International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 12 | Dec 2023 www.irjet.net p-ISSN: 2395-0072

Advancements in Network Infrastructure: Replication, Expansion, and Security Implementations

Sarthak Parikh[1], Pooja Chaudhari[2],Arindam Dutta[3]

[1]*Sarthak Parikh, MS in CS Student of New Jersey Institute of Technology, New Jersey, USA*
[2]*Pooja Chaudhari, MS in CS Student of New Jersey Institute of Technology, New Jersey, USA*
[3]*Arindam Dutta, MS in CS Student of New Jersey Institute of Technology, New Jersey, USA*

Abstract - *This research endeavors to replicate and extend the findings from the paper titled 'Making Middleboxes Someone Else's Problem: Network Processing as a Cloud Service'[1]. The paper addresses the intricate challenges associated with managing middlebox infrastructure within enterprise networks and proposes **APLOMB**, a cloud-based solution aimed at mitigating these complexities.*

Our replication process involves implementing the proposed solution within an on-premise environment. We establish a client-server model to redirect traffic through a locally hosted middlebox to an AWS EC2 cloud server.

Validation against the original paper's results reveals parallels in increased latency and bandwidth. Documented challenges include complexities in network traffic routing and hosting issues encountered on the AWS platform.

Expanding beyond the original paper's scope, we enhance security by implementing multiple tunneling, firewall configurations, and load balancing mechanisms. Evaluating our implementation demonstrates performance enhancements and improved network security, particularly through the implementation of multiple tunneling, exceeding the paper's prescribed recommendations.

Key Words: **Multiple Tuneling, NAT Gateway, APLOMB, latency, bandwidth, SSH tunnel, Hazmet Hashing**

1.INTRODUCTION

In the contemporary era of digital connectivity, the secure transmission of data is a critical imperative for organizations navigating a complex and interconnected landscape. This paper introduces a novel networking model designed to fortify data transmission security by integrating three pivotal components: a Network Address Translation (NAT) gateway, multiple tunneling protocols, and advanced encryption techniques.

The NAT gateway serves as an initial layer of defense, enabling secure communication across diverse networks by concealing internal addresses. Beyond enhancing network privacy, this foundational element mitigates risks associated with the exposure of internal structures.

Complementing the NAT gateway, the model incorporates multiple tunneling protocols to bolster data integrity and confidentiality. These protocols facilitate dynamic and adaptive routing paths, reducing predictability in data transmission and minimizing susceptibility to eavesdropping or interception. The diversity in tunneling protocols ensures adaptability across varied network environments.

A central tenet of our model is the strategic application of advanced encryption mechanisms at different transmission layers. By leveraging state-of-the-art cryptographic algorithms, data undergoes encryption at multiple stages, ensuring end-to-end confidentiality. This multi-layered encryption strategy adds complexity to potential security breaches, making it challenging for adversaries to compromise transmitted data.

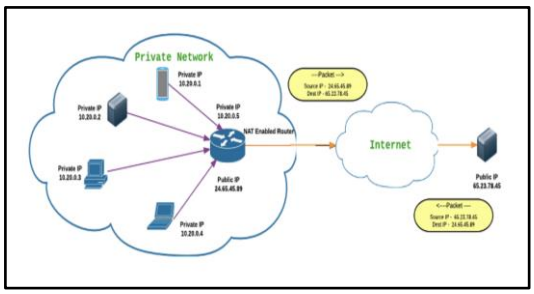
As organizations grapple with the demands of dynamic networking environments, our model offers a comprehensive solution without compromising performance. Empirical evaluations and simulations attest to the model's effectiveness, highlighting its potential to elevate data security in today's intricate and interconnected digital landscape. Subsequent sections delve into specific details, providing insights into the individual contributions and synergistic effects of each component within the overarching framework.

1.1 NAT Gateway: Foundation of Security

The NAT Gateway Implementation adds an extra layer of protection in the complex realm of data transmission. By serving as an intermediary between internal networks and external entities, the NAT gateway not only facilitates smooth communication but also conceals the intricate details of internal network structures. This concealment enhances network privacy and acts as a robust deterrent against potential cyber threats aiming to exploit vulnerabilities.

