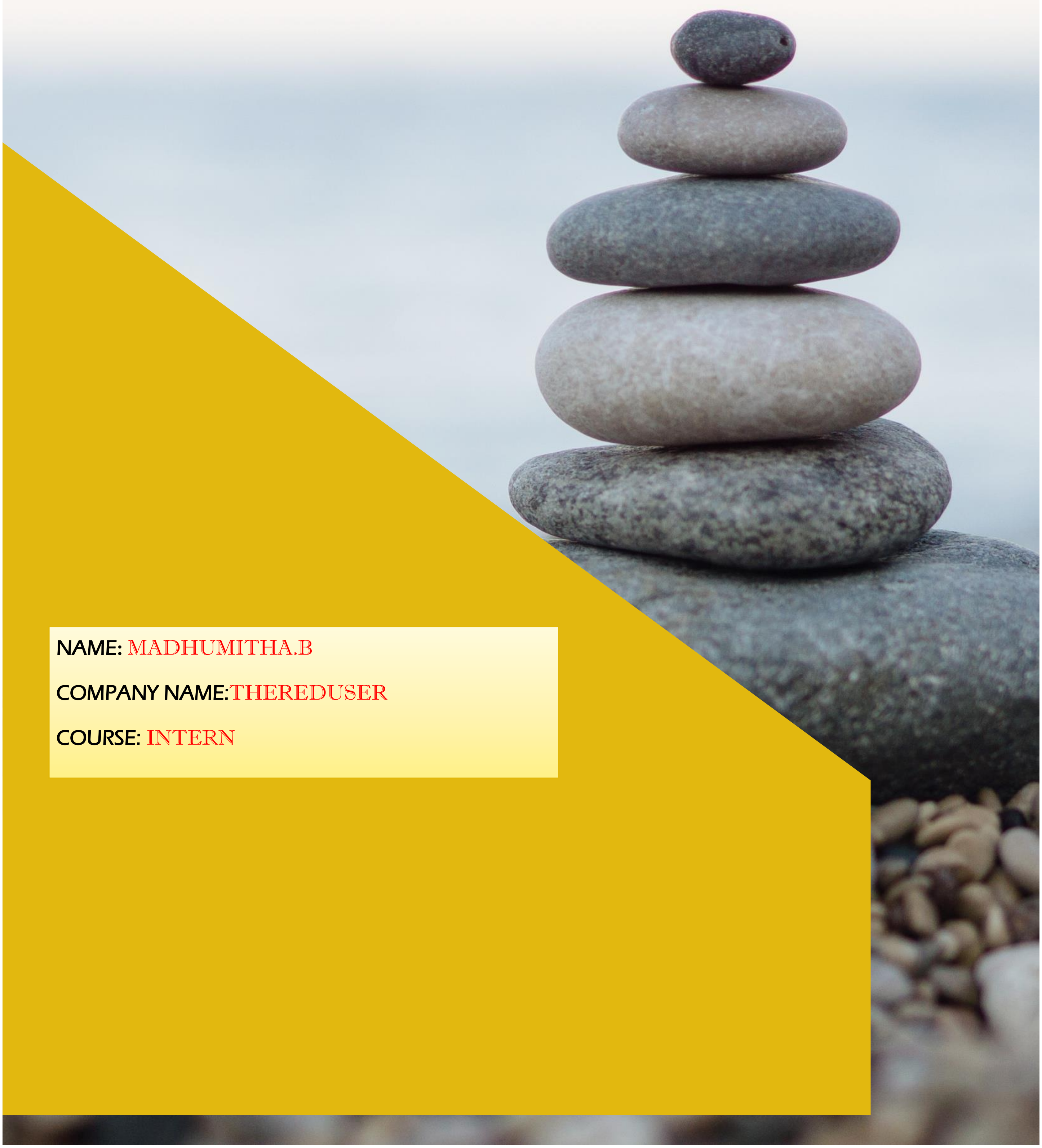
THEREDUSER CYBER INTERN

TASK 1: INTRODUCTION TO NETWORK SECURITY BASICS



NAME: MADHUMITHA.B

COMPANY NAME:THEREDUSER

COURSE: INTERN

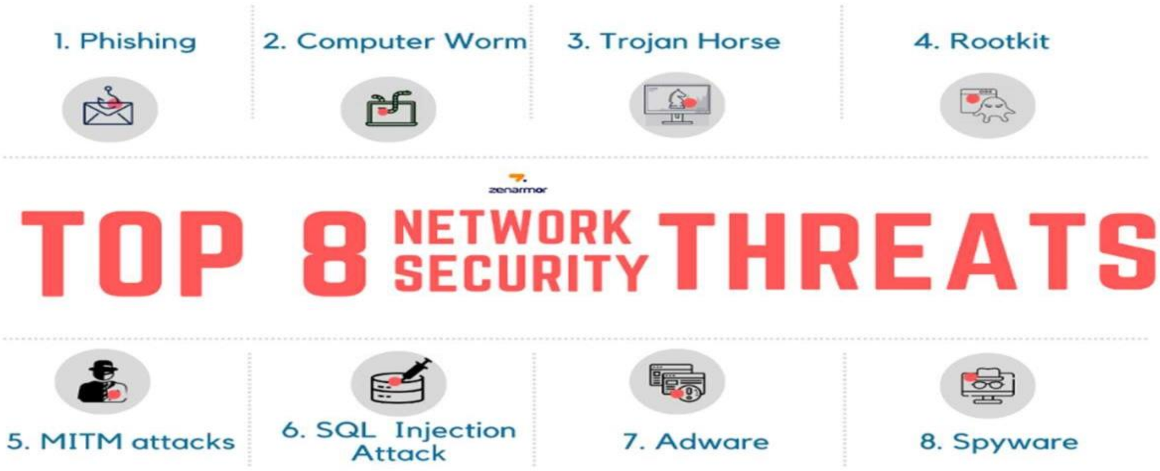
The Red Users: Internship Task 1

Different types of Network Threats

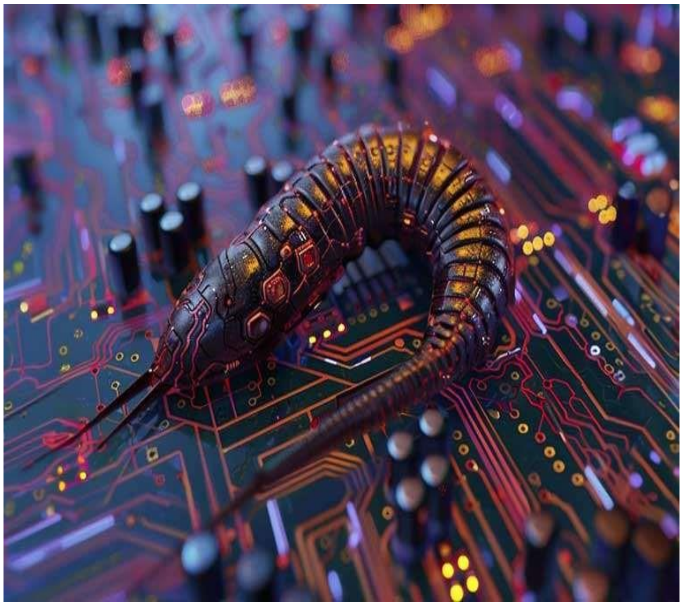
What are Network Threats?

- Let us suppose that, a group of people are connected to a network, i.e. a public WIFI, everything is fine until there is a malicious threat actor entering into the network, If I am using the public WIFI and sending some important files to an official and this threat actor may compromise the network through different methods and will gain access to the file and may tamper the file and send the malicious file to the destination, this total process can be said as Network threat, more simply a network which is under threat by an intelligent hacker.

Types of Network Threats



COMPUTER WORM



A computer worm is a type of malicious software (malware) that self-replicates and spreads across networks without the need for human intervention. Unlike viruses, which require a host file or user action to spread, worms are standalone programs that actively seek out networked computers to infect, spreading through vulnerabilities in systems or through network connections.

