Rochester Institute of Technology

RIT Digital Institutional Repository

Theses

2023

Multifactor Authentication Using Zero Trust

Mathews Rajan Alappat mra6658@rit.edu

Follow this and additional works at: https://repository.rit.edu/theses

Recommended Citation

Alappat, Mathews Rajan, "Multifactor Authentication Using Zero Trust" (2023). Thesis. Rochester Institute of Technology. Accessed from

This Thesis is brought to you for free and open access by the RIT Libraries. For more information, please contact repository@rit.edu.



MULTIFACTOR AUTHENTICATION USING ZERO TRUST

By

Mathews Rajan Alappat

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Computing Security

Supervised by

Dr. Wesam Almobaideen

Department of Electrical Engineering & Computing

Rochester Institute of Technology Dubai Campus

United Arab Emirates

2023

RIT

Master of Science in

Computing Security

Thesis Approval

Multifactor Authentication Using Zero Trust

Student Name: Mathews Rajan Alappat

Dr. Wesam Almobaideen Professor Dept. of Electrical Engineering and Computing	(Thesis Advisor)
Dr. Huda Saadeh Assistant Professor Dept. of Electrical Engineering and Computing	(Committee Member)
Dr. Khalil Al Husseini Assistant Professor Dept. of Electrical Engineering and Computing	(Committee Member)

Acknowledgements

First and foremost, I would like to express my heartfelt gratitude to the Almighty for granting me the strength, guidance, and perseverance throughout this journey of completing my thesis.

I am deeply indebted to my Thesis Advisor, Dr. Wesam Almobaideen, for his unwavering support, invaluable guidance, and profound knowledge in the field. His expertise and constructive feedback have played a pivotal role in shaping this thesis.

I would like to take this opportunity to express my heartfelt gratitude to Dr. Huda Saadeh and Dr. Khalil Al Husseini, who generously dedicated their time and expertise as members of my thesis committee. I would also like to extend my sincere appreciation to the Department of Electrical Engineering and Computing for providing me with the necessary resources and a conducive environment to carry out my research work.

To my beloved wife Juby, my sister Ria and my loving parents, I am immensely grateful for their unwavering love, understanding, and encouragement throughout this challenging endeavor. Their constant support and belief in my abilities have been a source of motivation and strength.

I would also like to acknowledge my colleagues at Digital Insights, whose support and encouragement have been invaluable.

I am truly fortunate to have had the guidance and mentorship of individuals like Sreeram and Roy. Their wisdom, expertise, and invaluable assistance have been instrumental in completing this work successfully.

Lastly, I would like to express my gratitude to all those who have supported and inspired me during this journey, including my friends and family members. Their words of encouragement and belief in my capabilities have been invaluable.

ABSTRACT

In today's world, industries are constantly integrating new technologies to improve workplace flexibility and customer service. However, this also creates a broader attack surface for attackers, making it easier for them to identify weaknesses and exploit them, leading to security lapses that cost businesses both money and goodwill. To address this issue, information technology security professionals have developed the Zero Trust framework. This framework focuses on carefully examining each and every attempt made to access the resources, restricting access only to those authorized individuals and providing them with minimum privileges to accomplish their specific tasks successfully. The underlying concept behind this approach is that businesses should not naively trust anything or anyone, whether inside or outside their boundaries without verification. In this thesis, we examine the effectiveness of the currently available Zero Trust frameworks and multifactor authentication techniques for improving information technology security and to overcome the limitations of current authentication systems to safeguard businesses against cyberattacks. This thesis provides a realistic Zero Trust Framework that combines Zero Trust principles with multifactor authentication techniques to enhance security. Unlike most existing research works, this thesis goes beyond theoretical proposals by providing an actual implementation and comprehensive guidelines for organizations looking to adopt Zero Trust. The security of the framework was further scrutinized through a security analysis, which involved assessing the system's security through practical testing, examination of potential attack vectors such as sniffing and password compromise, and evaluating the system's resilience against these threats, which is attributed to the combination of diverse security practices that is being discussed in detail in this thesis. In addition to evaluating the security effectiveness of the proposed Zero Trust framework, the thesis also delves into analyzing its performance efficiency and user satisfaction. While robust security measures are crucial, it is equally important to ensure that users are not inconvenienced by complex or time-consuming authentication processes. The analysis of performance efficiency and user satisfaction provides valuable insights into how the proposed framework achieves this balance, enhancing security while maintaining a positive user experience.

Keywords: Attack Surface, Zero Trust, Framework, Authentication, Least Privilege, Security.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	I
ABSTRACT	II
TABLE OF CONTENTS	.III
LIST OF FIGURES	V
LIST OF TABLES	.IX
CHAPTER 1: INTRODUCTION	.10
1.1 PROBLEM STATEMENT	.14
1.2 MOTIVATION.	.15
1.3 RESEARCH AIMS AND METHODOLOGY	.17
1.4 STRUCTURE OF THE THESIS	.19
CHAPTER 2: BACKGROUND AND LITERATURE REVIEW	.20
2.1 FRAMEWORKS	20
2.2 AUTHENTICATION MECHANISMS	.25
CHAPTER 3: PROPOSED ZERO TRUST FRAMEWORK	.34
3.1 ZERO TRUST MODEL & ZERO TRUST ARCHITECTURE (ZTA)	34
3.2 ELEMENTS OF THE PROPOSED ZERO TRUST FRAMEWORK	35
3.3 LOGICAL COMPONENTS OF THE PROPOSED ZERO TRUST FRAMEWORK	
(ZTF)	.44
3.4 WORKING MECHANISM OF THE PROPOSED ZERO TRUST FRAMEWORK	.48
3.5 MULTILAYER AUTHENTICATION MECHANISMS IN THE PROPOSED ZERO	
TRUST FRAMEWORK	.50
CHAPTER 4: IMPLEMENTATION OF THE PROPOSED ZERO TRUST	
FRAMEWORK	.53
4.1 IMPLEMENTATION OF THE PROPOSED ZERO TRUST FRAMEWORK	.53
4.2 IMPLEMENTATION OF MULTI FACTOR AUTHENTICATION IN THE PROPOSED)
ZERO TRUST FRAMEWORK	.54
4.3 WORKING MECHANISM OF THE IMPLEMENTATION OF THE PROPOSED ZERO)
TRUST FRAMEWORK	.59

CHAPTER 5: COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIE	NCY AND
USER SATISFACTION OF THE PROPOSED FRAMEWORK	65
5.1 COMPARATIVE ANALYSIS OF THE PROPOSED ZERO TRUST MFA	
FRAMEWORK	
5.1.1 WINDOWS LOGIN TIME COMPARISON	65
5.1.2 OPENVPN CLIENT LOGIN TIME COMPARISON	66
5.1.3 USER SATISFACTION	67
CHAPTER 6: INFORMAL SECURITY ANALYSIS OF THE PROPOSED Z	ERO TRUST
MULTI FACTOR AUTHENTICATION FRAMEWORK	68
6.1 SECURITY ANALYSIS OF THE PROPOSED ZTA FRAMEWORK	68
6.2 SECURITY PARAMETERS OF THE PROPOSED ZERO TRUST MFA FRA	MEWORK
	69
6.2.1 USER CERTIFICATE ISSUANCE	70
6.2.2 USER AUTHENTICATION AND VPN CONNECTION	
6.2.3 MULTIFACTOR AUTHENTICATION	71
6.2.4 TRUENAS FILE SERVER ACCESS	72
6.2.5 SECURITY MONITORING	73
6.2.6 ADVERSARIAL MODEL	73
CHAPTER 7: CONCLUSIONS AND FUTURE WORK	77
7.1 CONCLUSION	77
7.2 PROPOSED FUTURE WORK	
REFERENCES	80
APPENDIX A	
SETTING UP PFSENSE FIREWALL AND OPENVPN SERVER	88
SETTING UP ACTIVE DIRECTORY	
SETTING UP DUO SECURITY FOR TWO FACTOR AUTHENTICATION	105
SETTING UP TRUENAS FILE SERVER	115
SETTING UP ALIEN VAULT OSSIM SIEM	123

LIST OF FIGURES

FIGURE 1: NIST CYBER SECURITY FRAMEWORK	22
FIGURE 2: NIST ZERO TRUST FRAMEWORK	23
FIGURE 3: WORKING OF A VPN	36
FIGURE 4: WORKING OF A FIREWALL	37
FIGURE 5: RADIUS PROTOCOL	38
FIGURE 6: WORKING OF DUO AUTHENTICATION PROXY	42
FIGURE 7: ZERO TRUST LOGICAL COMPONENTS	45
FIGURE 8: PROPOSED ZERO TRUST FRAMEWORK WORKING MECHANISM	48
FIGURE 9: GENERAL AUTHENTICATION PROCESS AT DIFFERENT LAYERS	50
FIGURE 10: AUTHENTICATION AT VARIOUS LAYERS	52
FIGURE 11: PROPOSED ZERO TRUST FRAMEWORK	54
FIGURE 12: INTERNAL CERTIFICATE AUTHORITY	55
FIGURE 13: AD CREDENTIALS FOR LOGGING INTO THE DOMAIN	56
FIGURE 14: DUO MFA PUSH AUTHENTICATION FROM DUO MOBILE APP	57
FIGURE 15: DUO'S LOCATION BASED USER ACCESS POLICY	58
FIGURE 16: PROPOSED ZERO TRUST FRAMEWORK IMPLEMENTATION WORK	ING
MECHANISM	59
FIGURE 17: OPENVPN CLIENT LOGIN	60
FIGURE 18: DUO PUSH REQUEST NOTIFICATION AT THE TIME OF LOGIN	61
FIGURE 19: DUO MFA PUSH REQUEST TO USER'S PHONE	62
FIGURE 20: TRUENAS FILE SERVER CONSOLE PROTECTED BY DUO MFA	63
FIGURE 21: ALIEN VAULT SIEM DASHBOARD	63
FIGURE 22: ALIEN VAULT SIEM SECURITY ALARMS	64
FIGURE 23: WIRESHARK CAPTURE OF ENCRYPTED USER PASSWORD	75
FIGURE 24: VIRTUAL ENVIRONMENT SETUP USING VIRTUAL BOX 7.0	88
FIGURE 25: PFSENSE FIREWALL COMMAND LINE CONSOLE	89
FIGURE 26: PFSENSE FIREWALL WEB CONSOLE	89
FIGURE 27: INTERNAL CERTIFICATE AUTHORITY IN PFSENSE	90
FIGURE 28: DEF COMPANY SERVER CERTIFICATE	91

FIGURE 29: DEF COMPANY USER CERTIFICATE	91
FIGURE 30: SETTING UP RADIUS SERVER FOR AUTHENTICATION	92
FIGURE 31: CONFIGURING FIREWALL RULES	93
FIGURE 32: OPENVPN SERVER SETUP CONFIGURATION PART1	95
FIGURE 33: OPENVPN SERVER SETUP CONFIGURATION PART2	95
FIGURE 34: OPENVPN SERVER SETUP CONFIGURATION PART3	96
FIGURE 35: OPENVPN SERVER SETUP CONFIGURATION PART4	96
FIGURE 36: OPENVPN CLIENT EXPORT UTILITY	97
FIGURE 37: OPENVPN CLIENT DOWNLOAD	98
FIGURE 38: OPENVPN CLIENT LOGIN PROMPT	
FIGURE 39: RDP CONNECTION INITIATION	99
FIGURE 40: PROVIDING RDP CONNECTION CREDENTIALS	99
FIGURE 41: SETTING UP ACTIVE DIRECTORY IN SERVER 2019	100
FIGURE 42: SETTING UP DNS IN ACTIVE DIRECTORY	100
FIGURE 43: ACTIVE DIRECTORY USERS	101
FIGURE 44: VPN USERS GROUP	102
FIGURE 45: NETWORK POLICY SERVER	102
FIGURE 46: PFSENSE RADIUS CLIENT CONFIGURATIONS	103
FIGURE 47: SETTING UP NETWORK POLICY FOR VPN USERS GROUP	103
FIGURE 48: USER WORKSTATION WINDOWS LOGIN SCREEN	104
FIGURE 49: USER WORKSTATION CONNECTED TO COMPANY DOMAIN	104
FIGURE 50: DUO ADMIN LOGIN PROMPT	
FIGURE 51: DUO ADMIN WEB CONSOLE	
FIGURE 52: DUO PROXY CONFIGURATION FILE	106
FIGURE 53: DUO AUTHENTICATION PROXY MANAGER CONSOLE	107
FIGURE 54: ADDING A NEW DUO USER	108
FIGURE 55: LOCATION BASED ACCESS POLICY	109
FIGURE 56: DUO USER GROUP CREATION	109
FIGURE 57: ADDING USERS TO DUO GROUP	
FIGURE 58: ADDING THE GROUP TO THE USER'S ACCOUNT	
FIGURE 59: PROTECTING RADIUS APPLICATION IN DUO	

FIGURE 60: DUO LOGIN AUTHENTICATION REPORT	111
FIGURE 61: PROTECT RDP APPLICATION WITH DUO 2FA	112
FIGURE 62: SECRET CREDENTIALS FOR MICROSOFT RDP1 APP	112
FIGURE 63: DOWNLOADING DUO WINDOWS LOGIN APP	
FIGURE 64: INSTALLING DUO WINDOWS LOGIN APP	
FIGURE 65: WINDOWS USER LOGIN	114
FIGURE 66: DUO 2FA PUSH REQUEST FOR WINDOWS LOGIN	114
FIGURE 67: TRUENAS CORE LOGIN PROMPT	115
FIGURE 68: TRUENAS WEB CONSOLE DASHBOARD	116
FIGURE 69: JOINING TRUENAS TO ACTIVE DIRECTORY	116
FIGURE 70: SETTING UP NTP SERVER	117
FIGURE 71: CREATING A SHARED GROUP IN TRUENAS	117
FIGURE 72: TRUENAS STORAGE DISKS MENU	118
FIGURE 73: CREATING STORAGE POOLS	
FIGURE 74: PROVIDING ACCESS CONTROL PERMISSIONS TO THE USER	119
FIGURE 75: WINDOWS SHARES (SMB) MENU	119
FIGURE 76: ACL PERMISSIONS MENU	120
FIGURE 77: ENABLING 2FA IN TRUENAS	121
FIGURE 78: TRUENAS NETWORK DRIVE	121
FIGURE 79: TRUENAS SHARED POOL	122
FIGURE 80: TRUENAS SHARED FILES	122
FIGURE 81: ALIEN VAULT OSSIM COMMAND LINE CONSOLE	123
FIGURE 82: ALIEN VAULT OSSIM SHELL CONSOLE	123
FIGURE 83: ALIEN VAULT OSSIM WEB CONSOLE	124
FIGURE 84: ADDING USERS IN ALIEN VAULT OSSIM	124
FIGURE 85: ADDING AND DISCOVERING ASSETS	125
FIGURE 86: DISCOVERED ASSETS	126
FIGURE 87: DEPLOYING HIDS AGENTS	126
FIGURE 88: OSSIM SIEM ALARMS1	127
FIGURE 89: OSSIM SIEM ALARMS2	127
FIGURE 90: OSSIM SIEM EVENTS1	128

FIGURE 91: OSSIM SIEM EVENTS2	
FIGURE 92: GENERATING SIEM ALARM REPORTS	129
FIGURE 93: SIEM ALARM REPORT1	129
FIGURE 94: SIEM ALARM REPORT2	130
FIGURE 95: SIEM ALARM REPORT3	130
FIGURE 96: ALIEN VAULT OPEN THREAT EXCHANGE FEEDS	131

LIST OF TABLES

TABLE 1: AUTHENTICATION ATTRIBUTES	29
TABLE 2: APPLICATION BENEFITS OF ZERO TRUST IN VARIOUS FIELDS	32
TABLE 3: MAPPING OF NIST & THE PROPOSED FRAMEWORK	46
TABLE 4: AVERAGE LOGIN DURATIONS FOR OPENVPN AND WINDOWS	
AUTHENTICATION	66
TABLE 5: NOTATIONS AND THEIR DESCRIPTIONS	69
TABLE 6: CREATED ACTIVE DIRECTORY USERS LIST	101

Chapter 1: INTRODUCTION

In this fast-moving world we live in, technology is continuously advancing and industries are always looking for ways to integrate new technologies to improve their operations and achieve better results [1]. This is particularly important as organizations strive to provide the best possible customer service while maintaining a high level of workplace flexibility. Some of the most cutting-edge technologies being leveraged by companies today include cloud applications [2], the Internet of Things (IoT), blockchain and augmented reality. However, as organizations become more reliant on these technologies, it also means that they become more vulnerable to cyber-attacks. Hackers can easily exploit weaknesses [3] in these systems such as security misconfigurations, compromised passwords, etc., making it essential for companies to prioritize security to avoid costly security lapses [4].

Two crucial aspects of ensuring the security and privacy of digital systems and resources are authentication and access control. Authentication [5] verifies the identity of users or entities attempting to gain access to a system, often through the use of credentials such as passwords, biometrics, or security tokens. It establishes trust and confidence in the user's identity before granting access. Access control [6], on the other hand, involves determining and enforcing the level of permissions or privileges that a user has within a system or network. It ensures that users can only access the resources and perform actions that are appropriate for their authorized role or level of clearance. By combining robust authentication mechanisms with effective access control policies, organizations can mitigate the risks associated with unauthorized access, data breaches, and malicious activities.

In response to these cyberthreats, information technology security professionals have developed a novel strategy known as the Zero Trust framework [7]. This approach aims to safeguard companies against cyber-attacks by limiting access to resources and tightening the net around the attacker [1], even if they have already gained access to the network. The fundamental principle of the Zero Trust model is that businesses should carefully examine each and every attempt made to access their resources, rather than placing blind trust in anything or anyone, whether internal or external.

By implementing robust password management [8] practices and ensuring that every user or device meets the required permissions each time they seek access to data or networks, companies can enhance their security measures and minimize potential vulnerabilities.

The concept of Zero Trust security [9] is built upon the principle that nothing within a network should be deemed trustworthy without proper validation. This means that every user entering or leaving the network must go through a process of validation, approval, and authentication before being granted access. The existing authentication systems have a flaw, wherein once a user is granted network access, they are automatically trusted and given access to all resources. This poses a significant vulnerability to the entire organization in case the trusted user's account is compromised. The Zero-Trust strategy [10] overcomes this limitation by implementing continuous and multi-faceted verification methods to authenticate one's identity and maintain access to resources.

One of the most effective ways to strengthen security and overcome the drawbacks of current authentication systems is through multifactor authentication [11] techniques. These involve using multiple attributes to verify the user's identity, authenticate them, and authorize them to access various resources. Such attributes can include:

- Something the user knows, such as passwords.
- Something the user has, such as access cards or tokens.
- Something they are, such as fingerprints or retina scans.

By integrating and leveraging these various attributes collectively, organizations can greatly bolster their security measures when granting users access to data or resources within a network. This Thesis explores the Zero Trust [12] framework and its implementation combined with multifactor authentication techniques to improve security in organizations.

The existing traditional security methods employed by individuals and organizations fail to provide consistent and ongoing authentication and authorization for users and devices that connect to the network [13]. The existing security methodology trusts users and devices based on earlier behavior of access granted, but this approach leads to sensitive information disclosure [14] and network breaches. To address these issues, the Zero Trust approach should be adopted, which constantly authenticates and authorizes users/devices connecting to the network. In addition, the lack of strong password management techniques [8] and Multi Factor Authentication [11] (MFA) in legacy security practices results in high probability of system/network compromise due to old or compromised passwords being reused.

This Thesis aims to propose a Zero Trust Framework (ZTF) with multi-factor authentication to enhance security and mitigate the drawbacks of current legacy security practices. The proposed solution is a Zero Trust approach that requires rigorous vetting of users/devices with continuous authentication and authorization, providing the least privilege access necessary for their work based on their roles [9]. The Thesis also addresses the lack of actual design framework or guidelines to implement a Zero Trust Framework by providing a realistic Zero Trust approach that combines the best features of existing frameworks from NIST [7] and other security vendors.

The proposed Zero Trust Framework is strengthened by implementing the recommended practices of Multi-Factor Authentication (MFA) [11], which involves using various authentication methods such as passwords, one-time passwords (OTP), tokens, push requests and biometrics. This approach ensures that only authorized users with the appropriate access are able to connect to the network or access specific resources, as multiple layers of authentication [52] are required to verify their identity, which limits lateral escalation of privileges in the unlikely scenario of an account compromise in a particular part of the network.

This Thesis proposes an actual Zero Trust Framework that addresses the limitations of legacy security mechanisms [13] by constantly authenticating and authorizing users/devices connecting to the network with the use of multifactor authentication. The Thesis provides an actual framework design and guidelines for implementing a Zero Trust environment, which is lacking in most of the

research works in the field [1]. By offering an actual implementation, this Thesis provides a valuable resource for organizations that are interested in adopting a Zero Trust framework. Rather than leaving them with only theoretical concepts and high-level ideas, the Thesis offers a tangible example of how the framework can be put into practice. This implementation serves as a concrete reference point, allowing organizations to visualize the practical aspects of implementing a Zero Trust approach.

To validate the security effectiveness of the proposed Zero Trust framework a security analysis was conducted. The analysis involved evaluating the system's resilience against the following attack models: sniffing attack, where an attacker attempts to intercept sensitive information, as well as password compromise attack [8], where an attacker gains unauthorized access by obtaining or guessing user passwords. By evaluating the system's security against these attack vectors, the Thesis aimed to provide evidence supporting the security effectiveness of the proposed Zero Trust framework.

In addition to assessing the proposed framework's security effectiveness, this Thesis also focuses on evaluating its performance efficiency and user satisfaction. To measure performance efficiency, the average login times for both single-factor and multifactor authentication were calculated. By comparing the login times of single-factor and multifactor authentication [75], the aim was to find a balance between security and user convenience. Furthermore, user satisfaction surveys were conducted to gather feedback [76] and opinions from individuals who interacted with the implemented Zero Trust framework. By considering both performance efficiency and user satisfaction, this Thesis aims to strike a harmonious balance between security and user experience.

The establishment of a realistic, secure and efficient Zero Trust Framework, providing extensive guidelines to organizations for implementing the proposed Zero Trust Architecture with multi factor authentication, which was found to be secure against sniffing and password compromise attacks, was the main contribution of this Thesis.

1.1 PROBLEM STATEMENT

The current security approach employed in enterprise networks involves granting unlimited access privileges to authenticated and authorized users/devices for network resources. However, this practice presents a drawback, as it exposes the entire network to vulnerabilities in the unlikely event of a trusted user's account being compromised. Additionally, the shortcomings of existing legacy security mechanisms include the potential disclosure of sensitive information and network breaches due to the absence of regular and continuous authentication and authorization for connecting users/devices. Furthermore, the lack of robust password management techniques and Multi-Factor Authentication (MFA) in legacy security practices contributes to the reuse of old or compromised passwords, significantly increasing the likelihood of system or network compromise.

Another observation from a thorough examination of existing literature is that the majority of research in the field of Zero Trust primarily focuses on proposing frameworks and potential architectures, without providing concrete designs or practical guidelines for implementing or simulating a Zero Trust environment. This limitation stems from the intricacies involved and the insufficient understanding of operational efficiency and IT expenditure budget concerns within the field. Furthermore, there are very few research works that focus on the various authentication mechanisms based on Zero trust, and none actually focusing on implementing the Zero trust using MFA.

Hence our contribution in proposing and implementing the proposed Zero Trust MFA framework. Furthermore, we have provided extensive guidelines in the setting up of the proposed Zero Trust Framework environment for organizations trying to adopt the Zero Trust Framework.

1.2 MOTIVATION

The primary objective of this Thesis is to offer a practical and effective Zero Trust Framework by carefully examining existing frameworks from sources like NIST and other security vendors. By combining the valuable features of these frameworks, the aim is to strike a balance between security, performance efficiency, and user satisfaction. The proposed and implemented multifactor authentication mechanism in this Thesis is built on the Zero Trust architecture framework, overcoming the drawbacks of legacy security mechanisms and the lack of current research implementation guidelines in setting up a secure Zero Trust MFA environment. Unfortunately, it is a harsh reality that implementing a robust Zero Trust approach can save a substantial amount of time and money compared to the immense costs incurred from dealing with an attack or breach. These incidents often result in the disclosure of sensitive information or ransomware attacks, causing significant financial losses and damaging the reputation of individuals or organizations.

Some of the main advantages of a Zero Trust approach are as follows:

- Users/devices undergo a thorough and meticulous vetting process to establish their identity, and they are then authenticated and authorized accordingly.
- To access resources beyond their current eligibility, users/devices are required to provide extra verification to ensure secure access.
- All users are granted access privileges based on the principle of least privilege, meaning they are given the minimum level of access required for their specific roles and responsibilities.
- Networks are divided into smaller segments through micro segmentation, which enhances security by requiring multistep authentication processes for accessing different network segments.

The Zero Trust Framework is further strengthened through the integration of best practices from Multi-Factor Authentication (MFA). This approach enhances the security of the system/network by introducing multiple layers of authentication, involving different combinations of passwords, one-time passwords (OTP), tokens, and biometrics. Even if one level of authentication, such as passwords, is compromised, the attacker would still need to pass the second level of authentication to gain access. However, since they lack the necessary permissions or credentials, the breach attempt is effectively blocked. By combining MFA with the Zero Trust Framework, it ensures that only users with proper access can authenticate themselves, as multiple levels of authentication are required.

1.3 RESEARCH AIMS AND METHODOLOGY

The aim of this Thesis is to offer a practical and feasible Zero Trust Framework (ZTF) that incorporates Multi-Factor Authentication (MFA). Additionally, this Thesis provides a concrete implementation of the proposed framework along with comprehensive guidelines, enabling organizations, businesses, or individuals to successfully adopt the Zero Trust Framework within their environments. The Thesis also delves into the factors that necessitate the adoption of a Zero Trust model and explores the different types of authentications that can be utilized.

The goal was to comprehend the philosophy behind Zero Trust combining it with various authentication mechanisms to increase the security, at the same achieving a balance between performance and user satisfaction and help firms to adopt it using the extensive framework provided in this Thesis.

The objective of this Thesis is as follows:

To create a framework that combines the principles of a Zero Trust Architecture and multifactor authentication, with a specific emphasis on optimizing performance, enhancing security, and ensuring user satisfaction and provide comprehensive guidelines of implementation for organizations to adopt.

