BCN3043 NETWORK SERVICE ADMINISTRATION

LECTURER NAME: DR NOORHUZAIMI @ KARIMAH BINTI MOHD NOOR PROJECT

TITLE: DESIGN AND IMPLEMENTATION OF SERVER SECURITY

SUBMISSION DATE: 12 JANUARY 2024

GROUP MEMBERS:

NAME	MATRIC ID	SECTION
MUHAMMAD AFIQ BIN SHAMSUDIN	CA21083	01B
MUHAMAD ASYRAF MUHAIMIN BIN MAZLAN	CA21058	01A
SYAHMI IZZAT BIN SHUHAIMI	CA23093	01B
MUHAMMAD AZRAI HALIQ BIN MOHD RAFIS	CA23088	01B

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 INTRODUCTION TO DESIGN AND IMPLEMENTATION OF SERVER SECURITY

Server security is essential for protecting against various cyber attacks in an era where sensitive data and digital assets are essential parts of businesses. A server is the central component of any network, acting as a storehouse for information, programmes, and services, which makes it a target for hackers. The strategies used by hackers also evolve with technology, which emphasizes the significance of a thorough and proactive approach to server security.

Key ideas and recommended procedures for developing and executing server security are intended to be outlined in this handbook. Every aspect of server security, from sophisticated encryption techniques to physical barriers, strengthens the defense against illegal access, data breaches, and other security flaws. Organizations can build a strong security framework that safeguards their assets and guarantees the availability, confidentiality, and integrity of vital data by implementing a multi-layered approach.

The subsequent segments explore diverse facets of server security, offering practical perspectives for IT experts, system administrators, and security practitioners. Every suggestion, including the use of encryption techniques and physical security measures, adds to the development of a comprehensive and flexible security plan. The objective is to enable organizations to defend their servers against a constantly changing threat landscape, regardless of the issues surrounding network setups, user authentication, or incident response plans.

1.2 SUMMARIZE

The goal of this document is to provide a thorough overview of server security architecture and implementation. The introduction highlights how crucial it is to secure servers in the face of ever changing cyberthreats. The sections that follow address several facets of server security and offer in-depth explanations of the following crucial components:

1. Detail about the design and implementation:

   Explores the complexities involved in developing and putting into practice server security solutions, taking into account both software and hardware issues.

2. The importance of the design and implementation:

   Examines the vital role that a server security infrastructure that is well-designed and implemented plays in preventing potential dangers, preserving service availability, and protecting sensitive data.

3. Working mechanism (supported with figures):

   Uses diagrams and figures to show how the server security measures' complex operating mechanism works.Uses visual aids to improve knowledge by breaking down the design and execution processes.

4. Example of scenarios:

   Provides real-world examples showing how the planned and executed security measures perform in various network contexts. Demonstrates how businesses can modify their security infrastructure to meet unique requirements and overcome obstacles.

5. Advantages and disadvantages:

   Offers a fair evaluation of the benefits and drawbacks related to the selected design and implementation methodologies.

6. Citations and references:

   Cite and reference all sources and material included in the text to ensure accuracy and trustworthiness. Follows the APA reference and citation guidelines, giving readers a clear and trustworthy information trail.

1.3 TASK DISTRIBUTION

Subtopic	Contribution
• Introduction • Summarize • Task distribution	
• Details of design and implementation	
• Importance of design and implementation	
• How it works	
• Example of scenarios	azrai
• Advantages and disadvantages	Izzat
• Step by step configuration/coding	Afiq Asyraf
• Conclusion	
• In-text citations and references	
• Report format and rubric	Asyraf

• Hard copy report	

2.0 CONCEPT OF DESIGN AND IMPLEMENTATION OF SERVER SECURITY

2.1 DETAILS OF DESIGN AND IMPLEMENTATION OF SERVER SECURITY

Multiple factors must be taken into account while designing and implementing server security in order to create a strong defense against changing cyberthreats. Thorough planning which includes physical security measures, network protocols, authentication methods, encryption schemes, and thorough documentation is crucial during the design phase. Every component is thoughtfully designed to build a strong infrastructure that safeguards private information and guarantees service availability. These strategies are put into practice during the implementation phase, which involves the deployment of firewalls, intrusion detection systems, encryption methods, and strict access controls. A clear incident response plan, frequent updates, and ongoing monitoring strengthen the security posture even further. Additionally, regular security audits, compliance adherence, and user education all enhance the security framework's overall efficacy. The server security is kept strong and flexible to new threats by the cyclical nature of improvement and adaptation.

In actuality, server security design and execution necessitate a comprehensive viewpoint that goes beyond technical features. Through continuous training and user education, a security-conscious culture must be fostered within the company. Frequent compliance audits and security audits confirm that installed controls are effective and that they comply with industry standards. Mechanisms for continuous improvement, such as feedback loops and incident lessons learned, help create an agile security posture that can react quickly to new threats. In the end, a carefully thought-out and skillfully executed server security framework creates a solid foundation for a durable and adaptable digital infrastructure in the face of a constantly changing threat landscape, while also guarding against unwanted access and data breaches.

2.2 IMPORTANCE OF DESIGN AND IMPLEMENTATION OF SERVER SECURITY

Given that servers are the primary locations for sensitive data and vital business processes in today's digital environment, the significance of developing and putting into place strong server security measures cannot be emphasized. A carefully designed security architecture is essential for a number of important reasons.

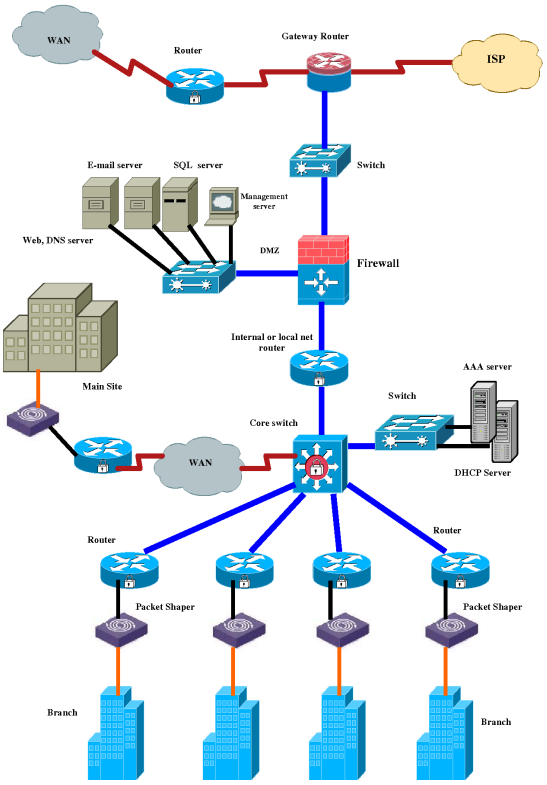
First and foremost, preventing unwanted access is made possible in large part by the planning and execution of server security. Important programmes, intellectual property, and private information are frequently stored on servers. Malicious actors may take advantage of weaknesses in security protocols, which could result in data breaches, illegal access, and even the possible compromise of organizational assets. In order to defend against such risks, a secure design makes sure that authentication procedures, access controls, and encryption methods are in place.

Second, to ensure company continuity and service availability, server security is essential. Security-related downtime can have serious consequences that impact revenue, consumer trust, and productivity. Measures like backup plans, disaster recovery plans, and ongoing monitoring are incorporated into well-designed security frameworks to lessen the impact of possible disruptions and guarantee that services continue to function even in the face of cyber attacks or unanticipated circumstances.

Security on servers is also necessary for regulatory compliance. Strict data protection and privacy laws apply to many industries, and non-compliance can have negative legal and reputational effects. By keeping compliance in mind when designing security measures, businesses can avoid legal repercussions and build a reputation for reliable data management processes by adhering to industry standards and regulatory requirements.