Prevention

1. **Keep Software Updated**: Regular updates and patches close vulnerabilities that worms may exploit.
2. **Use Strong Antivirus Software**: Quality antivirus software can detect and block worms before they spread.
3. **Firewalls**: Configuring firewalls can prevent unauthorized access and restrict worm propagation.

PHISHING

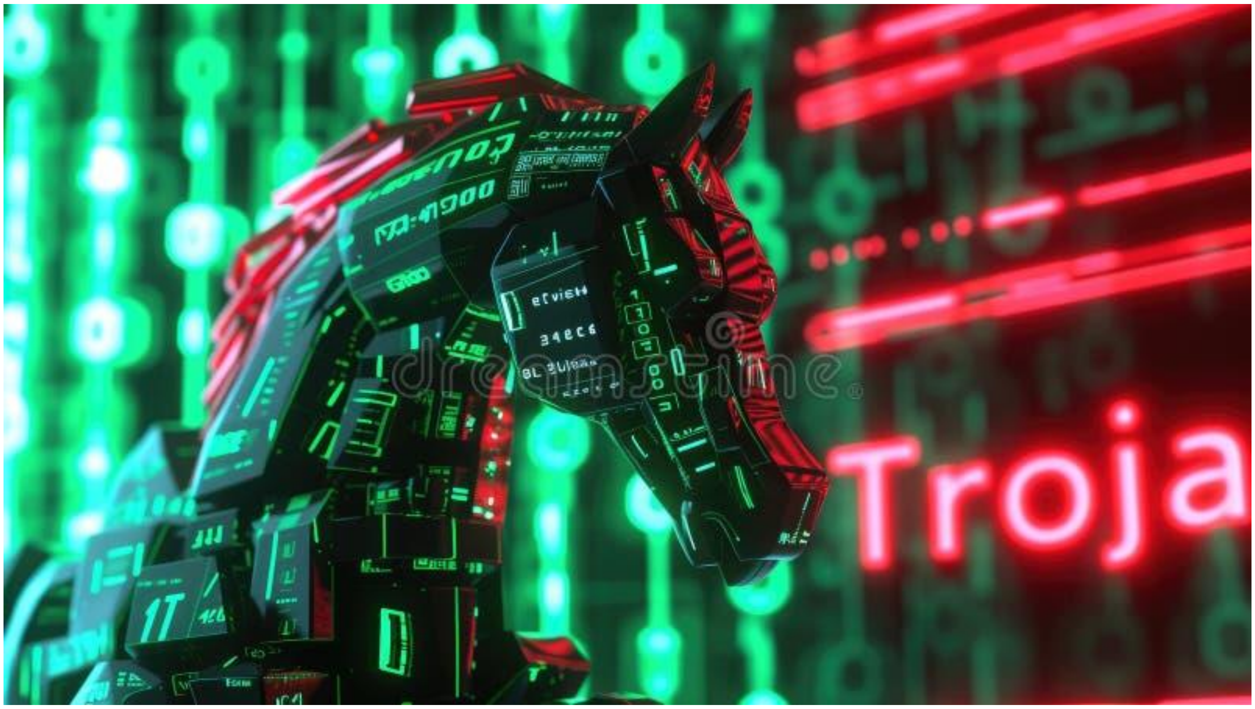
Phishing is a form of cyberattack where attackers impersonate a trusted entity to deceive individuals into revealing sensitive information, such as usernames, passwords, credit card details, or other personal data. Phishing attacks typically occur via email, text messages, or malicious websites that look legitimate, convincing users to click on malicious links, download malware, or provide sensitive information directly.

Common Types of Phishing

- **Email Phishing**: The most common type, where attackers send fraudulent emails with malicious links or attachments.
- **Spear Phishing**: Targeted phishing attacks aimed at specific individuals or organizations using personalized information to increase credibility.
- **Smishing and Vishing**: Smishing involves SMS messages, while vishing uses voice calls to trick victims into sharing sensitive data.
-

How to Protect Against Phishing

1. **Verify the Source**: Always check the sender's email address and hover over links to verify their destination.
2. **Be Cautious with Attachments and Links**: Avoid clicking on links or downloading attachments from unknown or unsolicited messages.
3. **Enable Multi-Factor Authentication (MFA)**: MFA adds an additional layer of security, making it harder for attackers to access accounts even with stolen credentials.
4. **Keep Security Software Updated**: Modern antivirus and anti-malware programs can detect phishing attempts and block malicious websites.
5. **Educate and Stay Informed**: Regularly educate yourself and others about phishing techniques to stay vigilant against new tactics.



A Trojan horse, often just called a "Trojan," is a type of malicious software (malware) that disguises itself as legitimate software to trick users into installing it. Named after the ancient Greek story of the deceptive wooden horse used to infiltrate Troy, a Trojan masquerades as a harmless or useful program but, once installed, can give attackers unauthorized access to a system, enabling them to steal data, install additional malware, or control the device remotely.

Common Types of Trojans

- **Backdoor Trojans**: Allow attackers to remotely control the system, often to steal data or install other malicious software.
- **Banking Trojans**: Specifically target banking information by capturing sensitive data like login credentials.
- **Spyware Trojans**: Monitor user activities, such as keystrokes, screenshots, and browsing history, to gather sensitive information.
- **Ransomware Trojans**: Encrypt files on the system and demand payment (ransom) to decrypt them.

Preventing Trojan Horse Infections

- **Download Software from Trusted Sources**: Avoid downloading software from unverified or third-party websites.
- **Use Strong Security Software**: Regular antivirus and anti-malware software can help detect and block Trojans before they are installed.
- **Stay Wary of Phishing Emails**: Avoid opening attachments or links in emails from unknown sources, as these may contain Trojans.

- **Keep Software Updated**: Regular updates ensure security patches are applied, reducing the chances of Trojans exploiting vulnerabilities.

MITM attack

A Man-in-the-Middle (MITM) attack is a cybersecurity threat where an attacker secretly intercepts and potentially alters the communication between two parties who believe they are directly communicating with each other. By positioning themselves in the middle of the interaction, the attacker can eavesdrop on sensitive information, like login credentials, personal data, or financial information, or manipulate the data being transmitted.

How MITM Attacks Work

In a typical MITM attack, the attacker intercepts the data exchange by impersonating each party to the other. For instance, in a public Wi-Fi setting, an attacker could set up a fake network with a name similar to the legitimate one. Once users connect to this fake network, the attacker gains access to the data flowing between users and any sites or services they interact with.

Common Techniques for MITM Attacks

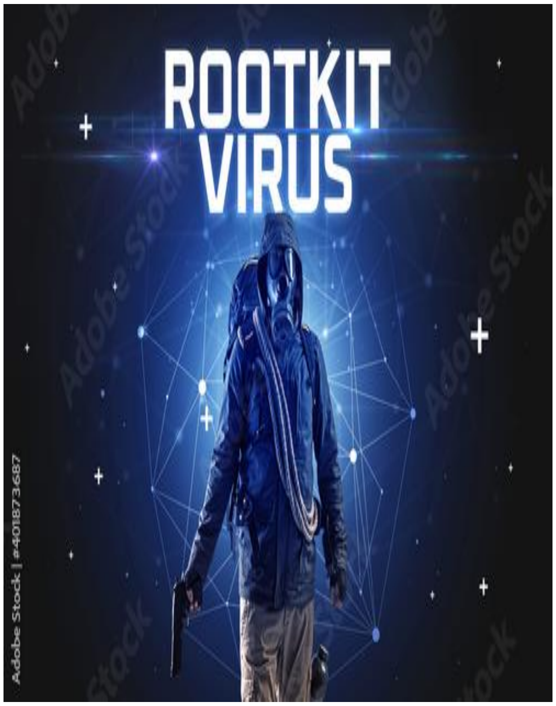
- **Spoofing**: An attacker pretends to be a trusted entity to intercept communications.
- **Session Hijacking**: An attacker steals session tokens to gain access to a user's authenticated session.
- **Packet Injection**: The attacker intercepts network packets and inserts malicious ones into the communication.