Methodology

The research methodology for this Thesis involves several key steps. The initial step is to conduct a comprehensive literature review, which aims to explore existing frameworks, multifactor authentication mechanisms and best practices related to the adoption of the Zero Trust in organizations. This review will provide a solid foundation for designing a robust framework that guides the implementation process effectively.

The main objective of the Thesis is to propose a comprehensive framework that organizations can utilize to successfully implement ZTF combined with multifactor authentication for secure

access. The framework will address the challenges and considerations associated with adopting the ZTF approach, such as secure user and device identification, continuous and multifactor authentication, authorization and access control. The focus will be on finding a balance between security and performance by incorporating multifactor authentication (MFA) mechanisms and granting the minimum necessary privileges for work without compromising the user experience.

In addition to proposing the framework, the Thesis will also include the practical implementation of the proposed framework. A virtual setup will be created to simulate an enterprise environment, allowing for the demonstration and evaluation of the framework's effectiveness. The implementation will involve the utilization of various roles, including users, devices, applications, and hierarchical structures within the organization. This will provide a realistic representation of an office setup with multiple users in different roles and departments, each having different levels of access and privileges.

To facilitate the implementation, multiple tools and virtual machine environments will be employed. These resources will enable the creation of a working enterprise environment that closely mirrors real-world scenarios. By utilizing these tools, the research will demonstrate how the proposed framework can effectively guide the implementation in organizations, ensuring a balance between security and performance.

Through this research methodology, the Thesis aims to contribute to the field by providing a comprehensive framework for organizations to implement the ZTF with MFA. By conducting a thorough literature review, designing the framework, and implementing it in a virtual environment, the Thesis will validate the effectiveness and validity of the proposed framework in real world scenarios.

1.4 STRUCTURE OF THE THESIS

Chapter 1, provides an introduction about the research topic. Chapter 2 provides a review of the existing literature on Zero Trust frameworks, multifactor authentication and related research studies. Chapter 3 discusses the proposed Zero Trust Framework and the multifactor authentication mechanisms. A discussion of the implementation of the proposed Zero Trust Framework and its multi factor authentication setup are covered in Chapter 4. Chapter 5 discusses the performance efficiency and user satisfaction of the proposed framework. Informal security analysis of the proposed and implemented framework is discussed in Chapter 6. Finally, Chapter 7 brings the Thesis to a conclusion.

Chapter 2: BACKGROUND AND LITERATURE REVIEW

In the literature review section, we explored various studies, research articles, and scholarly publications related to Zero Trust, frameworks, and multifactor authentication mechanisms. Our aim was to gather comprehensive knowledge and insights into the existing body of work on these topics. The literature review focused on understanding the principles and concepts behind Zero Trust frameworks, examining different models and approaches proposed by researchers and industry experts. Additionally, we explored the literature related to multifactor authentication mechanisms, which are a crucial component of a robust Zero Trust model. We examined various authentication factors, such as biometrics, one-time passwords, smart cards, and mobile authenticators.

By conducting this literature review, we gained valuable insights into the current state of research and industry practices regarding Zero Trust frameworks and multifactor authentication mechanisms. This knowledge served as a foundation for the development of our proposed framework and the design of our multifactor authentication system, ensuring that our Thesis is informed by the latest advancements and best practices in the field.

2.1 Frameworks

The NIST CSF [7] (Cybersecurity Framework), is a set of guidelines, standards, and best practices designed to help organizations manage and improve their cybersecurity posture. It provides a comprehensive framework for organizations to assess and strengthen their security controls, risk management processes, and incident response capabilities. This framework is a voluntary set of guidelines, built upon existing standards, rules, and practices, aimed at effectively managing and reducing cybersecurity risks for critical infrastructure organizations [15]. The framework is a living document that undergoes regular updates to align with evolving industry requirements. As it is designed to be optional, achieving full compliance in every situation can be highly demanding.

The NIST Cybersecurity Framework works by following a risk-based approach. It consists of five core functions: Identify, Protect, Detect, Respond, and Recover [15] as seen from Figure 1. These functions represent the key areas that organizations should focus on to establish a robust cybersecurity program.

The major components [7] of the NIST Cybersecurity Framework include:

- Identify: Organizations need to understand their assets, risks, and vulnerabilities [7]. They should conduct a thorough inventory of their systems, data, and network infrastructure to identify potential risks and prioritize their security efforts.
- Protect: Organizations should implement safeguards to protect their systems, networks, and data from cyber threats. This involves the use of access controls, encryption, secure configurations, and regular security awareness training for employees [15].
- Detect: Organizations should establish mechanisms to detect and identify cybersecurity events. This includes implementing continuous monitoring, intrusion detection systems, and security analytics to identify potential security incidents promptly [7].
- Respond: Organizations should have a robust incident response plan in place to effectively respond to cybersecurity incidents. This involves defining roles and responsibilities, establishing communication channels, and conducting drills to ensure a swift and coordinated response [15].
- Recover: Organizations should develop strategies and plans for recovering from cybersecurity incidents. This includes restoring systems, data, and services to their normal operations, conducting post-incident analysis, and implementing necessary improvements[7].

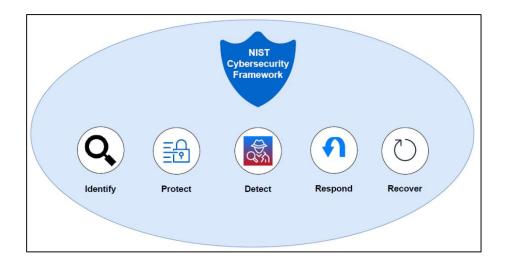


Figure 1 : NIST Cyber Security Framework [15]

The International Organization for Standardization (ISO) has introduced a framework, ISO/IEC 27001:2013(en) [16], to aid individuals, businesses, and organizations in safeguarding their data securely and efficiently. This is achieved by implementing an Information Security Management System (ISMS). The framework outlines a systematic approach to managing sensitive information, prioritizing its confidentiality, integrity, and availability [17]. Rather than solely focusing on technology, the emphasis is placed on effective risk management, providing valuable guidance for ensuring information security in a streamlined manner. The framework works by following a risk management approach. It requires organizations to identify their information assets, assess risks, and implement appropriate security controls to mitigate those risks.

The major components [16] of the ISO/IEC 27001:2013 framework include:

• Context Establishment: Organizations need to define the scope of their ISMS [17] and establish the context in which it operates. This includes identifying stakeholders, setting security objectives, and defining the scope of information security management.

- Risk Assessment: Organizations should conduct a thorough assessment of risks to their information assets [16]. This process entails identifying weaknesses, evaluating the probability and consequences of potential hazards, and prioritizing actions to address and mitigate risks.
- Risk Treatment: Based on the risk assessment, organizations should implement appropriate security controls to mitigate identified risks. This includes establishing policies, procedures, and technical measures to protect information assets [17].
- Performance Evaluation: Organizations need to observe and evaluate the effectiveness of their ISMS. This involves performing regular security audits [16], reviewing security performance, and taking corrective actions to address any identified deficiencies.
- Continuous Improvement: Organizations should continuously improve their ISMS by identifying opportunities for enhancement, learning from security incidents [17], and implementing lessons learned.

NIST Special Publication 800-207 [18] is a guidance document by the National Institute of Standards and Technology (NIST) that provides recommendations for implementing the Zero Trust architecture as seen from Figure 2. It outlines the principles, concepts, and components of Zero Trust and offers practical guidance for organizations.

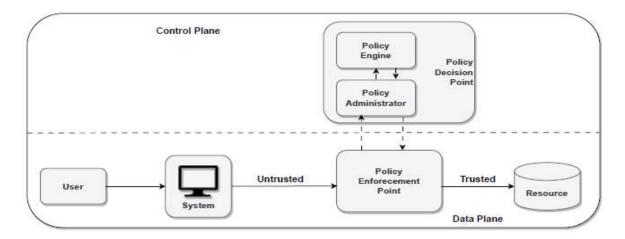


Figure 2 : NIST Zero Trust Framework [18]

The major components of NIST SP 800-207 include [18]:

- Zero Trust Principles: The document introduces the core principles of Zero Trust, such as assuming breach, minimizing trust, and strict access control [19].
- Zero Trust Concepts: It explains key concepts like network segmentation [18], continuous monitoring, and strong authentication as essential components of the Zero Trust architecture.
- Zero Trust Architectural Constructs: The guidance provides an overview of architectural constructs like identity and access management [19], secure connectivity, and analytics-driven security for building a Zero Trust environment.
- Implementation Guidelines: It offers practical steps and recommendations for organizations to implement Zero Trust, including risk assessment [18], policy development, and network segmentation strategies.

All the above discussed frameworks and standards provide valuable guidance for cybersecurity, but they may lack some elements when viewed from a Zero Trust perspective:

NIST Cyber Security Framework: While the framework offers a holistic approach [7] to cybersecurity, it does not explicitly focus on zero trust principles and concepts. It may not provide detailed guidance on implementing strict access controls, continuous monitoring, and microsegmentation, which are essential aspects of a Zero Trust architecture.

ISO/IEC 27001:2013 Framework: The ISO/IEC 27001:2013 framework primarily emphasizes establishing an information security management system (ISMS) [16]. While it covers risk management and controls, it may not specifically address the Zero Trust mindset and the need for constant verification and authentication of users and devices.

NIST Special Publication 800-207: Although this publication focuses on implementing the Zero Trust architecture, it may lack comprehensive guidance on integrating zero trust principles into existing security measures [18]. It does not address specific challenges related to identity and access management and secure connectivity within a zero trust environment.

In [20] the authors introduces a framework that focuses on implementing comprehensive guidelines related to risk management, cybersecurity, and compliance within complex organizations. The framework highlights the importance of practical implementation of security solutions and ensures their alignment with governance and financial objectives at the board level. The authors of this [21] paper proposes a new trust evaluation algorithm called Tag based Trust Evaluation (TBTE) for Zero Trust Architecture (ZTA). The TBTE framework combines the score-based and criteria-based approaches to assess trust. It generates security tags considering user behavior and device security. A simple trust evaluation rule is applied using these tags, making the results more interpretable and reducing complexity in authorization policies.

Therefore, we propose to implement a Zero Trust framework for organizations. This approach ensures that access is only granted after thorough authentication and authorization of users, devices, and resources, effectively eliminating the risk of data breaches and unauthorized access.

2.2 Authentication Mechanisms

The authors of [1], suggests adopting biometric-based multi-factor authentication as a standard practice to enhance cybersecurity in public institutions. It proposes the redesign of network architecture using a Zero Trust approach for improved network and data security. The proposed system ensures compliance with the existing General Data Protection Regulation (GDPR) standards and regulations. The approach is more focused on meeting the compliance requirements rather than the Zero Trust security requirements, since the biometric data stored in the proposed USB design can be physically tampered with or stolen, leading to the violation of data confidentiality, integrity and availability.

In [22], the authors propose a system that generates a collection of attributes for users, applications, and devices. These attributes encompass user-specific information such as user ID, location, and package name, device-related details like operating system version and manufacturer, and application-specific attributes such as version and type. The Zero Trust architecture is leveraged to utilize these data attributes in a risk-based authentication mechanism. This mechanism compares the incoming request's attributes to the stored attributes and calculates a risk score. Depending on the analysis of this risk score and the variations in attribute values, additional authentication challenges may be requested. The variance is computed using various machine learning models or predefined policies.

In [23], the authors propose the utilization of blockchain technology to eliminate the need for a trusted authority or node responsible for authentication using secret values or keys. Through the implementation of a realistic Byzantine fault tolerance consensus process, a node is selected to generate the secret keys and public parameters for the devices involved. The devices are categorized into trusted, suspicious, and untrusted groups. Only the trusted and suspicious devices are permitted to participate in the authentication process, while different security factors and time-out restrictions of varying lengths are employed to strike a balance between security and efficiency. Additionally, the authors illustrate the efficacy of the suggested authentication scheme in terms of security, highlighting the superiority of a decentralized authentication authority over a centralized one that is susceptible to vulnerabilities.

In [24], the authors propose a smart identity authentication system that combines static and dynamic authentication strategies, centered around the principles of the Zero Trust paradigm. This proposal introduces a bidirectional authentication protocol between the user and the server, with a particular emphasis on attribute encryption. The system conducts ongoing trust assessments and risk analysis based on static user authentication. By integrating static and dynamic authentication methods, the proposed system safeguards the confidentiality of the authentication ciphertext and effectively counters any attempts at falsification, as further demonstrated through extensive security analysis.

The authors of [25] propose the integration of hardware root trust and a password-free authentication approach. They suggest incorporating a trusted chip as the root of trust to enhance the security of communication between the authentication server and associated computers. While the specific authentication technique and encryption method were not explicitly specified in this research, it highlights the utilization of a server for storage and the execution of the entire authentication process.

In [26], the authors suggest a three-factor authentication (3FA) system that combines two-factor authentication with real-time facial recognition. This 3FA method enhances the security aspect but may result in reduced efficiency due to increased system requirements.

In [27], the authors suggest enhancing digital key systems by incorporating both dynamic and static authentication phases. During the static authentication phase, the system establishes secure connections between the user, gateway, and device. In the dynamic authentication phase, NFC and fingerprints are utilized, followed by ongoing identity verification through facial recognition. While the use of biometrics provides increased security, one drawback of this approach is the requirement for additional hardware, including fingerprint sensors, NFC technology, and cameras, in addition to the hardware needed for static authentication processing.

The authors of [2] propose a steganographic overlay technique to protect against unwanted traffic and unauthorized access. This technique involves embedding network authentication tokens within TCP connection requests, effectively hiding resources from potential attackers and preventing reconnaissance attempts. The paper also introduces a practical identity management and authentication strategy for the transport layer, specifically designed for businesses. Additionally, the authors demonstrate that by avoiding any response to illegitimate packets at the transport layer, the proposed strategy successfully prevents fingerprinting of critical resources such as the SDN controller.

In [28], a Zero Trust and edge intelligence (ZTEI) approach to enhance the security of satellite networks is discussed. A multi-dimensional Zero Trust architecture is developed, considering

various factors such as subject, object, environment, behavior, and physical entity. Continuous authentication is implemented through proactive monitoring and re-evaluation of variable attributes, supported by a Neural-Backed Decision Trees (NBDTs) based edge intelligence algorithm. Evaluation results demonstrate a 27% improvement in authentication accuracy compared to traditional approaches, with acceptable processing performance.

The authors of [29], propose MUFAZA, a rapid and self-governing authentication framework, which is specifically created to safeguard 5G networks. This framework prioritizes evaluating trust from the perspective of agents and making access decisions accordingly to tackle the everchanging threats. It integrates a dynamic trust evaluation that considers multiple security evidence sources, taking into account the credibility of information and offering recommendations on incorporating extra data for trust evaluation. By conducting a case study on a hybrid 5G-enabled network, the paper demonstrates the effectiveness and resilience of the suggested approach.

The use of outdated security models and the absence of granular security in these mechanisms undermine their overall security compared to the Zero Trust model [26]. Typically, access is granted to devices that have been previously authenticated and added to a trusted list, without any subsequent verification of their status or behavior. This unchecked access often leads to security vulnerabilities and lapses.

Therefore, we propose the implementation of a Zero Trust Framework for businesses and organizations, where access is granted only after each user undergoes authentication whenever they attempt to access a service. By adopting this approach, the occurrence of unauthorized access or breaches can be significantly reduced or even eliminated. Table 1 provides an overview of various authentication attributes related to users, devices, and applications, which are utilized for multifactor authentication to enhance security. Our objective is to combine multifactor authentication using these attributes with the Zero Trust model to effectively enhance overall security.

After reviewing several publications with relevant background information, a comparison for the different authentication attributes was created as seen from Table 1:

Reference	Description	Year	Static / Dynamic Authentication	Multifactor Authentication Attributes	Recommendations
[22]	Proposes an	2021	Static	User attributes such	Implement a dynamic
	adaptive			as location and user	authentication
	authentication			id. Application	mechanism that
	approach			attributes include	considers multiple
	based on a			the package name or	attributes for user
	composite			version, followed	authentication to
	attribute set			by device attributes	enhance security and
				like operating	adaptability to
				system, make, and	different contexts
				model.	
[23]	Leveraging	2022	Dynamic	Using the realistic	Employ a continuous
	blockchain to			Byzantine fault	authentication
	eliminate			tolerance consensus	mechanism that
	trusted nodes			process, a node is	analyzes user
	or authorities			chosen to produce	behavior and context
	that manage			the secret and public	in real-time to detect
	authentication			keys for the devices.	any anomalies and
	using secret				ensure ongoing
	values or keys.				verification
[24]	Combines	2021	Static and	User ID, device	Examine the
	dynamic and		Dynamic	characteristics, trust	implementation of
	static			evaluation value,	multi-level two-way
	authentication			and application	identity
	techniques			service security	authentication

Table 1 : Authentication Attributes

	with a focus			level are all	schemes within the
	on the Zero			authentication	context of Zero Trust
	Trust			attributes.	
	paradigm to				
	suggest a				
	smart identity				
	authentication				
	solution.				
[25]	Recommends	2007	Dynamic	Zero-knowledge	Assess the feasibility
	a mix of a			proofs and	and security
	password free			cryptographic	implications of the
	authentication			techniques	proposed "pseudo
	method and				trust" approach.
	hardware root				
	trust.				
[26]	Proposes a	2021	Static and	Combines facial	Incorporate
	real time 3FA		Dynamic	feature detection	contextual
	using facial			with real-time data	information and
	biometrics.			via an immediate	behavior analysis as
				live feed from the	part of multifactor
				user's camera.	authentication to
					implement a robust
					Zero Trust model
[27]	Suggests	2022	Dynamic	Credentials for	Evaluate the
	combining the			Users and Biometric	proposed scheme's
	static and			identification.	performance and
	dynamic				security
	authentication				characteristics.
	phases as a				
	digital key				
	system				

[2]	Proposes first-	2016	Dynamic	Embeds network	Assess the
	packet			authentication	effectiveness of these
	authentication			tokens in a TCP	mechanisms in
	and a			connection request,	enhancing the
	steganographi			thereby avoids	security of cloud
	c overlay that			unwanted traffic	networks.
	embeds			from completing	
	authentication			requests.	
	tokens in the				
	TCP packet				
	request.				
[28]	Continuous	2022	Dynamic	Proactive	Leverage satellite
	authentication			monitoring and re-	network information,
	for satellite			evaluation of	user behavior, and
	networks with			variable attributes,	contextual data for
	improved			supported by a	continuous
	accuracy and			Neural-Backed	authentication.
	proactive			Decision Trees	
	monitoring			(NBDTs) based	
	using zero			edge intelligence	
	trust and edge			algorithm.	
	intelligence.				
[29]	Proposes a	2022	Dynamic	Agent centric trust	Evaluate the
	multi-source			evaluation that	performance and
	fast and			integrates multiple	security benefits of
	autonomous			sources of security	the proposed
	Zero Trust			evidence.	MUFAZA approach.
	authentication				
	scheme for 5G				
	networks				
[1]	Enhancing	2022	Static and	Combines biometric	Explore the
	Cybersecurity		Dynamic	credentials, local	integration of
	with			and public	enhanced biometric
	Biometrics				security measures

		cryptographic keys,	within the Zero Trust
		and user passwords,	architecture

Table 2 showcases the advantages of implementing Zero Trust in diverse fields, based on the findings from the above-mentioned research papers. Highlights the positive impacts and benefits that can be derived by applying Zero Trust principles in these areas.

Reference	Fields	Applications
[3]	IoT	Enhanced device security and data protection, secure
		communication between IoT devices, protection
		against unauthorized access.
[30]	Machine	Secure and private training data, protection against
	Learning	adversarial attacks, ensuring model integrity and
		authenticity.
[23]	Blockchain	Immutable and tamper-proof transactions, secure
		decentralized networks, protection against
		unauthorized modifications or tampering of data.
[28]	Satellite	Secure communication channels for satellite data
	Technology	transmission, protection against unauthorized
		interception or tampering of data.
[29]	5G	Secure and reliable network connections, protection
		against network vulnerabilities, enhanced privacy
		and data integrity.
[24]	Mobile	Secure mobile communication, protection against
	Internet	mobile malware, secure access to sensitive
		information and applications.

Table 2 : Application Benefits of Zero Trust in Various Fields

[31]	Hospital	Securing patient data and medical records,
	Field	protecting critical medical devices from
		unauthorized access or tampering, secure
		communication between healthcare systems.
[1]	Public	Enhanced security for sensitive government
	Institutions	information, protection against cyber threats, secure
		access controls for government services and
		systems.
[32]	Smart	Secure control and management of connected
	Home	devices, protection against unauthorized access or
		control of smart home systems, secure remote
		access.
[10]	UAV	Secure control and communication of unmanned
		aerial vehicles, protection against unauthorized
		access or control of UAV systems, data privacy and
		security during UAV operations.
[33]	Wearable	Secure transmission and storage of personal health
	Devices	data, protection against unauthorized access to
		sensitive user information, ensuring data privacy and
		integrity.
[2]	Cloud	Secure access and storage of cloud-based resources,
	Computing	protection against unauthorized access or data
		breaches, secure sharing and collaboration of data.

Chapter 3: PROPOSED ZERO TRUST FRAMEWORK

3.1 Zero Trust Model & Zero Trust Architecture (ZTA)

The "no trust, but always verify" [12] principle is the foundation of the Zero Trust security approach. Put simply, it is important to regard end users, computers, networks, and applications as potentially hostile until their legitimacy is established. In this Thesis, we discuss how to create a Zero Trust Framework with MFA, implement the proposed framework with the help of a virtual environment and provide guidelines for corporates to adopt the framework. The key requirement in this paradigm is to ensure that all users, regardless of whether they are internal or external to the organization, undergo continuous vetting, validation, and authentication before being granted access to resources such as applications or data.

The implementation of Zero Trust Architecture (ZTA) [7] is a comprehensive strategy for enhancing cybersecurity within an organization. It encompasses various aspects such as IT infrastructure, networks, workflows, and access control policies. By adopting the Zero Trust Framework, companies establish a plan, known as a Zero Trust initiative, that covers both physical and virtual components, along with operational guidelines. The primary objective is to prevent unauthorized access to data and services by implementing highly detailed access control measures. In other words, only authorized and recognized entities, including users, devices, and appliances, are granted access to the data, while potential threats like hackers and cybercriminals are excluded. It's worth noting that in the context of Zero Trust, the term "asset" may be used interchangeably with "data" emphasizing the focus on securing access to valuable resources.

3.2 ELEMENTS OF THE PROPOSED ZERO TRUST FRAMEWORK

In order to enhance security and address the limitations of traditional security models, the proposed Zero Trust Framework encompasses several key elements. These elements work together to establish a robust security framework that promotes the principle of never trust, always verify, and ensures secure access to resources. The elements of the proposed framework are as follows:

1. VPN & VPN Client

A VPN (Virtual Private Network) works by creating a secure and encrypted connection, that is a VPN tunnel between the user's device and a remote destination on the internet as seen from Figure 3 with the help of the VPN server. This connection allows the user to access the internet or private networks while maintaining privacy and security. A VPN client is a program that employs encryption to establish a secure link between a user's computer and a VPN server, ensuring their connection is protected. [34]. The VPN server is responsible for upholding the security policies, data encryption algorithms and other security configurations related to encryption. Certain VPN clients operate silently in the background, automatically performing their functions, whereas others offer interactive interfaces, giving users the ability to personalize and adjust their preferences. It enhances security and anonymity for users accessing websites and online services. When using a VPN, the data exchange taking place between the client and the remote destination is "tunneled [35]," hiding the user's real public IP address. VPN packets travel through a tunnel to reach the private network destination. Many VPNs employ the IPsec protocol family, and in this Thesis, we utilize the open-source VPN solution called OpenVPN as an example. VPN is used to encrypt the data communication which is a part of Zero Trust ensuring the confidentiality of the data.

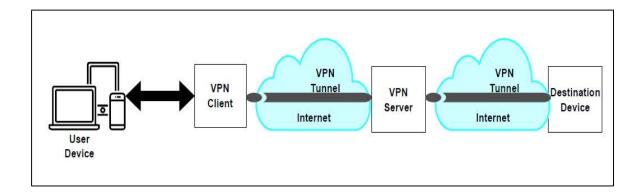


Figure 3 : Working of a VPN

OpenVPN

OpenVPN is a software application that enables users to establish secure connections over the internet. It functions as a type of VPN software [36] that encrypts data while it travels between two devices. This encryption makes it significantly more difficult for unauthorized individuals to intercept or eavesdrop on the transmitted data. The OpenVPN Community Edition (CE) is an open-source VPN project that utilizes a unique security protocol based on SSL/TLS to establish secure connections over the internet. OpenVPN [35] plays a significant role in implementing a Zero Trust model by providing a secure and encrypted connection for remote access. It ensures that users must authenticate themselves and their devices before accessing network resources. OpenVPN's robust encryption protocols and tunneling capabilities enable secure transmission of data over untrusted networks, mitigating potential risks. In this Thesis we use the OpenVPN as an example, which encrypts the communication between the OpenVPN client which takes the user's active directory login credentials and the OpenVPN server using TLS 1.2 encryption.

2. Firewall

A firewall is a network security tool responsible for monitoring and filtering incoming and outgoing network traffic based on predefined security policies [37]. It acts as a barrier between a trusted internal network and an untrusted external network, such as the internet. As seen from

Figure 4, the firewall isolates internal LAN traffic from the outside WAN traffic. It monitors and controls incoming and outgoing network traffic based on predetermined rules and policies. In our Thesis, we utilize the open source pfSense Firewall as an example, which is a robust firewall solution. It can enforce strict access policies based on user roles and attributes, implement network segmentation to isolate sensitive data and systems, and provide secure remote access through VPNs.

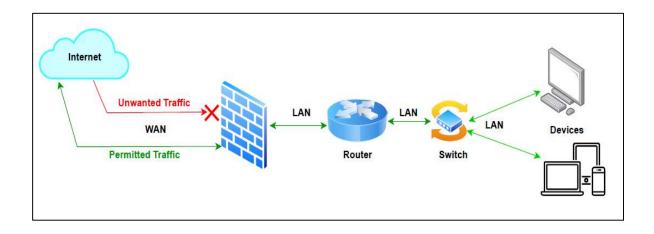


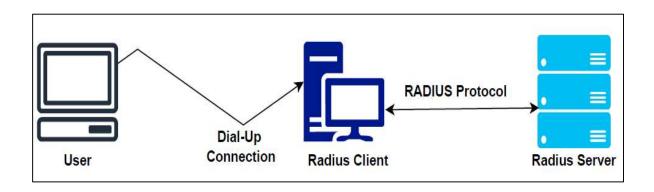
Figure 4 : Working of a Firewall

pfSense Firewall

The pfSense Firewall [38] is firewall and router software based on FreeBSD. It can be installed on either a physical computer or a virtual machine to establish a dedicated firewall/router specifically designed for a network. The pfSense Community Edition (CE) is an open-source distribution used for this purpose. It provides advanced features and functionality, including firewalling, routing, VPN, and intrusion detection/prevention system (IDS/IPS). pfSense [39] is used in this Thesis to implement Zero Trust by configuring it to enforce strict access controls, and traffic filtering based on user identities, device characteristics for multifactor authentication. All the communication traffic passes through the pfSense firewall and the OpenVPN server before entering the network which can be either allowed or denied based on the preconfigured rules and policies.