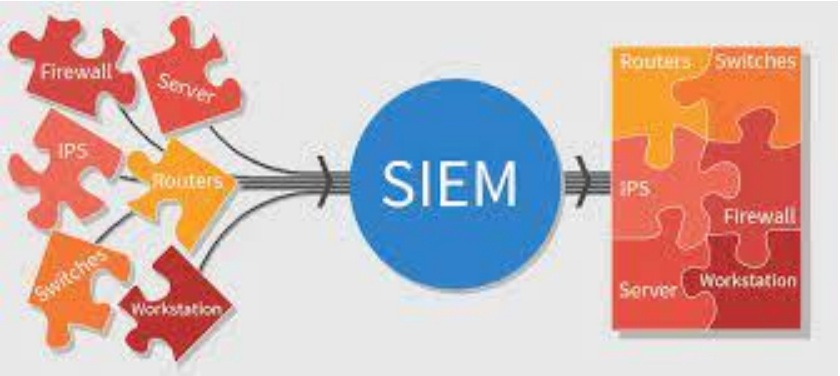
2.3 HOW IT WORKS

Server security employs a comprehensive strategy that combines hardware, software, and procedural components to create a strong barrier against possible intrusions. Access control and authentication comprise the first layer. Only authorized people or systems are allowed access by means of secure protocols like multi-factor authentication, which verify users. The second layer consists of network security technologies, such as firewalls and intrusion detection/prevention systems, which actively monitor and control data traffic to thwart unauthorized access. By protecting the privacy of data transferred between the server and linked devices, encryption, when used on both in-transit and at-rest data, offers another degree of protection.



Continuous monitoring and logging, in which the server creates thorough logs of operations, is a crucial component of server security. These logs might provide light on possible security problems. By utilizing Security Information and Event Management (SIEM) solutions, these logs can be examined in real-time or at regular intervals for the purpose of identifying suspicious patterns or anomalies. The operating system and software of the server

are protected against known vulnerabilities by the third layer's proactive procedures, which include patch management and routine updates. A thorough backup and disaster recovery plan is also put in place to protect against data loss or corruption, and an incident response plan directs steps in the case of a security incident to reduce impact and downtime.



The main concept is continuous improvement, with frequent security audits assessing the efficacy of current procedures. The server security framework can respond to new threats with the help of this adaptive methodology and a proactive culture of user education and training. By combining these components, server security guarantees the robustness of the server architecture against a dynamic and ever-changing threat landscape in addition to safeguarding against unauthorized access and data breaches.

2.4 EXAMPLE OF DESIGN AND IMPLEMENTATION OF SERVER SECURITY SCENARIO

1. **Unauthorized Access Attempt:**
   - Scenario: A malicious actor attempts to gain unauthorized access to your server by exploiting a vulnerability in an outdated software component.
   - Security Measures:
   - Regularly update and patch software to address known vulnerabilities.
   - Implement strong authentication mechanisms, such as multi-factor authentication (MFA).
   - Monitor server logs for unusual login patterns and use intrusion detection systems to detect and block suspicious activities.

2. **Data Breach:**
   - Scenario: An attacker successfully penetrates your server and gains access to sensitive customer data.
   - Security Measures:
   - Encrypt sensitive data at rest and in transit.
   - Implement access controls and role-based permissions to restrict user privileges.
   - Conduct regular security audits and penetration testing to identify and address vulnerabilities.

3. **Denial of Service (DoS) Attack:**
   - Scenario: Your server is targeted in a distributed denial of service (DDoS) attack, causing a disruption in service availability.
   - Security Measures:
   - Deploy firewalls and intrusion prevention systems to filter and block malicious traffic.
   - Use content delivery networks (CDNs) to distribute traffic and mitigate the impact of DDoS attacks.
   - Implement rate limiting and traffic monitoring to identify and respond to abnormal traffic patterns.

4. **Insider Threat:**

- Scenario: An employee with malicious intent tries to access or manipulate data on the server.
- Security Measures:
- Enforce the principle of least privilege through role-based access controls.
- Implement user activity monitoring and logging to detect unusual or suspicious behavior.
- Conduct regular employee training on security policies and the consequences of unauthorized actions.

5. **Ransomware Attack:**

- Scenario: A server is infected with ransomware, encrypting critical data and demanding payment for decryption.
- Security Measures:
- Regularly backup important data and store backups in an isolated environment.
- Implement robust antivirus and antimalware solutions.
- Train employees to recognize phishing attempts, as they are common vectors for ransomware.

6. **Physical Security Breach:**

- Scenario: An unauthorized person gains physical access to the server room and attempts to tamper with hardware.
- Security Measures:
- Restrict physical access to the server room with key card access or biometric authentication.
- Install surveillance cameras and alarms to monitor and alert in case of unauthorized entry.
- Implement environmental controls to prevent damage from factors like temperature and humidity.

7. **Failure to Apply Security Patches:**

- Scenario: The organization neglects to apply critical security patches, leaving servers vulnerable to known exploits.
- Security Measures:
- Establish a patch management process to regularly apply updates.
- Test patches in a controlled environment before applying them to production servers.
- Monitor security advisories and alerts from software vendors to stay informed about potential vulnerabilities.

In each of these scenarios, a well-designed and implemented server security strategy can significantly mitigate the risks and impact of security incidents, underscoring the importance of a proactive and comprehensive approach to server security.

2.5 ADVANTAGES AND DISADVANTAGES

Aspect	Advantages	Disadvantages
Security Enhancement	• Mitigates the risk of unauthorized access • Protects sensitive data from unauthorized users • Minimizes the risk of data breaches	• Implementation may be complex and time-consuming • Potential for false positives/negatives • Continuous monitoring and updates are required
Data Integrity	• Ensures the integrity of stored data • Prevents data tampering and manipulation • Supports secure data transfer	• Performance overhead due to encryption • Key management complexities • Potential for compatibility issues
Availability	• Reduces the risk of server downtime • Implements redundancy for high availability • Protects against denial-of-service attacks	• Resource-intensive security measures • Inadequate planning may lead to disruptions
User Authentication	• Ensures only authorized users access the server • Implements multi-factor authentication	• Forgotten passwords leading to access issues • Authentication vulnerabilities

	• Enhances accountability and traceability	

3.0 STEP BY STEP CONFIGURATION/CODING

3.1 FIGURE WITH CAPTION AND EXPLANATION

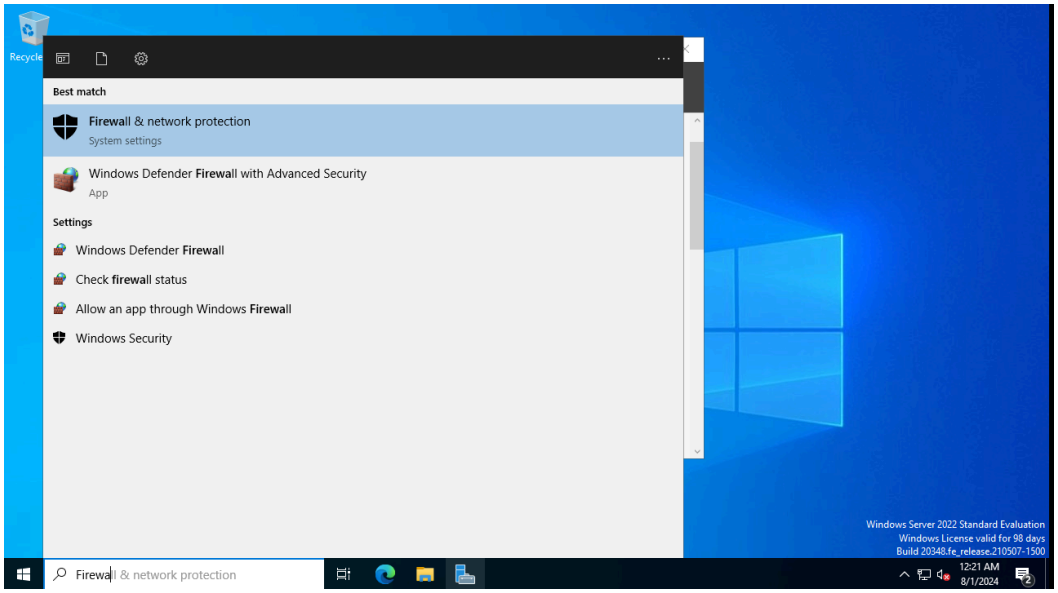


Figure 1 : Open Windows Defender Firewall with Security

Based on figure 1 above, We open Firewall & network protection in Windows Server 2022 by finding it in the search bar.