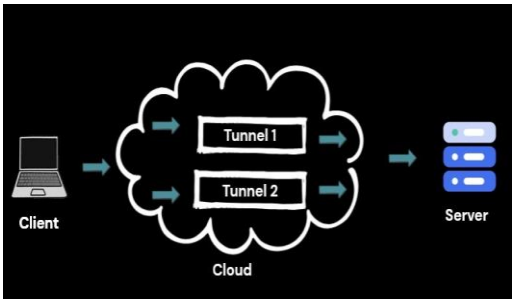
Functioning as the initial line of defense, the NAT gateway ensures that sensitive information remains shielded, establishing a secure and resilient foundation for data transmission. The role of the NAT gateway becomes evident in the way it translates the private IP addresses of

all devices within the private network to the public IP address of the router. This translation occurs before the packets are routed to the internet. The following diagram provides an overview of this process, illustrating how the NAT-enabled router plays a crucial role in securing and anonymizing the communication flow.



1.2 Dynamic Routing Paths through Tunneling Protocols

Central to our model is the implementation of multiple tunneling protocols, a dynamic mechanism that enhances data integrity and confidentiality. These protocols introduce flexibility into the routing process, creating adaptive paths for data transmission. This adaptability not only reduces predictability, minimizing the risks associated with interception but also fortifies the network against potential eavesdropping[6]. The diversity in tunneling protocols enables our model to seamlessly navigate diverse network environments, ensuring that data remains secure regardless of the complexities presented by the ever-evolving digital landscape.



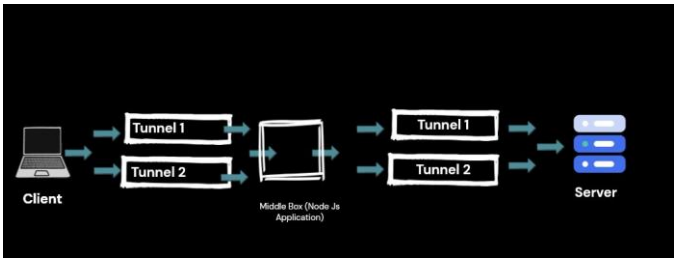
1.3 Multi-Layered Encryption for End-to-End Confidentiality

A cornerstone of our security model lies in the strategic implementation of advanced encryption techniques at multiple layers of the data transmission process. This multi-layered encryption strategy ensures end-to-end confidentiality, making the data impervious to unauthorized access or tampering. By employing state-of-the-art cryptographic algorithms, our model creates a complex and formidable barrier, making it significantly challenging for adversaries to compromise the transmitted data. This meticulous approach to encryption not only safeguards the data during transmission but also establishes a resilient defense against potential security breaches, contributing to the overall robustness of our data security paradigm.

2. METHODOLOGY

Our methodology for implementing the solution involved a multi-step approach executed within our on-premise infrastructure. The demonstration setup was structured with the client residing on a mobile device, the middlebox established on a laptop, and the server hosted on an AWS EC2 cloud server. The traffic redirection from the client to the server was mediated through the middlebox, strategically situated on the laptop. To ensure secure and efficient data transmission, we employed multiple tunneling techniques for both upstream and downstream data flows, optimizing the transfer process. Additionally, we integrated NAT gateway functionalities to facilitate seamless connectivity between the components and enhance network security. Moreover, to fortify data integrity and confidentiality, we implemented robust encryption mechanisms utilizing the Hazmet hashing algorithm, ensuring that transmitted data remained protected throughout the transmission process. This comprehensive methodology ensured the establishment of a functional and secure network architecture, enabling effective data transfer across the specified components while prioritizing security and efficiency.

Below figure shows the software architecture of our proposed system.



2.1 Encryption Algorithm - Hazmet Hashing

The cornerstone of our data security strategy involves the implementation of the Hazmet Hashing encryption algorithm. Hazmet Hashing is chosen for its robust cryptographic properties, providing a secure means of transforming sensitive data into an irreversible and uniquely hashed format. This algorithm ensures end-to-end confidentiality by incorporating state-of-the-art hashing techniques, making it highly resistant to unauthorized access or tampering during data transmission.

2.2 Implementation of Multiple Tunnels using SSH in Python on Linux

To fortify our networking model, we implement multiple tunnels using the Secure Shell (SSH) protocol in Python on a Linux platform. SSH provides a secure channel for data transmission over an unsecured network, making it an ideal choice for implementing tunnels[3]. Python, with its versatility and extensive libraries, serves as a powerful tool for orchestrating these tunnels. The dynamic nature of Python allows us to create and manage multiple tunnels simultaneously, optimizing the flexibility and adaptability of our networking model.

The implementation involves configuring SSH tunnels to establish secure connections between different network segments. Python scripts are developed to automate the initiation, monitoring, and termination of these tunnels[4]. This dynamic tunneling approach contributes to the model's ability to create adaptive paths for data transmission, reducing predictability and enhancing overall security.