- **SSL Stripping**: This technique downgrades a secure HTTPS connection to HTTP, making data easier to intercept.

How to Prevent MITM Attacks

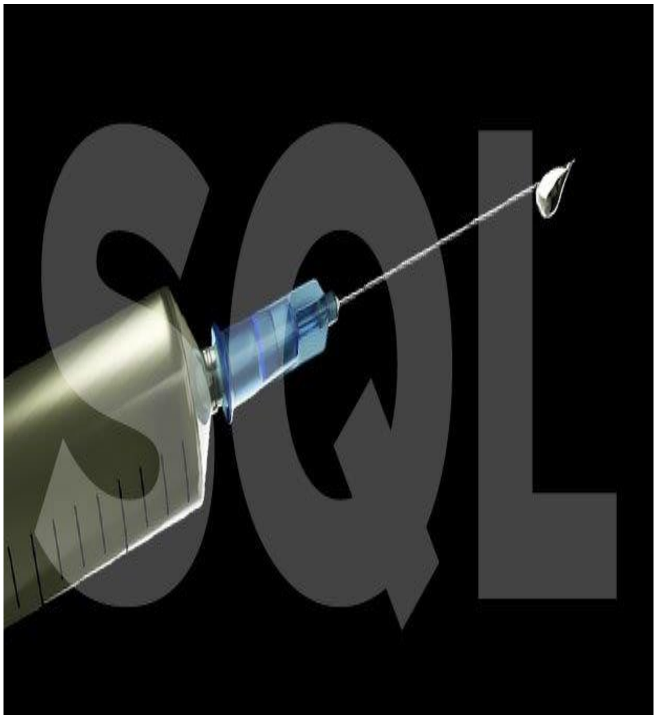
- **Use Encryption**: Strong encryption like HTTPS for websites and VPNs for secure network connections helps prevent unauthorized interception.
- **Authentication**: Implementing multi-factor authentication (MFA) adds a layer of security, making it harder for attackers to gain unauthorized access.
- **Secure Wi-Fi Networks**: Avoiding open or unsecured Wi-Fi networks can minimize the risk of falling victim to MITM attacks.
- **Certificate Pinning**: This technique ensures that clients recognize and accept only a specific certificate, preventing interception by an attacker with a fake certificate.

ROOTKIT



- A rootkit is a type of malicious software designed to gain unauthorized access to a computer system while concealing its presence from the user and security software.
- Rootkits typically enable attackers to take control of a system at the most privileged level, often allowing them to manipulate or monitor the system without detection.
- They are often used to hide other types of malware, like keyloggers or viruses, making it difficult to detect and remove them.
- Rootkits can be installed by exploiting system vulnerabilities, or they may be unknowingly installed by users when downloading infected software.
- Once installed, they modify core operating system components, enabling attackers to intercept and alter system operations and hide files or processes from detection tools.
- There are different types of rootkits, including kernel-level rootkits (which target the operating system's core) and user-mode rootkits (which work at the application level).

SQL INJECTION



- SQL injection is a cybersecurity vulnerability where attackers inject malicious SQL code into a database query, typically through user input fields that aren't properly secured.
- By manipulating the query, attackers can access or modify sensitive data, execute unauthorized commands, and potentially control the database.
- SQL injection occurs when an application fails to sanitize user inputs, allowing attackers to bypass security measures and perform actions such as bypassing login authentication, extracting sensitive data, or even deleting records.
- Preventing SQL injection involves practices like using parameterized queries, input validation, stored procedures, and implementing the principle of least privilege.

ADWARE

Adware is a type of software designed to display unwanted advertisements on a user's device, often in the form of pop-ups, banners, or redirects. While some adware programs are legitimate and provide free software in exchange for showing ads, malicious adware is often installed without user consent and can collect data, slow down devices, and cause significant annoyance.

Preventing and Removing Adware

1. **Download Software from Trusted Sources**: Avoid downloading software from untrusted websites, as adware often hides in free or pirated downloads.

2. **Read Installation Prompts Carefully**: Many adware programs are installed through "optional" add-ons; choose custom installation to avoid extra unwanted software.

UNDERSTANDING FIREWALLS, ENCRYPTION AND SECURE NETWORK CONFIGURATIONS

A **firewall** is a security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks (such as the Internet).

Types of Firewalls:

- **Packet-Filtering Firewalls**: Examine packets and allow or block them based on source and destination IP addresses, ports, and protocols.
- **Stateful Inspection Firewalls**: Track the state of active connections and make decisions based on the context of traffic.
- **Proxy Firewalls**: Act as intermediaries for requests from clients seeking resources from servers. They can filter traffic and provide additional security.
- **Next-Generation Firewalls (NGFW)**: Include features such as deep packet inspection, intrusion prevention systems (IPS), and application awareness.

Configuring Firewalls:

1. **Define Security Policies**: Create rules for allowed and denied traffic based on your organization's needs.
2. **Regular Updates**: Keep the firewall firmware and software up to date to protect against vulnerabilities.
3. **Monitor Logs**: Regularly review logs for unusual activity or potential security breaches.

2. Encryption

Encryption is the process of converting data into a coded format to prevent unauthorized access. Only those with the correct decryption key can access the original data.

Types of Encryption:

- **Symmetric Encryption**: Uses the same key for both encryption and decryption (e.g., AES, DES). It's fast but requires secure key management.
- **Asymmetric Encryption**: Uses a pair of keys (public and private). The public key encrypts the data, and the private key decrypts it (e.g., RSA, ECC). It's slower but enhances security for key exchange.
- **Hashing**: Converts data into a fixed-size string of characters, which is typically a digest (e.g., SHA-256). It’s one-way and used for data integrity verification.

Best Practices for Encryption:

1. **Use Strong Algorithms**: Choose robust encryption standards (e.g., AES-256) to ensure data security.
2. **Encrypt Data at Rest and in Transit**: Protect sensitive data stored on devices and during transmission over networks.
3. **Secure Key Management**: Store encryption keys securely and restrict access to authorized users only.

3. Secure Network Configurations

Secure network configurations involve setting up and managing network devices to minimize vulnerabilities and protect against attacks.

Key Elements of Secure Network Configurations:

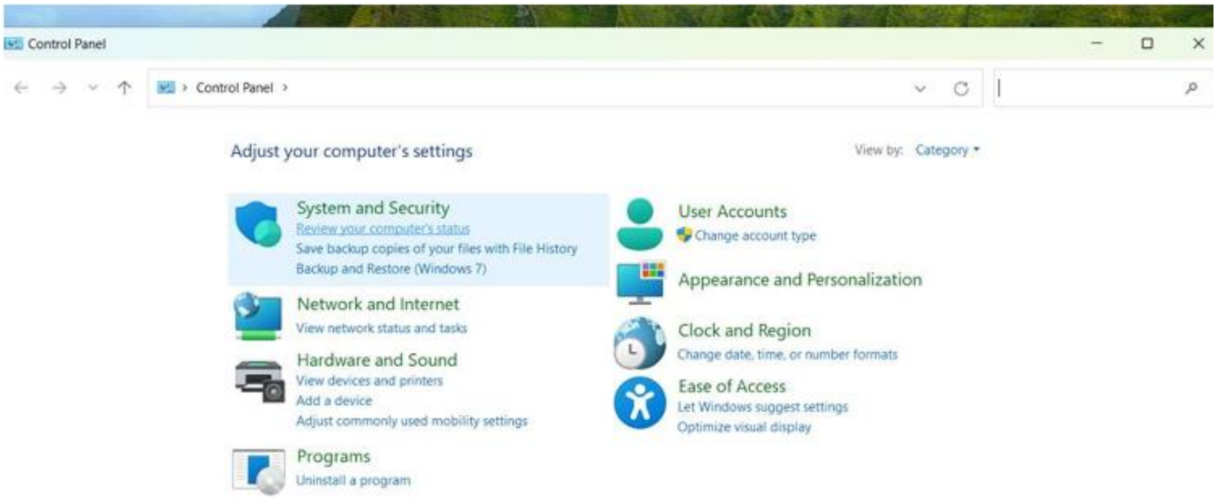
- **Change Default Settings**: Modify default usernames, passwords, and settings on routers, switches, and other devices.
- **Network Segmentation**: Divide a network into smaller segments to limit access and contain potential breaches (e.g., using VLANs).
- **Implement Access Control**: Use tools like Role-Based Access Control (RBAC) to restrict access to sensitive resources based on user roles.
- **Regular Audits and Updates**: Conduct periodic audits of network configurations and ensure all devices are updated with the latest security patches.
- **Use VPNs**: Implement Virtual Private Networks to secure remote access and encrypt data traveling over public networks.
- **Disable Unused Services and Ports**: Turn off unnecessary services and close unused ports to reduce the attack surface.