3. RADIUS Protocol

The RADIUS (Remote Authentication Dial-In User Service) protocol [40] is a networking protocol commonly used for authentication, authorization, and accounting (AAA) in computer networks. It enables centralized authentication and access control for users attempting to connect to network services. RADIUS works through a client-server model as seen from Figure 5.





RADIUS Client & Server

The RADIUS client [41], such as a network access server or VPN gateway, sends authentication requests to a RADIUS server. The client encapsulates user credentials, such as username and password, and forwards them to the RADIUS server for verification. A network access server (NAS) is a device that allows users to connect to a larger network. When a NAS uses a RADIUS infrastructure, it functions as a RADIUS client by sending connection requests and accounting messages to a RADIUS server for authentication and authorization. In this Thesis both the OpenVPN server and the Network Policy Server (NPS) inside the windows active directory act as the RADIUS client.

A RADIUS server [42] serves as a centralized server that handles authentication, authorization, and accounting management for users who connect to a network service. It acts as a central point of control, ensuring secure and efficient user access to the network while keeping track of user activities for accounting purposes. RADIUS was designed as an authentication and accounting protocol for access servers. By maintaining a common database accessible to all remote servers,

RADIUS [43] allows businesses to keep track of user profiles. Centralizing the database enhances security and allows the implementation of policies from a single network point. The DUO authentication proxy server acts as the RADIUS server in this Thesis.

4. Active Directory

Active Directory (AD) is a directory service developed by Microsoft that works in conjunction with Windows Server [44]. It provides administrators with the ability to manage and control access to network resources, as well as assign permissions to users and groups. The data in the Active Directory is stored as objects [45], representing components such as users, teams, programs, or machines. Active Directory simplifies access and usage of this information for administrators and users. It organizes directory data in a logical, hierarchical structure based on a structured data store. Active Directory is present in most Windows Server operating systems and was initially used for centralized domain management. We are using the AD services for hosting the company domain, the DNS server and the NPS server for authentication in this Thesis. We also create user accounts with various permissions but by providing the least privilege necessary for work as per their roles, satisfying one of the basic requirements [12] of Zero Trust.

5. Domain Name System (DNS) Server

A DNS server [46] plays a vital role in the functioning of the internet by converting user-friendly domain names into numeric IP addresses. This conversion allows users to easily access websites and resources using familiar domain names instead of complex IP addresses. When a user enters a domain name [47] in a web browser, the DNS server is responsible for finding and providing the corresponding IP address, enabling seamless communication and access to the desired online destination. The DNS server stores a database of domain name records, including the IP address associated with each domain. The DNS server plays a crucial role in enforcing security policies and controlling access to resources. We use the DNS server services in our Zero Trust framework to ensure that only the users belonging to our company's domain are being granted access to the network and resources.

6. Network Policy Server (NPS)

The Network Policy Server (NPS) [48] is a Microsoft Windows Server role that provides authentication, authorization, and accounting (AAA) services for network access. It allows organizations to centrally manage and control access to network resources based on policies and conditions. When a user or device attempts to connect to the network, the NPS server receives the authentication request from a network access server, such as a VPN gateway or wireless access point. The server validates the user's credentials against a user database, such as Active Directory, and checks for compliance with defined policies and conditions. Based on the authentication and authorization results, the NPS server either grants or denies access to the network. It can also enforce additional policies, such as multi-factor authentication, device health checks, or time-based restrictions, to ensure a secure and controlled network environment. NPS [50] is configured as a RADIUS proxy to forward connection requests to the RADIUS server, facilitating domain authentication and authorization in this Thesis.

7. Certificate Authority (CA)

A certificate authority (CA) [49] an entity responsible for issuing and managing digital certificates used in public key infrastructure (PKI) systems. It plays a crucial role in establishing trust and verifying the authenticity of digital identities, such as websites, servers, or individuals. Web browsers use these certificates to validate material sent from web servers. A certificate authority keeps, signs, and issues digital certificates, which attest to the ownership of a public key by the named subject. By issuing digital certificates, the CA helps authenticate and verify the identities of users, devices, or services accessing network resources. These certificates can be used for various purposes, such as secure communication (TLS/SSL certificates) or user authentication (client certificates). By incorporating an internal CA into our proposed Zero Trust framework with the help of pfSense firewall, we have enforced strict authentication, validate identities, and establish a higher level of trust, contributing to a more secure and controlled access environment.

8. Authentication Proxy Server

An authentication server [27] is an application that simplifies the process of verifying an entity's identity when attempting to access a network. This entity could be a user or an external server. Various devices such as a dedicated computer, ethernet switch, access point, or network access server can function as authentication servers. An authentication proxy [50] server is a tool that adds an additional layer of security to the login process, safeguarding sensitive information and accounts. Essentially, it acts as a gatekeeper, verifying the identity of the person attempting to log in. This is crucial because passwords can be stolen or guessed. By introducing a second form of authentication, such as a code sent to a user's phone, unauthorized access becomes significantly more challenging. In this Thesis, we utilize the DUO MFA proxy as an authentication proxy server as an example.

DUO MFA Authentication Proxy

The DUO MFA proxy is specifically designed to work with DUO Security, a popular two-factor authentication service. When someone tries to log in to a protected application or system, the DUO MFA proxy intercepts the request and sends a notification to the user's phone as seen from Figure 6. The user is then required to enter a code from their phone [33] or authorize access through a prompt to complete the login process. This ensures that even if someone steals or guesses the user's password, they cannot log in without access to the user's phone. DUO MFA proxy used in this Thesis, queries the windows AD using the LDAP protocol to verify the user's credentials against the Windows AD database.

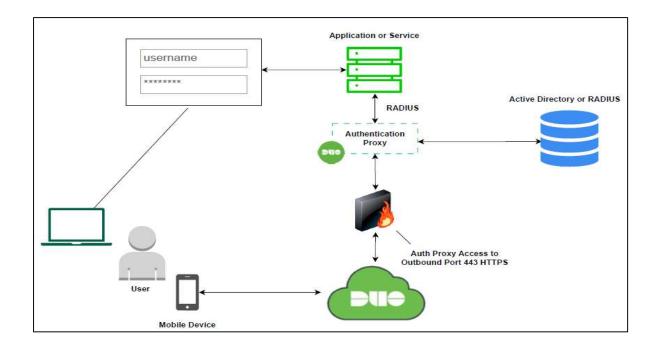


Figure 6 : Working of DUO Authentication Proxy [51]

9. Two Factor Authentication (2FA)

Two-factor authentication is a security measure that adds an extra layer of protection by requiring users to provide two distinct forms of verification to verify their identity [1]. It goes beyond a single piece of information, such as a password, to enhance system security. The second factor used can be a security token, a fingerprint scan, or another form of authentication depending on the application. Implementing 2FA [52] is a measure businesses can take to strengthen defense against unauthorized access and data theft. With multi-factor authentication, users must successfully submit two or more authentication factors to access a website or application. We have used DUO Security's PUSH authentication as the second factor of authentication as an example in our proposed Zero Trust Framework in this Thesis.

10. File Server

A file server [53] is a computer or network device that stores and manages files, allowing users to access and share them over a network. It provides a centralized storage location for files,

enabling efficient collaboration and data management within an organization. It can be compared to a virtual filing cabinet that everyone in the office can access. This facilitates collaboration on projects and makes information sharing easier, eliminating the need to constantly send files via email. In this Thesis, we utilize the TrueNAS Core as the network file server as an example.

TrueNAS File Server

TrueNAS Core is a popular file server software solution that is based on the open-source FreeNAS project. It is a specific type of file server that operates on the FreeBSD operating system. It is designed to be user-friendly and manageable, even for individuals without extensive IT expertise. Once set up, users can access files on the server [54] from their own devices, including desktop computers, laptops, and mobile devices. This allows everyone in the office to work on the same files regardless of their location or device. It offers advanced features for data storage and file sharing, including support for various protocols such as SMB (Windows file sharing) [55], NFS (Unix file sharing), and FTP. TrueNAS ensures data integrity, redundancy, and security through features like RAID (Redundant Array of Independent Disks), encryption, and access controls. We have set up privilege based access controls for different users in our Zero Trust framework such read only, read/write and no access based on their respective job roles using TrueNAS Core.

11. Lightweight Directory Access Protocol (LDAP)

LDAP (Lightweight Directory Access Protocol) [56] is a communication protocol utilized to access and handle directory information services. It is widely employed in network environments to facilitate tasks such as authentication, authorization, and directory services. LDAP works by providing a standardized way to interact with directory servers. It is utilized by the DUO proxy server for fetching and verifying primary authentication credentials against the Active Directory [57] database server in this Thesis. The DUO proxy server relies on LDAP as a communication channel to interact with the Active Directory. Through LDAP, the proxy server can retrieve user credentials stored in the directory and validate them against the provided authentication data. By integrating LDAP into our Zero Trust framework, we can authenticate and authorize users, control

access to resources, and ensure that only authorized entities gain access to sensitive data or systems.

3.3 Logical Components of The Proposed Zero Trust Framework (ZTF)

The components of the ZTF communicate over a control plane and the application data are communicated over a different data plane. Figure 7 shows the key Zero Trust components of the proposed framework.

- Policy Decision Point (PDP) it is one of the major components of the ZTF. It mainly consists of two parts namely Policy Engine (PE) [18] and Policy Administrator (PA).
- Policy Engine (PE) the supreme authority of granting access to an enterprise data/resource for a user/device lies with the PE. The PE allows, denies, and revokes access [18] to a resource based on a trust algorithm which takes as input the enterprise policies and data from various intelligence sources such as Continuous Diagnostics and Mitigation (CDMs) and Security Information and Event Management (SIEMs). The PE makes and records the decisions such as allowed or denied, whereas the Policy Administrator enforces those decisions. The firewall plays the role of the Policy Engine in the network. A VPN agent is required on the user's device for enabling the VPN connection and a proxy agent for the MFA login using the proxy server.

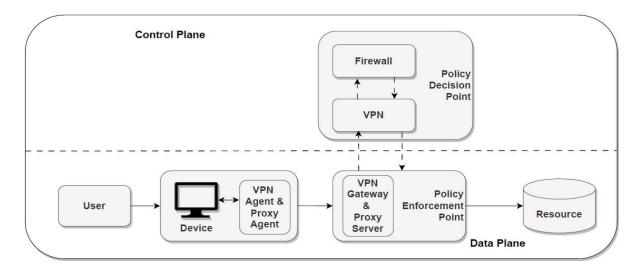


Figure 7 : Zero Trust Logical Components

- Policy Administrator (PA) establishes and terminates interaction between a user and the requested resource. A user can access a resource in the case of a valid session, using session authentication tokens or credentials created by the PA. The PA asks the PEP [18] to establish the session once the session authorization and request authentication is completed. PA asks the PEP to shut down the contact if the session is denied. The PA communicates with PEP through the control plane. The VPN plays the role of the Policy Administrator in the network.
- Policy Enforcement Point (PEP) PEP is accountable for establishing, observing, and closing connections [18] between a user/device and an enterprise resource. All the resource access requests are forwarded by the PEP to the PA and the responses and policy updates are sent back by the PA to the PEP. The PEP can be considered as two components: the client side like an agent on a device and the resource side such as an access control gateway in front of the resource or in total as a single component that acts as a bidirectional gateway between the client and resource. The VPN Gateway and the proxy server play the role of the Policy Enforcement Point in the network. After the PEP, comes the trust zone where the enterprise resource is located.

In addition to the enterprise policy, several data sources provide input to the policy engine in making the access decisions which can be external as well, such SIEMs, Threat Feeds, Application, System and Data logs, Policies, Public Key Infrastructure, and IAMs. Table 3 provides a Mapping of the NIST Zero Trust Framework [18] with respect to the Proposed Zero Trust Framework. From Table 3 we can see that the proposed Zero Trust MFA framework offers several advantages over the NIST Zero Trust Framework. Although implementing the proposed Zero Trust MFA framework may require additional configuration efforts and integration of multiple components, its adoption provides increased security, multifactor authentication, and the added benefits from the principles of Zero Trust. These factors make it a robust and effective approach to securing network access compared to the NIST Zero Trust Framework.

Component	NIST Zero Trust	Proposed Zero Trust MFA
Component	Framework	Framework
System	User's Device	VPN Agent for VPN connection & Proxy Agent for windows login
Policy Enforcement Point (PEP)	PEP System consists of single/multiple components described in general.	VPN Gateway and Proxy Server performs the function of policy enforcement.
Policy Decision Point (PDP)	Policy Engine (PE) and Policy Administrator (PA). Provides a generalized description of PE & PA.	Firewall (PE) and VPN (PA) performs the function of policy decision making.
Authentication Method	Dependent on the individual or organization's choice	MFA Authentication Using DUO with AD credentials as primary authentication and user certificates for user/device verification.
Authentication Factors	Typically, username and password	Multiple factors (e.g., username, password, Duo MFA, etc.)

Table 3 : Mapping of NIST & The Proposed Framework

Trust Model	Trust but verify	Zero Trust (never trust, always verify)	
Access Control	Role-based access control	Role & location-based access control and least privilege methodology.	
Continuous Monitoring	Continuous monitoring of device behavior and network traffic	Continuous monitoring of device behavior and network traffic	
Advantages	Provides a framework to implement Zero Trust principles without actual guidelines.	In addition to providing detailed guidelines for implementing Zero Trust, combines multifactor authentication (MFA) from DUO for enhanced security.	
	Provides guidelines for risk assessment, access control, and continuous monitoring.	Incorporates the principle of least privilege through role & location- based access control and provides continuous monitoring of network for security attacks.	
Disadvantages	May require significant changes to existing infrastructure and processes. Requires careful planning and implementation to ensure proper enforcement of policies.	Implementation may require additional configuration and setup efforts, which is compensated with the added benefits of enhanced security with the addition of multifactor authentication and the practice of least privilege.	

3.4 Working Mechanism of The Proposed Zero Trust Framework (ZTF)

The overall operational process of the proposed Zero Trust Framework (ZTF) is outlined through the following steps and illustrated in the accompanying Figure 8. This provides a general understanding of how the framework operates:

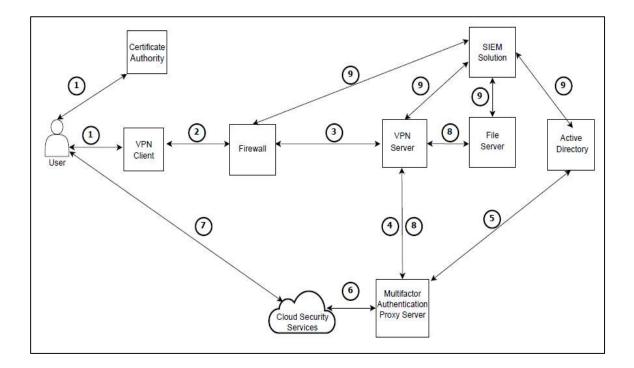


Figure 8 : Proposed Zero Trust Framework Working Mechanism

- Users receive certificates from the certifying authority, which verifies the identity of user and the device from which they are trying to access the network. Then the user connects to the network using the VPN client, providing Active Directory credentials (username and password) as primary authentication.
- 2. The login request from the user passes from the VPN client to the firewall, which either allows or denies the traffic based on the preconfigured rules.

- 3. The login request, if allowed, then passes from the firewall and reaches the VPN server.
- 4. The VPN server forwards the request to the multifactor authentication proxy server.
- 5. The proxy server verifies the primary credentials against the Active Directory database using LDAP protocol.
- 6. If the primary credentials are correct, the authentication proxy server requests additional authentication from the cloud security service.
- 7. The cloud security service sends a PUSH request to the user's registered mobile device as the second factor of authentication.
- 8. The authentication proxy server informs the VPN server to grant the user network access, once the user approves the PUSH request received on the mobile device. The user with the proper permissions configured in the Active Directory & the File Server can now access the data resources in the file server.
- 9. A SIEM solution is implemented for continuous monitoring of the network, user activity, and authentication information. The SIEM receives syslog from the firewall and is connected to the network server and Active Directory to enhance visibility and enable effective security monitoring and auditing.

The provided steps offer a high-level summary of the proposed Zero Trust Framework. For a more comprehensive understanding and practical implementation of the framework, the subsequent chapter provides detailed explanations and a real-world implementation example. This is intended to help organizations better understand and easily adopt the framework when transitioning to a Zero Trust strategy.

3.5 Multilayer Authentication Mechanisms in The Proposed Zero Trust Framework

In this Thesis, we have implemented a multi-layered security model to protect against unauthorized access. This model leverages various authentication mechanisms at different layers of the TCP/IP model to ensure that only authorized users can access the network and associated resources. Figure 9 shows the generalized authentication process happening at various layers, in case of the proposed framework. Figure 10 shows the authentication process at various layers specific to the actual implementation of the proposed framework.

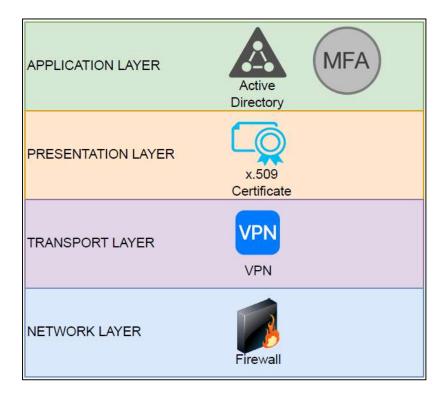


Figure 9 : General Authentication Process at Different Layers

• At the Network Layer, the firewall (e.g. pfSense) [38] performs access control by filtering incoming and outgoing traffic based on predefined rules. This provides an additional layer of security that ensures only authorized users can access the network and associated resources.

- At the Transport Layer, VPN (e.g. OpenVPN) Authentication [35] is used, which relies on the Transport Layer Security (TLS) protocol for secure communication between the client and the server. This provides a secure channel for transmitting sensitive data and ensures confidentiality, integrity, and authentication.
- At the Application Layer, Active Directory Credential Verification and the MFA solution (e.g. DUO MFA) is used to authenticate users against the Active Directory database and provide two-factor authentication for additional security [44]. Active Directory uses the LDAP Protocol to verify user login requests forwarded by the Proxy Server (e.g. DUO proxy). DUO uses the RADIUS protocol to communicate between the DUO proxy client and the DUO proxy server. This provides a robust authentication process that ensures only authorized users can access the network.
- At the Presentation Layer, Certificate Verification is used to ensure that the server's digital certificate is valid and issued by a trusted Certificate Authority (CA) [58]. This provides an additional layer of security against man-in-the-middle attacks and other threats that could compromise the security of the network.
- Finally, at the Application Layer, Windows Login Authentication is used to authenticate users against the Active Directory database using Kerberos protocols. These protocols use TCP/IP to communicate between the client and the server, providing a secure channel for transmitting authentication data.

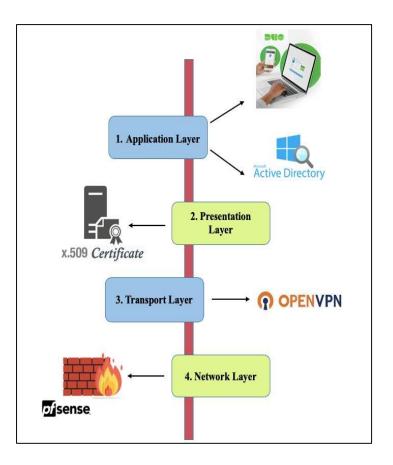


Figure 10 : Authentication at Various Layers

In summary, the proposed multi-layered security model provides robust security at different layers of the TCP/IP model, ensuring that only authorized users can access the network and associated resources. This model leverages a range of authentication mechanisms to provide confidentiality, integrity, and authentication, protecting against a range of security threats and vulnerabilities.

Chapter4: IMPLEMENTATION OF THE PROPOSED ZERO TRUST FRAMEWORK

4.1 Implementation of the Proposed Zero Trust Framework

Following are the key points that needs to be considered when implementing Zero Trust based on the proposed framework as seen from Figure 11:

- 1. Identify and categorize assets: identify [59] and categorize all the assets that need to be protected, including devices, applications, data, and users. In this Thesis we first identified the assets which need to be protected, namely the users, the data, the applications, the active directory server, the authentication server, the file server and finally the user workstations.
- 2. Establish strict access controls: Once the assets which needs to protected are identified, establish strict access controls [60] to limit access to only those who need it. This includes using multi-factor authentication, role and location based access control, and privileged access management. We implemented user-device certificate verification, password, and DUO PUSH as the primary and secondary form of authentication in this Thesis.
- **3.** Monitor and log all activities: Implement real-time monitoring and logging of all activities [59] to detect any anomalies and potential threats. This includes monitoring user behavior, network traffic, and system logs with the help of SIEM solutions. We implemented a sample SIEM solution e.g., Alien Vault to monitor and log all activities in the network as part of the implementation of the proposed framework.
- **4.** Security assessments: Conduct regular security assessments [60] and audits to identify vulnerabilities and address them proactively.



Figure 11 : Proposed Zero Trust Framework

4.2 Implementation of Multi Factor Authentication in the Proposed Zero Trust Framework

The different authentication strategies used in the implementation of the Proposed Zero Trust Framework are discussed below:

1. Certificates

Certificates are the first step of authentication which are used to identify the user and device from where the connection request to access the network is coming from. Each user is provided with a unique user certificate, which they use to identify themselves, and at the same time verify the device they are using to access the network. An internal certification authority (CA) has been set up in pfSense firewall to distribute the user & server certificates. In this Thesis we have set up a sample company named "DEF Company "as an example as seen Figure 12, for which we are implementing a Zero Trust Based Multi Factor Authentication Security Strategy for the company network, employees, and assets. For more details related to user certificates refer to Appendix A. We have also set up a sample domain for the company as "DEFCOMPANY.COM" in the active directory server and a sample internal certificate authority named "DEF Company CA". Also

created a server certificate - "DEF Company Server Certificate" for verification during authentication as an example.

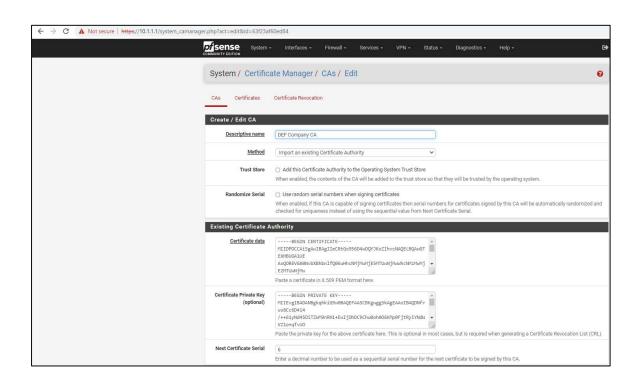


Figure 12 : Internal Certificate Authority

• CA Certificate

"DEF Company CA" acts as an internal certificate authority for the DEF Company Domain.

• User Certificate

Various sample user certificates have been created, that are signed by the CA's public key, which contains the user details and the user's public key. We created user certificates for the administrator, a test user and users named "Peter Parker" and "Johny Depp" as examples to show the different users in the organization.

The following are the created user certificates:

DEF_Administrator_Certificate DEF_Test_User_Certificate DEF_PeterParker_Certificate

• Server Certificate

"DEF Company Server Certificate" is used by the VPN (OpenVPN) server to verify itself with other servers and computers during the authentication process.

2. Username/Password Credentials

Each user is provided with a username and password which has been set up in the Active Directory (AD) of the company domain controller as seen in Figure 13. All users must provide these when logging into the VPN (OpenVPN) client application when accessing the network and also at the time of logging in to their necessary workstations or accounts, all maintained by the active directory services. For more details related to the AD credentials refer to Appendix A.

Windows Security	×	
Enter your credentials		
These credentials will be used to	connect to 10.1.1.20.	
johnydepp		
••••••		
DEFCOMPANY\johnydepp		
Remember me		
More choices		
ОК	Cancel	

Figure 13 : AD Credentials for Logging into the Domain

3. MFA

After providing the username/password credentials, the system requests for an additional step of authentication based on DUO's MFA as an example in this Thesis. This requests the user to verify the login is legitimate with the use of DUO Mobile App PUSH request on the respective user's phone as seen in Figure 14. The user can either allow or deny the PUSH request from the DUO mobile app, if the activity is not performed by them. The PUSH request was chosen as the type of MFA authentication to ease the process of authentication for users. This requests the users to allow or deny access instead of the tiresome OTP requests, thereby achieving an efficient balance between performance and security. For more details related to DUO MFA refer to Appendix A.

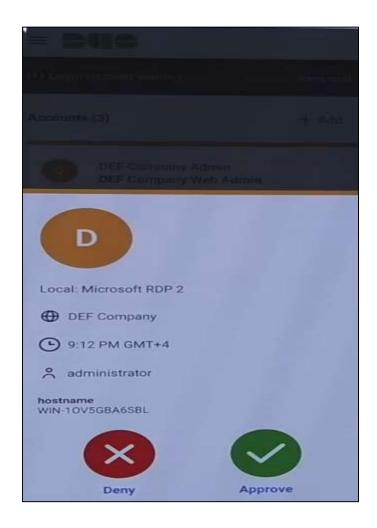


Figure 14 : DUO MFA PUSH Authentication from DUO Mobile App

4. Location Based Access

Incorporating DUO's Location Based User Access Policy into the proposed Zero Trust framework adds an additional layer of security and control. By leveraging location data, the model can restrict access to resources based on the physical location of the user or device as seen from Figure 15. This feature ensures that access is granted only from trusted locations, such as the company premises or specified secure networks. By implementing location-based access policies, the framework can mitigate the risk of unauthorized access from unknown or untrusted locations, further reinforcing the principles of Zero Trust. This functionality provides an effective means of enforcing access control and enhancing the overall security posture of the system. For more details related to DUO's Location Based User Access Policy refer to Appendix A.