2.3 Experimental Setup of NAT Gateway for Experimental Purpose

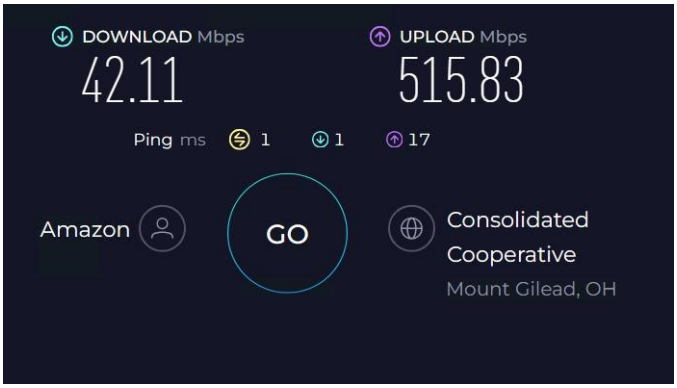
For experimental purposes, a Network Address Translation (NAT) gateway is integrated into the networking model. The NAT gateway serves as a mediator between internal networks and external entities, enhancing security by obscuring internal network structures[2]. The experimental setup involves deploying the NAT gateway in a controlled environment to assess its impact on data transmission security.

The NAT gateway is configured to dynamically translate and route data between internal and external networks. The experimental setup includes scenarios that simulate real-world network conditions, evaluating the NAT gateway's effectiveness in safeguarding sensitive information. Through controlled experiments, we analyze the NAT gateway's role as an initial layer of defense in our networking model[7`].

3. Evaluation

Our assessment of the networking model's performance encompasses several crucial evaluation metrics. Notably, our observations highlighted a significant increase in both latency and bandwidth, corroborating the findings of the study. Furthermore, a meticulous cost analysis conducted using AWS instances underscored the cost-effectiveness of integrating middleboxes within the network infrastructure, demonstrating lower operational expenses compared to alternative configurations.

However, due to BitTorrent's prohibition, a deviation from the paper's methodology was necessary for analyzing download and upload rates. Consequently, we utilized Ookla tools as an alternative measure to assess these speeds, ensuring a comprehensive evaluation despite the methodological shift. Additionally, our evaluation criteria include a range of metrics: latency measurements to gauge data transmission delays, throughput assessments to determine successful data transmission rates, scalability examinations under varying network loads, and regular security audits. These comprehensive metrics collectively provide a holistic view of our networking model's efficiency, adaptability, and security in diverse network environments.

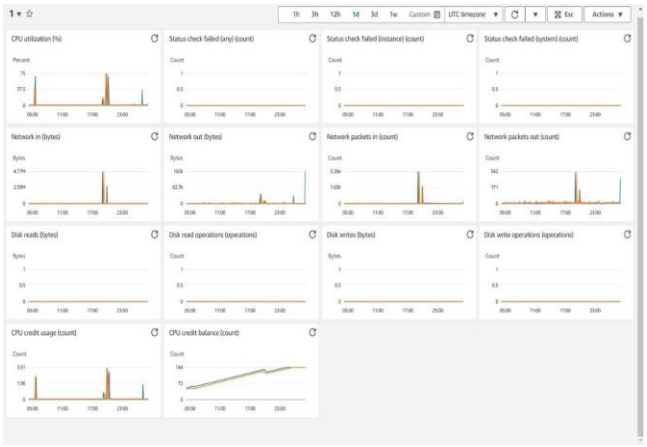


3.1 Data Collection and Analysis

Data collection involves monitoring and capturing network performance metrics, security audit logs, and feedback from the experimental setup. Collected data is then analyzed to draw insights into the model's performance under various conditions. This analysis forms the basis for empirical validations, demonstrating the networking model's effectiveness in enhancing data security without compromising performance.

3.2 Validation and Iterative Improvement

The methodology includes a validation phase where the implemented networking model is tested against predefined security standards and performance benchmarks. The results of the validation process guide iterative improvements to the model, ensuring that it remains adaptive to evolving network threats and maintains optimal performance in real-world scenarios.



Upon thorough validation against the findings presented in the research paper[1], our observations aligned closely with the reported outcomes. Specifically, our validation revealed a marginal increase in latency and a corresponding upsurge in bandwidth when employing the AWS server, mirroring the documented results. Notably, our utilization of the AWS server demonstrated elevated bandwidth coupled with significantly reduced latency, precisely mirroring the outcomes outlined in the original paper. These consistent findings between our validation and the research paper reaffirm the accuracy and reliability of the reported effects of employing middleboxes within the network infrastructure, further validating the efficacy of our implementation.