Conclusion

Understanding and implementing firewalls, encryption, and secure network configurations are critical components of network security. By employing these practices, organizations can better protect their data and infrastructure from unauthorized access and cyber threats.

We will see how to implement advanced security rules in windows to be more secured.

- ➤ **Click on control panel**



Control Panel

Control Panel ›

Adjust your computer's settings

View by: Category ▾

System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)

Network and Internet
View network status and tasks

Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings

Programs
Uninstall a program

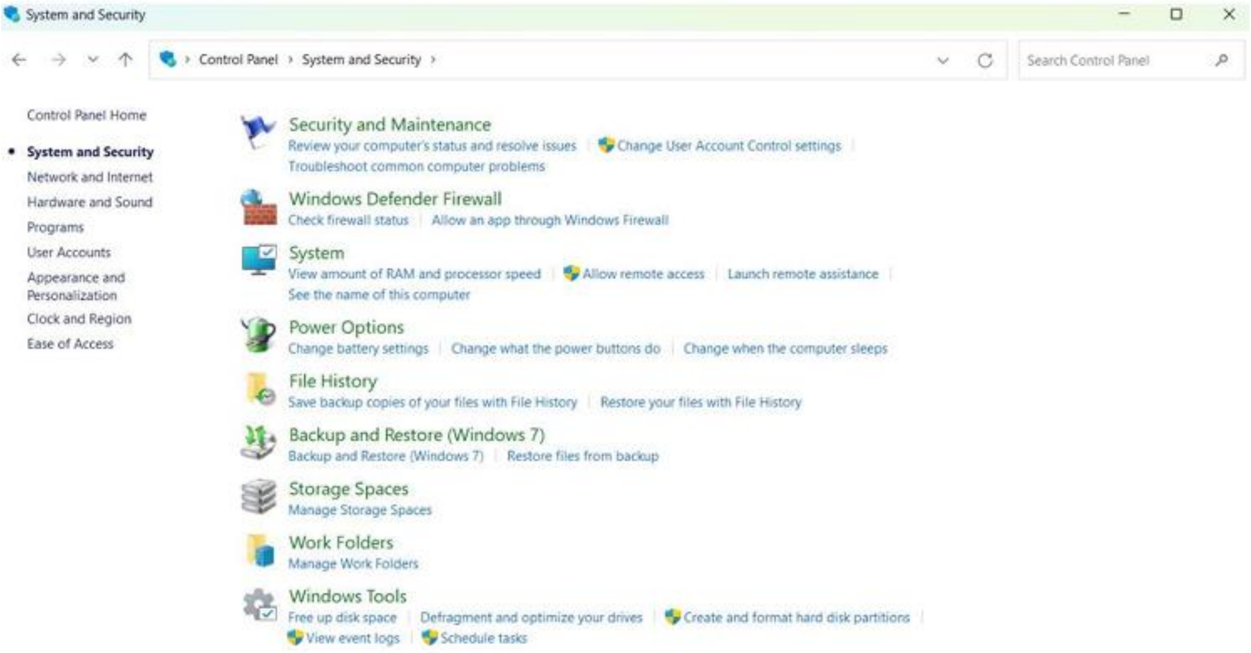
User Accounts
Change account type

Appearance and Personalization

Clock and Region
Change date, time, or number formats

Ease of Access
Let Windows suggest settings
Optimize visual display

- ➤ **Click system and security**



System and Security

Control Panel › System and Security ›

Search Control Panel

Control Panel Home
- System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access

Security and Maintenance
Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems

Windows Defender Firewall
Check firewall status | Allow an app through Windows Firewall

System
View amount of RAM and processor speed | Allow remote access | Launch remote assistance | See the name of this computer

Power Options
Change battery settings | Change what the power buttons do | Change when the computer sleeps

File History
Save backup copies of your files with File History | Restore your files with File History

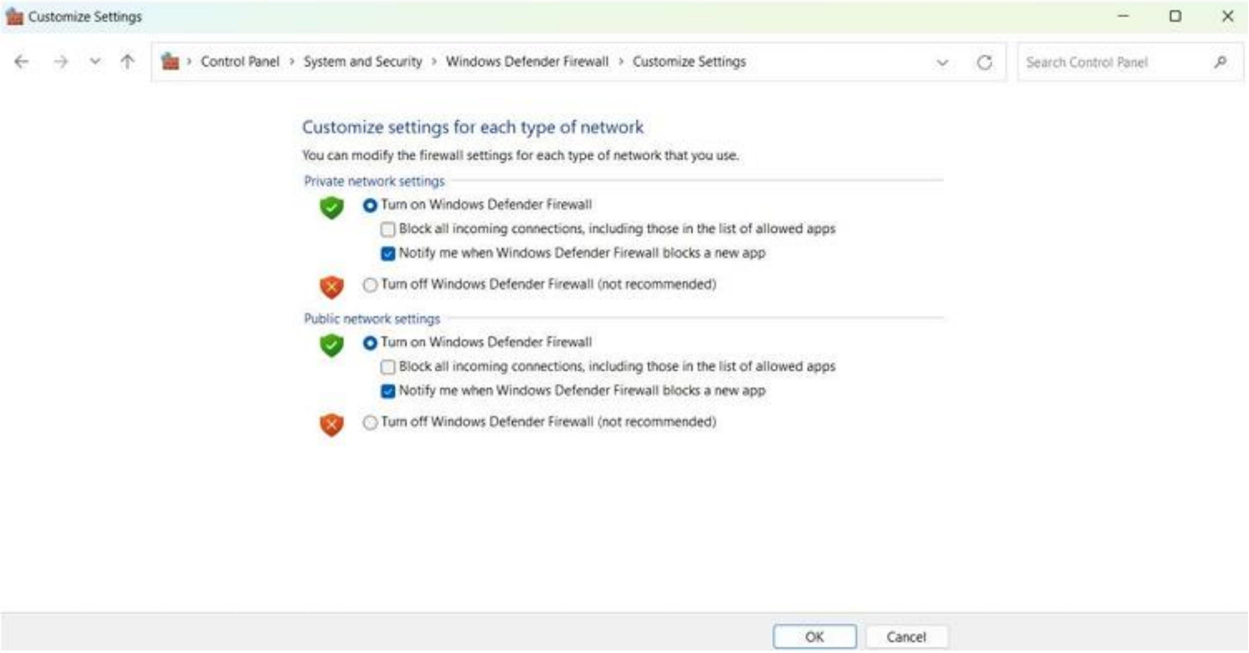
Backup and Restore (Windows 7)
Backup and Restore (Windows 7) | Restore files from backup

Storage Spaces
Manage Storage Spaces

Work Folders
Manage Work Folders

Windows Tools
Free up disk space | Defragment and optimize your drives | Create and format hard disk partitions | View event logs | Schedule tasks