Device Insight Policies	Outside UAE User	Authentication Log
Applications Single Sign-On	Looking for group policy? You can now apply specific policies to certain groups. This configuration lives on the application page.	
Users Groups Add Group Endpoints	Group name Outside UAE User	
2FA Devices Administrators Trust Monitor	Description User logins from outside the UAE	
Reports Settings Billing	Status Active Require two-factor authentication (default) Bypass	
Need Help? Email Support Call us at 1-855-386-2884 Versioning Core Authentication Service:	Skip two-factor authentication Disabled Automatically deny access This controls the two-factor authentication process for users in this group.	
D282.12 Admin Panet: D282.17 <u>Read Release Notes</u> Cf Account ID	Administrative Units Adsign administrative units Select which administrative units this group belongs to.	
1246-8222-91 Deployment ID	Save Changes	

Figure 15 : DUO's Location Based User Access Policy

4.3 Working Mechanism of The Implementation of The Proposed Zero Trust Framework

The detailed operational process of the implemented Zero Trust Framework (ZTF) is outlined through the following steps and illustrated in the accompanying Figure 16. This provides a detailed understanding of how the implemented framework operates in a real-world scenario:

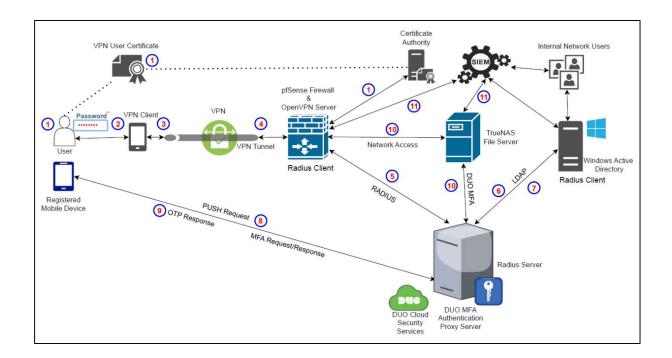


Figure 16 : Proposed Zero Trust Framework Implementation Working Mechanism

The pfSense's internal certificate authority issues user certificates for each AD user. Each AD user has their own OpenVPN config file to use for the OpenVPN client, containing the CA's certificate, the user's certificate, the user's private key, and the TLS key of the authentication server, to access the VPN client application installed on their device. Each user downloads the VPN client application in their machines and loads their VPN config file to access the VPN to the enterprise network. For more details steps related to the actual implementation refer to Appendix A.

- 1. The user installs the OpenVPN client application on their device and launches the OpenVPN client. The user certificate is used to authenticate the user's device to the OpenVPN server.
- The user enters the AD username and AD password in the OpenVPN login prompt to connect to the network. Sample user "Peter Parker" logins to the OpenVPN as seen in Figure 17. For more details refer to Appendix A.

Current Stati	pfSense-	UDP4-1198-DEF_PeterP	×
Wed Ma Wed Ma Wed Ma	Usemame: Password: Save pass OK		ie/0357ceb877687faa] Windows-MSV Windows 10 or greater) 64bit SSL 1.1.1s 1 Nov 2022, LZO 2.10
<	_	13	,
			OpenVPN GUI 11.31.0.0/2.5.8

Figure 17 : OpenVPN Client Login

- The OpenVPN client sends a connection request to the OpenVPN server, which is located behind the firewall. The pfSense firewall examines the request and allows or denies it based on the configured security rules.
- 4. If the firewall allows the connection, the OpenVPN server requests the user's certificate to authenticate the device. Once the user certificate is verified, and the OpenVPN server establishes a secure VPN connection between the user's device and the internal network.
- 5. The OpenVPN server sends a request to the DUO MFA Proxy Server which is connected to the DUO security cloud service for authenticating the user with DUO MFA. The model includes a DUO MFA Proxy Server & DUO cloud security for an additional layer of

authentication. The user receives a DUO PUSH request in the DUO mobile App and the protected user workstation also receives the DUO notification as seen from Figure 18. For more details refer to Appendix A.

\varTheta Duo Security				×
	Device:	Android (*XXX XX XXX 9958)		~
	Choose	an authentication method		
		Duo Push	Send Push	
Powered by Duo Security	Ċ	Phone Call	Call Me	
		Passcode	Enter a Passcode	
Pushed a login request to your	device		Cancel	

Figure 18 : DUO PUSH Request Notification at the time of Login

- 6. The DUO MFA Proxy Server uses the LDAP protocol to communicate with the Active Directory to authenticate the user's credentials.
- 7. The Active Directory verifies the user's credentials against the Active Directory database and sends a response back to the DUO MFA Proxy Server.
- 8. If the user's credentials are valid, the DUO MFA Proxy Server sends a request to the user's device, asking them to provide an additional layer of authentication, such as a DUO PUSH notification, SMS message, or a phone call as seen from Figure 19. For more details refer to Appendix A.

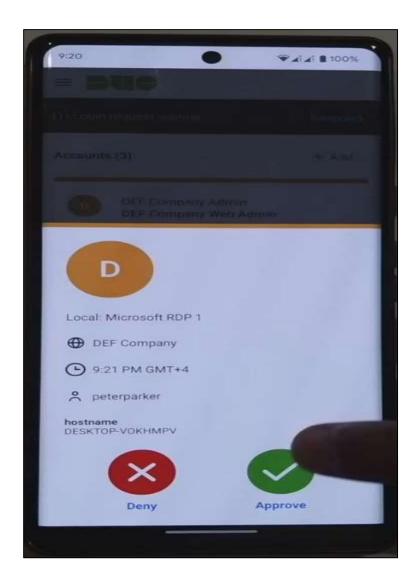


Figure 19 : DUO MFA PUSH Request to User's Phone

- 9. Once the user completes the multifactor authentication, the DUO MFA Proxy Server sends a response back to the OpenVPN server, allowing the user to access the network resources.
- 10. The Active Directory user with proper permissions can now access the TrueNAS shared file server to access resources & data. The fileserver's administrative console is also protected by the DUO MFA solution as seen from Figure 20. For more details refer to Appendix A.

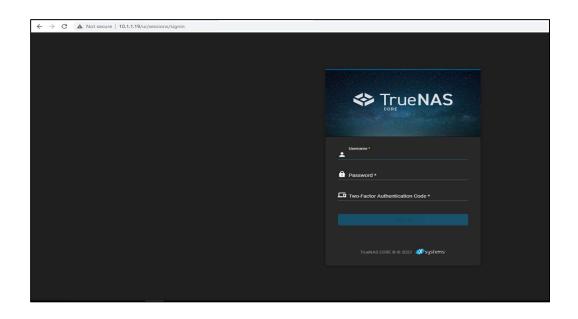


Figure 20 : TrueNAS File Server Console Protected By DUO MFA

11. Alien Vault's open-source SIEM solution OSSIM is integrated into the environment to collect the system, application, and data logs for monitoring and analysis thereby providing continuous monitoring of the enterprise's network for security threats and incidents as seen in Figure 22. Alien Vault SIEM dashboard console is shown in Figure 21. For more details refer to Appendix A.

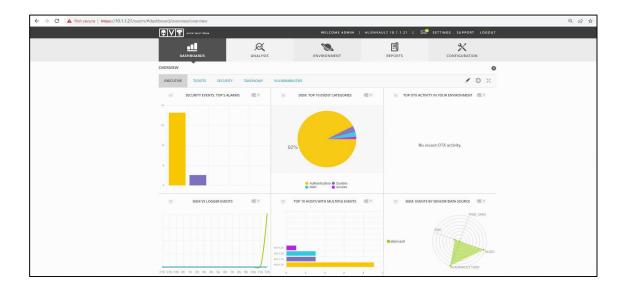


Figure 21 : Alien Vault SIEM Dashboard

→ C A Not secure https://10.1.1	.21/ossim/#analysis/security_events/security_events								
		X Alysis	EN	VIRONA	AENT	E	CONFIG		
	AllenVault HIDS: Windows Network Logon	2023-04-10 13:39:58	allenvault	N/A	Host-10-1-1-12:55439	Host-10-1-1-12	1+>2	LOW (0)	Ŕ
	AllenVault HIDS: Windows User Logoff.	2023-04-10 13:39:58	allenvault	N/A	Host-10-1-1-12	Host-10-1-1-12	1->2	LOW (0)	\$
	AllenVault HIDS: Windows Network Logon	2023-04-10 13:39:58	alienvault	N/A	Host-10-1-1-12:55441	Host-10-1-1-12	1->2	LOW (0)	\$
	AllenVault HIDS: Windows User Logoff.	2023-04-10 13:39:58	allenvault	N/A	Host-10-1-1-12	Host-10-1-1-12	1->2	LOW (0)	\$
	AllenVault HIDS: Special privileges assigned to new logo	2023-04-10 13:39:58	allenvault	N/A	Host-10-1-1-12	Host-10-1-1-12	1->2	LOW (0)	j
	AllenVault HIDS: Special privileges assigned to new logo	2023-04-10 13:39:58	allenvault	N/A	Host-10-1-1-12	Host-10-1-1-12	1+>2	LOW (0)	\$
	AllenVault HIDS: Windows Network Logon	2023-04-10 13:39:42	alienvault	N/A	Host-10-1-1-12:55436	Host-10-1-1-12	1->2	LOW (0)	\$
	AllenVault HIDS: Special privileges assigned to new logo	2023-04-10 13:39:42	allenvault	N/A	Host-10-1-1-12	Host-10-1-1-12	1->2	LOW (0)	1
	AllenVault HIDS: Windows User Logoff.	2023-04-10 13:39:42	allenvault	N/A	Host-10-1-1-12	Host-10-1-1-12	1->2	LOW (D)	

Figure 22 : Alien Vault SIEM Security Alarms

Overall, this proposed framework provides a secure and efficient solution for accessing enterprise network resources through VPN with the added benefit of multifactor authentication and continuous monitoring for security threats.

Chapter 5: COMPARATIVE ANALYSIS OF PERFORMANCE EFFICIENCY AND USER SATISFACTION OF THE PROPOSED FRAMEWORK

5.1 Comparative Analysis of the Proposed Zero Trust MFA Framework

This Thesis presents a comprehensive comparative analysis of the performance efficiency and user satisfaction of implementing a Zero Trust multifactor authentication (MFA) framework, focusing on the use of single-factor authentication versus the Duo MFA solution. Specifically, it compares the login time difference between single-factor authentication using normal Active Directory (AD) credentials and the time taken for authentication when combining primary AD credentials with secondary DUO proxy authentication via DUO MFA proxy PUSH requests. The Thesis investigates the user experience and satisfaction levels during login processes for both OpenVPN and Windows authentication. Additionally, the Thesis also explores how the use of PUSH requests has simplified the secondary authentication process, replacing traditional methods such as one-time passwords (OTP), text messages, or verification calls.

To conduct this analysis, we performed a series of experiments in a controlled environment using a sample group of users. The test involved measuring the login time for both Windows authentication and OpenVPN client authentication using two different authentication approaches: single-factor authentication using standard Active Directory (AD) credentials and primary AD credentials combined with secondary DUO MFA authentication through DUO MFA proxy PUSH requests. Additionally, user satisfaction surveys were conducted to gather feedback on their experience and perception of the authentication methods.

Results of the Comparative Analysis is as follows:

5.1.1 Windows Login Time Comparison

Table 4 shows the average login time in seconds for each authentication method for Windows authentication. 'A' represents the average login time when using single factor authentication with

standard AD credentials, while 'B' represents the average login time when combining primary AD credentials with secondary DUO MFA authentication. Based on our findings, the Windows login time for the primary AD and DUO MFA authentication method (B) was slightly longer compared to the single-factor authentication method (A). However, the difference was within an acceptable range and did not significantly impact on user experience.

5.1.2 OpenVPN Client Login Time Comparison

Table 4 shows the average login time in seconds for each authentication method for the OpenVPN client. 'C' represents the average login time when using single-factor authentication with standard AD credentials, while 'D' represents the average login time when combining primary AD credentials with secondary DUO MFA authentication via DUO MFA proxy push requests.

Similar to the Windows login time, the OpenVPN client login time for the primary AD + DUO MFA authentication method (D) was slightly longer compared to the single-factor authentication method (C). However, the difference was within an acceptable range and did not significantly impact user experience.

Table 4 : Average	Login Durations	for OpenVPN and	Windows Authentication

Authentication Method	Windows Login Time (Avg.)	OpenVPN Login Time (Avg.)	
Single-Factor Authentication	5-10 seconds (A)	8-16 seconds (C)	
Primary AD + DUO MFA	10-18 seconds (B)	16-22 seconds (D)	

Kindly note that the login times provided in the table are approximate averages and can vary based on network conditions, server performance, and other factors specific to the environment.

5.1.3 User Satisfaction

The user satisfaction surveys revealed the following insights: the implementation of a Zero Trust multifactor authentication framework, particularly combining primary AD credentials with DUO MFA proxy PUSH requests, positively impacts user satisfaction [75]. Despite the slightly longer login times [76], users appreciate the enhanced security and the simplified secondary authentication process.

The use of DUO PUSH requests for secondary authentication has simplified the user experience by eliminating the need for additional steps such as entering OTP or waiting for text messages. Users find the PUSH request method more efficient and less cumbersome [75], resulting in improved overall satisfaction and user acceptance of the multifactor authentication system.

The Thesis findings demonstrate that implementing a Zero Trust multifactor authentication framework, specifically utilizing DUO MFA as a secondary factor, positively impacts user satisfaction, enhances security without compromising overall performance efficiency for both Windows authentication and OpenVPN client authentication. While the login times may be slightly longer when using primary AD credentials combined with DUO MFA [76], users value the added security and appreciate the simplified secondary authentication process, which outweighs this minor inconvenience.

It is recommended that organizations prioritize the adoption of the Zero Trust multifactor authentication framework, using MFA e.g., DUO MFA in this case, for both Windows and VPN access. This proactive approach not only fortifies their security posture but also enhances user satisfaction by streamlining the login process and ensuring a seamless experience. Additionally, implementing these measures acts as a powerful defense mechanism against potential cyber threats.

Chapter 6: INFORMAL SECURITY ANALYSIS OF THE PROPOSED ZERO TRUST MULTI FACTOR AUTHENTICATION FRAMEWORK

6.1 Security Analysis of the Proposed ZTA Framework

In this section, we will conduct an informal security analysis to demonstrate how our proposed ZTA framework integrates multiple authentication features securely. By utilizing a combination of certificates, encryption algorithms, multifactor authentication, and continuous monitoring, our proposed framework ensures a high level of security and guards against unauthorized access. This comprehensive approach ensures a high level of security and protection for the system. When evaluating security effectiveness, the following observations were made:

Single-Factor Authentication: Single-factor authentication solely relies on the user's credentials (e.g., username and password) for both Windows authentication and OpenVPN client authentication. This method is vulnerable to various security threats, such as password-based attacks, phishing, and credential theft. Hackers gaining access to a user's credentials can easily bypass security measures and gain unauthorized access to both the Windows environment and the VPN network.

DUO Multifactor Authentication: Implementing DUO MFA as a secondary factor of authentication significantly enhances security for both Windows and OpenVPN access. By combining primary AD credentials with DUO MFA proxy PUSH requests, users are required to authenticate themselves through their registered mobile devices. Since the user's mobile phone is further protected by its own security mechanisms such as security pin codes, passwords or fingerprints.

In the unlikely scenario the device is stolen, the attacker needs to bypass the phone's security protocols to authenticate the DUO PUSH request received which is not possible since the attacker needs to know both the primary AD login credentials as well as the access credentials to the user's phone which is not very likely. This additional layer of authentication significantly reduces the

risk of unauthorized access, as attackers would need both the AD credentials and physical possession of the registered device. The use of DUO MFA effectively mitigates risks associated with password-based attacks, credential theft, and unauthorized access to both the Windows environment and the network.

6.2 Security Parameters of the Proposed Zero Trust MFA Framework

In order to enhance the comprehensibility of this Thesis, we employ a systematic approach by introducing preliminary information using notations to represent each component of the proposed framework as seen from Table 5. This allows for a more structured and organized presentation of the informal security analysis, making it easier for readers to grasp the key concepts and understand the underlying framework.

Notations	Description
%%	Comments
Ui	The ith user
Idi	Identity of Ui
PWi	Password of Ui provided by AD Server
Fpf	pFsense Firewall
Ci	User certificate issued by internal CA for Ui
Cs	Server certificate issued by internal CA
Sovpn	Open VPN Server
Sad	Active Directory (AD) Server
Sduo	DUO Proxy Server
Snas	TrueNAS File Server
Ssiem	SIEM Syslog Server
CLduo	DUO Cloud Security Service

Table 5 : Notations and their Descriptions

VPNc	Open VPN Client
Dph	DUO Push Request
DUOw	DUO Windows Local Logon Agent
Mi	Mobile device of Ui for DUO MFA
А	Adversary

6.2.1 User Certificate Issuance

In this Thesis, pfSense's (Fpf) internal certificate authority (CA) is utilized to issue user certificates for each Active Directory (AD) user. The user certificate (Ui) uses 4096 bits key and SHA256 as the digest algorithm for better security. Each user is assigned their own OpenVPN configuration file, containing the necessary certificates and keys. These files include the CA's certificate, the user's certificate, the user's private key, and the TLS key of the OpenVPN (Sovpn) authentication server, which are used by the VPN client application installed on the user's device.

Fpf -> Ci %% pfSense's (Fpf) internal CA generates user certificate for Ui.

Fpf -> Cs %% pfSense's (Fpf) internal CA generates server certificate for server validation.

Sovpn -> Ui %% OpenVPN server issues the VPN configuration file for Ui.

6.2.2 User Authentication and VPN Connection:

To connect to the network, users enter their AD username (Idi) and password (PWi) in the OpenVPN client (VPNc) login prompt. The Fpf then examines the request and applies security rules to determine whether to allow or deny the connection. If the Fpf allows the connection, the Sovpn requests the Ci to authenticate Ui's identity. Once the certificate is successfully verified, a secure VPN connection is established between the user's device and the internal network.

Ui -> VPNc %% User Ui enters Idi (username) and PWi (AD password) in the OpenVPN client application.

Fpf after checking the incoming request allows the connection based on the configuration rules.

Ui -> Sovpn : Ci %% OpenVPN server request Ui to provide the Ci for user verification.

6.2.3 Multifactor Authentication

This framework incorporates a DUO MFA Proxy Server (Sduo) to enhance security through an additional layer of authentication. The Sduo communicates with the Active Directory (Sad) using the LDAP protocol to verify the user's credentials. If the user's credentials are valid, the Sduo then requests the DUO cloud security (CLduo) service for the two-factor authentication. The CLduo then prompts the user's device (Mi) for an extra authentication factor, such as a DUO PUSH (Dph) notification. After completing the multifactor authentication process, the Sduo sends a response to the Sovpn granting the user access to the network. Similarly, the Sduo sends a response to the DUO Windows Local Logon Agent (DUOw) for granting the user local windows login access.

Remote Desktop Logon Using OpenVPN

Sduo -> Sad : Idi, PWi %% DUO proxy server checks the user's credentials against the Active directory server database.

Sduo -> CLduo %% DUO proxy server sends a request to the DUO cloud security service for 2FA.

CLduo -> Mi : Dph %% DUO cloud security sends DUO PUSH request to the user's device.

Sduo -> Sovpn %% DUO proxy server replies to the OpenVPN server granting user network access.

Windows Local Logon

Sduo -> Sad : Idi, PWi %% DUO proxy server checks the user's credentials against the Active directory server database.

Sduo -> CLduo %% DUO proxy server sends a request to the DUO cloud security service for 2FA.

CLduo -> Mi : Dph %% DUO cloud security sends DUO PUSH request to the user's device.

Sduo -> DUOw %% DUO proxy server replies to the Windows Logon Agent granting the user windows login access.

6.2.4 TrueNAS File Server Access

AD users with appropriate permissions can access the TrueNAS shared file server, which provides resources and data within the enterprise network. The file server's administrative console is also safeguarded by the DUO MFA solution, ensuring secure access to administrative functions.

Snas -> Ui %% The user with the proper permissions can access the network file server provided they have the necessary permissions.

6.2.5 Security Monitoring

To continuously monitor the enterprise's network for security threats and incidents, the model integrates Alien Vault's open-source SIEM solution, OSSIM. OSSIM collects the system, application, and data logs, allowing for comprehensive security monitoring and analysis. Remote syslog forwarding is enabled in Fpf, to forward all the syslog data to Alien Vault SIEM's syslog server (Ssiem). All the user logons are logged in the SIEM dashboard for SOC analysts to ensure that only the authorized users are accessing the network as a part of continuous monitoring in the Zero Trust strategy.

Fpf -> Ssiem %% the firewall forwards all syslog data to the SIEM for continuous network monitoring.

6.2.6 Adversarial model

The adversary in this Thesis is assumed to have following capabilities:

A. The adversary (A) can sniff the network traffic using the Wireshark tool to collect sensitive data.

B. Adversary A has gained knowledge of a particular user's AD password.

In this Thesis, we evaluated the security of the authentication mechanism used in the proposed framework that utilizes the OpenVPN-pfSense client with Active Directory credential as primary authentication and DUO MFA proxy for DUO PUSH as the secondary authentication. To achieve this, the Wireshark tool was used to capture and analyze the network traffic.

Results of A:

The analysis revealed that the proposed authentication mechanism is indeed secure even if captured by Wireshark by Adversary(A). The proposed framework requires a two-step authentication process to access the network, with the first step being the use of VPNc with {Idi, PWi} as the primary authentication and Dph as the secondary authentication method. The second step also uses {Idi, PWi} as primary authentication and Dph as secondary authentication in the Windows login screen. This dual authentication approach enhances the security of the overall system.

DUO Security employs the Sduo and CLduo to provide an extra layer of security for both local logon and Remote Desktop Protocol (RDP) applications. When users attempt to log in to a Windows system either locally or through RDP, the Sduo and CLduo comes into play. It integrates with the authentication process and requires a Dph request as the second factor of authentication. This means that after users enter their primary {Idi, PWi} credentials, they receive a notification on their mobile devices prompting them to verify the login attempt. Only after successfully completing this second authentication step can users gain access to the network and resources.

Similarly, when using OpenVPN, once users provide their {Idi, PWi} primary credentials and are verified, the CLduo triggers a Dph request as the second factor of authentication. By approving the push notification on their mobile devices, users validate their identities and establish a secure connection to the OpenVPN network.

In both cases, DUO Security's integration of the DUO proxy (Sduo and CLduo) with OpenVPN, local and RDP applications strengthens the authentication process, protecting against unauthorized access and reinforcing the principles of zero trust security.

Furthermore, the use of Ci created by the internal CA to validate the user logging in, as well as the use of a Cs for the Sovpn for server validation. Additionally, the Diffie-Hellman parameter (DH)

was set to 4096 bits in the OpenVPN, which provides a high level of security and makes it difficult for attackers to crack the encryption keys. The data encryption algorithms chosen, namely AES-256-GCM, are known for their high level of security and are widely used in secure communication protocols. Finally, TLS 1.2 encryption is used to secure OpenVPN communication, which adds another layer of security to the overall authentication mechanism.

		apture Analyze Statistics 🕅 🙆 🍳 🗭 🏓 🚟 🗿 🖠		пер	
ply a	a display filter <ct< th=""><th>rl-/></th><th></th><th></th><th></th></ct<>	rl-/>			
F	Packet bytes 🗸 🗸	Narrow & Wide 🛛 🗸 🗌	Case sensitive String	✓ pe	ter Find
	Time	Source	Destination	Protocol	Length Info
	1 0.000000	10.1.1.15	40.81.94.65	NTP	90 NTP Version 3, client
	2 0.047970	40.81.94.65	10.1.1.15	NTP	90 NTP Version 3, server
	3 4.670278	PcsCompu_92:c7:f2	PcsCompu_fb:b7:c6	ARP	42 Who has 10.1.1.1? Tell 10.1.1.15
	4 4.670954	PcsCompu_fb:b7:c6	PcsCompu_92:c7:f2	ARP	60 10.1.1.1 is at 08:00:27:fb:b7:c6
	5 17.357894	10.1.1.1	10.1.1.15	RADIUS	183 Access-Request id=187
	6 17.365019	10.1.1.15	10.1.1.12	TCP	66 49818 → 389 [SYN, ECE, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
	7 17.366831	10.1.1.12	10.1.1.15	TCP	66 389 → 49818 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
	8 17.366972	10.1.1.15	10.1.1.12	TCP	54 49818 → 389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
	9 17.369778	10.1.1.15	10.1.1.12	LDAP	122 bindRequest(22) " <root>" , NTLMSSP_NEGOTIATEsas1</root>
	10 17.370498	10.1.1.12	10.1.1.15	LDAP	358 bindResponse(22) saslBindInProgress , NTLMSSP_CHALLENGE
	11 17.373651	10.1.1.15	10.1.1.12	LDAP	524 bindRequest(23) " <root>" , NTLMSSP_AUTH, User: DEFCOMPANY\service_accsasl</root>
	12 17.377137	10.1.1.12	10.1.1.15	LDAP	78 bindResponse(23) success
	13 17.388618	10.1.1.15	10.1.1.12	LDAP	157 SASL GSS-API Privacy: payload (83 bytes)
	14 17.389577	10.1.1.12	10.1.1.15	LDAP	205 SASL GSS-API Privacy: payload (131 bytes)
	15 17.394626	10.1.1.15	10.1.1.12	LDAP	371 SASL GSS-API Privacy: payload (297 bytes)
	16 17.399106	10.1.1.12	10.1.1.15	LDAP	480 SASL GSS-API Privacy: payload (406 bytes)
	17 17.409253	10.1.1.15	10.1.1.12	LDAP	142 SASL GSS-API Privacy: payload (68 bytes)
	18 17.410360	10.1.1.12	10.1.1.15	LDAP	378 SASL GSS-API Privacy: payload (304 bytes)
	19 17.417120	10.1.1.15	10.1.1.12	LDAP	544 SASL GSS-API Privacy: payload (470 bytes)
	20 17.420223	10.1.1.12	10.1.1.15	LDAP	98 SASL GSS-API Privacy: payload (24 bytes)
	21 17.428967	10.1.1.15	10.1.1.12	TCP	54 49818 → 389 [RST, ACK] Seq=1537 Ack=1274 Win=0 Len=0
	22 17.436406	10.1.1.15	10.1.1.12	DNS	88 Standard guery 0x3dc3 A api-4a4df253.duosecurity.com
	23 17 563430	10 1 1 12	10 1 1 15	DNS	104 Standard query response 0x3dc3 A ani-4a4df253 duosecurity com A 52 19 127 204
		to this request is in t	frame 631		▲ 0000 08 00 27 92 c7 f2 08 00 27 fb b7 c6 08 00 45 00 ·······E·
	Attribute Valu				0010 00 a9 93 ec 00 00 40 11 d0 46 0a 01 01 01 0a 01@ F
		ice-Type(6) l=6 val=Log			0020 01 0f 52 68 07 14 00 95 4e 73 01 bb 00 8d c8 e6 Rh Ns 0030 94 d8 8e ef 88 31 db ff 22 a3 1f ad a5 7c 06 061"
		-Name(1) l=13 val=peter	parker		0040 94 08 86 ef 88 31 00 ft 22 33 11 a0 a5 76 06 06
	Type: 1				0050 72 02 12 c4 7d 6e 02 c3 2b df 6b 9f 6e d7 44 81 $r + k \cdot n \cdot D$
	Length: :				0060 4a 04 83 04 06 0a 01 01 01 20 09 6f 70 65 6e 56 J openV
		e: peterparker			0070 50 4e 1f 14 31 39 32 2e 31 36 38 2e 37 2e 31 39 PN 192. 168.7.19
		-Password(2) l=18 val=E	ncrypted		0080 36 3a 31 31 39 38 1e 25 30 38 3a 30 30 3a 32 37 6:1198 % 08:00:27
	Type: 2				0090 3a 66 62 3a 62 37 3a 63 36 3a 70 66 53 65 6e 73 :fb:b7:c 6:pfSens
	Length: :				00a0 65 2e 68 6f 6d 65 2e 61 72 70 61 3d 06 00 00 0 e.home.a rpa=····
		sword (encrypted): c47d		14a0483	00b0 05 05 06 00 00 04 ae
		IP-Address(4) l=6 val=1			
		Identifier(32) 1=9 val=			
	> AVP: t=Call	ing-Station-Id(31) 1=20	val=192.168.7.196:11	.98	v
					>

Figure 23 : Wireshark Capture of Encrypted User Password

From the traffic capture of Sduo using the Wireshark tool by A, as seen in Figure 23, we can conclude that the username of the user is "peterparker" which is unencrypted but the password "c47d6e02c32bdf6b0f6ed744814a0483" is encrypted, thereby achieving secure multifactor authentication based on Zero Trust as proposed in this Thesis.