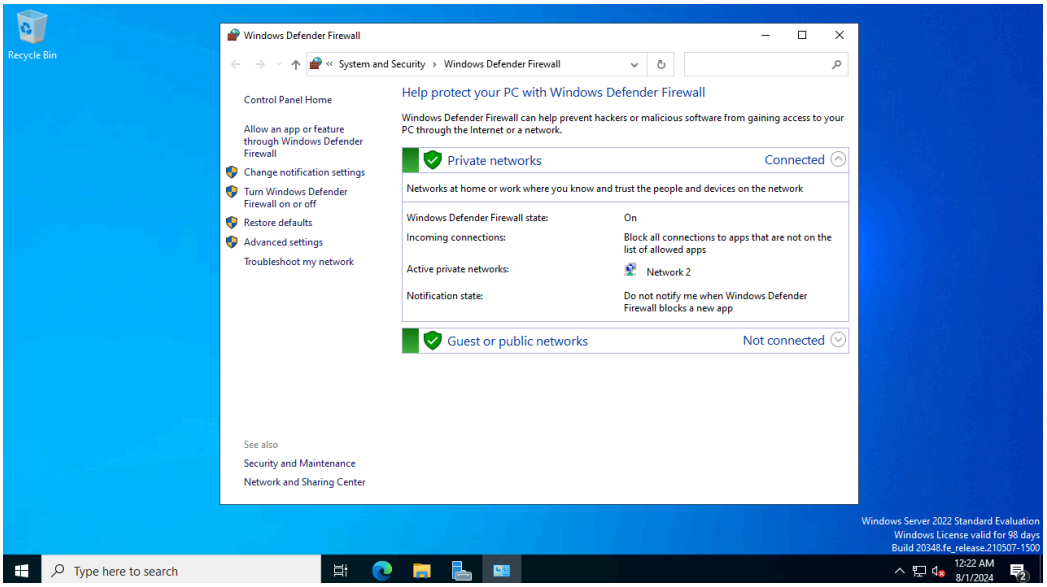


Figure 2 : Windows Defender Firewall Interface

Figure 2 shows the Windows Defender Firewall Interface. Next we need to click "Turn Windows Defender Firewall on or off".

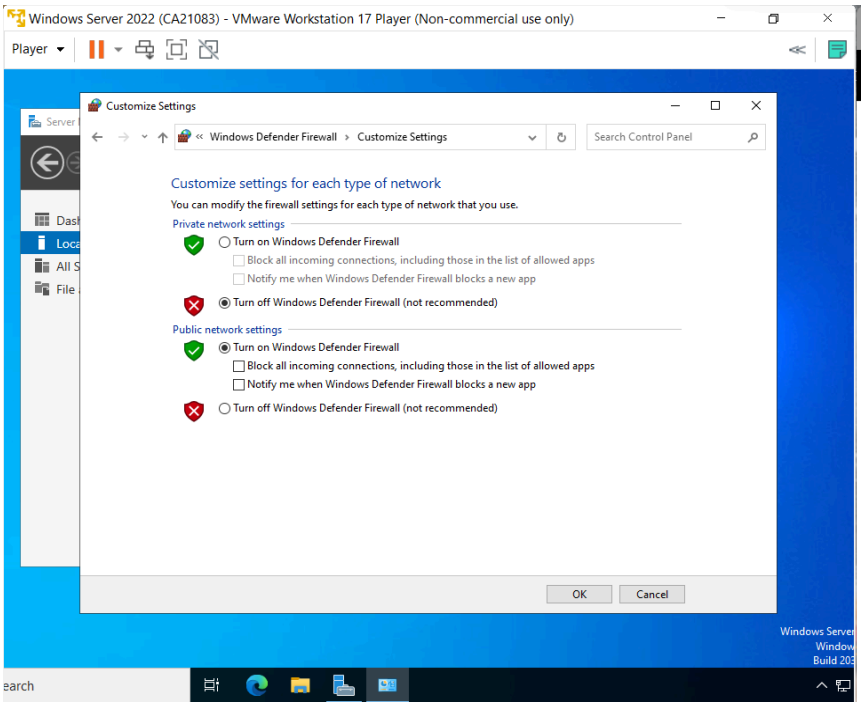


Figure 3 : Turn off the windows defender firewall

In figure 3 we have the option to customize the setting for each type of network . Next click the "Turn off windows defender firewall " in the private network setting and click "ok" to save the changes .

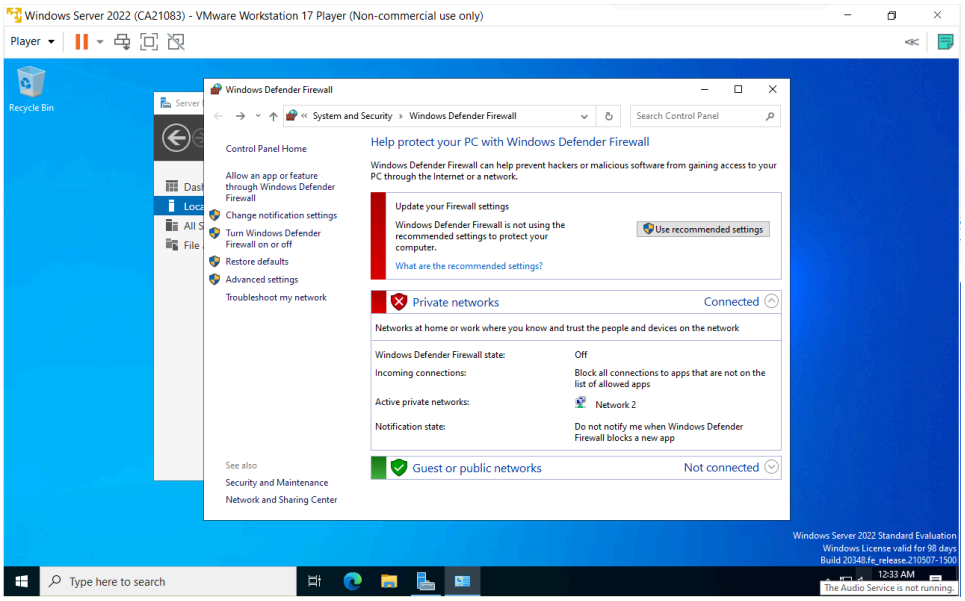


Figure 4 : Shows the warning because not using recommended settings

Based on figure 4 , We will receive 1 warning from windows defender firewall because not using recommended settings. So we need to click on the "use recommended settings" then the red bar will turn green. Next we need to click "Allow an app or feature through Windows Defender Firewall".

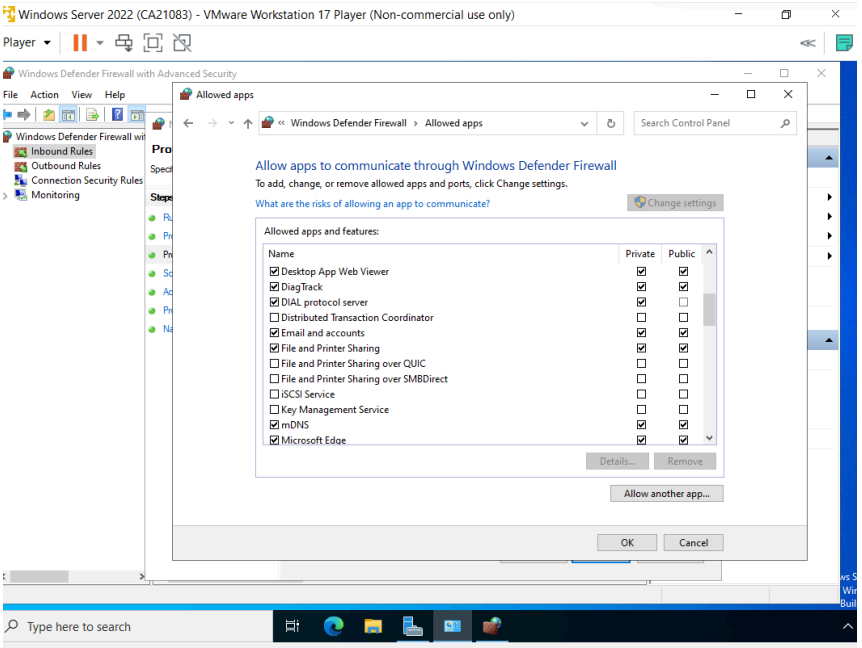


Figure 5 : Allow apps to communicate through windows defender firewall

In figure 5 we need to check and click the feature that we want to allow through the window firewall . In this console we choose to click the "File and printer sharing" . Next we click "ok" to save the changes.