- **click on windows defender firewall**


Customize Settings
Control Panel › System and Security › Windows Defender Firewall › Customize Settings
Search Control Panel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

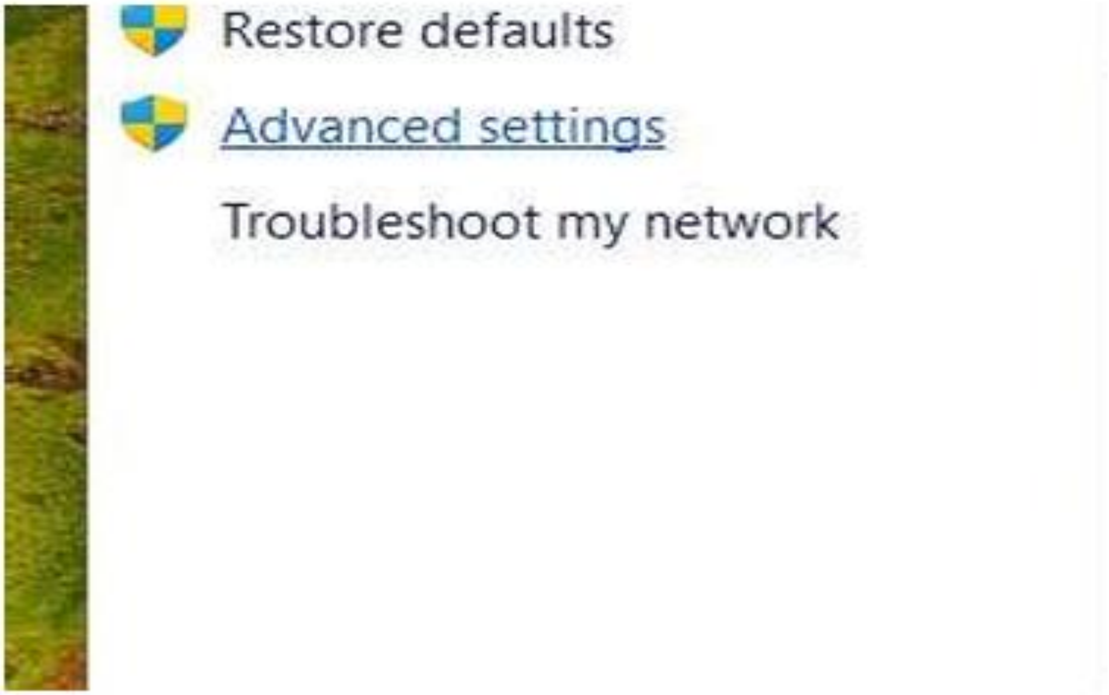
☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

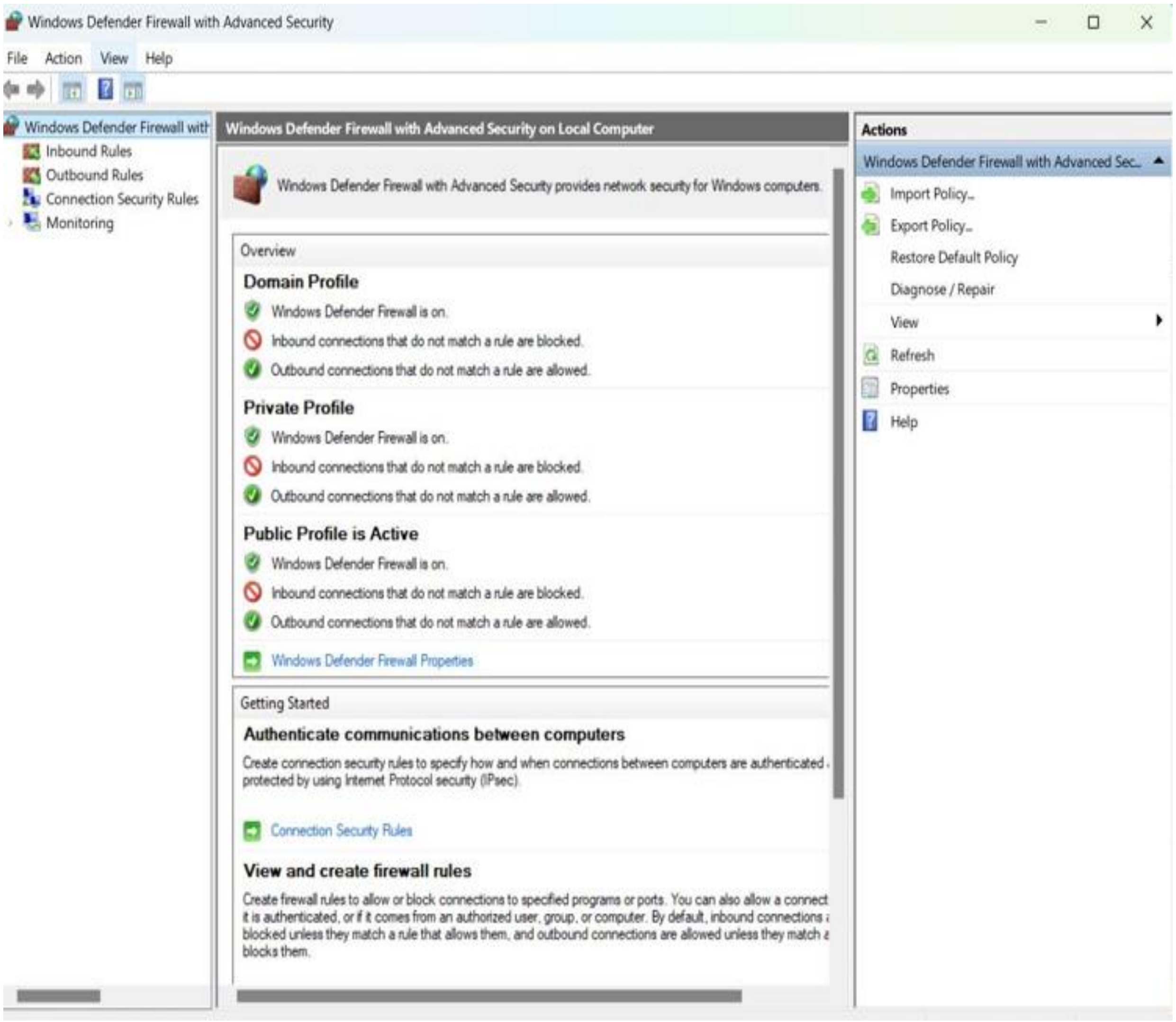
When you click on windows fire wall turn on and off option on you will see the above screen, the firewall is on and it working perfectly.

Now this firewall run on some rules, we can edit and create rules of oncoming requests and also the outgoing requests.