Results of B:

The analysis revealed that that in the unlikely case the Ui's {Idi, PWi} credentials used for the primary authentication are compromised, A needs to provide the second factor of authentication Dph. Since the secondary authentication is handled by the Sduo and CLduo, the Dph request is send to the registered Ui's Mi which is further protected by the Mi's internal security such as security pin, password, or fingerprint. Thereby reducing the chance of compromising the two-factor authentication, even if Ui's Mi is stolen.

The proposed framework provides a secure and efficient solution for accessing enterprise network resources using multi factor authentication based on the Zero Trust approach. By using a combination of certificates, encryption algorithms, multifactor authentication, and continuous monitoring, the proposed framework provides a high level of security and protection against unauthorized access.

Chapter 7: CONCLUSIONS AND FUTURE WORKS

7.1 CONCLUSION

The implementation of a Zero Trust Framework has become a critical need for organizations due to the increase in remote working and the reliance on cloud computing and IoT devices. The traditional perimeter-based security models have proven to be inadequate in protecting sensitive data and services from unauthorized access.

The implementation of DUO MFA, Active Directory credentials, and digital certificates in conjunction with OpenVPN and pfSense firewall has been instrumental in creating a Zero Trust multifactor authenticated environment framework. This Thesis offers a comprehensive guide to deploying the Zero Trust Framework in an enterprise environment, utilizing cutting-edge technologies to tackle the security risks stemming from the blurry boundaries of corporate networks. By minimizing the attack surface and relying only on authenticated and authorized access instead of blind trust, the proposed framework enhances security while decreasing the organization's exposure to potential cyberattacks.

The use of DUO MFA provides an extra layer of security by requiring users to provide twofactor authentication before granting access to the network. The Active directory credentials help to streamline the authentication process and grant access based on user roles and permissions. The use of digital certificates further enhances security by ensuring that only authorized devices are allowed access.

The proposed Zero Trust Framework (ZTF) in this Thesis goes beyond just theory and offers practical implementation steps for organizations to adopt a more secure and efficient ZTF. What sets this Thesis apart is that it focuses on implementing Zero Trust together with multifactor authentication, which is crucial in today's cybersecurity landscape. Surprisingly, there are very few papers that discuss implementing Zero Trust together with multifactor. However,

in this Thesis, we have not only proposed this model, but also implemented it in a virtual environment and provided detailed steps on how to set up this proposed framework. By following the steps outlined in this Thesis, organizations can effectively reduce their attack surface and significantly improve their security posture, all while minimizing additional expenses.

Security analysis resulting in the capture and analysis of the network traffic showed that the proposed Zero Trust MFA framework is secure against sniffing and password compromise attacks. Further analysis of performance efficiency and user satisfaction provided valuable insights into how the proposed framework achieves a balance between performance and security, while maintaining a positive user experience. The dual authentication approach and encryption methods provide a high level of security and protection against unauthorized access. The proposed framework is an effective solution for organizations looking to enhance their security posture.

7.2 PROPOSED FUTURE WORK

In future research, there are a few areas that can be explored to enhance the implementation of the Proposed Zero Trust MFA Framework:

Network Segmentation: Investigate and develop advanced techniques for network segmentation to further strengthen the isolation of different network segments. This can involve exploring software-defined networking (SDN) solutions and advanced firewall configurations to create robust and fine-grained network boundaries.

Privileged Access Management (PAM) and Granular Access Control: Extend the Zero Trust framework by incorporating effective Privileged Access Management mechanisms. Explore methods to implement granular access control policies that enforce least privilege principles, ensuring that users and systems have access only to the resources they require.

By addressing these future areas of focus, the Thesis can contribute to the continuous improvement and practical implementation of Zero Trust Framework in conjunction with multifactor authentication, leading to stronger security postures and better protection against advanced threats.

REFERENCES

- C. A. Iordache, A. V. Dragomir, and C. V. Marian, "Public Institutions Updated Enhanced Biometric Security, Zero Trust Architecture and Multi-Factor Authentification," 2022 15th Int. Symp. Electron. Telecommun. ISETC 2022 - Conf. Proc., pp. 5–8, 2022, doi: 10.1109/ISETC56213.2022.10010127.
- [2] C. Decusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, "Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication," *Proc. - 2016 IEEE Int. Conf. Smart Cloud, SmartCloud 2016*, pp. 5–10, 2016, doi: 10.1109/SmartCloud.2016.22.
- Y. K. Lee, Y. H. Kim, and J. N. Kim, "IoT standard platform architecture that provides defense against DDoS attacks," 2021 IEEE Int. Conf. Consum. Electron. ICCE-Asia 2021, pp. 6–8, 2021, doi: 10.1109/ICCE-Asia53811.2021.9641892.
- S. Schmeelk, K. Thakur, M. L. Ali, D. M. Dragos, A. Al-Hayajneh, and B. R. Pramana, "Top Reported Data Security Risks in the Age of COVID-19," 2021 IEEE 12th Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2021, pp. 204–208, 2021, doi: 10.1109/UEMCON53757.2021.9666573.
- [5] H. A. Dinesha and V. K. Agrawal, "Multi-level authentication technique for accessing cloud services," *2012 Int. Conf. Comput. Commun. Appl. ICCCA 2012*, pp. 1–4, 2012, doi: 10.1109/ICCCA.2012.6179130.
- [6] M. Uddin, S. Islam, and A. Al-Nemrat, "A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control," *IEEE Access*, vol. 7, pp. 166676–166689, 2019, doi: 10.1109/ACCESS.2019.2947377.
- [7] National Institute of Standards And Technology, "Framework for Improving Critical Infrastructure Cybersecurity," 2018, [Online]. Available: https://doi.org/10.6028/NIST.CSWP.04162018
- [8] P. Tarwireyi, S. Flowerday, and A. Bayaga, "Information security competence test with regards to password management," 2011 Inf. Secur. South Africa - Proc. ISSA 2011 Conf., 2011, doi: 10.1109/ISSA.2011.6027524.

- [9] A. Wylde, "Zero trust: Never trust, always verify," 2021 Int. Conf. Cyber Situational Awareness, Data Anal. Assessment, CyberSA 2021, 2021, doi: 10.1109/CyberSA52016.2021.9478244.
- C. Dong, F. Jiang, S. Chen, and X. Liu, "Continuous Authentication for UAV Delivery Systems Under Zero-Trust Security Framework," pp. 123–132, 2022, doi: 10.1109/edge55608.2022.00027.
- P. Sharma, "A contemplate on multifactor authentication," *Proc. 2019 6th Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2019*, pp. 824–827, 2019.
- [12] D. Horne and S. Nair, "Introducing Zero Trust by Design: Principles and Practice Beyond the Zero Trust Hype," no. April, 2021, [Online]. Available: https://www.researchgate.net/publication/353324913
- [13] D. Campara and N. Mansourov, "How to tackle security issues in large existing/legacy systems while maintaining development priorities," 2008 IEEE Int. Conf. Technol. Homel. Secur. HST'08, pp. 167–172, 2008, doi: 10.1109/THS.2008.4534443.
- [14] D. Kolevski, K. Michael, R. Abbas, and M. Freeman, "Cloud Data Breach Disclosures: The Consumer and their Personally Identifiable Information (PII)?," 2021 IEEE Conf. Norbert Wiener 21st Century Being Hum. a Glob. Village, 21CW 2021, pp. 1–9, 2021, doi: 10.1109/21CW48944.2021.9532579.
- [15] "NIST CYBERSECURITY FRAMEWORK." https://cyberwatching.eu/nistcybersecurity-framework (accessed Jun. 12, 2023).
- [16] ISO/IEC 27001, "Information technology Security techniques Information security management systems - Overview and vocabulary," *Iso/Iec*, vol. 2005, p. ISO/IEC 27000:2005(E), 2005.
- [17] "ISO/IEC 27001 Information security management systems." https://www.iso.org/standard/27001 (accessed Jun. 12, 2023).
- [18] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," National Institute of Standards and Technology, NIST Special Publication (SP) 800-207, 2020.
- [19] "SP 800-207 Zero Trust Architecture." https://csrc.nist.gov/publications/detail/sp/800-207/final (accessed Jun. 12, 2023).

- [20] Y. Bobbert and J. Scheerder, "Zero Trust Validation: from Practice to Theory : An empirical research project to improve Zero Trust implementations," *Proc. 2022 IEEE 29th Annu. Softw. Technol. Conf. STC 2022*, pp. 93–104, 2022, doi: 10.1109/STC55697.2022.00021.
- [21] C. Zhang et al., "Tag-Based Trust Evaluation In Zero Trust Architecture," 2022 4th Int. Acad. Exch. Conf. Sci. Technol. Innov., pp. 772–776, 2023, doi: 10.1109/iaecst57965.2022.10062213.
- [22] V. Krishnan and C. S. Sreeja, "Zero Trust-Based Adaptive Authentication using Composite Attribute Set," 2021 IEEE 3rd PhD Colloq. Ethically Driven Innov. Technol. Soc. PhD Ed. 2021, pp. 2–3, 2021, doi: 10.1109/PhDEDITS53295.2021.9649474.
- [23] L. Meng, D. Huang, J. An, X. Zhou, and F. Lin, "A continuous authentication protocol without trust authority for zero trust architecture," *China Commun.*, vol. 19, no. 8, pp. 198–213, 2022, doi: 10.23919/jcc.2022.08.015.
- [24] L. Chen, Y. Sun, and Z. Sun, "A Mobile Internet Multi-level Two-way Identity Authentication Scheme Based on Zero Trust," 2021 IEEE 23rd Int. Conf. High Perform. Comput. Commun. 7th Int. Conf. Data Sci. Syst. 19th Int. Conf. Smart City 7th Int. Conf. Dependability Sensor, Cl, no. 61972208, pp. 1650–1656, 2022, doi: 10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00243.
- [25] L. Lu, J. Han, L. Hu, J. Huai, Y. Liu, and L. M. Ni, "Pseudo Trust : Zero-Knowledge Based Authentication in Anonymous Peer-to-Peer Protocols State Key Lab of Information Security Dept . of Computer Science and Engineering Graduate School of Chinese Academy Science Hong Kong University of Science and Technolo," *Design*, 2007.
- [26] F. Al-Ayed, "Zero-Trust Model of Cybersecurity: A Significant Challenge in the Future," *Proc. - 2021 Int. Conf. Comput. Sci. Comput. Intell. CSCI 2021*, vol. 0, pp. 852–854, 2021, doi: 10.1109/CSCI54926.2021.00200.
- Y. Song, F. Jiang, S. W. Ali Shah, and R. Doss, "A New Zero-Trust Aided Smart Key Authentication Scheme in IoV," 2022 IEEE Int. Conf. Pervasive Comput. Commun. Work. other Affil. Events, PerCom Work. 2022, pp. 630–636, 2022, doi: 10.1109/PerComWorkshops53856.2022.9767534.
- [28] P. Fu, J. Wu, X. Lin, and A. Shen, "ZTEI: Zero-Trust and Edge Intelligence Empowered

Continuous Authentication for Satellite Networks," 2022 IEEE Glob. Commun. Conf. GLOBECOM 2022 - Proc., pp. 2376–2381, 2022, doi: 10.1109/GLOBECOM48099.2022.10000958.

- [29] Y. Ge and Q. Zhu, "MUFAZA: Multi-Source Fast and Autonomous Zero-Trust Authentication for 5G Networks," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, vol. 2022-Novem, pp. 571–576, 2022, doi: 10.1109/MILCOM55135.2022.10017839.
- [30] S. Hoppe and M. Toussaint, "Qgraph-bounded Q-learning: Stabilizing Model-Free Off-Policy Deep Reinforcement Learning," 2020, [Online]. Available: http://arxiv.org/abs/2007.07582
- [31] N. Bannour, P. Wajsbürt, B. Rance, X. Tannier, and A. Névéol, "Privacy-preserving mimic models for clinical named entity recognition in French," *J. Biomed. Inform.*, vol. 130, no. April, 2022, doi: 10.1016/j.jbi.2022.104073.
- [32] T. Dimitrakos *et al.*, "Trust aware continuous authorization for zero trust in consumer internet of things," *Proc. 2020 IEEE 19th Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2020*, pp. 1801–1812, 2020, doi: 10.1109/TrustCom50675.2020.00247.
- [33] D. H. Hwang, J. M. Shin, and Y. H. Choi, "Authentication Protocol for Wearable Devices Using Mobile Authentication Proxy," *Int. Conf. Ubiquitous Futur. Networks, ICUFN*, vol. 2018-July, pp. 700–702, 2018, doi: 10.1109/ICUFN.2018.8436650.
- [34] M. Pudelko, P. Emmerich, S. Gallenmüller, and G. Carle, "Performance Analysis of VPN Gateways," *IFIP Netw. 2020 Conf. Work. Netw. 2020*, pp. 325–333, 2020.
- [35] M. Du, "Implementation of a host-to-host VPN based on UDP tunnel and OpenVPN Tap interface in Java and its performance analysis," *Proc. 8th Int. Conf. Comput. Sci. Educ. ICCSE 2013*, no. Iccse, pp. 940–943, 2013, doi: 10.1109/ICCSE.2013.6554047.
- [36] I. Coonjah, P. C. Catherine, and K. M. S. Soyjaudah, "Experimental performance comparison between TCP vs UDP tunnel using OpenVPN," 2015 Int. Conf. Comput. Commun. Secur. ICCCS 2015, pp. 1–5, 2016, doi: 10.1109/CCCS.2015.7374133.
- [37] S. Krit and E. Haimoud, "Overview Of Firewalls : Types And Policies," 2017 Int. Conf. Eng. MIS, pp. 1–7, 2017.
- [38] P. Senthilkumar and M. Muthukumar, "A study on firewall system, scheduling and

routing using pfsense scheme," *Proc. IEEE Int. Conf. Intell. Comput. Commun. Smart World, I2C2SW 2018*, pp. 14–17, 2018, doi: 10.1109/I2C2SW45816.2018.8997167.

- [39] "PfSense 2.4.3 OpenVPN with RADIUS via Active Directory pfSense Part 13." https://www.youtube.com/watch?v=xyRNQ6TkYLc (accessed Jun. 12, 2023).
- [40] J. Feng, "Analysis, implementation and extensions of RADIUS protocol," *Proc. 2009 Int. Conf. Netw. Digit. Soc. ICNDS 2009*, vol. 1, pp. 154–157, 2009, doi: 10.1109/ICNDS.2009.44.
- [41] J. Feng, "Design and implementation of radius client based on finite state machine," *Proc.* 2009 Pacific-Asia Conf. Circuits, Commun. Syst. PACCS 2009, pp. 435–438, 2009, doi: 10.1109/PACCS.2009.53.
- [42] R. V. Deshmukh, "RADIUS accounting server behavior with interactive model," 2nd Int. Conf. Innov. Comput. Technol. INTECH 2012, pp. 87–90, 2012, doi: 10.1109/INTECH.2012.6457812.
- [43] "How to Install Radius Server Linux on Ubuntu (Step by Step)."
 https://cloudinfrastructureservices.co.uk/radius-server-linux/ (accessed Jun. 12, 2023).
- [44] H. Kai, "The design and realization of server virtualization based on active directory," *Proc. - 2009 Int. Forum Inf. Technol. Appl. IFITA 2009*, vol. 1, pp. 740–742, 2009, doi: 10.1109/IFITA.2009.531.
- [45] "Configuring Active Directory (Windows Server) RADIUS Protocol for OpenVPN Access Server." https://openvpn.net/vpn-server-resources/openvpn-access-server-andactive-directory-radius/ (accessed Jun. 12, 2023).
- [46] M. H. Jalalzai, W. B. Shahid, and M. M. W. Iqbal, "DNS security challenges and best practices to deploy secure DNS with digital signatures," *Proc. 2015 12th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2015*, pp. 280–285, 2015, doi: 10.1109/IBCAST.2015.7058517.
- [47] "How To add DNS Forward Lookup Zone in Windows Server 2019."
 https://computingforgeeks.com/how-to-add-dns-forward-lookup-zone-in-windows-server/ (accessed Jun. 12, 2023).
- [48] C. Tang, X. Fu, and P. Tang, "Policy-Based Network Access and Behavior Control

Management," Int. Conf. Commun. Technol. Proceedings, ICCT, vol. 2020-Octob, pp. 1102–1106, 2020, doi: 10.1109/ICCT50939.2020.9295916.

- [49] Y. Yuan, Q. Liu, and F. Li, "A design of certificate authority based on elliptic curve cryptography," Proc. - 9th Int. Symp. Distrib. Comput. Appl. to Business, Eng. Sci. DCABES 2010, pp. 454–457, 2010, doi: 10.1109/DCABES.2010.99.
- [50] A. Demidov, D. Polovinkin, T. Potlova, R. Shateev, and E. Sopina, "Algorithms of authentication and authorization by proxy in distributed information-computing environment," *11th IEEE Int. Conf. Appl. Inf. Commun. Technol. AICT 2017 - Proc.*, pp. 1–5, 2019, doi: 10.1109/ICAICT.2017.8687048.
- [51] "Duo Authentication Proxy." https://help.duo.com/s/article/3357?language=en_US (accessed Jun. 12, 2023).
- [52] S. Ibrokhimov, K. L. Hui, A. Abdulhakim Al-Absi, H. J. Lee, and M. Sain, "Multi-Factor Authentication in Cyber Physical System: A State of Art Survey," *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2019-Febru, pp. 279–284, 2019, doi: 10.23919/ICACT.2019.8701960.
- [53] A. Bhide, E. N. Elnozahy, and S. P. Morgan, "Implicit replication in a network file server," *Proc. Work. Manag. Replicated Data*, pp. 85–90, 1990, doi: 10.1109/mrd.1990.138251.
- [54] D. Z. Han and J. Z. Huang, "Security for the storage network merging NAS and SAN," *Proc. 2006 Int. Conf. Mach. Learn. Cybern.*, vol. 2006, no. August, pp. 736–741, 2006, doi: 10.1109/ICMLC.2006.258445.
- [55] "Documentation Hub/TrueNAS CORE/Configuration Tutorials/Storage/Pools/Creating Pools." https://www.truenas.com/docs/core/coretutorials/storage/pools/poolcreate/ (accessed Jun. 12, 2023).
- [56] M. A. Qadeer, M. Salim, and M. Sana Akhtar, "Profile management and authentication using LDAP," *Proc. - 2009 Int. Conf. Comput. Eng. Technol. ICCET 2009*, vol. 2, pp. 247–251, 2009, doi: 10.1109/ICCET.2009.126.
- [57] R. Nikhil, B. S. Anisha, and P. Ramakanth Kumar, "Users Sync Authentication using External Ldap in Organizations," 2020 IEEE Int. Conf. Innov. Technol. INOCON 2020,

pp. 1–4, 2020, doi: 10.1109/INOCON50539.2020.9298432.

- [58] M. Cano, R. Toledo-valera, and F. Cerdan, "A Certification Authority for Elliptic Curve X.509v3 Certificates," pp. 7–12, 2007.
- [59] M. Campbell, "Beyond Zero Trust: Trust Is a Vulnerability," *Computer (Long. Beach. Calif).*, vol. 53, no. 10, pp. 110–113, 2020, doi: 10.1109/MC.2020.3011081.
- [60] Y. Tao, Z. Lei and P. Ruxiang, "Fine-Grained Big Data Security Method Based on Zero Trust Model," 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, 2018, pp. 1040-1045, doi: 10.1109/PADSW.2018.8644614
- [61] "Latest Stable Version (Community Edition)." https://www.pfsense.org/download/ (accessed Jun. 12, 2023).
- [62] "How to set up your own OpenVPN server in pfSense."
 https://www.comparitech.com/blog/vpn-privacy/openvpn-server-pfsense/ (accessed Jun. 12, 2023).
- [63] "Active Directory Setup Guide." https://www.ittsystems.com/active-directory-setupguide/ (accessed Jun. 12, 2023).
- [64] "How to Install Windows Server 2019 on Oracle VM VirtualBox." https://www.sysnettechsolutions.com/en/install-windows-server-2019-oracle-vmvirtualbox/ (accessed Jun. 12, 2023).
- [65] "How to Install Windows Server 2019 in VirtualBox (Step By Step Guide)." https://www.youtube.com/watch?v=ZjQSuyuN0nA (accessed Jun. 12, 2023).
- [66] "How to setup a domain controller?" https://www.manageengine.com/products/activedirectory-audit/kb/how-to/how-to-setup-a-domain-controller.html (accessed Jun. 12, 2023).
- [67] "Authenticating from Active Directory using RADIUS/NPS." https://docs.netgate.com/pfsense/en/latest/recipes/radius-windows.html (accessed Jun. 12, 2023).
- [68] "DUO Setting up Multi-Factor Authentication for OpenVPN on pfSense." https://www.rmtechteam.com/blog/duo-setting-up-multi-factor-authentication-for-

openvpn-on-pfsense/ (accessed Jun. 12, 2023).

- [69] "Duo Two-Factor Authentication with RADIUS and Primary Authentication." https://duo.com/docs/radius#first-steps (accessed Jun. 12, 2023).
- [70] "Duo Administration Enroll Users." https://duo.com/docs/enrolling-users (accessed Jun. 12, 2023).
- [71] "Duo Enrollment Guide to Two-Factor Authentication · Duo Security." https://guide.duo.com/enrollment (accessed Jun. 12, 2023).
- [72] "Duo Authentication for Windows Logon & RDP | Duo Security." https://duo.com/docs/rdp#offline-access (accessed Jun. 12, 2023).
- [73] "How to install FreeNAS VM on VirtualBox (Windows,Linux or MacOS)." https://www.how2shout.com/how-to/how-to-install-freenas-vm-on-virtualboxwindowslinux-or-macos.html (accessed Jun. 12, 2023).
- [74] "OSSIM Part 1 Install OSSIM on VirtualBox." https://medium.com/psimss/ossim-part-1-install-ossim-on-virtualbox-e1d20f7dcbe4#:~:text=Click on the Network tab,or Host only Adapter option.&text=After completed%2C you can click,to deploy your OSSIM machine.&text=Choose Install Alienvault OSSIM to start (accessed Jun. 12, 2023).
- [75] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A usability study of five two-factor authentication methods," Proc. 15th Symp. Usable Priv. Secur. SOUPS 2019, pp. 357–370, 2019.
- [76] M. S. Bohuk, M. Islam, S. Ahmad, M. Swift, T. Ristenpart, and R. Chatterjee, "Gossamer: Securely Measuring Password-based Logins," Proc. 31st USENIX Secur. Symp. Secur. 2022, pp. 1867–1884, 2022.

APPENDIX A

Set up the virtual environment by installing VirtualBox 7.0 for installing the virtual machines as seen in Figure 24.

