the company to control the direction and rout of the traffic [12]. This attack allowed the attackers to avoid detection and to access sensitive financial data of the company. Due to this attack the company faced major disruption in their operations. And also, they face significant reputational damage.

Evaluation of Traditional vs. Modern Proxy Solutions

Traditional proxies have played a foundational role in network security, particularly web proxies and forward proxies are very important for network security. The primary functions of these proxies are filtering URL, access control and content caching. But these proxies are facing limitations, because new techniques and sophisticated methods are being used by the attackers to breach these proxy solutions. Following are few limitations of these proxies.

- Limited Visibility: Traditional proxies are facing difficulties to examine encrypted traffic. This weakness is making them less effective against modern threats. For example, the inspection of HTTPS based encrypted traffic is quite difficult for these proxies [2].

- Static Rule Sets: Traditional proxies are depending on static rule sets. And this makes traditional proxies less effective to block or avoid emerging threats. Also, this static rule set is not effective for latest intrusion techniques.

- Scalability Issues: The network traffic is growing, while traditional proxies are face scalability challenges. In the long run these challenges are leading towards performance bottlenecks [11].

The modern proxies like secure web gateways (SWGs) and cloud-based proxies are quite useful to address many limitations of traditional solutions. Following are few advance features of these modern proxy solutions:

- Deep Packet Inspection (DPI): The modern proxy solutions are using DPI to analyze the content of data packets in real-time. This feature is providing better detection of malware. And suspicious activities can be flagged as a proactive security measure.

- Real-Time Threat Intelligence: Modern proxy solutions are integrated with threat intelligence feeds. And this threat intelligence feed allows modern proxies to upgrade with new threats dynamically. This feature is improving their effectiveness to control latest and sophisticated attacks.

- Encryption Handling: These proxies are equipped with enhanced capabilities to inspect and handle encrypted traffic quite efficiently. Also, this capability is not compromising their performance or security at any level.

- Scalability and Flexibility: The cloud-based proxies are offering scalability and flexibility. That’s why, cloud-based proxies are accommodating the needs of growing networks and providing flexibility to remote users.

Comparative Effectiveness

The qualitative and quantitative analyses reveal that modern proxy solutions are secure as compare to the traditional proxy solutions. In this research the modern proxy solutions significantly outclass the traditional proxies in terms of security effectiveness, scalability, and adaptability in different framework environments. The organizations using modern proxies experienced less successful breaches as compare to the traditional proxies. The incident response times of modern proxy solutions is fast as compared to the traditional proxy solutions. That is why, modern proxy solutions are more effective as compare to the traditional solutions, because modern proxy solutions can really protect the systems from all sophisticated attacks.

Findings from Case Studies

- Enhanced Detection: The modern proxies were helpful in detecting and mitigating advanced cyber security threats in real-time. The detailed responses by organizations like i2VPN and OKX are showing that modern proxies are providing enhanced detection [12].

- Improved Incident Response: The organizations with modern proxy solutions are more effective in incident response activity. This positivity of modern solutions is minimizing the impact of breaches.

- Regulatory Compliance: The enhanced data encryption and monitoring capabilities of modern proxies helped the organizations to meet different strict regulatory requirements. That is why, this feature of modern proxies is reducing the risk of legal and financial penalties [12].

Broader Implications and Future Directions

The increasing complexity of cyber-attacks is demanding continuous developments in proxy solutions. The attackers are developing new evasion techniques to target different security vulnerabilities in the systems. That is why, the proxy technologies must evolve to provide robust defense mechanisms. The future proxy solutions are likely to integrate artificial intelligence (AI) and machine learning (ML) to meet future requirements of cyber security [11]. The combination of AI and ML in proxy solutions can be helpful to predict and counter emerging threats proactively.

Integrating proxy solutions with various security frameworks can be even more useful in making an overall cybersecurity approach possible. When defining lateral entry safeguarding in cyberspace, Zero Trust Architecture (ZTA) and Secure Access Service Edge (SASE) frameworks are invaluable. Crucial in this upcoming battle will be the implementation of these frameworks alongside current proxies, ensuring universal coverage. These frameworks provide continuous verification and the least privileged access to safeguard the security architecture of organizations. When combined with proxy solutions, these methods and frameworks can assist in implementing dynamic policy enforcement, which helps organizations enforce a much more secure posture.

Recommendations for Organizations

- Adopt Modern Proxy Solutions: Organizations should move towards modern proxy solutions. Moreover, ensure that they choose a trustworthy proxy solution that includes advanced threat detection and debugging support on real-time alerts, preparing the enterprise for another 10 years of scalability.