- **For that go back and click on advanced settings**



- When you click on advanced settings, we will see the below page


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Actions
Windows Defender Firewall with Advanced Sec...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

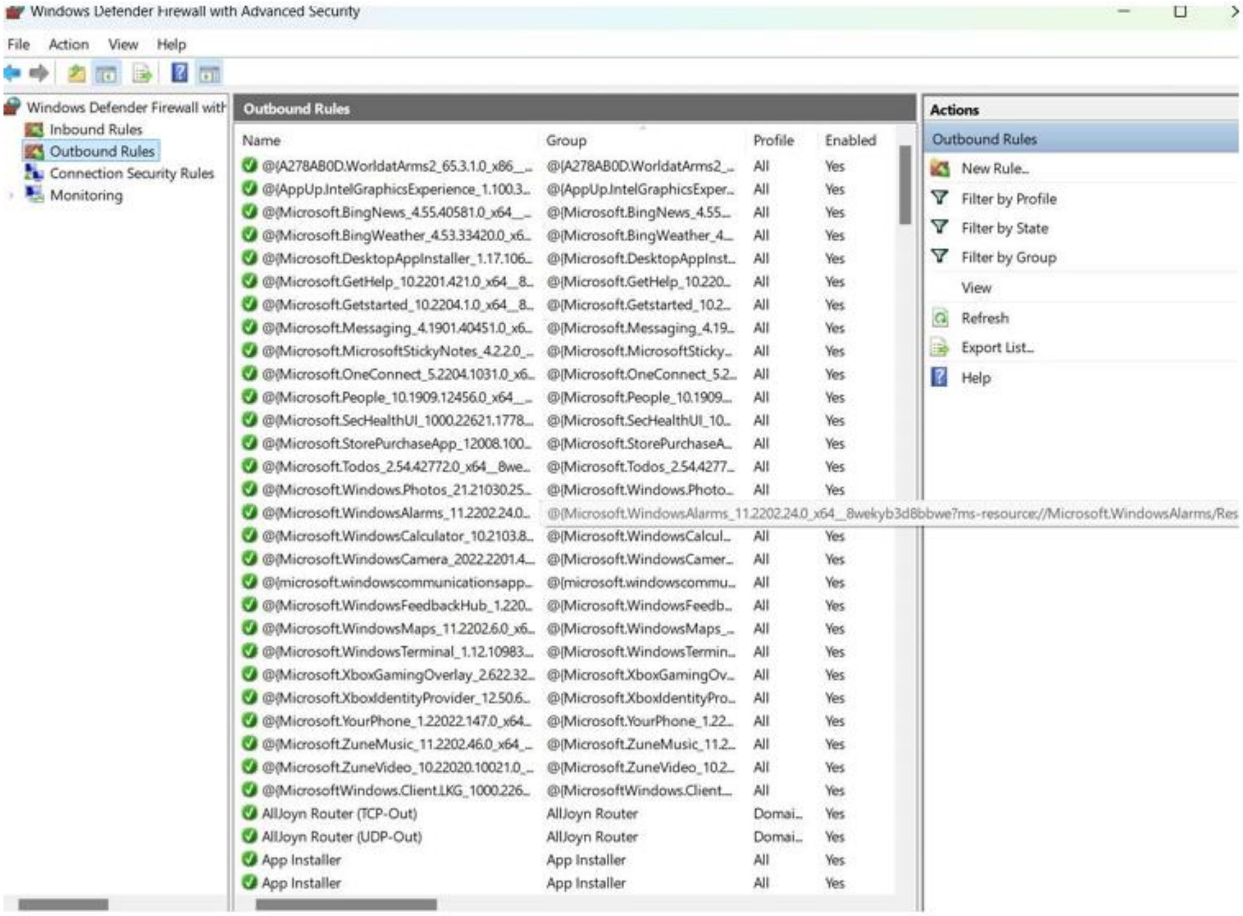
Create connection security rules to specify how and when connections between computers are authenticated protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connect it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections blocked unless they match a rule that allows them, and outbound connections are allowed unless they match blocks them.

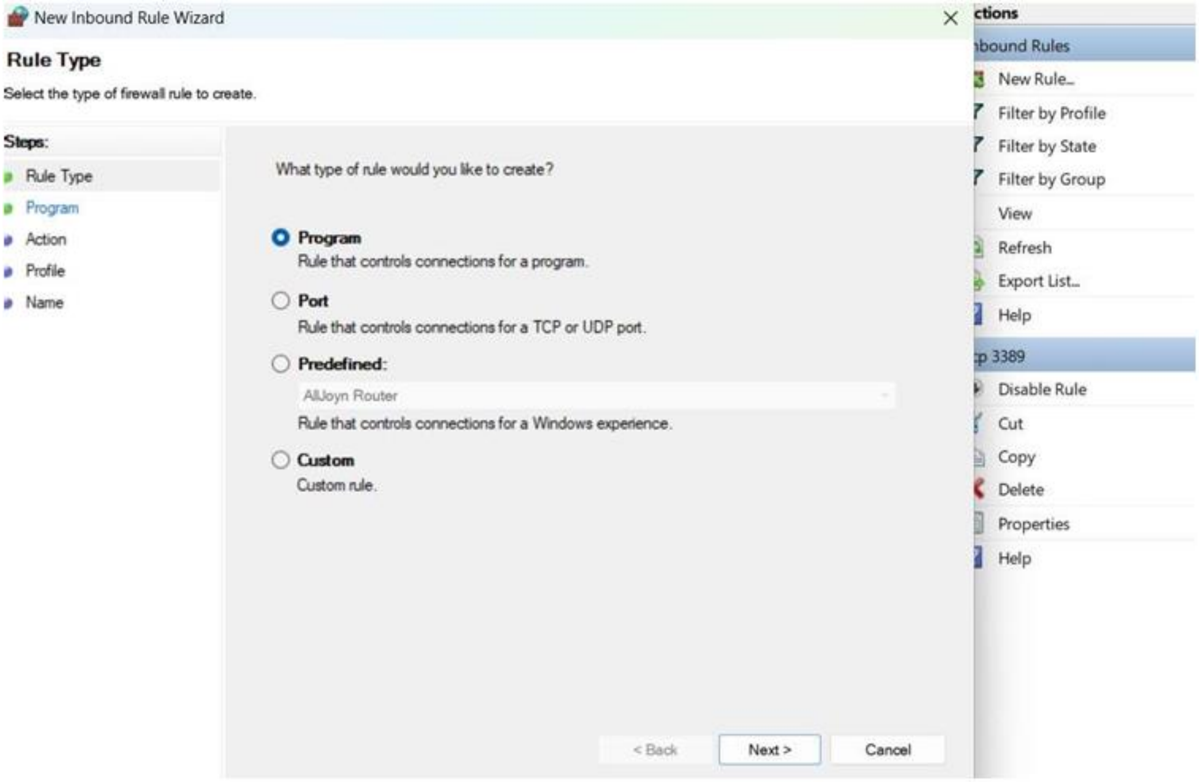
- Now, as you can see on the left there are 2 options inbound rules and outbound rules, also you can import policy and export policy in the system as shown in the right.
- I will just show you how to create an outbound rule in this project and you can try it for inbound rule.