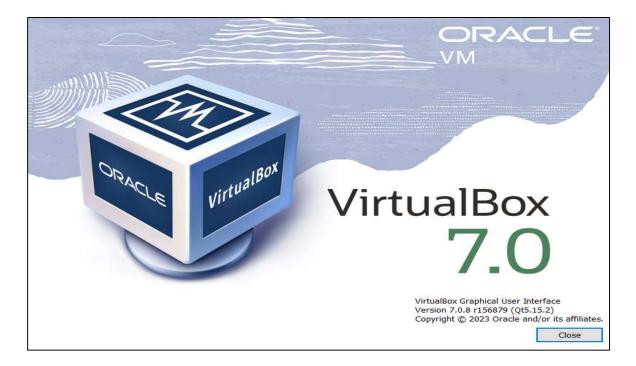


Figure 24 : Virtual Environment Setup Using Virtual Box 7.0

- Next download & install pfSense firewall [61] community edition 2.6 iso (pfSense-CE-2.6.0-RELEASE-amd64.iso) in VirtualBox.
- 2. Two network adaptors are assigned for pfSense in VirtualBox.
- 2.1. WAN (em0) to communicate to the outside internet with IPv4 settings with dynamic IP 192.168.7.196/24.
- 2.2. LAN (em1) to communicate with the internal users with IPv4 settings with IP 10.1.1.1/24.Create a local area network with 10.1.1.0/24, with the firewall being assigned the static IP 10.1.1.1 as seen from Figure 25.

pfSense Firewall [Running] - Oracle VM Virtu	JalBox – L X
File Machine View Input Devices Help	
Starting package OpenVPN Client Exp	
Starting package freeradius3done pfSense 2.6.0-RELEASE amd64 Mon Jan	
Bootup complete	51 15.51.55 010 2022
bootap compiete	
FreeBSD/amd64 (pfSense.home.arpa) (t	tyv0)
VirtualBox Virtual Machine - Netgate	Device ID: 505a829023d05f4cf0c0
	(
*** Welcome to pfSense 2.6.0-RELEASE	(amab4) on pisense ***
WAN (wan) $\rightarrow em\Theta$ $\rightarrow v4$	/DHCP4: 192.168.7.196/24
[[[[상황] 5월 25] · · · · · · · · · · · · · · · · · · ·	: 10.1.1.1/24
0) Logout (SSH only)	9) pfTop
1) Assign Interfaces	10) Filter Logs
2) Set interface(s) IP address	11) Restart webConfigurator
3) Reset webConfigurator password	
 Reset to factory defaults Reboot system 	13) Update from console 14) Enable Secure Shell (sshd)
6) Halt system	15) Restore recent configuration
7) Ping host	16) Restart PHP-FPM
8) Shell	
Enter an option:	
	🔽 💿 💯 🚽 🖉 🗐 🛄 🚰 🕼 🧭 🚺 Right Ctrl

Figure 25 : pfSense Firewall Command line Console

3. Open the web browser and go to IP 10.1.1.1 to access the firewall web console as seen from Figure 26.

← → C ▲ Not secure https://10.1.1.1		
	System - Interfaces - Firewall - Services - VPN	- Status - Diagnostics - Help -
Status / D	ashboard	B + 0
System Info	rmation 🖌 🖯 😒	Netgate Services And Support 🕞 😣
Name	pfSense.home.arpa	Contract type Community Support
User	admin@10.1.1.12 (Local Database)	Community Support Only
System	VirtualBox Virtual Machine Netgate Device ID: 505a829023d05f4cf0c0	NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006	If you purchased your piSense gateway firewall appliance from Netgate and elected Community Support at the point of sale or installed piSense on your own
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 1957.53 UTC 2022 FreeBSD 12.3-STABLE The system is on the latest version. Version information updated at Tue Apr 4 10.23 50 UTC 2023 💋	Community supports at we point to save on instance processor in point own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY. You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. Were always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
CPU Type	Intel(R) Core(TM) 17-6600U CPU @ 2.60GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No	Upgrade Your Support Community Support Resources Netgate Global Support FAQ Official pfSense Training by Netgate
Hardware crypto		Netgate Professional Services Visit Netgate.com
Kernel PTI	Enabled	
MDS Mitigation	Inactive	If you decide to purchase a Netgate Global TAC Support subscription, you
Uptime	04 Hours 05 Minutes 50 Seconds	MUST have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place.
Current date/time	Tue Apr 4 10:27:18 UTC 2023	You can purchase TAC support here
DNS server(s)	 127.0.0.1 8.8.8 1.1.1.1 192.168.7.1 	Interfaces ✔ ○ ⊗
Last config chan	Mon Apr 3 7:01:16 UTC 2023	LAN 1000baseT <full-duplex> 192.106.7.190</full-duplex>
State table size	0% (11/198000) Show states	

Figure 26 : pfSense Firewall Web Console

4. Next, we set up a Certification Authority (CA) "DEF Company CA" in pfSense as seen from Figure 27.

As Certificates	Certificate Revocation	
reate / Edit CA		
Descriptive name	DEF Company CA	
Method	Create an internal Certificate Authority	~
Trust Store	Add this Certificate Authority to the Operating S When enabled, the contents of the CA will be added	
Randomize Serial	Use random serial numbers when signing certif When enabled, if this CA is capable of signing certi checked for uniqueness instead of using the seque	ficates then serial num
ternal Certificate A	uthority	
Key type	RSA	~
	4096	~
	The length to use when generating a new RSA key, The Key Length should not be lower than 2048 or s	
Digest Algorithm	sha256	~
	The orgest method used when the CA is signed. The best practice is to use an algorithm stronger th	an SHA1. Some platfo
Lifetime (days)	3650	
Common Name	internal-ca	
	The following certificate authority subject component	ents are optional and r
Country Code	None	~
State or Province	e.g. Texas	
City	e.g. Austin	
Organization	e.g. My Company Inc	
Organizational Unit	e.g. My Department Name (optional)	

Figure 27 : Internal Certificate Authority in pfSense

4.1. We give a descriptive name for the CA, select internal CA, RSA key 4096 bits and SHA 256 as digest algorithm and click save.

5. Create a server certificate to use with OpenVPN authentication server as seen in Figure 28.

CAs Certificates	Certificate Revocation	
Add/Sign a New Cert	ificate	
Method	Create an internal Certificate	~
Descriptive name	DEF Company Server Certificate	
nternal Certificate		
Certificate authority	DEF Company CA	~
Key type	RSA	~
	4096	~
	The length to use when generating a new RSA The Key Length should not be lower than 2048	
Digest Algorithm	sha256	~
	The digest method used when the certificate i The best practice is to use an algorithm strong	
Lifetime (days)	3650	
	The length of time the signed certificate will be Server certificates should not have a lifetime of	
Common Name	DEF Company Server Certificate	

Figure 28 : DEF Company Server Certificate

6. Create user certificates to use for authentication, sample user – Administrator. Follow the same process from step 5, as seen in Figure 29.

COMMUNITY EDITION System	Interfaces -	Firewall -	Services -	VPN -	Status -
System / Certifica	ate Manager /	Certifica	tes / Edit		
CAs Certificates	Certificate Revocation				
Add/Sign a New Cert	ificate				
Method	Create an internal C	ertificate			~]
Descriptive name	DEF_Administrator_Certificate				
Internal Certificate					
Certificate authority	DEF Company CA				~
Key type	RSA				~
	4096				~
	The length to use whe The Key Length shoul				s may consider
Digest Algorithm	The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms ma				
Lifetime (days)	Lifetime (days) 3650				
	The length of time the Server certificates sho				me platforms r
Common Name	DEF_Administrator_Certificate				

Figure 29 : DEF Company User Certificate

7. Then go to System > User Manager > Authentication Servers and create an authentication server "Radius_Server_DUO. Select the type as "RADIUS", protocol as Password Authentication Protocol (PAP), IP address of DUO Proxy Server 10.1.1.15, shared secret generated in the NPS server and set ports 1812, 1813 for authentication and accounting respectively as seen in Figure 30.

System / User Ma	anager / Authentication Servers / E	dit		
Users Groups S	Settings Authentication Servers			
Server Settings				
Descriptive name	Radius Server_DUO			
Туре	RADIUS	~		
RADIUS Server Settin	gs			
Protocol	PAP	~		
Hostname or IP address	10.1.1.15			
Shared Secret				
Services offered	Authentication and Accounting			
Authentication port	1812			
Accounting port	1813			
Authentication Timeout	70			
	This value controls how long, in seconds, that the RAD seconds. NOTE: If using an interactive two-factor auth and enter a token.			
RADIUS NAS IP Attribute	LAN - 10.1.1.1	~		

Figure 30 : Setting up Radius Server for Authentication

8. To set up the firewall rules, go to Firewall > Rules > WAN. Select the action as "PASS", interface as "WAN", address family as "IPv4", protocol as "UDP", source as "Any", destination as "WAN Address" and destination port as "1198" as seen in Figure 31.

Firewall / Rules /	Edit				
Edit Firewall Rule		_	_	_	
Action		n block and reject is the			port unreachable for UDP) is ref
Disabled	Disable this rule Set this option to disable the	nis rule without removin	g it from the list.		
Interface	WAN Choose the interface from	which packets must co	rne to match this rule.		
Address Family	IPv4 Select the Internet Protoco	l version this rule applie	► s to.		
Protocol	UDP Choose which IP protocol t	his rule should match.	~		
Source Source	Invert match	any		~	Source Address
	Chapter Advanced The Source Port Range for Its default value, any.	a connection is typical	y random and almost never e	equal to the (destination port. In most cases t
Destination Destination	Invert match	WAN address		~	Destination Address
Destination Port Range	(other) 🗸	1198 Custom	(other) To	~	1198 Custom

Figure 31 : Configuring Firewall Rules

- 9. To setup the OpenVPN server [62] [39] go to VPN > OpenVPN > Servers, click add server.
- 9.1. Select the server mode as "Remote Access (SSL/TLS + User Auth).
- 9.2. Select the previously created authentication server "Radius Server_DUO".
- 9.3. Protocol UDP on IPv4 only, interface "WAN" and port "1198".
- 9.4. Select tick box "Use a TLS Key".
- 9.5. Select the created Certification Authority "DEF Company CA" and server certificate "DEF Company CA Server Certificate".

- 9.6. DH parameter Length 4096 bit.
- 9.7. Data Encryption Algorithms: AES-256-GCM, AES-128-GCM and CHACHA20-POLY1305.
- 9.8. Fallback Data Encryption Algorithms: AES-256-CBC (256 bit key, 128-bit block).
- 9.9. Auth Digest Algorithm: SHA256(256-bit).
- 9.10. Tick Client Certificate Key Usage Validation.
- 9.11. Set IPv4 tunnel network as 17.1.1.0/24 and tick redirect IPv4 gateway.
- 9.12. In advanced configuration add "reneg-sec 0", to prevent the DUO MFA from asking to reauthenticate after every 1 hour.
- 9.13. Enable UDP Fast I/O for fast UDP writes.
- 9.14. Select gateway creation as "IPv4 only".

VPN / OpenVPN	/ Servers / Edit
Servers Clients	Client Specific Overrides Wizards Client Export Shared Key Export
General Information	
Description	DEF Company VPN Server - DUO Auth A description of this VPN for administrative reference.
Disabled	Disable this server Set this option to disable this server without removing it from the list.
Unique VPN ID	Server 5 (ovpns5)
Mode Configuration	
Server mode	Remote Access (SSL/TLS + User Auth)
Backend for authentication	Active Directory NPS Active Directory Free Radius Auth Server Radius Server_DUO
Device mode	tun - Layer 3 Tunnel Mode 🗸 🗸
	"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mo "tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configurat	ion
Protocol	UDP on IPv4 only
Interface	WAN The interface or Virtual IP address where OpenVPN will receive client connections.
Local port	1198 The port used by OpenVPN to receive client connections.

Figure 32 : OpenVPN Server Setup Configuration Part1

Cryptographic Settin	gs
TLS Configuration	Vise a TLS Key A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.
<u>TLS Key</u>	# # 2048 bit OpenVPN static key #BEGIN OpenVPN Static key V1 776079d0e555A426a3a3ce0a793dfec4 Paste the TLS key here. This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.
TLS Key Usage Mode	TLS Authentication TLS Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.
TLS keydir direction	Use default direction
Peer Certificate Authority	DEF Company CA
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check	Check client certificates with OCSP
Server certificate	DEF Company CA Server Certifcate (Server: Yes, CA: DEF Company
DH Parameter Length	4096 bit Diffie-Hellman (DH) parameter set used for key exchange. (1)
ECDH Curve	Use Default The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Data Encryption Negotiation	Enable Data Encryption Negotiation This option allows OpenVPN clients and servers to negotiate a compatible set of acceptable cryptographic data encryption algorithms from those selected in the Data Encryption Algorithms list below. Disabling this feature is deprecated.

Figure 33 : OpenVPN Server Setup Configuration Part2

Data Encryption Algorithms	AES-128-CBC (128 bit key, 128 bit block) AES-128-CFB (128 bit key, 128 bit block) AES-192-CFB (192 bit key, 128 bit blo	AES-256-GCM AES-128-GCM CHACHA20-POLY1305 Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list
Fallback Data Encryption	AES-256-CBC (256 bit key, 128 bit block)	ected by OpenVPN. This list is ignored in Shared Key mode.
Algorithm		el packets when communicating with clients that do not support data encryption algorithm y included in the Data Encryption Algorithms list.
Auth digest algorithm	SHA256 (256-bit)	~
Hardware Crypto		School channel process in a close year present. School with this digest is used for the control channel only, not the data channel. SHA1 is the default for OpenVPN, this algorithm is insecure. V
Certificate Depth	One (Client+Server) When a certificate-based client logs in, do not accept certific generated from the same C _k as the server.	▼] ates below this depth. Useful for denying certificates made with intermediate CAs
Strict User-CN Matching	Enforce match When authenticating users, enforce a match between the co	mmon name of the client certificate and the username given at login.
Client Certificate Key Usage Validation	Enforce key usage Verify that only hosts with a client certificate can connect (E	KU: "TLS Web Client Authentication").
Tunnel Settings		
IPv4 Tunnel Network		single entry used for private communications between this server and client hosts sable address in the network will be assigned to the server virtual interface. The remaining

Figure 34 : OpenVPN Server Setup Configuration Part3

Advanced Configurat	ion
Custom options	Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
Username as Common Name	 Use the authenticated client username instead of the certificate common name (CN). When a user authenticates, if this option is enabled then the username of the client will be used in place of the certificate common name for purposes such as determining Client Specific Overrides.
UDP Fast I/O	Use fast I/O operations with UDP writes to tun/tap. Experimental. Optimizes the packet write event loop, improving CPU efficiency by 5% to 10%. Not compatible with all platforms, and not compatible with OpenVPN bandwidth limiting.
Exit Notify	Reconnect to this server / Retry once Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel networks at it will cause the server to exit and not restart.
Send/Receive Buffer	Default Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.
Gateway creation	O Both IPv6 only IPv6 only If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.
Verbosity level	default • Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output. None: Only fatal errors Default through 4: Normal usage range 5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets. 6-11: Debug info range

Figure 35 : OpenVPN Server Setup Configuration Part4

- 10. Then go to System > Package Manager > Available Packages, search and install "openvpnclient-export" utility. Go to VPN > OpenVPN > Client Export as seen in Figure 36.
- 10.1. Select Remote Access server "DEF Company VPN Server DUO Auth UDP4:1198"
- 10.2. Host Name Resolution Interface IP Address.

← → C ▲ Not secure https://10.1.1.1/vpn_openvpn_export.php	
System	Interfaces * Firewall * Services * VPN * Status * Diagnostics * Help *
OpenVPN / Clien	it Export Utility 🛛 🕹
Server Olient C	Ilent Specific Overrides Wizards Client Export Shared Key Export
OpenVPN Server	
Remote Access Server	DEF Company VPN Server - DUO Auth UDP4:1198
Client Connection Bo	chavior
Host Name Resolution	Interface IP Address
Verify Server CN	Automatic-Use verify-x509-name where possible Optionally verify the server certificate Common Name (CN) when the client connects.
Block Outside DNS	Block access to DNS servers except access OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Legacy Client	Do not include OpenVPN 2.5 settings in the client configuration. When using an idder client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client, configuration.
Silent Installer	Create Windows installer for unattended deploy; Create a selemt Windows installer for unattended deploy; installer must be run with elevated permissions. Since this installer is not signed, you may need special software to deploy if creatly.
Bind Mode	Do not bind to the local port f OpenVPN client binds to the default OpenVPN port (1194), two clients may not run concurrently.
Certificate Export O	ptions
PKCS#11 Certificate Storage	Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.
Microsoft Certificate Storage	Use Microsoft Certificate Storage instead of local files.
Password Protect Certificate	Use a password to protect the pixcs12 file contents or key in Viscosity bundle.
Proxy Options	
Use A Proxy	Use proxy to communicate with the OpenVPN server.

Figure 36 : OpenVPN Client Export Utility

10.3. Download the OpenVPN Connect application and config file for the individual user depending on the client OS. After installing the client app, import the config file to use the VPN as seen in Figure 37.

← → C ▲ Not secure https://10.1.1.1/vpn_openvpn_export.php			
		Enter any additional options to add to the OpenVPN client export EXAMPLE: remote-random;	configuration here, separated by a line break or semicolon.
		Save as default	
	Search		•
	Search term		Q Search D Clear
		Enter a search string or "nix regular expression to search.	
	OpenVPN Clients	Certificate Name	Export
	Certificate with External Auth		- Inline Configurations: - Most Clients - Most Client
			Bundled Configurations Configurations Construction (2.5.5 bit)
	Certificate with External Auth	n DEF_JohnyDepp_Certificate	- Infine Configuration: - Infine Configuration: - Bundled Configurations: - Config Factors Televise - Config Factors Televise - Config Factors Televise - Config Factors Televise - Config Factors - Config Fa
	Only OpenVPN-compatible use	er certificates are shown	
		is not associated with a user when local database authentication is	r instance and the client certificate, the client certificate does not exist on this senabled.

Figure 37 : OpenVPN Client Download

11. Then open the OpenVPN client, provide the credentials and submit to logon to the network. The DUO mobile client will send the DUO PUSH prompt to the assigned mobile device as the second factor authentication step to authenticate the user's credentials as seen in Figure 38 and permit login.

Sat May 27 11:42:09 2	023 OpenVPN 2.5.8 [gitnone/0357ceb877687faa] Windows-MS 023 Windows version 10.0 (Windows 10 or greater) 64bit 023 library versions: OpenSSL 1.1.1s 1 Nov 2022, LZO 2.10	vo [SSE (OpenSSE)] [EZO] [EZ4] [r
	Username: Administrator Password:	
<	Save password OK Cancel	

Figure 38 : OpenVPN Client Login Prompt

12. Then open remote desktop application, provide the IP to the DEF_Administrator account, provide the credentials and authenticate using DUO MFA as seen in Figure 39.

Nemote E	Desktop Connection	8 8		×
	Remote Desktop Connection			
Computer: User name: You will be as	10.1.1.12 DESKTOP-NRP14EU\Administrator ked for credentials when you connect.	×		
Show Op	tions	Connect	He	lp

Figure 39 : RDP Connection Initiation

Windows Security	×
Enter your credentials	
These credentials will be used to conr	nect to 10.1.1.12.
Administrator	
Password	
DESKTOP-NRP14EU\Administrator	
Remember me	
More choices	
ОК	Cancel

Figure 40 : Providing RDP Connection Credentials

13. Next, we set up Microsoft Windows Active Directory [63] by installing Windows Server [64][65] 2019 as seen in Figure 41.

Server Manager							- 0
🐑 🕘 🐐 Server M	lanager • Dashboard					• © 🏲 Marage	
Dashboard Local Service Al Service Al Services Al Services Al Services Al Services DNS DNS File and Storage Services P NPAS Remote Destatop Services P	Quick state 2 Add 3 Add	gure this local server roles and features other servers to manage the a server group					
	S Con LLANV MORE ROLES AND SERVER GROUPS Roles 6 Sever groups 1 Severs total 1	E DNS	File and Storage	ilo IIS 1	NPAS 1	Remote Desktop	Hide
	Manageability Events Services Performance BPA results	Anageability Events Services Performance BPA results	Services Manageability. Events Services Performance BPA results	Manageability Events Services Performance BPA results	Manageability Events Services Performance BPA results	Services Services Manageability Events Services Performance BPA results 4/4/2022 10.47 AM	
	Local Server: 1 Manageability Events Services	All Servers 1 Manageability Events Services					

Figure 41 : Setting Up Active Directory in Server 2019

- 14. After opening the server manager as Administrator, select add roles and install Active Directory Domain Services to set up active directory. Then add this server as domain [66] controller as seen in Figure 42.
- **15.** Then set up the DNS services [47] by creating the domain "DEFCOMPANY.COM" & assign static IP 10.1.1.12.

🚡 Server Manager							- 6	Х
Server Ma	inager • Local Ser	ver			• 🕲 🖡	Manage	Tools View H	lelp
III Dashboard	PROPERTIES For WIN-10V5GBA6SBL						TASKS 🔻	1
Local Server All Servers All DDS DNS	Computer name Domain	WIN-10V5GBA56L defcampany.com	Last installed updates Windows Update Last checked for updates	2/23/2023 9:57 PM Download updates only, using Windows Update Today at 10:47 AM				
III: File and Storage Services ▷ III: N NPAS Ø Remote Desktop Services ▷	Windows Defender Firewall Remote management Remote Desktop NIC Teaming Ethernet 2	Public: On Enabled Enabled Disabled 10.1.1.12	Windows Defender Anthinus Feedback & Diagnostics IE Enhanced Security Configuration Time zone Product ID	Real-Time Protection: On Settings Off (UTC +04:00) Abu Dhabi, Muscat 00431-20000-00000-4A782 (activated)				
	Operating system version Hardware information	Microsoft Windows Server 2019 Datacenter Evaluation innotek GmbH VirtualBox	Processors Installed memory (RAM) Total disk space	Intel(R) Core(TM) 17-6600U CPU @ 2.60GHz 4 GB 28:46 GB				

Figure 42 : Setting Up DNS in Active Directory

- **16.** Next to setup active directory users, open Active Directory Users and Computers. Add users and provide the necessary permissions as seen in Figure 43.
- 16.1. Created the following Active Directory users as seen in Table 6.

Name Of Account	Purpose
Administrator	Admin Account
CaptainAmerica	User Account
DEF_Test	User Account
DEF_TrueNas_Shared_Acc	Shared Account For NAS
JohnyDepp	User Account
NAS Admin	Admin Account For NAS
Service Acc	Service Account for MFA Authentication Proxy
Tony Stark	User Account
Peter Parker	User Account

 Table 6 : Created Active Directory Users List

Action View Help				
	m 🕺 🕱 📾 🔻 🖂 🕱			
Users A	Name	Туре	Description	
> & Administrator				
> & Allowed RODC Password Replication	& Administrator	User	Built-in account for administering the computer/domain	
3 & captainamerica	Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their passwords replicated to all r	
> SR. Cert Publishers	S captainamerica	User	Manager	
> & Cloneable Domain Controllers	Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish certificates to the	
DEF Test	Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers may be cloned.	
B DEF_TrueNas_Shared_Acc	& DEF_Test	User		
B Denied RODC Password Replication	B DEF_TrueNas_Shared_Acc	Security Group - Global		
> 🤮 DnsAdmins	Contraction Group	Security Group - Domain Local	Members in this group cannot have their passwords replicated to	
> 😹 DnsUpdateProxy	R DnsAdmins	Security Group - Domain Local	DNS Administrators Group	
😣 Domain Admins	A DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic updates on b	
> 🧟 Domain Computers	🗟 Domain Admins	Security Group - Global	Designated administrators of the domain	
> 🤮 Domain Controllers	A Domain Computers	Security Group - Global	All workstations and servers joined to the domain	
> 😣 Domain Guests	A Domain Controllers	Security Group - Global	All domain controllers in the domain	
> 🎎 Domain Users	A Domain Guests	Security Group - Global	All domain guests	
Set Enterprise Admins	A Domain Users	Security Group - Global	All domain users	
Sector Strategy Admins Sector Strategy Admins Sector Se	A Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise	
Sector Strategy Enterprise Read-only Domain Contraction	A Enterprise Key Admins	Security Group - Universal	Members of this group can perform administrative actions on key	
Search Contraction Contraction Contraction Search Contraction Contractica C	Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Controllers in the	
🗧 🤱 Guest	B Group Policy Creator Owners	Security Group - Global	Members in this group can modify group policy for the domain	
5 🔱 johnydepp	2. Guest	User	Built-in account for guest access to the computer/domain	
> 🍇 Key Admins	S johnydepp	User	Accounts	
> 🛃 krbtgt	Key Admins	Security Group - Global	Members of this group can perform administrative actions on key	
> 🛃 NAS Admin	2. krbtgt	User	Key Distribution Center Service Account	
> 🤽 Protected Users	ANAS Admin	User	ney on nour of the needed	
RAS and IAS Servers	Reprotected Users	Security Group - Global	Members of this group are afforded additional protections agains	
> 🍇 RDP Users	RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access remote access properties of users	
	R RDP Users	Security Group - Global	servers in this group can access remote access properties of users	
ServiceAcc	Read-only Domain Controllers	Security Group - Global	Members of this group are Read-Only Domain Controllers in the	
ServiceAcc	R Schema Admins	Security Group - Universal	Designated administrators of the schema	
NTDS Quotas	ServiceAcc	User	Designated administrators of the schema	
TPM Devices	a tonystark	User	Sales	
The volution	Conystark	Oser	29162	

Figure 43 : Active Directory Users

16.2. Created a group called VPN users and added the users who are allowed access to the network through VPN as seen in Figure 44.

Object	Sec	curity	Attribute Editor	
General	Members	Member O	f Managed	By
embers:				
Name SAdministrat Captainam DEF_Test	tor defcompa erica defcompa	ectory Domain Se ny.com/Users ny.com/Users ny.com/Users	ervices Folder	
iohnydepp		ny.com/Users		
Lonystark		ny.com/Users ny.com/Users		
Add	Remove	-		

Figure 44 : VPN Users Group

17. Setup Network Policy Server [67] for Authenticating the users against the AD database as seen in Figure 45. Configure the pfSense firewall with IP 10.1.1.1 as the radius client & generate a shared secret to be shared with the authentication server as seen in Figure 46.

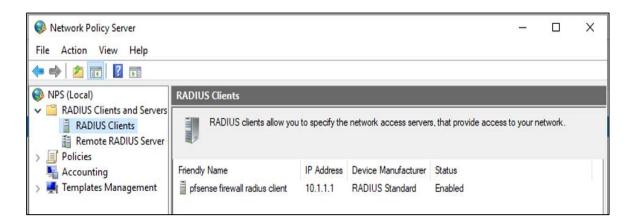


Figure 45 : Network Policy Server

	client Properties	2
ettings Advanced		
Enable this RADIUS	client	
Select an existing te	mplate:	
		1
Name and Address		
Friendly name:		
pfsense firewall radius	s client	
Address (IP or DNS):		
10.1.1.1	Verify	Ê .
Shared Secret		
Select an existing Sha	ared Secrets template:	
None	~	2
secret, click Generate secret entered here. S	ared secret, click Manual. To automatically generate a shared . You must configure the RADIUS client with the same shared shared secrets are case-sensitive.	
 Secret, click Generate secret entered here. S Manual Shared secret: 	 You must configure the RADIUS client with the same shared shared secrets are case-sensitive. 	
 Secret, click Generate secret entered here. S Manual Shared secret: 	You must configure the RADIUS client with the same shared shared secrets are case-sensitive. Generate	
secret, click Generate secret entered here. S Manual Shared secret: Confirm shared secret:	You must configure the RADIUS client with the same shared shared secrets are case-sensitive. Generate	
secret, click Generate secret entered here. S Manual Shared secret: Confirm shared secret:	. You must configure the RADIUS client with the same shared shared secrets are case-sensitive. Generate	

Figure 46 : pfSense Radius Client Configurations

18. Set up a network policy allowing only users from the group "VPN Users" to be authenticated & allowed access to the network as seen in Figure 47.