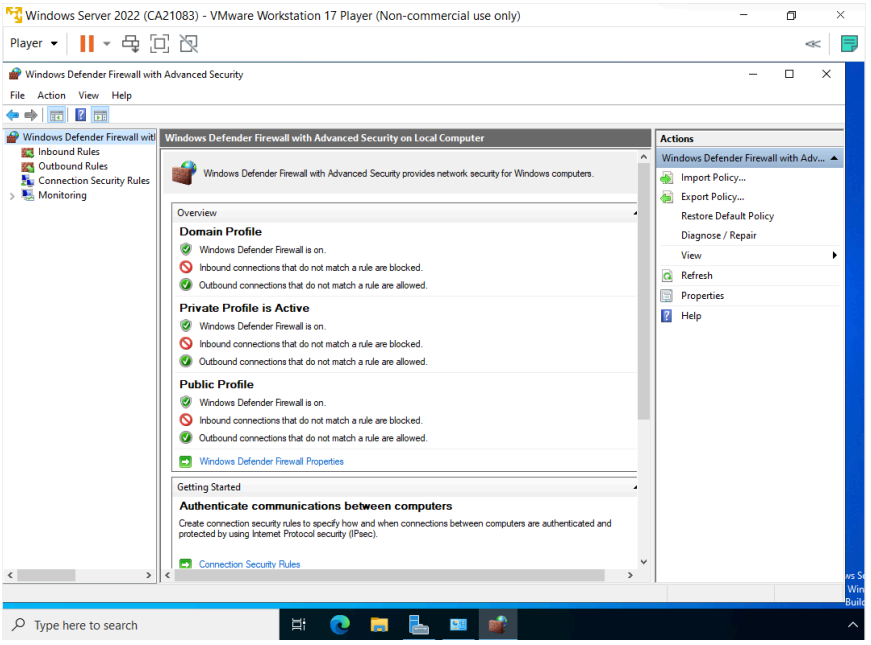


Figure 6 : Advance settings

Next we open the advanced setting. Figure 6 shows the Advanced setting for Windows defender firewall

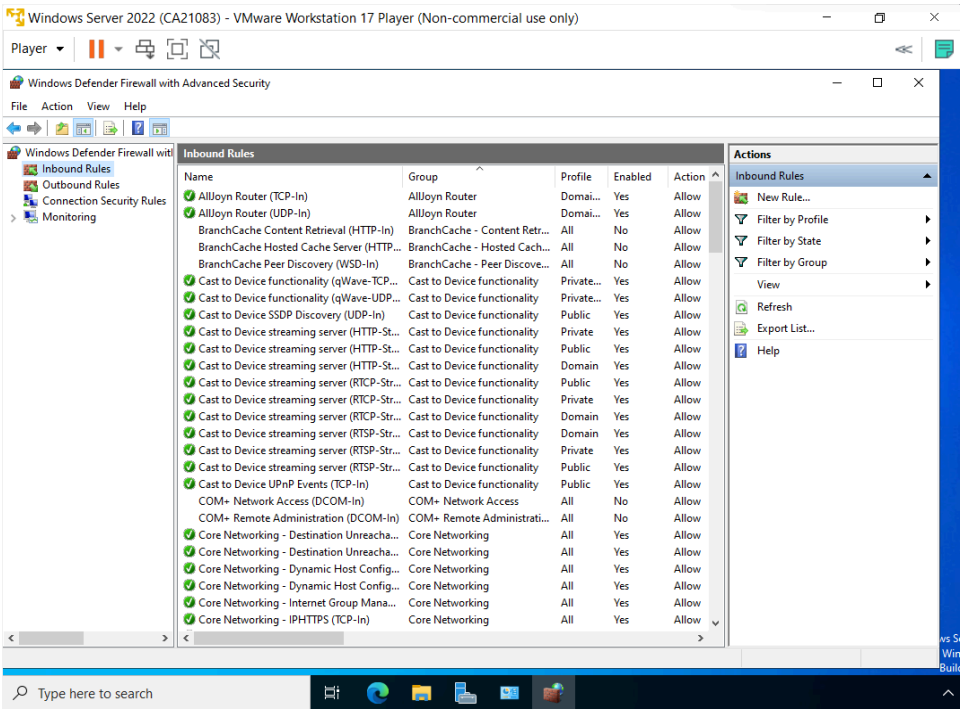


Figure 7 : Inbound Rules

Figure 7 shows that we click the Inbound Rules . The green correction symbols show that the rule is enabled .

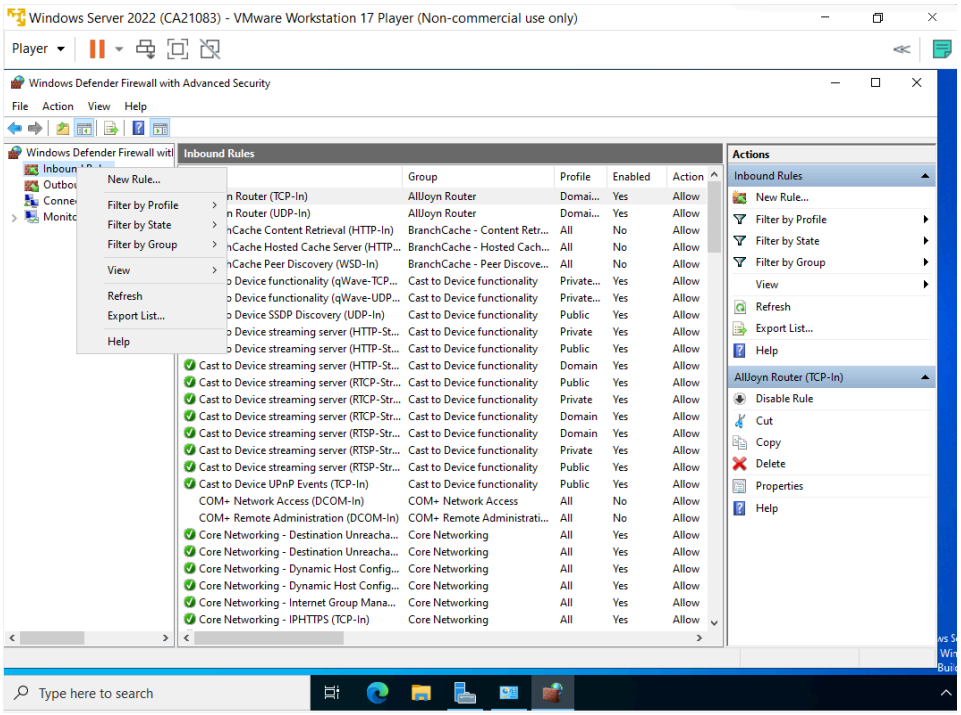


Figure 8 : Create new rule

To create a new inbound rules right click on the inbound rules and click "New rule.." shown in figure 8

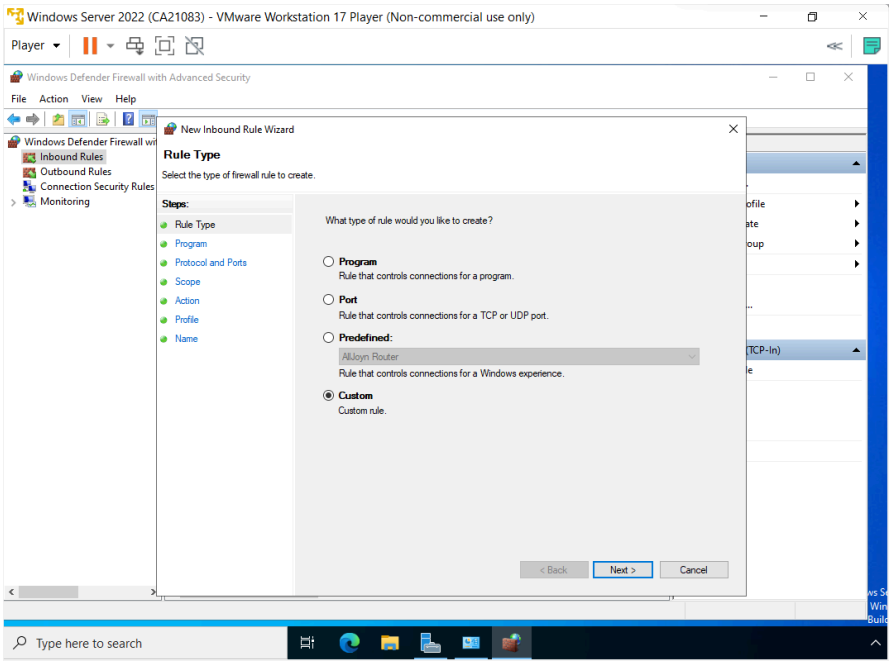


Figure 9: create custom rule

Based on figure 9 we choose custom because we want to create a custom rule .