- Continuous Monitoring and Updating: A vital recommendation that helps to keep the network assets secure from cyber threats. Regularly upgrade proxy configurations for an organization. They should also correlate with threat intelligence feeds that help predict the cyber security threats that would crop up.

- Employee Training: The organizations should implement comprehensive cyber security training programs. Because these training programs can prepare employees to recognize different security threats. This training can guide the employee to respond different phishing and social engineering attacks.

- Incident Response Planning: Incident response is very important for any cyber security solution. That is why, the organizations must develop a comprehensive incident response plan. Also, they need to regularly test incident response plans to ensure quick and effective response against potential breaches.

CONCLUSION

This comparative analysis of traditional and modern proxy solutions is showing the critical role of advanced proxy technologies. All modern proxy solutions are more proactive to defend against sophisticated cyber threats. The integration of modern proxies with security frameworks is providing proactive threat intelligence. Overall, the modern proxies are providing robust incident response strategies. The integrated version of modern proxies with security frameworks is very important for organizations. Because, with these necessary tools the organizations can protect sensitive data and can maintain operational integrity. With the passage of time the cyber security threat landscape continues to grow. That’s why, the adoption of cutting-edge proxy solutions will be essential to protect digital assets of organizations in the whole world.

ETHICAL DECLARATION

Conflict of interest: No declaration required. **Financing:** No reporting required. **Peer review:** Double anonymous peer review.

REFERENCES

[1] M. S. Pour, C. Nader, K. Friday, and E. Bou-Harb, "A comprehensive survey of recent internet measurement techniques for cyber security," *Computers & Security*, vol. 128, p. 103123, Jan. 2023, doi: 10.1016/j.cose.2023.103123.

[2] P. Triantafillou and I. Aekaterinidis, "ProxyTeller: A tool for guiding web proxy cache placement decisions," *WWW (Posters)*, 2003. Accessed: Aug. 19, 2024. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=e905ee9a2ace5432b9d1d01a48145d62a46c164d

[3] O. Obi, O. Akagha, S. Dawodu, A. Anyanwu, S. Onwusinkwue, and I. Ahmad, "Comprehensive review on cybersecurity: Modern threats and advanced defense strategies," *Computer Science & IT Research Journal*, vol. 5, pp. 293-310, 2024. doi: 10.51594/csitrj.v5i2.758.

[4] J. Yeh, "Key factors in building a Secure Web Gateway," M.S. thesis, Master of Cyber Security (MCS), Univ. of Waikato, Hamilton, New Zealand, 2017. [Online]. Available: https://hdl.handle.net/10289/11548

[5] S. Kim and I. Lee, "IoT device security based on proxy re-encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, pp. 1267–1273, 2018. doi: 10.1007/s12652-017-0602-5.

[6] T. O. Abrahams, S. K. Ewuga, S. O. Dawodu, A. O. Adegbite, and A. O. Hassan, "A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection," *Computer Science and IT Research Journal*, vol. 5, no. 1, pp. 1–25, Jan. 2024, doi: 10.51594/csitrj.v5i1.699.

[7] K. Kavya and A. Rengarajan, "Reverse proxy technology," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 12, pp. 1067-1071, 2024. doi: 10.15680/IJIRCCE.2024.1202057.

[8] J. M. Couretas, "Cyber security and defense for analysis and targeting," An Introduction to Cyber Analysis and Targeting, pp. 119–150, 2022, doi: 10.1007/978-3-030-88559-5_6.

[9] R. -V. Tkachuk, D. Ilie and K. Tutschku, "Towards a secure proxy-based architecture for collaborative AI engineering," in *2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW)*, Naha, Japan, 2020, pp. 373-379, doi: 10.1109/CANDARW51189.2020.00077.

[10] R. M. da C. Costa Caldas, "Proxy-based solution for legacy IoT security and privacy," M.S. thesis, Univ. of Porto, Porto, Portugal, 2021. [Online]. Available: https://hdl.handle.net/10216/135000

[11] K. Obour Agyekum et al., "A secured proxy-based data sharing module in IoT environments using blockchain," *Sensors*, vol. 19, no. 5, p. 1235, Mar. 2019, doi: https://doi.org/10.3390/s19051235.

[12] CISSM Cyber Attacks Database, Mar. 2024, "University of Maryland CISSM Cyber Attacks Database,". [Online]. Available: https://cissm.liquifiedapps.com/