😵 Network Policy Server							×
File Action View Help							
🗢 🄿 🖄 📰 🚺 🖬							
🚳 NPS (Local)	Network Policies						
ADJUS Clients and Servers RADJUS Clients Remote RADJUS Server Policies	Network policies allow you to designate who is authorized to conne cannot connect.	ct to the ne	work and the circur	nstances under	which they (can or	
Connection Request Po	Policy Name	Status	Processing Order	Access Type	Source		
Network Policies	Allow From pfSense firewall	Enabled		Grant Access			
Accounting	- RDG Marker Policy (985F7B54-FCE8-4f55-AEBF-DF8827A44068) -	Enabled		Deny Access			2
> 💐 Templates Management	Connections to other access servers		999999 1000000	Grant Access Deny Access			
	Conditions - If the following conditions are met:						- ^
	Condition Value						
	Settings - Then the following settings are applied:						_
< >>	Setting Value						~

Figure 47 : Setting up Network Policy for VPN Users Group

- **19.** Setting up User Workstation as seen in Figure 48.
- 19.1. Download and install Windows 10 Pro.
- 19.2. After setting up the machine, join the machine to the company domain DEFCOMPANY.COM and login as a registered AD user (e.g., user Johny Depp).

DEF_UserWorkstation [Running] - Oracle VM VirtualBox File Machine View Input Devices Help	- o ×
X I	
Johny Depp	
Password >	
A Johny Depp	
R Other user	町 🕁 🖒
	D Columnation of the second se

Figure 48 : User Workstation Windows Login Screen

DE DE	F_UserWorkstation [Running] - Oracle VM	VirtualBox			
File 1	Machine View Input Devices Help				
Setting	Settings				
ធា	Home	Your info			
Find	d a setting	You need to activate Windows before you can personalize your PC.			
L	A disconing (
Accounts		Activate Windows now.			
83	Your info				
ел в	Email & accounts	\bigcirc			
۹. s	Sign-in options				
	Access work or school				
0 :	Sync your settings	JOHNY DEPP DEFCOMPANYjohnydepp			
		Create your picture			
		Gerea Camera			
		Browse for one			
	Q Type here to search				
	P Type here to search	H 😑 🚃 💼 🕿 🌣			

Figure 49 : User Workstation Connected to Company Domain

- **20.** Setting up DUO MFA Authentication Proxy for Multifactor Authentication [68]. Install windows server 2019 in the same manner as the Active Directory and then install DUO authentication proxy client in the server with admin privileges.
- Then login to DUO admin account using the link <u>https://admin.duosecurity.com/</u> and setup DUO account [69] as seen in Figure 50.

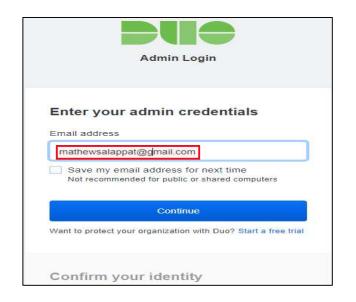


Figure 50 : DUO Admin Login Prompt

21.1. Go to applications menu, select protect an application "RADIUS", this will generate the integration key, secret key, and API hostname as seen in Figure 51, to be included in the proxy's configuration file.

DUO	A Search for users, grou	sps, applications, or devices		DEF Company ID: 1246-6222-91 Mathews A	ė
Dashboard Device Insight	Dashboard > Applications	> RADIUS		Authentication Log 📋 💼 Remove Applicatio	0
Policies Applications Protect an Application	See the RADIUS docume	ntation to integrate Duo into your RADIUS-enabled platt	orm.		
Single Sign-On	Details			Reset Secret Key	
Users	Integration key	DIPGB4SWWLA6JTMOBHZZ	Сору		
Groups Endpoints	Secret key		Сору		
2FA Devices Administrators	API hostname	Don't write down your secret key or share it with anyone.	Сору		
Trust Monitor					
Reports Settings	Policy				
Billing	Policy defines when and	how users will authenticate when accessing this application	n. Your global policy a	always applies, but you can override its rules with custom policies.	

Figure 51 : DUO Admin Web Console

22. After installing the proxy client in Step 20, navigate to C:\Program Files (x86)\Duo Security Authentication Proxy\conf\authproxy.cfg to edit the proxy file as seen in Figure 52.

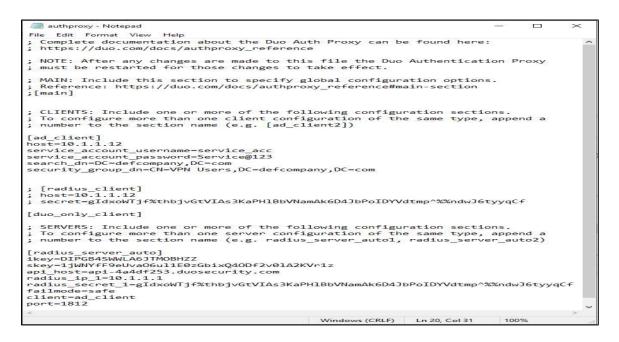


Figure 52 : DUO Proxy Configuration File

23. Launch the DUO Authentication Proxy Manager and start the proxy as seen in Figure 53.

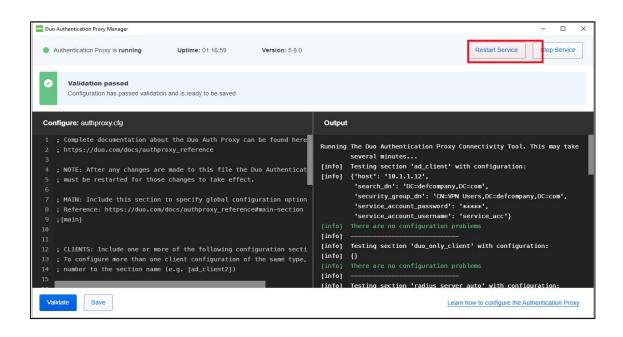


Figure 53 : DUO Authentication Proxy Manager Console

24. Go to the DUO admin portal, click users to add new users [70] as seen in Figure 54. Provide email and phone number for verification and enable 2FA. Download the DUO mobile app and add the registered user by clicking on the enrollment [71] received from DUO. DUO will request a push notification as a secondary authentication method when the user tries to login to the network through the VPN after providing the AD credentials.

Dashboard	Dashboard > Users > johny	depp
Device Insight	is housed a new	
Policies	johnydepp	Logs Send Duo Push 💼 Send to Trash
Applications		
Single Sign-On	Username	Johnydepp
Users		
Add User	Username aliases	Username alias 1 👻 💩
Pending Enrollments		johnydepp@defcompany.com
Bulk Enroll Users		
Import Users		+ Add a username alias
Directory Sync		Users can have up to 8 allases.
Bypass Codes		Optionally, you may choose to reserve using an alias number for a specific alias (e.g., Username alias 1 should only be used for Employee ID).
Groups		
Endpoints		
2FA Devices	Full name	
Administrators		
Trust Monitor	Email	mathewsalappat@gmail.com
Reports		
Settings	Status	Active
	122-127-122-12-1	Require nutli-factor authentication (default).
Billing		Bypass
		Allow users to skip two-factor authentication and log in with only a password. Passwordless authentication is not skipped.
Need Help? Email Support		Disabled
Call us at 1-855-386-2884		Automatically deny access
Versioning		This controls the user's two-factor authentication process.

Figure 54 : Adding a new DUO User

25. To enable location-based access, create a policy "Location Based User Access Policy", in which access from UAE is allowed with 2FA and access is denied for all other countries as seen in Figure 55.

Edit Policy		×
There are new, m policies have bee	icy settings are more secure! ore secure defaults available to help you protect your applications and users. None of your existing n changed. If you add new custom policy sections, they will have the new defaults. defaults released in Dec 2022 and Jan 2023 C	×
This policy applies to 6 app Learn more about policies	lications: Microsoft RDP, Microsoft RDP 1, Microsoft RDP 2, Microsoft RDP 3, Microsoft RDP 4, RADIUS	
Policy name	User location	×
Location Based User	Duo will do a country lookup on the host IP address and can apply actions based on the country.	
New User policy Authentication policy User location	▼ United Arab Emirates ▼ Require 2FA ◆	
Devices	All other countries	

Figure 55 : Location Based Access Policy

26. Create a "UAE Group" and select users who are allowed to access from the UAE. Will deny access to all other users not in this group as seen in Figure 56.

UAE Groups >	
	group policy? apply specific policies to certain groups. This configuration lives on the applicat
Details	
Group name	UAE Group
Description	User Logins From Inside UAE
Status	Active Require two-factor authentication (default)

Figure 56 : DUO User Group Creation

27. Add users to the created group to grant or deny access based on the location policy. Then in the corresponding user's account select the newly created group as seen in Figure 57.

Users + Add Users to Group			٩	
Username 🔨	Name 🛇	Status 🛇	Last Login (+04) 🛇	
administrator		Active	۲۷ مايو ۲۲۰۲ ۲۸ ۱۹	۵.
duo proxy server		Active	۲۷ ماین ۲۰۲۳ ۱٤:۲۷	面
johnydepp		Active	۲۵ مایو ۲۰۲۲ ۱۸:۲۹	<u>iii</u>
peterparker		Active	۲۱ مایو ۲۰۲۲ ۱۸: ۱۰	Î

Figure 57 : Adding Users to DUO Group

administra	Logs Send Duo F
Username	administrator
Username aliases	Username alias 1 👻 💣
	administrator@defcompany.com
	+ Add a username alias Users can have up to 8 aliases.
	Optionally, you may choose to reserve using an alias number for a specific alias (e.g., Username alias 1 should only be used for Employee (D).
Full name	
Email	mathewsalappat@gmail.com
Status	Active Require multi-factor authentication (default).
	 Bypass Allow users to skip teo-factor authentication and log in with only a password. Passwordless authentication is not skipped.
	Disabled Automatically deny access
	This controls the user's two-factor authentication process.
Groups	× UAE Group

Figure 58 : Adding the Group to the User's Account

28. Then go to applications and select RADIUS. Select and apply the group policy. In the default global policy all users from UAE are allowed access and users from all other countries is denied access. Figure 59 shows the integration details for protecting the RADIUS application in DUO. By going to the Authentication logs menu, all the access granted and access denied logins can be seen, as shown in Figure 60.

DUO	A Search for users, gro	ups, applications, or devices		DEF Company ID: 1246-6222-91 Mathews A ~
Dashboard Device Insight	Dashboard > Applications	> RADIUS		
Policies	RADIUS			Authentication Log 🛱 Remove Application
Applications	See the RADIUS docum	entation 😅 to integrate Duo into your RADIUS-enab	led platform.	
Protect an Application Single Sign-On	Details			Reset Secret Key
Users	Integration key	DIPGB4SWWLA6JTMOBHZZ	Сору	
Groups	Secret key	Vr1z	Сору	
Endpoints	Secret key	Don't write down your secret key or stare it with a		
2FA Devices		Cont write down your secret key or share it with a	Tyone.	
Administrators	API hostname	api-4a4df253.duosecurity.com	Сору	

Figure 59 : Protecting RADIUS Application in DUO

	Q. Search for users, group	s, applications, or o	tevices			DEF Company	I ID: 1246-6222-91	Mathews A 🗸
Dashboard	Dashboard > Authentication					•	•	
Device Insight	Authenticat		1					Export ~
Policies Applications	> Last 24 hours 🔻 I							
Single Sign-On	7 Authentications							
Users Groups	Shown at every 15 minute	25.						
Endpoints								
2FA Devices Administrators	0 افر	۲۲من پتر مایو ۲۷	۽ هن	۲سی	٩من	میت, ماین ۲۷ مېت, ماین ۲۷	er.	0
Trusted Endpoints								
Trust Monitor Reports	Showing 1-7 of 7 item:	s					Showing	25 V rows
Authentication Log	Timestamp (+04) 🗸	Result	User	Application	Trust Assessment 0	Access Device	Authentication Method	
Single Sign-On Log Telephony Log Administrator Actions	۲ 5 : ۲۸: ۲ ۲ : ۲۰ نمبر ۲۷	 Granted User approved 	administrator	Microsoft RDP 3	Policy not applied	WIN-10V5GBA6SBL Location Unknown	> Duo Push Dubai, DU, United.	Arab Emirates
Authentication Summary Denied Authentications Deployment Progress	۱٤:۲۷:۵۱ ۲۰۰۰ میر ۲۰	 Granted User approved 	duo proxy server	Microsoft RDP 4	Policy not applied	WIN-1BKQAKTDARH Location Unknown	 Duo Push Dubai, DU, United. 	Arab Emirates
Policy Impact Universal Prompt Progress	11:27:1A ۲۰۱۰ میلو ۲۰	× Denied No response	administrator	RADIUS	Policy not applied	Location Unknown	> Duo Push Location Unknown	1

Figure 60 : DUO Login Authentication Report

- **29.** To configure MFA for windows logon using DUO MFA, install the DUO MFA client on the windows device.
- 29.1. In the DUO admin portal, go to applications. Click protect an application and select "Microsoft-RDP" and select protect as seen in Figure 61.

Due	۹. Search for users, groups, applications, or devices		DEF Company ID: 1246-6222-91 Mathews A 🗸
Dashboard Device Insight Policies	Dashboard > Applications > Protect an Application Protect an Application		
Applications	rdd		
Protect an Application Single Sign-On	Application	Protection Type	
Users Groups	Microsoft RDP	2FA	Documentation of Protect

Figure 61 : Protect RDP Application with DUO 2FA

29.2. Save the integration, secret keys and API hostname to add in the DUO MFA windows client application as seen in Figure 62.

← → C 🔒 admin-4a4df253.duosecurity.com/applications/DIKR	5HGV8DPVT3GKRP2			
⇒u≎	Q Search for users, grou	os, applications, or devices		DEF Company ID: 1246-6222-91 Mathews A ~
Dashboard	-			
Device Insight	Successfully ad	ded Microsoft RDP to protected applications. Add another.		
Policies				
Applications	Dashboard > Applications			
Protect an Application	Microsoft I	RDP 1		Authentication Log 🗎 Remove Application
Single Sign-On	See the RDP documentat	ion 🖆 to integrate Duo into your Microsoft RDP deployment.		
Users				
Groups	Details			Reset Secret Key
Endpoints	Integration key	DIKRT5HGV8DPVT3GKRP2	Сору	
2FA Devices				
Administrators	Secret key	······vAai	Сору	
Trust Monitor		Don't write down your secret key or sha e it with anyone.		
Reports	API hostname	api-4a4df253.duosecurity.com	Сору	
Settings				
Billing				
	Policy			
Need Help? Email Support	Policy defines when and I	now users will authenticate when accessing this application.	Your global policy alway	s applies, but you can override its rules with custom policies.
Call us at 1-855-386-2884				
Versioning Core Authentication Service:	Group policies	Apply a policy to groups of users		

Figure 62 : Secret Credentials for Microsoft RDP1 App

29.3. Go to DUO RDP documentation page, download, and install the DUO MFA windows client application [72] as seen in Figure 63. Fill in the secret credentials to complete the installation as seen in Figure 64.

Product Editions & P	ricing Solutions Partnerships Support Duo Documentation Resources Contact Sales
Contents	First Steps
Important Notes	Before moving on to the deployment steps, it's a good idea to familiarize yourself with Duo administration concepts and
TLS Requirements	like options for applications, available methods for enrolling Duo users, and Duo policy settings and how to apply them
System Requirements	Duo Administrator documentation.
Duo Factor Support Enroll Users Before Installation	1 Sign up for a Duo account.
Video Overview First Steps	2 Log in to the Duo Admin Panel and navigate to Applications
Remembered Devices for Windows Logon	3 Click Protect an Application and locate the entry for Microsoft RDP in the applications list. Click Protect to the 1
Deployment Tip	configure the application and get your integration key, secret key, and API hostname. You'll need this information
Run the Installer	complete your setup. See Protecting Applications for more information about protecting applications in Duo and ac
Test Your Setup	application options.
Offline Access	
Updating Duo Authentication for Windows Logon	We recommend setting the <u>New User Policy</u> for your Microsoft RDP application to Deny Access , as no unenrolle complete Duo enrollment via this application.
Uninstalling Duo	
Advanced Deployment and Configuration using Group Policy	5 If you'd like to enable offline access with Duo MFA you can do that now in the "Offline Access Settings" section of
Troubleshooting	application page, or return to the Admin Panel later to configure offline access after first verifying logon success w factor authentication.
Network Diagram	taulut automituautun.
Related	6 Download the Duo Authentication for Windows Logon Installer package. View checksums for Duo downloads here
I≢ Windows Logon Instructions	

Figure 63 : Downloading DUO Windows Login App

Duo Connectivi	ty Check			-
	nostname for your integra	tion to contific come		
Please enter the	lostname for your integra	tion to verify conne		
API Hostname:				
api-4a4df253.du	osecurity.com			
This hostname ca select a Microsoft	n be found in the <u>Duo Adn</u>	<u>nin Panel</u> under App	lications, configure or	
Select a Microsoft	RDP application.			
Configure mar	ual proxy for Duo traffic ((Uses System settin	gs if unspecified)	
Proxy Host:				
Proxy Port:				
	erified your environment on stallation can proceed!	can successfully cor	nect to Duo -	
		can successfully cor	meet to Duo -	

Figure 64 : Installing DUO Windows Login App

29.4. After the installation, sign-out of the account. When logging back in, after providing the username and password as seen in Figure 65, DUO MFA will ask for DUO multifactor authentication for the login as seen in Figure 66.

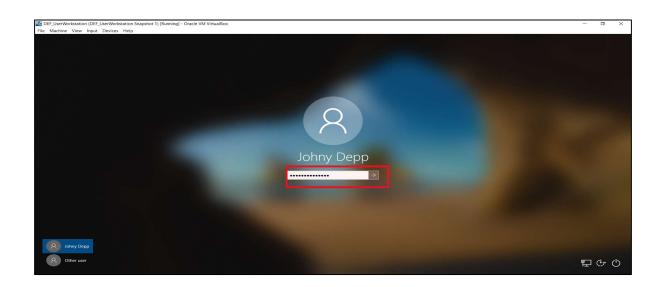


Figure 65 : Windows User Login

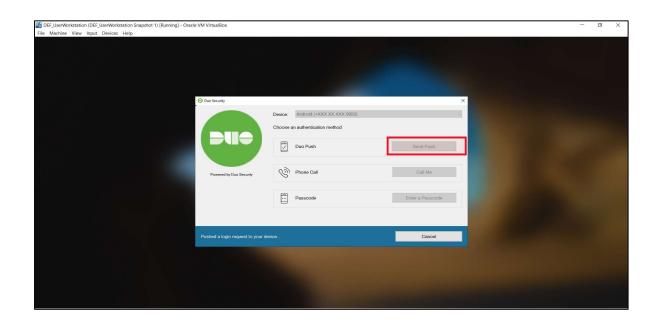


Figure 66 : DUO 2FA PUSH Request for Windows Login

- 30. To setup a file sharing server [73] in the company domain, download and install True NAS Core 13.0.
- 30.1. Assign static IP 10.1.1.19 for accessing the file server through the web browser as seen in Figure 67 and configure the DNS by setting the IP of the DNS server as 10.1.1.12 in windows network settings.
- 30.2. Then go to the browser and open the IP 10.1.1.19 to access the TrueNAS console as seen in Figure 68 which is secured using the admin credentials and MFA authentication using DUO MFA.

← → C ▲ Not secure 10.1.1.19/ui/sessions/signin	
	CORE
	Usemane *
	-
	Password *
	_
	Two-Factor Authentication Code *
	TrueNAS CORE © © 2022. 🗱 systems

Figure 67 : TrueNAS Core Login Prompt

← -	C A Not secure 10	0.1.1.19/ui/dashboard				or @ ☆ 🔲
	🛠 TrueNAS	≡ <				🗱 systems: 🕸 🗊 🖨 🌲 🌣
	ê roat					TrueNAS CORE® @ 2022 - Ksyst
	burnas Scal Dashboard Accounts - System - Tasks - Network - Storage - Directory Services -		System Information overview Platform: Genetic Version: TrueNAS-13.04.05.1 HostName: Truenas.local Uptime: 4 minutes as of 12:51	CPU trite(itr) Core 2% Any Usage Stats Per Thread	(TM) 17-6600J CPU @ 2.60GHZ Threads: 1 threads Highest Ukage: 2% (Thread #0) Hottest: Data not provided @ Usage	Memory 1.9 GiB total available 9 Prec: 0.2 GiB 275 Gade: 0.1 GiB 5 Services: 1.6 GiB
	Sharing -					
幸	Services	Pool	¢ 0	Interface	¢ 0	TrueNAS Help
*	Plugins		Overview		Overview	The TrueNAS Documentation Site is a collaborative website with helpful quides and information about your new storage
	Jails	NAS Pool	Path: /mnt/NAS Pool	em0	Media Type: Ethernet	with helpful guides and information about your new storage system.
	Reporting	Total Disks : 1 (data)	Available Space: 38.07 MiB	LINK STATE UP	Media Subtype: 1000baseT	The TrueNAS Community Forums are the best place to ask questions and interact with fellow TrueNAS users.
	Virtual Machines	Pool Status: ONLINE Disks w/Errors: 0 Used Space: 21%	Data: 1 vdev Caches: 0	> In: 0.03 KiB/s Out: 0.08 KiB/s	IP Addresses: 10.1.1.19/24	You can join the TrueNAS Newsletter for monthly updates and
4	Display System Processes		Caches: 0 Spares: 0		VLANS: U	natest developments.
Ŧ	오 표 🩋 属	SFX 🥥				へ ■ 〒 40 4/5/2023

Figure 68 : TrueNAS Web Console Dashboard

30.3. After accessing the TrueNAS portal, to link the True NAS server with the Active Directory go to Directory Services > Active Directory. Give the domain name, create an AD account "NAS Admin" with privileges to interact with TrueNAS server as seen in Figure 69.

	TrueNAS	≡ <				() systems	¢ i é		٥	ወ
	C root						TrueNAS COR	E® © 2022		
	truenas local		Domain Credentials							
	Dashboard		Domain Name * DEFCOMPANY.COM			0				
-	Accounts		Enable (requires password or Kerberos principal)	0						
	System		Verbose logging (2)	🗸 Allow DNS updates 🧑						
	Tasks		Allow Trusted Domains (?)	Disable FreeNAS Cache (0					
x	Network		Use Default Domain ⊘	🔲 Restrict PAM ⊘						
III	Storage									
•			Site Name Default First Site Name	0	OHD Timmout 10	0				
			Kerbens Radin DEFCOMPANY.COM	• 0	Winbind NSS info	• @				
	LDAP		Raters Present TRUENAS\$@DEFCOMPANY.COM	• 0	Netlius Name * truenes	0				
	NIS		Computer Account QU	0	NetBIOS alias	Ø				
	Kerberos Realms		AD Timewit 60	0						
	Kerberos Keytabs		SAVE BASIC OPTIONS EDIT IDM	AP REBUILD DIRECTOR	Y SERVICE CACHE LEAVE DOMAIN					
	Kerberos Settings			- di	<u>, </u>					
8	Sharing									
1022										

Figure 69 : Joining TrueNAS to Active Directory

30.4. Go to System > NTP Servers to add an NTP server to sync the time properly when 2FA is enabled, to avoid failed logons due to time mismatch between the TrueNAS server and DUO MFA proxy server at the time of logon as seen in Figure 70.

<i>←</i>	C A Not secu	ure 10.1.	1.19/ui/system/ntpservers					~ 윤 ☆ [
	STrue NAS		≡ <				đ≯ syst	iems: 🕼 🖲 🗎 🌲 🕯	ф ()
5	Dashboard							TrueNAS CORE® @ 2022 - D	
*	Accounts								
			NTP Servers				Q Filter NTP Serv	rers COLUMNS -	ADD
	General		Address	Burst	IBurst	Prefer	Min. Poll	Max. Poll	
			0.freebsd.pool.ntp.org	no	yes				
	Boot		1.freebsd.pool.ntp.org		yes				
	Advanced		2.freebsd.pool.ntp.org		yes				
	Email		ae.pool.ntp.org		yes				
	System Dataset		pool.ntp.org		yes				
	Reporting		1-5 of 5						
	Alert Services								ļ

Figure 70 : Setting Up NTP Server

30.5. Create a group "DEF_TrueNas_Shared_Acc" both in Active Directory and True NAS server to add users who will be allowed to access the shared folder in True NAS. The AD users are only added to the group in the active directory as seen in Figure 71.

	STrue NAS	≡ <			🕅 systems	¢ i i	¢	\$ ሀ
	🖨 root					TrueNAS CORE	® © 2022 -	Xsystems, Inc.
	truenas.local							
	Dashboard	Groups		۹	Filter Groups	COLUMNS -	ADD	•
**		Group	GID	Builtin	Permit Sudo			
		Group	GID	Bullun	Permit Sudo			
		DEF_TrueNas_Shared_Acc	1001					
	Users	Samba Authentication: true						
	System 👻							
23		🚉 members 🧪 edit 🥤 delete						

Figure 71 : Creating a Shared Group in TrueNAS

30.6. Under Storage > Disks menu we can see the disk "ad0" (8GB) where the True NAS OS is installed and disk "ad1" (2.1GB) the storage disk which is utilized for the shared network storage as seen in Figure 72.

Strue NAS	≡ <			🕅 systems 🛛	¢ () 🗎	\$	ሳ
₿ root					TrueNAS CORE®	© 2022 - <mark>iXsy</mark>	stems, Inc.
truenas.local							
Dashboard	Disks			Q Filter Disks	[COLUMNS	-
🚉 Accounts 👻	Name	Serial	Disk Size	Pool			
🛄 System 👻	ada0	VB2270f1bf-0d48b6b3	8 GiB	boot-pool			5
🖶 Tasks 👻	ada1	VBd3b6e9a3-1593add8	2.1 GiB	NAS Pool			8
Maturaek -							

Figure 72 : TrueNAS Storage Disks Menu

30.7. Under Storage > Pools menu we create a new pool [55] named "NAS as seen in Figure 73. After creating the NAS pool we create the dataset named as "DEF Shared Folder" and "SMB" windows share is selected.