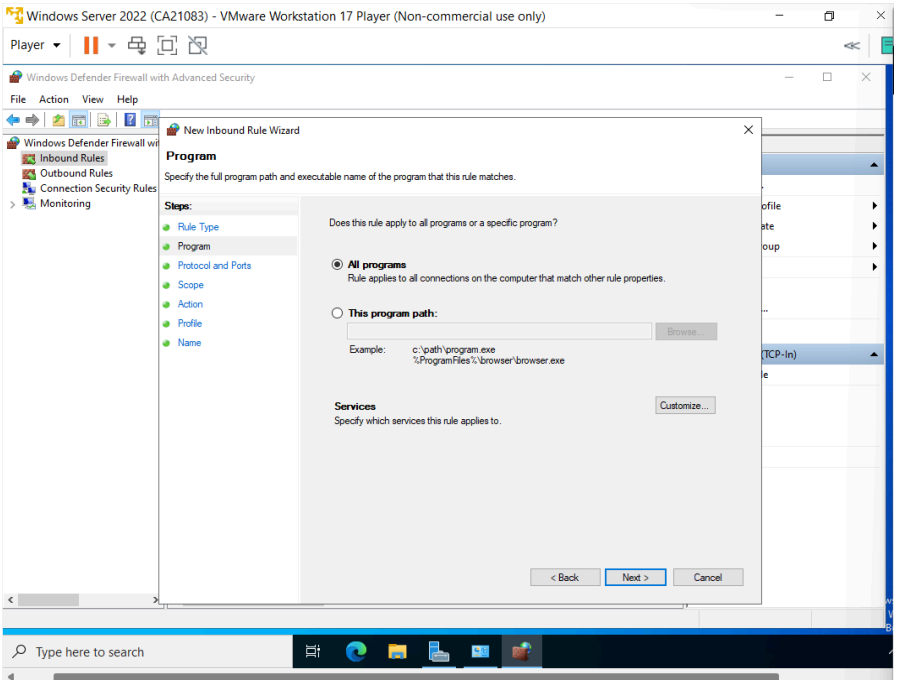


Figure 10 : All programs

Here in figure 10 we select All programs and click on “Next”.

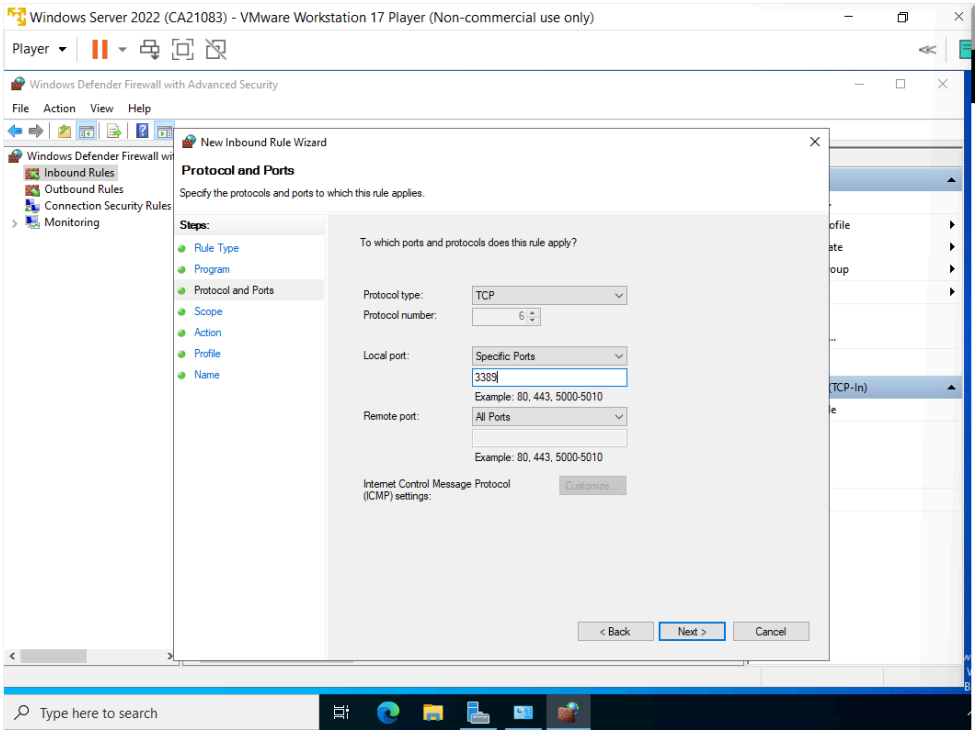


Figure 11 : Select the port and protocol that rule should apply to

In this console we can select the port and protocol that rule should apply to . based on figure 11 we choose the "TCP" protocol type and the protocol number will automatically change to 6 . on the local port we choose the specific ports and for the ports number we choose "3389". Then we click "Next".

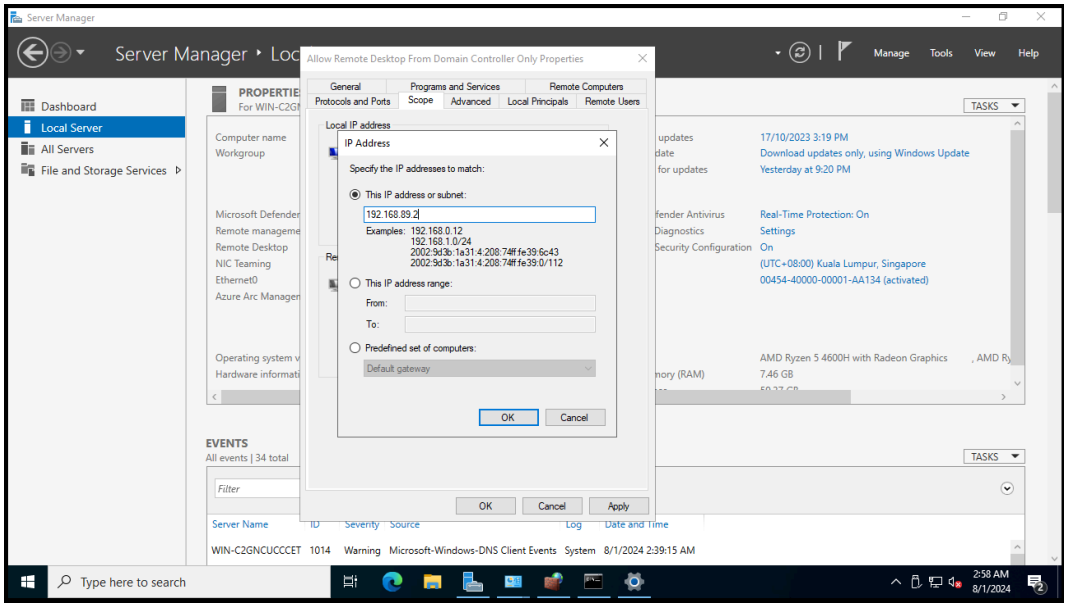


Figure 12 : Put remote IP address

Here we put the remote IP address that this rule applies to . Next click “OK”.

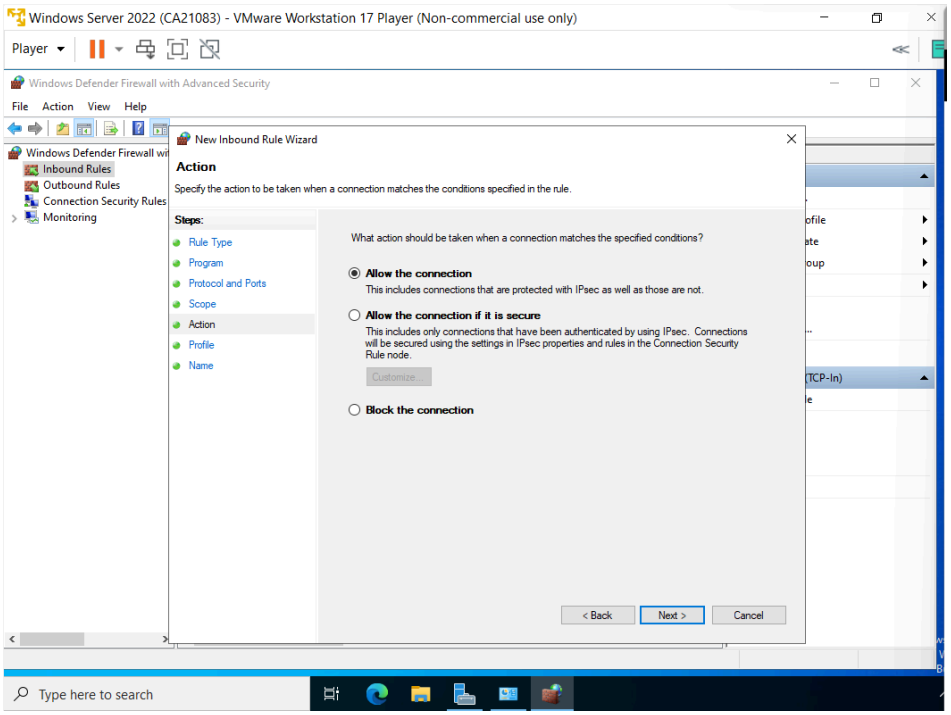


Figure 13 : Allow the connection

Here we will leave it on default and this allows the connection. Then click “next”.