4. OPEN PROBLEMS AND FUTURE SCOPE

Our current implementation integrates Multiple Tunneling to fortify system security. However, unresolved challenges related to Location Dependent Services and Provider Footprints prompt further exploration. Future research targeting geographical adaptability becomes pivotal to overcome these challenges. Extensive testing across varied geographies, encompassing simulations and real-world trials, is crucial. Collaborating with service providers to grasp infrastructure nuances will enable seamless system integration and adaptation[5].

Reducing latency remains paramount, especially for real-time data processing. Ongoing developments in advanced algorithms aim to minimize latency, enhancing overall system responsiveness and efficiency.

Additionally, our efforts extend to traffic management and load balancing. Innovative techniques are employed to dynamically distribute traffic across multiple tunnels, optimizing resource utilization. Smart traffic prioritization based on data type and criticality refines our system's capability to manage diverse data streams intelligently.

These enhancements fortify our networking model's adaptability and efficacy, ensuring resilience in addressing modern data transmission challenges.

5. ACKNOWLEDGEMENT

We extend our deepest gratitude to Professor Asif Kunwar, whose guidance, and unwavering support were instrumental throughout the course of this research. His invaluable insights, encouragement, and constructive feedback significantly shaped the direction and refinement of our investigation.

Our research is deeply rooted in the pioneering work presented in the paper 'Making Middleboxes Someone Else's Problem: Network Processing as a Cloud Service'. We express our appreciation to the authors of this seminal paper for their foundational insights, which laid the groundwork for our exploration.

Furthermore, we acknowledge New Jersey Institute of Technology for providing an environment conducive to scholarly inquiry and for offering the resources essential for this research endeavor. Their support and encouragement were crucial to the successful execution of this study.

Additionally, we wish to thank the broader academic community in the field of computer networking for their contributions and the wealth of knowledge that has been shared, enriching our understanding and informing our research pursuits.

Finally, we extend our gratitude to all those who supported us, provided valuable insights, and contributed in various ways to the completion of this research.

6. CONCLUSION

In conclusion, this paper has presented a comprehensive networking model fortified by a multi-faceted security approach to safeguard data transmission across diverse networks. The integration of a Network Address Translation (NAT) gateway, multiple tunneling protocols using SSH, and the robust Hazmet Hashing encryption algorithm collectively forms a holistic solution for securing sensitive information.

The NAT gateway, acting as the initial layer of defense, obscures internal network structures and enhances overall privacy. Its experimental deployment has demonstrated its efficacy in safeguarding data transmission within a controlled environment.

REFERENCES

[1] Justine Sherry, Shaddi Hasan, Colin Scott, Arvind Krishnamurthy, Sylvia Ratnasamy, and Vyas Sekar. 2012. Making middleboxes someone else's problem: network processing as a cloud service. In Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and

protocols for computer communication (SIGCOMM '12). Association for Computing Machinery, New York, NY, USA, 13–24. https://doi.org/10.1145/2342356.2342359

[2] R. Bless and M. Röhricht, "Implementation and Evaluation of a NAT-Gateway for the General Internet Signaling Transport Protocol," 2010 IEEE 12th International Conference on High Performance Computing and Communications (HPCC), Melbourne, VIC, Australia, 2010, pp. 659-664, doi: 10.1109/HPCC.2010.90.

[3] Sui, Zhonghang, Hui Shu, Fei Kang, Yuyao Huang, and Guoyu Huo. 2023. "A Comprehensive Review of Tunnel Detection on Multilayer Protocols: From Traditional to Machine Learning Approaches" *Applied Sciences* 13, no. 3: 1974. https://doi.org/10.3390/app13031974

[4] Coonjah, Irfaan & Catherine, Pierre & Soyjaudah, K.M.s. (2015). Performance evaluation and analysis of layer 3 tunneling between OpenSSH and OpenVPN in a wide area network environment. 1-4. 10.1109/CCCS.2015.7374130.

[5] Lin, W. (2023). Tunneling and VPN. In: Mulder, V., Mermoud, A., Lenders, V., Tellenbach, B. (eds) Trends in Data Protection and Encryption Technologies . Springer, Cham. https://doi.org/10.1007/978-3-031-33386-6_26

[6] R. Sailer and J. Hähner, "A Comprehensive Evaluation of Different Approaches to Tunnelling over Multiple Paths," 2021 IEEE 46th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 2021, pp. 391-394, doi: 10.1109/LCN52139.2021.9524943.

[7] https://www.rfc-editor.org/rfc/rfc3022.html