	STrue NAS	≡ <							Ø	systems	¢ ()	Ê	Ņ	¢ ሀ
											TrueNAS	CORE®	ə 2022 - I	
	Snapshots	Pools												ADD
	VMware-Snapshots	NAS Pool (System Dataset Po	ol)		online 🤡	10.24 MiB (21%) Used	37.76 MiB Free						:	¢ ^
	Disks	Name 🗢	Туре 🗢	Used 🗢	Available 🗢	Compression 🗢	Compression Ratio 🗢	Readonly 🗢	Dedup 🖨	Comments 🖨				
	Import Disk	✓ NAS Pool	FILESYSTEM	10.24 MiB	37.76 MiB	lz4	14.34	false	OFF					
•	Directory Services 👻	DEF Shared Folder	FILESYSTEM	96 KiB	37.76 MiB	Inherits (124)	1.03	false	OFF					

Figure 73 : Creating Storage Pools

30.8. The click edit permissions under the dataset, edit ACLs, then select the user "DEFCOMPANY\johnydepp" who has been granted full permissions to the shared folder and the group ("DEF_TrueNas_Shared_Acc") of users who can access and view the shared folder as seen in Figure 74.

÷	→ C ▲ Not secu	ure 1	0.1.1.19/ui/storage/pools/id/NAS%20Pool/dataset/acl/NA	S%20Pool%2FDEF%20Shared%20Fol	der		
			≡ <				₫≫ sy:
	🖨 root						
	truenas.local			File Information		Access Control List	
	Dashboard			Path /mnt/NAS Pool/DEF Shared Folder		who* User	• (2)
	Accounts			User DEFCOMPANY\johnydepp	• @	User* DEFCOMPANY\johnydepp	_* @
	System			Apply User ⊘		ACL Type * Allow	- °0
	Tasks			Group DEF_TrueNas_Shared_Acc	_*@	Permissions Type *	
x	Network			Apply Group 🕜		Basic Permissions *	<u>•</u> Ø
						Full Control	• @
				SELECT AN ACL PRESET		Basic Regs*	• @
	Snapshots					Inherit	• @
							DELETE
	VMware-Snapshots					who+ Group	•
	Disks					Group * DEF_TrueNas_Shared_Acc	• 0
	Import Disk					ACL Type * Allow	• (2)
8	Directory Services					Permissions Type * Basic	• @
	Sharing					Permissions * Modify	• @
	Services					Flags Type *	
						Basic	• (?)

Figure 74 : Providing Access Control Permissions to the User

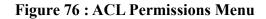
- 30.9. In the services tab ensure that SMB is running.
- 30.10. Then go to Sharing >Windows Shares (SMB) click add and browse down to the DEF Shared Folder created earlier and save, as seen in Figure 75.

	TrueNAS	≡ <		∭ systems ⁻	¢ i)	ф ()
	Dashboard				TrueNAS CO	æø © 2022 - I	Xsystems, Inc.
*	Accounts		Basic				
	System		Print *				
	Tasks		+ minutus - houlder - shared - hour				
x	Network		Nama NAS Pool	0			
	Storage		Pupose Default share parameters • (?) Description	0			
₿	Directory Services		Enabled ③				
	Apple Shares (AFP)		SAVE CANCEL ADVANCED OPTIONS				

Figure 75 : Windows Shares (SMB) Menu

31. Then click on the 3 dots of the newly created SMB share and select "Edit Filesystem ACL". Then select the user "DEFCOMPANY\johnydepp" who has been granted full permissions to the shared folder and the group ("DEF_TrueNas_Shared_Acc") of users who can access, and view the shared folder as seen in Figure 76.

÷	→ C A Not sec	cure 10	0.1.1.19/ui/storage/pools/id/NAS%20Pool/dataset/acl/N/	AS%20Pool%2FDEF%20Shared%20Fol	der		
			≡ <				₫≫ sy
	🛱 root						
	truenas.local			File Information		Access Control List	
	Dashboard			Path /mnt/NAS Pool/DEF Shared Folder		wwo* User	• (2)
*	Accounts			User DEFCOMPANY\johnydepp	• @	User* DEFCOMPANY\johnydepp 🗸 📎	®
	System			Apply User ⑦	- •	ACL Type *	~
	Tasks			Group DEF_TrueNas_Shared_Acc 	_*⊘	Allow Permissions Type *	• 0
*	Network			Apply Group ⑦		Basic 	• 0
						Full Control	• 0
				SELECT AN ACL PRESET		Flags Type * Basic	•0
						Fiegs 4 Inherit	• 0
	Snapshots						DELETE
	VMware-Snapshots					wno* Group	• (2)
	Disks					Group * DEF_TrueNas_Shared_Acc ⑦	
	Import Disk					ACL Type* Allow	• (2)
•	Directory Services					Permissions Type *	
	Sharing					Basic Permissions *	•
	Services					Modify	•
	, ii					Flags Type * Basic	• (?)



32. Then go to System > 2FA and select enable two factor authentication as seen in Figure 77. Open the DUO mobile app, click on the plus icon and scan the QR code from the TrueNAS console. Logout of the console.

TrueNAS	≡ <		(∲ systems	5 🕸 🖨 🌲 🗢 U
System Dataset				TrueNAS CORE® © 2022 - iXsystems, Inc.
Reporting		a su		
Alert Services		User Settings Use this form to set up Two-Factor Authentication for this system. Then link the system to an authenticator app (such as Google A	wthenticator	
Alert Settings		LastPass Authenticator, etc.) on a mobile device.		
Cloud Credentials		Con Time Passend (019) Digits * 6 ▼ ⑦ 1	0	
SSH Connections		Internet O Enable Two-Factor Auth for SSH @		
SSH Keypairs				
Tunables		System-Generated Settings Swort (Next only)		
Update		<u> </u>		
		Provincing URI (ncludes Scoret - Read only):		
CAs		Two-factor authentication is NOT enabled.		
Certificates		SAVE ENABLE TWO-FACTOR AUTHENTICATION SHOW OR RENEW SECRET		
ACME DNS				
Support				
2FA				

Figure 77 : Enabling 2FA in TrueNAS

- **33.** When logging in again the TrueNAS will ask for the username/password credentials and DUO MFA OTP to login to the TrueNAS console.
- 34. Next, we navigate to the shared folder from the user workstation by going to TrueNAS > NAS Pool as seen in Figures 78. We can see 3 files which the user "Johny Depp" has full control and the members of group "DEF_TrueNas_Shared_Acc" can we view but cannot modify.

			ot 1) [Running] - Oracle VM VirtualB	lox
→ → → Netwo		out Devices Help		
File Network	View			
← → ▼ ↑ 🥩 >	Networ	k >		
🗸 🖈 Quick access	~ (Computer (3)		
Desktop	*	VBOXSVR	truenas	WIN-1BKQAKTDARH
Downloads Documents	A - A			
Pictures	#			
1 Music				
NAS Pool				
Videos				
> 🥌 OneDrive				
> 🛄 This PC				
🗸 🇀 Network				
> 🛄 truenas				
> 🔜 VBOXSVR				
> VIN-1BKQAKTE	DARI			

Figure 78 : TrueNAS Network Drive

🐝 DEF_UserWorkstation (DEF_UserWorkstation Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
💻 🔄 🔜 🗢 truenas
File Home Share View
$\leftrightarrow \rightarrow \checkmark \uparrow \blacksquare$ Network > truenas >
✓ Unspecified (1)
Desktop MAS Pool
Downloads
Documents
Music
NAS Pool
Videos
OneDrive
This PC
P Network
🛄 truenas
VBOXSVR
WIN-1BKQAKTDARI

Figure 79 : TrueNAS Shared Pool

BEF_UserWorkstation (DEF_UserWorkstation Snaps	shot 1) [Running] - Oracle VM \	/irtualBox		
File Machine View Input Devices Help				
🖳 🔄 🧾 🖛 NAS Pool				
File Home Share View				
← → ~ ↑ 晃 > Network > truenas > NAS Pool				
Name	Date modified	Туре	Size	
★ Quick access DEF_Admin	4/5/2023 3:21 PM	Text Document	1 KB	
Desktop	3/28/2023 1:49 PM	Text Document	1 KB	
Downloads	3/28/2023 1:49 PM	Text Document	1 KB	
Documents				
E Pictures				
Music				
Videos Videos				
OneDrive				
This PC				
💣 Network				
🛄 truenas				
VBOXSVR				
WIN-1BKQAKTDARI				

Figure 80 : TrueNAS Shared Files

- **35.** Next, we are setting up a SIEM solution for continuous monitoring of the organization's environment. Download and install AT&T's open-source Alien Vault OSSIM SIEM solution [74].
- 35.1. We assign a static IP 10.1.1.21 to the SIEM and add IP 10.1.1.12 as the DNS server in the configuration setting. By providing the admin credentials we can get access's the SIEM's shell for additional configuration as seen in Figure 81.

 Alien Vault SIEM (Alien Vault SIEM Snapshot 1) [Running] - Oracle VM VirtualBox File Machine View Input Devices Help 		×
https://cybersecurity.att.com/		
AlienVault USM 5.8.14 - x86_64 - tty1 alienvault login:		

Figure 81 : Alien Vault OSSIM Command Line Console

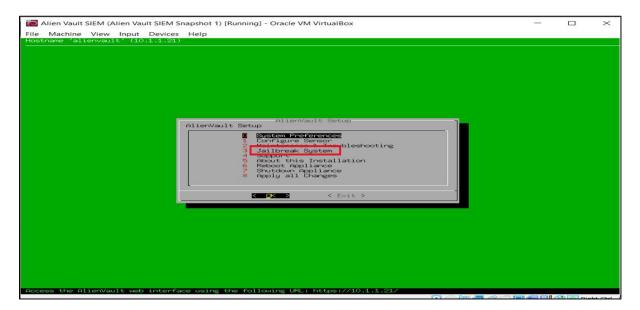


Figure 82 : Alien Vault OSSIM Shell Console

35.2. We can also access the SIEM's console through the web browser by going to https://10.1.1.21/ as seen in Figure 83.

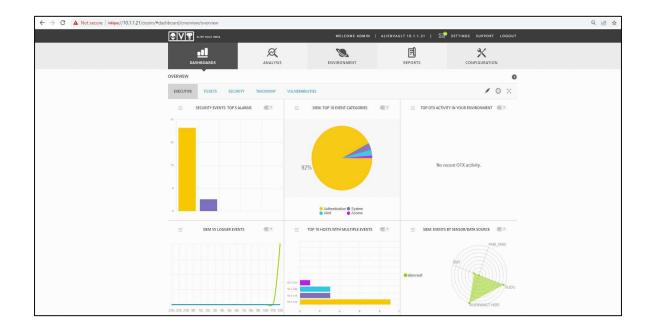


Figure 83 : Alien Vault OSSIM Web Console

35.3. We can add users and analysts for SOC monitoring under Configuration > Administration as seen in Figure 84.

	LIEN VAULT OSSIM		WELCOME ADMIN	ALIENVAULT 10.1.1.21 🖂	SETTINGS SUPPORT LOGOUT
	DASHBOARDS	ANALYSIS		REPORTS	
100	ADMINISTRATION				0
	USERS MAIN BACKUPS				
	USER INFORMATION ACTIV	ИТҮ			
				NEW (ODIFY	DELETE SELECTED DUPLICATE SELECTED
	LOGIN NÂME	EMAIL	VISIBILITY STATUS	LANGUAGE CREATIC	IN DATE LAST LOGIN DATE
	admin 🔱 admin	mathewsalappat@gmail.com		English 2023-03-3	0 11:36:16 2023-04-10 13:10:24
					< PREVIOUS NEXT> 💆

Figure 84 : Adding Users in Alien Vault OSSIM

35.4. Then we go to discover and add assets in the network by going to Environment > Assets & Groups > Add assets by giving the IP address or scanning the domain subnet. From the below screenshot we can see the different assets that have been discovered in the network scan as seen in Figure 85.

ALIEN VAULT OSSIM					w	LCOME ADM	IN ALIENVAULT	0.1.1.21	🖂 SETT	INGS SUPPORT L	060
DASHBOARDS		ANALYSIS			ENVIR			PORTS			
ASSETS & GROUPS						•					
ASSETS ASSET GROUPS	NET	WORKS NETWORK G	ROUPS	SCHEDU	LE SCAN						
Search	Ass	ets								ADD ASSETS	•
🗌 Has Alarms											
Has Events										6 Assets	
Vulnerabilities										Clear	AIF
Asset Value											
	20	* ASSETS								6 ACD	
HIDS Status	0	HOSTNAME	▲ IP		٥	DEVICE TYPE	OPERATING SYSTEM	ASSET	VULN SCAP SCHEDULEI	d ≎ status ≎	,
Disconnected Not Deployed		Host-10-1-1-20	10	1.1.1.20			Microsoft Windows 10 64-bit	3	No	Disconnected	
Availability Status		Host-10-1-1-19	10	L 1 .1.19		Server:File Server	PreeBSD	4	No	Not Deployed	
O Down O Unconfigured		Host-10-1-1-15	10	.1.1.15			Microsoft Windows Server 2019 Standard Edition on x64	5	No	Connected	
Show Assets Added Last Day Last Week	0	Host-10-1-1-12	10	1.1.12		Server:Active Directory Server / Domain Controller	Microsoft Windows Server 2019 Standard Edition on x64	1	No	Connected	
O Last Month O Date Range		Host-10-1-1-1	10	11.1.1		Network Device:Firewall	FreeBSD	2	No	Not Deployed	
Last Updated	0	allenvault	10	1.1.1.21			AllenVault OS	2	No	Connected	
Last Day Last Week Last Month Date Range	SHOW	ING 1 TO 6 OF 6 ASSETS								< PREVIOUS 1 N	

Figure 85 : Adding and Discovering Assets

35.5. Then we go to discover and add assets in the network by going to Environment > Detection
 >Agents to deploy HIDs agents to collect logs from the discovered assets as seen in Figure 86.

ALIEN VAULT OSSIM			WELCOME ADMIN ALIEN	NVAULT 10.1.1.21 🖂	SETTINGS SUPPORT LOGO
DASHBOARDS	ANALYS	s E		E	
DETECTION		1			
OVERVIEW AGENTS	AGENTLESS	EDIT RULES CONFIC	HIDS CONTROL		
HIDS EVEN	NTS TREND			HIDS DATA S	SOURCES
4 Abr 5 Apr 6 Apr 7 A	Apr 8 Apr 9 Apr	10 Apr	Sysio	ows [132] [43] heck [40] ks [8] dieck [6]	Systog Windows Authenti
Search		AGE	NT INFORMATION		
ID 🔺 ASSET	O IP/CIDR :	CURRENT IP CURRENT U	ISER STATUS	0 TRE	ND (TIME UTC)
					nart not available
() 000 alienvault	127.0.0.1	127.0.0.1 -	Active/iocal	Trend c	
000 alienvault 001 Host-10-1-1-12	127.0.0.1	127.0.0.1 -	Active/local	4 Apr S Apr S Apr	
				4. pr SApr GApr	
001 Host-10-1-1-12	10.1.1.12	10.1.1.12	Active	4 Apr 5 Apr 6 Apr 4 Apr 5 Apr 6 Apr	740r 840r 940r 1040r
001 H055-10-1-1-12 003 H055-10-1-1-15	10.1.1.12	10.1.1.12 · 10.1.1.15 ·	Active	4 Apr 5 Apr 6 Apr 4 Apr 5 Apr 6 Apr	THE BADE BADE TO ADE

Figure 86 : Discovered Assets

\$V\$	VAULT OSSIM			WELCOME ADMIN	ALIENVAULT 10.1.1.21	SETTINGS SUPPORT LOGOU
DASHB			EN		REPORTS	
DETECTION OVERVIEW AGENT CONTROL		AGENTLESS EDIT RU	LES CONFIG	HIDS CONTROL		•
Search	agent is only available for asse agent to a Windows machine	ts with a Windows OS defined in the s, you may need to update the OS for p IP/CIDR		U BYE T INFORMATION CURRENT USER	STATUS \$	ADD AGENT
000	alienvault	127.0.0.1	127.0.0.1		Active/local	⊕ ❷ 🐂 🖬 🖉 🕒 🖬 🖉 📋
001	Host-10-1-1-12	10.1.1.12	10.1.1.12		Active	@ 🥝 🕵 🖻 💕 🕗 🖻 🗔 🔗 🗉
0 003	Host-10-1-1-15	10.1.1.15	10.1.1.15		Active	@ Ø 🕵 🗟 📽 🔘 🖬 🖉 🔟
0 0030 004	Host-10-1-1-15 Host-10-1-1-20	10.1.1.15	10.1.1.15		Active Disconnected	⊌ ❷ ¶.]: £ ○]: 7 0 11 ⊎ ❷ ¶.]: £ ○]: 7 0 11
	Host-10-1-1-20					

Figure 87 : Deploying HIDs Agents

35.6. Then we go to Analysis > Alarms, to see the Alarms generated in the SIEM console from monitoring the network as seen in Figure 88.

← → C ▲ Not secure https://10.1.1.21/ossim/#ana	lysis/alarms/alarms								
	V * ALIEN VAULT OF	SIM		WEL	COME ADMIN A	LIENVAULT 10.1.1.21	1 🖙 se	TTINGS SUPPORT LO	GOUT
	DASHBOARDS		A ANALYSIS	ENVIRON		REPORTS			
	ALARMS		•						0
	LIST VIEW GROUP	/IEW							
	1			Next refresh in 269 seconds.	Or click here to refresh now				
	SEARCH AND FILTER Sensor		Asset G	roup		Label [Manage La	bels]	Show Alarm Graph Yes	E
	Alarm Name / ID	~	Intent		* *	OTX Pulse		~	
	Source IP Address		Directiv			Only OTX Put	se Activity		
	Destination IP Address		Contain	s the Event Type		Do not resolve			
	Date		<=			Hide closed al			
			Low	el in alarms Medium	High				
				SEAR	сн				
	31 DAYS	23-04-05	23-04-06	23-04-07	23-04-08	23-04-09	23-04-10	23-04-11	
	System Compromise								
	Exploitation & Installation								
	Delivery & Attack								

Figure 88 : OSSIM SIEM Alarms1

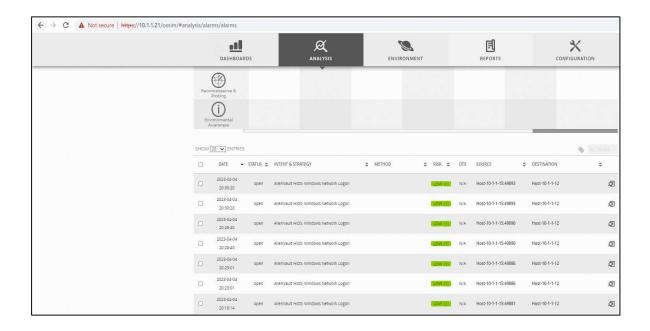


Figure 89 : OSSIM SIEM Alarms2

35.7. Then we go to Analysis > Security Events (SIEM), to see the events generated, which further trigger Alarms in the SIEM console from monitoring the network as seen in Figure 90.

← → C ▲ Not secure https://10.1.1.21/ossim/#ar	nalysis/security_events/security	_events			
	ALIEN VAULT OSSIM		WELCOME ADMIN	ALIENVAULT 10.1.1.21 🖂	settings support logout
	DASHBOARDS		ENVIRONMENT	E	
	SECURITY EVENTS (SIEM)				Ø
	Search	Event Name 🗸 😡 🧿			Ð
	SHOW EVENTS Clast Hour Clast Day Clast Week: Clast Month Diste Range	DATA SOURCES DATA SOURCE GROUPS SENSORS EXCLUDE	ASSET GROUPS NETWORK GROUPS RISK	OTX IP REPUTATION	CLEAR FLITERS Q
	Luserdata1 Luserdata1 Luserdata1 Luserdata1 Luserdata1 Luserdata3 L	TIMELINE			ADVANCED SEARCH CHANGE VIEW ACTIONS A
	EVENT NAME	▼ <u>DATE GMT+4:00</u>	SENSOR OTX SOURCE	DESTINATION	ASSET S 🛥 D RISK

Figure 90 : OSSIM SIEM Events1

→ C A Not secure https://10.	1.1.21/ossim/#analysis/security_events/security_events								
		ALYSIS	EN	VIRONI	MENT	REPORTS	CONFIG	·	
	AllenVault HIDS: Windows Network Logon	2023-04-10 13:39:58	alienvault	N/A	Host-10-1-1-12:55439	Host-10-1-1-12	1->2	LOW (0)	Ĺ,
	AllenVault HIDS: Windows User Logoff.	2023-04-10 13:39:58	allenvault	N/A	Host-10-1-1-12	Host-10-1-1-12	1->2	LOW (0)	¢
	AllenVault HIDS: Windows Network Logon	2023-0 <mark>4-10 13:39:58</mark>	allenvault	N/A	Host-10-1-1-12:55441	Host-10-1-1-12	1->2	LOW (0)	4
	AllenVault HIDS: Windows User Logoff.	2023-04-10 13:39:58	allenvault	N/A	Host-10-1-1-12	Host-10-1-1-12	1->2	LOW (0)	¢
	AllenVault HIDS: Special privileges assigned to new logo	2023-0 <mark>4</mark> -10 13:39:58	allenvault	N/A	Host-10-1-1-12	Host-10-1-1-12	1->2	LOW (0)	\$
	AllenVault HIDS: Special privileges assigned to new logo	2023-04-10 13:39:58	alienvault	N/A	Host-10-1-1-12	Host-10-1-1-12	1->2	LOW (0)	¢
	AllenVault HIDS: Windows Network Logon	2023-04-10 13:39:42	allenvault	N/A	Host-10-1-1-12:55436	Host-10-1-1-12	1->2	LOW (0)	\$
	AllenVault HIDS: Special privileges assigned to new logo	2023-04-10 13:39:42	allenvault	N/A	Host-10-1-1-12	Host-10-1-1-12	1->2	LOW (0)	1
	AllenVault HIDS: Windows User Logoff.	2023-04-10 13:39:42	allenvault	N/A	Host-10-1-1-12	Host-10-1-1-12	1->2	LOW (0)	1

Figure 91 : OSSIM SIEM Events2

35.8. We can generate reports after analyzing the SIEM generated alarms and events for security audit purposes by going Reports and download the respective reports as seen in Figure 92.

	WELCOME ADMIN	ALIENVAULT 10.1.1.21	SETTINGS SUPPORT LOGOUT	
DASHBOARDS	ANALYSIS ENVIRONMENT	REPORTS		
OVERVIEW			0	
REPORT NAME	REPORT	OPTIONS	ACTIONS	
Alarms Report The rays The rays The rays The IV Analysis	Date Range 11 2023-00-11 - 11 2023-04-10		Download PDF	
Asset Details	Host Name/IP/Network:		View Report	
Availability Report	Section: Trends		View Report	
Business & Compliance ISO PCI Repo	nt Date Range 중 2022-06-11 - 중 2022-06-10		Deventing FDF Deventing FDF Deventing FDF	
Geographic Report	Date Range		Download PDF	

Figure 92 : Generating SIEM Alarm Reports

35.9. The SIEM automatically generates reports based on the data collected from the various sources. A sample of the generated report is attached below as seen in Figure 93.

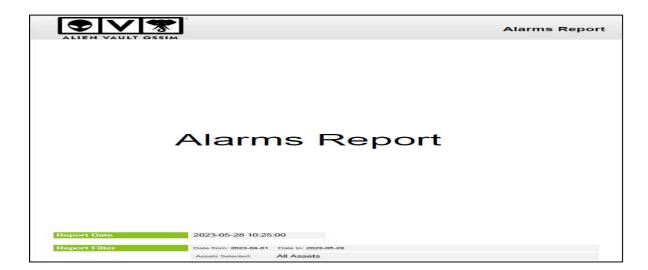


Figure 93 : SIEM Alarm Report1

Alarms	Report - Top 10 Attacker	Host	from: 2023-04-0	1 to: 2023-05-28
Host	Occurrences			
Host-10-1-1-24 🍂	83	100 E		
Host-10-1-1-19 🔰	71	80 -		
Host-10-1-1-15 🍂	57	60		
		40		_
		20		_
		0		
		Host-10-1-1-24	Host-10-1-1-19	Host-10-1-15



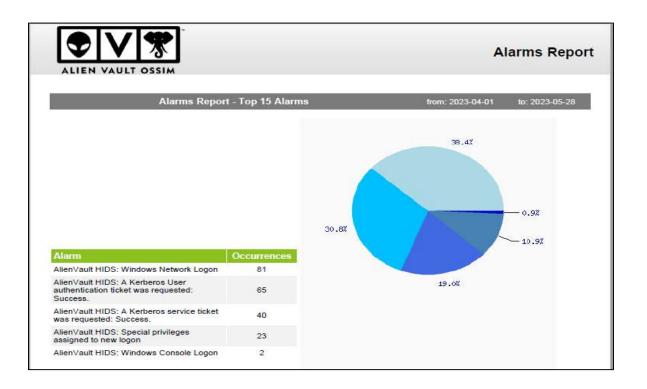


Figure 95 : SIEM Alarm Report3

35.10. The OSSIM SIEM is also connected to the Open Threat Exchange (OTX) for receiving update malware signatures and detections available worldwide as seen in Figure 96. We can subscribe to various OTX subscriptions based on the organization's requirements.

← → C ▲ Not secure https://10.1.1.21/ossim/#configuration/otx/otx						
			WELCOME ADMIN	ALIENVAULT 10.1.1.2	1 🖙 SETTINGS	SUPPORT LOGOUT
	DASHBOARDS	ANALYSIS	ENVIRONMENT	REPORTS		
	OPEN THREAT EXCHANGE					° Ø
	OTX Account					ACTIONS -
	OTX Key: b278b01f77610e8af856c1ed3db9546a7b408f979a469e025aa6515b3f4419a0			Contribute to OTX:	Yes	
	OTX Username: dic	_support		Last Updated:	2023-04-10 13:53:04	
	OTX Subscriptions (5112)					
	Who Broke NPM? Malicious Packages Flood Leading to Denial of Service VEW IN OTX 2023-04-08 00 23 by Alexhair We have been spin carrely as the pack by the baset spin carrely as a spin spin spin spin spin spin spin spin					
	NPM					
	2023-04-07 21:09:10 by AlienVault	tte Targets Vulnerable Backup Installati aka BlackCat ransomware) ransomware affiliate, tracker mments.		Backup Exec installations, vulnerab	ble to CVE-2021-27876, CVE-200	VIEW IN OTX 21-27877 and CVE-2021-
	BLACKCAT RANSOMWARE VERI	TAS BACKUP EXEC ALPHY UNC4466				

Figure 96 : Alien Vault Open Threat Exchange Feeds