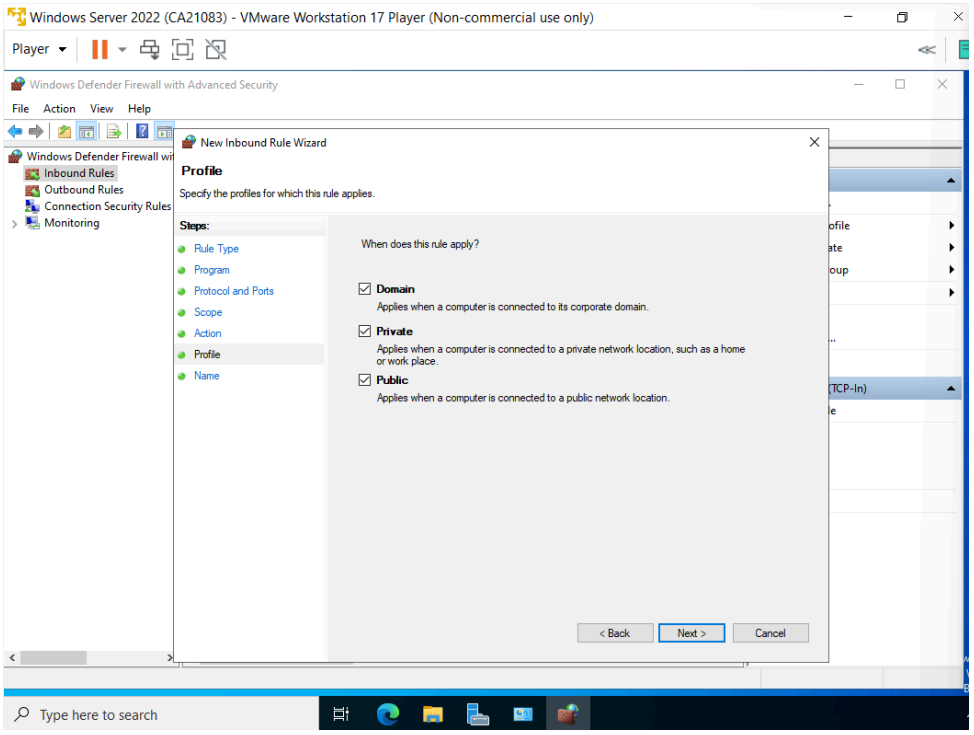


Figure 14 : When the rule apply to

Here we can select when this rule applies to . We will leave it by default and click “next”.

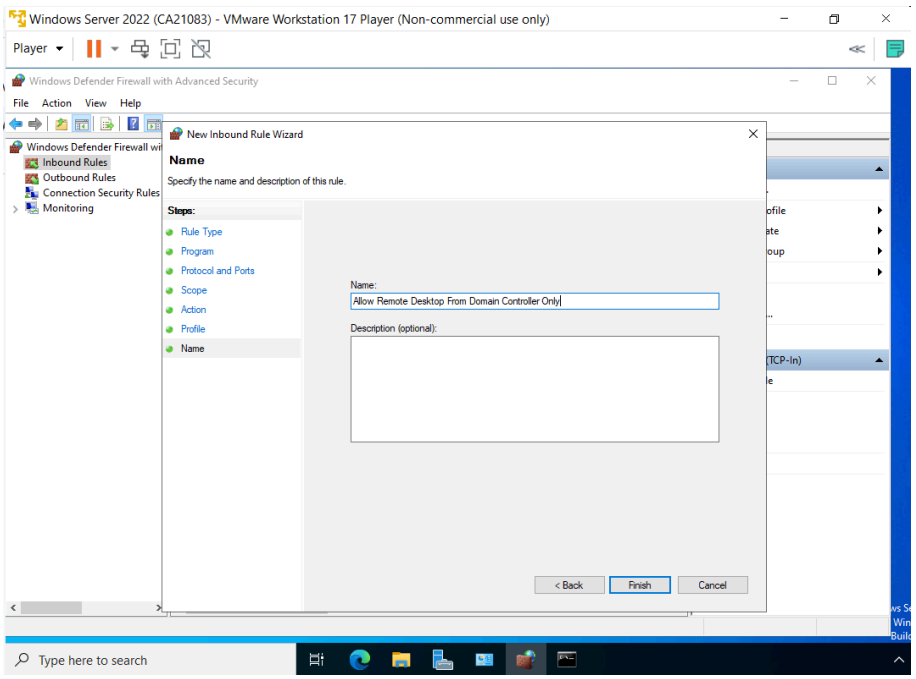


Figure 15 : Specify inbound rule name and description

In figure 15 , here we can specify the name and description for this inbound rule . Here we specify the name "Allow Remote Desktop From Domain Controller only". Next click on "Finish".

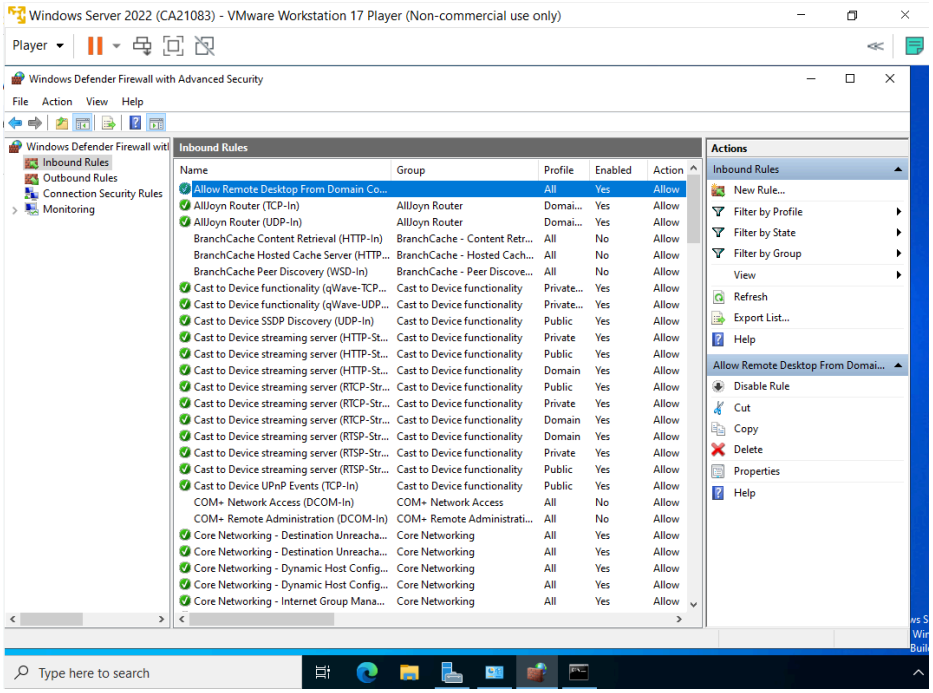


Figure 16 : Shows the new inbound rules

Figure 16 shows that the new rule will now show in the top of the inbound rules above all the default rules.

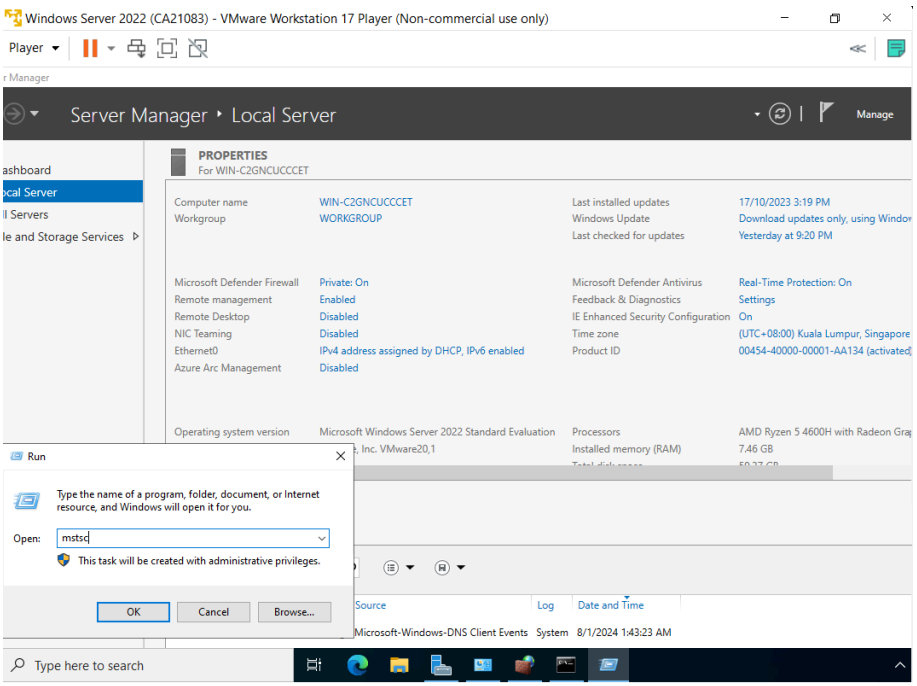


Figure 17 : Open remote desktop connection

Here we run the "mstsc" to open the remote desktop connection and click "OK"

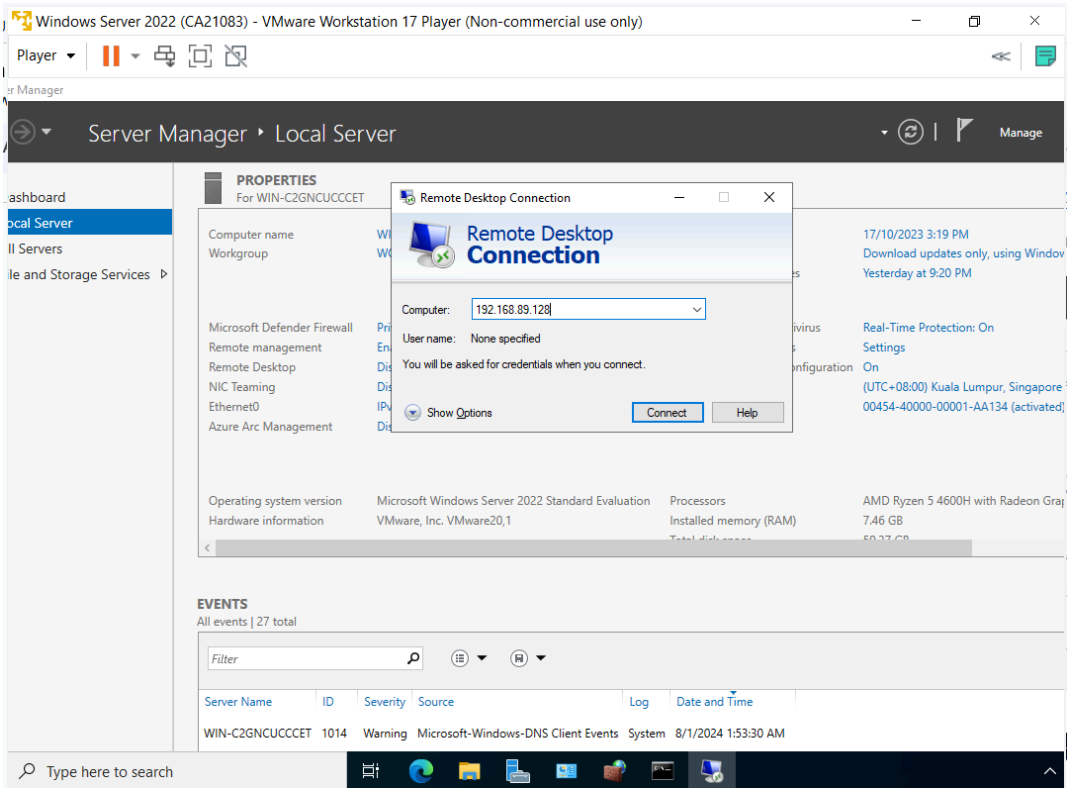


Figure 18 : Specify the member server IP address

Based on figure 18 we specify the IP address of our member server and click the “connect” button .

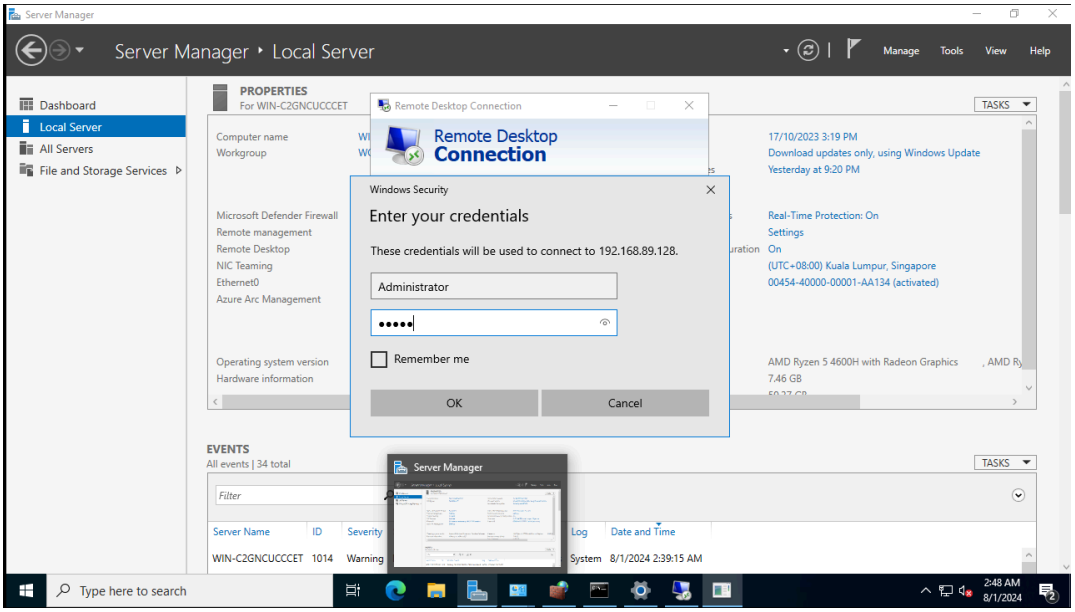


Figure 19 : Insert user password

In this figure we insert the user password .

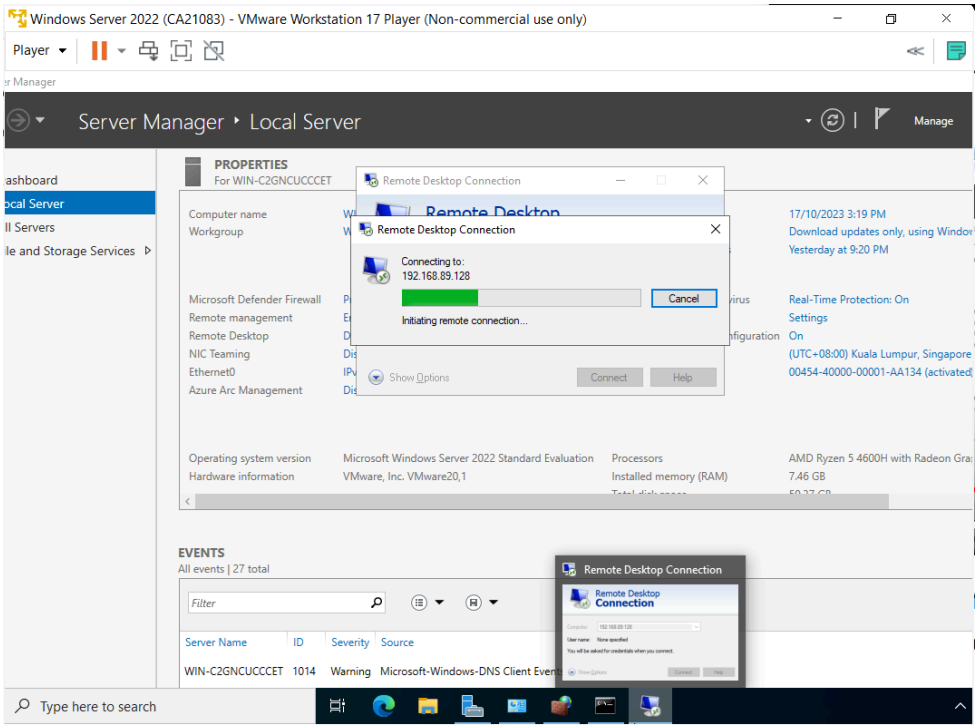


Figure 20 : Connect remote desktop

Here it will connect to the remote desktop .

Figure 21 : Open another member server windows

Figure 21 shows we go to another member server windows and login.

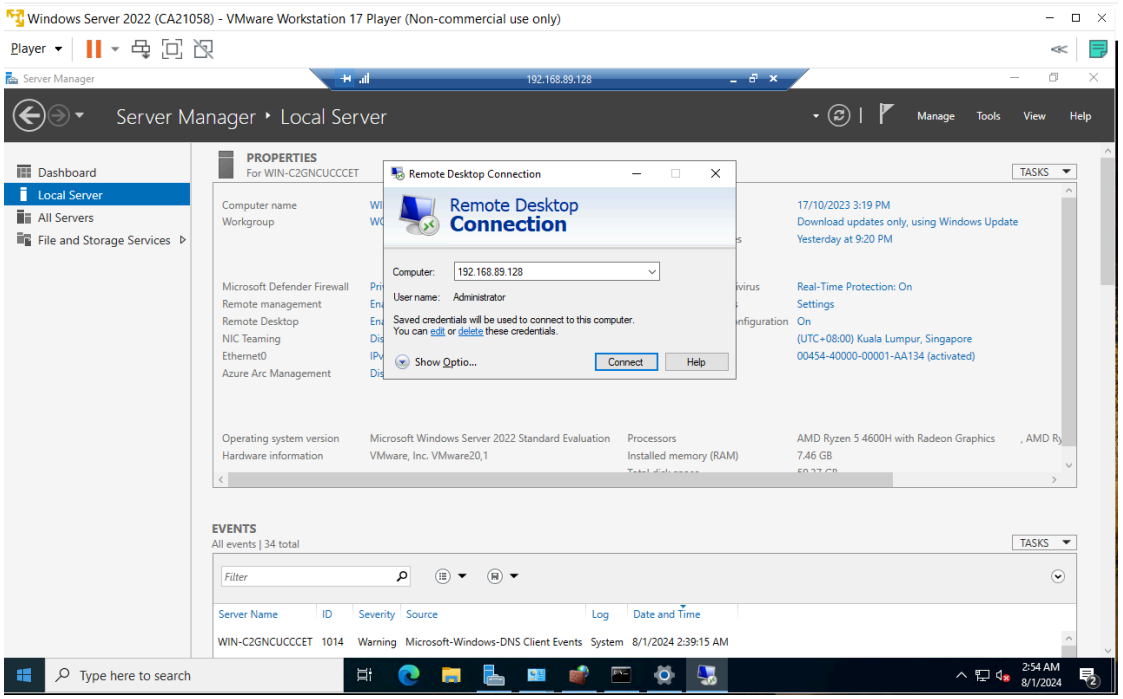
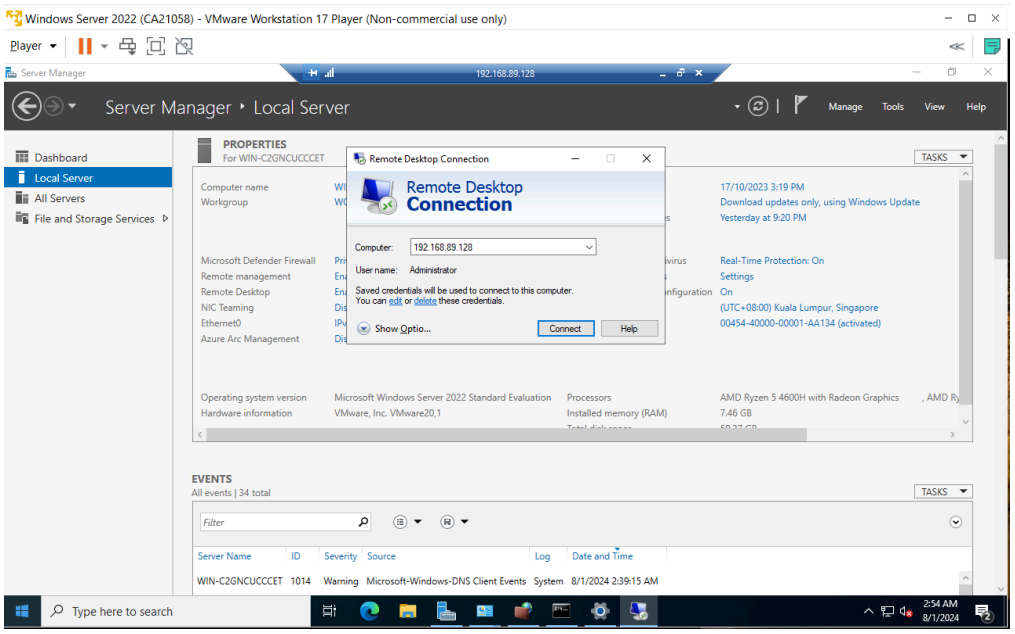


Figure 22 : Connect the remote desktop connection

Open remote desktop connection and put the member server IP Address to connect .

3.2 RESULT



Server successfully connected to the remote desktop connection. To achieve this user needs to create new inbound rules at the window defender firewall with advanced security. All the window firewall defender can do are:

Monitoring and Logging:

- Window defender firewall with advanced security can monitor and detect the logging activities to the server. By having these features, it will be easier to detect any potential security threat.

Rule-based Filtering:

- Rules that are both inbound and outbound can be created by administrators using a range of criteria, such as IP addresses, protocols, ports, and applications. This allows for exact control over the types of network traffic that are permitted and prohibited.

Notification and User interface:

- Administrators will get the notifications from the firewall about the blocked inbound connections and be able to personalize the user interface for controlling the firewall settings .

4.0 CONCLUSION

In summary, protecting vital digital assets, preserving operational continuity, and reducing the constant danger of cyberattacks all depend on the design and execution of strong server security measures. The complex interaction of network security protocols, encryption techniques, authentication methods, and access rules creates a strong barrier against unwanted access, data breaches, and service interruptions. Continuous server activity monitoring, logging, and analysis facilitates prompt security incident detection and response, enabling a proactive approach against ever-evolving threats.

One cannot stress the importance of patch management, regular updates, and a clear incident response plan since they enhance the flexibility and resilience of the server security system. Furthermore, the dedication to user education, compliance observance, and recurring security audits guarantees that the security posture stays strong and compliant with industry norms. A proactive culture combined with a group commitment to continuously develop results in a dynamic defense system that can quickly address new threats and changing attack methods.

A well-thought-out and well executed server security infrastructure is not only necessary, but also strategically crucial in an era where digital assets are essential to organizational success. To manage the complexity of the digital age with resilience and confidence, organizations need to stay attentive, continuously reevaluate their security postures, and cultivate a security-conscious culture as the threat landscape changes. The pursuit of server security excellence is ultimately a continuous commitment to safeguarding the availability, integrity, and confidentiality of critical data, assuring the long-term viability of contemporary businesses in the face of a constantly evolving cybersecurity environment.

5.0 REFERENCES

1. What is Server Security? | Glossary. (2024). Hpe.com. https://www.hpe.com/us/en/what-is/server-security.html#:~:text=Server%20security%20is%20of%20utmost%20importance%20for%20several%20reasons%3A&text=Protecting%20Data%3A%20Ensures%20confidentiality%2C%20integrity
2. *Tabletop Exercises: real life scenarios and best practices*. (2023, December 20). https://www.threatintelligence.com/blog/cyber-tabletop-exercise-example-scenarios
3. QAwerk US. (2023, December 19). *Insecure Design vulnerability: Explanation and examples | QAWerk*. QAwerk. https://qawerk.com/blog/insecure-design/
4. *61. Configure Windows Defender Firewall with Advanced Security | Server 2019*. (n.d.).https://www.youtube.com/watch?v=o4KXp9Wefbw
5. Darrington, J. (2023, August 2). Server Security: What it is and How to Implement It. Graylog. https://graylog.org/post/server-security-what-it-is-and-how-to-implement-it/#:~:text=To%20protect%20sensitive%20information%2C%20you