Outbound Rules

Name	Group	Profile	Enabled
✓ @{A278AB0D.WorldatArms2_65.3.1.0_x86__...	@{A278AB0D.WorldatArms2_...	All	Yes
✓ @{AppUp.IntelGraphicsExperience_1.100.3...	@{AppUp.IntelGraphicsExper...	All	Yes
✓ @{Microsoft.BingNews_4.55.40581.0_x64__...	@{Microsoft.BingNews_4.55...	All	Yes
✓ @{Microsoft.BingWeather_4.53.33420.0_x6...	@{Microsoft.BingWeather_4...	All	Yes
✓ @{Microsoft.DesktopAppInstaller_1.17.106...	@{Microsoft.DesktopAppInst...	All	Yes
✓ @{Microsoft.GetHelp_10.2201.421.0_x64__8...	@{Microsoft.GetHelp_10.220...	All	Yes
✓ @{Microsoft.Getstarted_10.2204.1.0_x64__8...	@{Microsoft.Getstarted_10.2...	All	Yes
✓ @{Microsoft.Messaging_4.1901.40451.0_x6...	@{Microsoft.Messaging_4.19...	All	Yes
✓ @{Microsoft.MicrosoftStickyNotes_4.2.2.0_...	@{Microsoft.MicrosoftSticky...	All	Yes
✓ @{Microsoft.OneConnect_5.2204.1031.0_x6...	@{Microsoft.OneConnect_5.2...	All	Yes
✓ @{Microsoft.People_10.1909.12456.0_x64__...	@{Microsoft.People_10.1909...	All	Yes
✓ @{Microsoft.SecHealthUI_1000.22621.1778...	@{Microsoft.SecHealthUI_10...	All	Yes
✓ @{Microsoft.StorePurchaseApp_12008.100...	@{Microsoft.StorePurchaseA...	All	Yes
✓ @{Microsoft.Todos_2.54.42772.0_x64__8we...	@{Microsoft.Todos_2.54.4277...	All	Yes
✓ @{Microsoft.Windows.Photos_21.21030.25...	@{Microsoft.Windows.Photo...	All	Yes
✓ @{Microsoft.WindowsAlarms_11.2202.24.0...	@{Microsoft.WindowsAlarms_11.2202.24.0_x64__8wekyb3d8bbwe?ms-resource://Microsoft.WindowsAlarms/Res		
✓ @{Microsoft.WindowsCalculator_10.2103.8...	@{Microsoft.WindowsCalcul...	All	Yes
✓ @{Microsoft.WindowsCamera_2022.2201.4...	@{Microsoft.WindowsCamer...	All	Yes
✓ @{microsoft.windowscommunicationsapp...	@{microsoft.windowscommu...	All	Yes
✓ @{Microsoft.WindowsFeedbackHub_1.220...	@{Microsoft.WindowsFeedb...	All	Yes
✓ @{Microsoft.WindowsMaps_11.2202.6.0_x6...	@{Microsoft.WindowsMaps_...	All	Yes
✓ @{Microsoft.WindowsTerminal_1.12.10983...	@{Microsoft.WindowsTermin...	All	Yes
✓ @{Microsoft.XboxGamingOverlay_2.622.32...	@{Microsoft.XboxGamingOv...	All	Yes
✓ @{Microsoft.XboxIdentityProvider_12.50.6...	@{Microsoft.XboxIdentityPro...	All	Yes
✓ @{Microsoft.YourPhone_1.22022.147.0_x64...	@{Microsoft.YourPhone_1.22...	All	Yes
✓ @{Microsoft.ZuneMusic_11.2202.46.0_x64_...	@{Microsoft.ZuneMusic_11.2...	All	Yes
✓ @{Microsoft.ZuneVideo_10.22020.10021.0_...	@{Microsoft.ZuneVideo_10.2...	All	Yes
✓ @{MicrosoftWindows.Client.LKG_1000.226...	@{MicrosoftWindows.Client...	All	Yes
✓ AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes
✓ AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes
✓ App Installer	App Installer	All	Yes
✓ App Installer	App Installer	All	Yes

- **Click on new rule, shown in the right side and you will see the following**



Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Program
- Action
- Profile
- Name

What type of rule would you like to create?

● **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

When you click on "New Rule" in the Advanced Windows Firewall setings, you're presented with a series of options to define the specific criteria for the rule. The "Rule Type" option is the first step in this process.

- **Inbound Rules**
- Program: This option allows you to create a rule based on a specific application or process. You can select a program from a list or browse for it.
- Port: This option allows you to create a rule based on a specific port number. You can enter a port number or select a predefined service.
- Custom: This option provides the most flexibility and allows you to define multiple criteria, such as program, port, remote IP address, and protocol.
- **Outbound Rules**
  - Program: Similar to inbound rules, this op on allows you to create a rule based on a specific application or process.
  - Port: Similar to inbound rules, this option allows you to create a rule based on a specific port number.
  - Custom: Similar to inbound rules, this option provides the most flexibility and allows you to define multiple criteria.

Once you've selected a rule type, you'll be guided through a series of steps to define the specific criteria for the rule.

These steps may vary depending on the rule type you've chosen. For example, if you select the "Program" rule type, you'll be asked to:

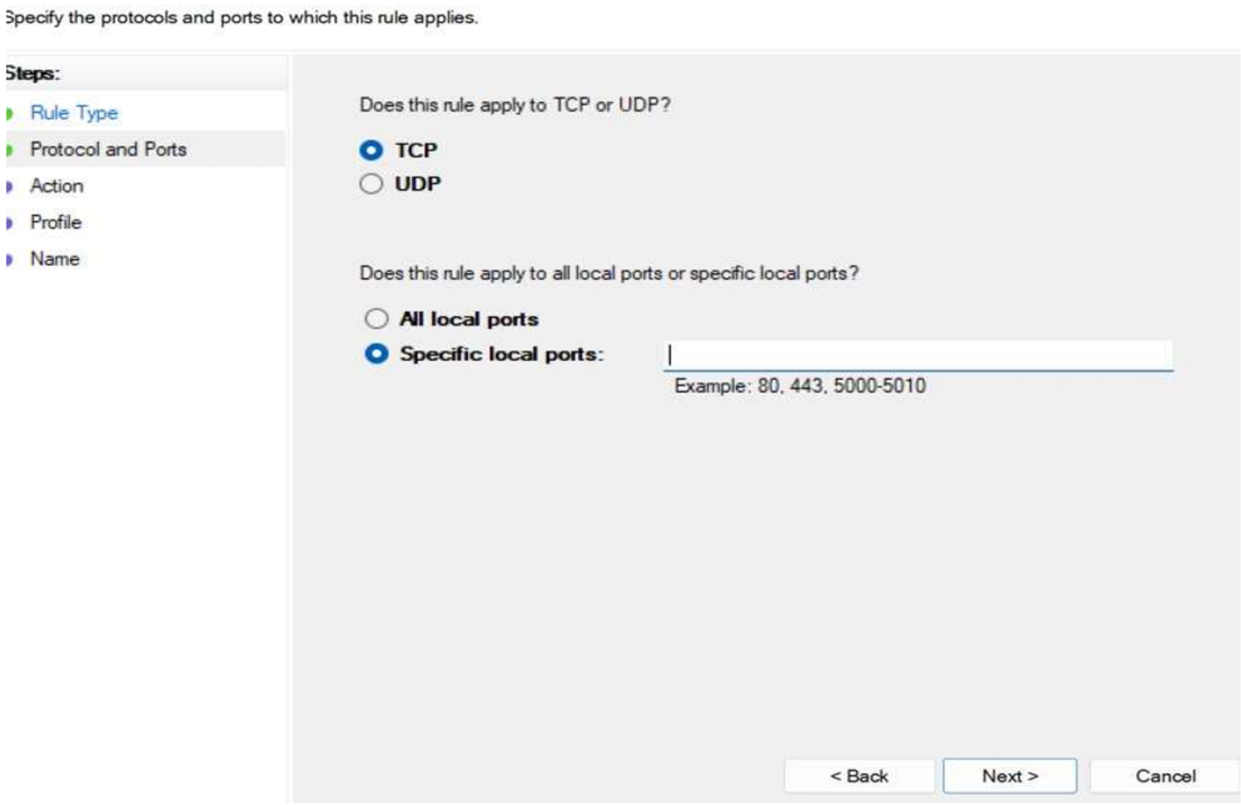
1. This program: Choose the specific application or process that the rule applies to.

2. Scope: Select the scope of the rule (e.g., domain, private, public).

3. Action: Choose whether to allow or block the traffic.

4. Name and description: Provide a name and description for the rule.

Now lets go with a specific port and do the following steps.



Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

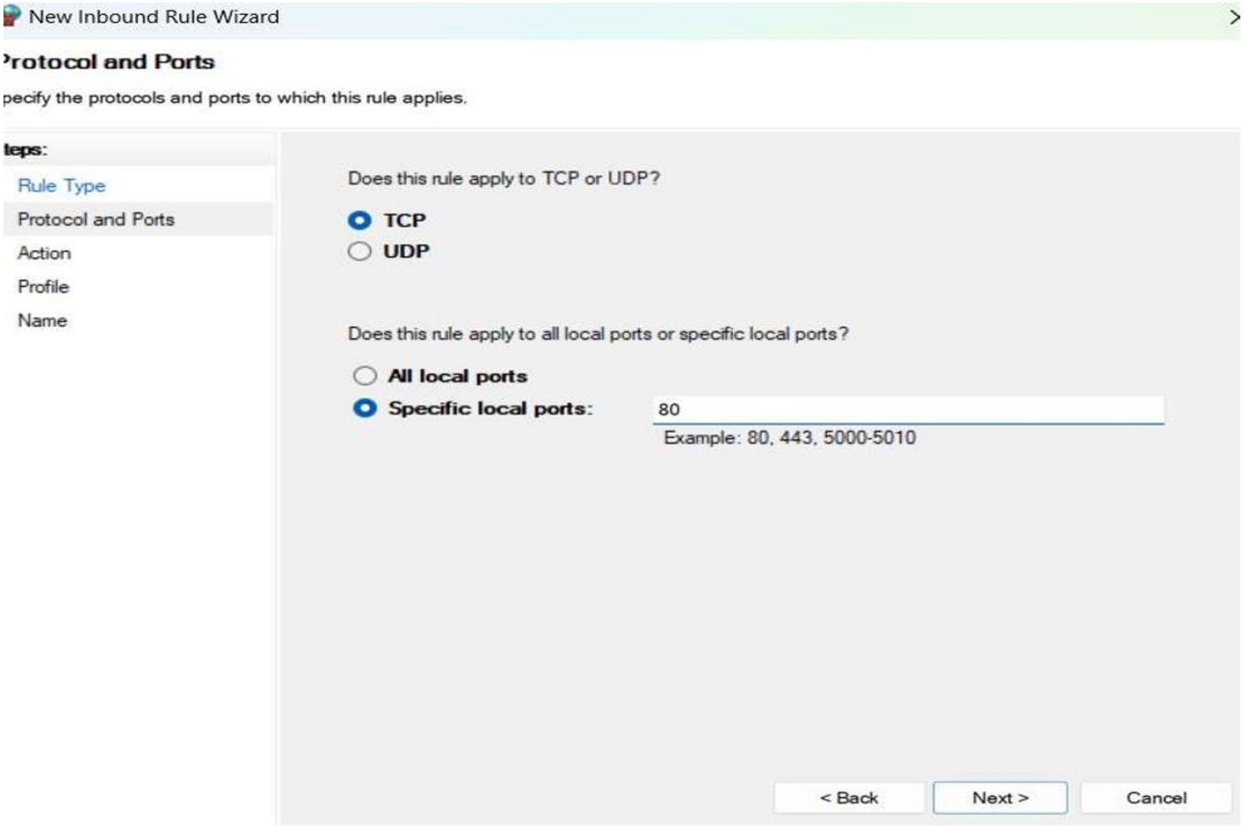
Does this rule apply to TCP or UDP?

● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports:

Example: 80, 443, 5000-5010



New Inbound Rule Wizard

Protocol and Ports

pecify the protocols and ports to which this rule applies.

teps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

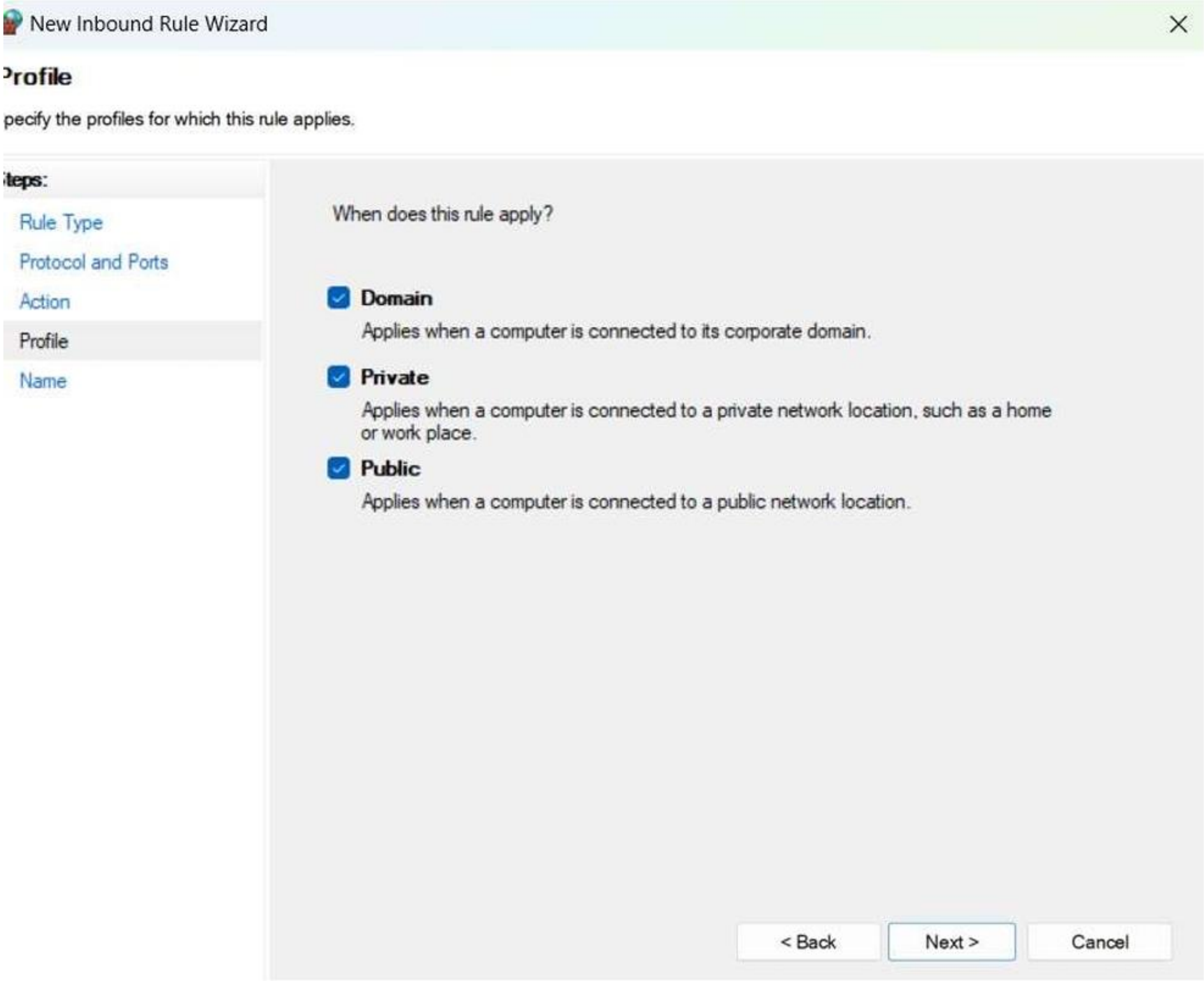
● TCP
○ UDP

Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 80

Example: 80, 443, 5000-5010

SO, now click on ports and selected the port as a tcp port and entered the port number i.e.80 then click on next



New Inbound Rule Wizard

Profile

pecify the profiles for which this rule applies.

When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☑ **Public**
Applies when a computer is connected to a public network location.

You will see profiles dialogue box

What are profiles?

Profiles are a fundamental concept in many security settings, including advanced firewall configurations.

They allow you to create different sets of rules and settings that apply to specific network environments or situations.

This helps you tailor your security measures to match the needs of different contexts.

Common Profile Types:

- Domain: This profile is typically used for network connections within your corporate domain. It might have stricter rules and settings to protect sensitive corporate data.

- Private: This profile is used for network connections within your home or private network. It might have more relaxed rules, allowing for greater flexibility and convenience

- Public: This profile is used for network connections on public networks, such as Wi-Fi hotspots. It often has stricter rules to protect your computer from potential threats in untrusted environments.

How Profiles Work:

- Rule association: You can associate different rules with each profile, allowing you to customize the security settings for different network environments.

- Automatic switching: Your firewall can automatically switch between profiles based on your network connection. For example, it might switch to the "Public" profile when you connect to a public Wi-Fi network.

Benefits of Using Profiles:

- Tailored security: Profiles allow you to create security settings that are appropriate for different network environments.

- Simplified management: By organizing rules into profiles, you can manage your security settings more efficiently.

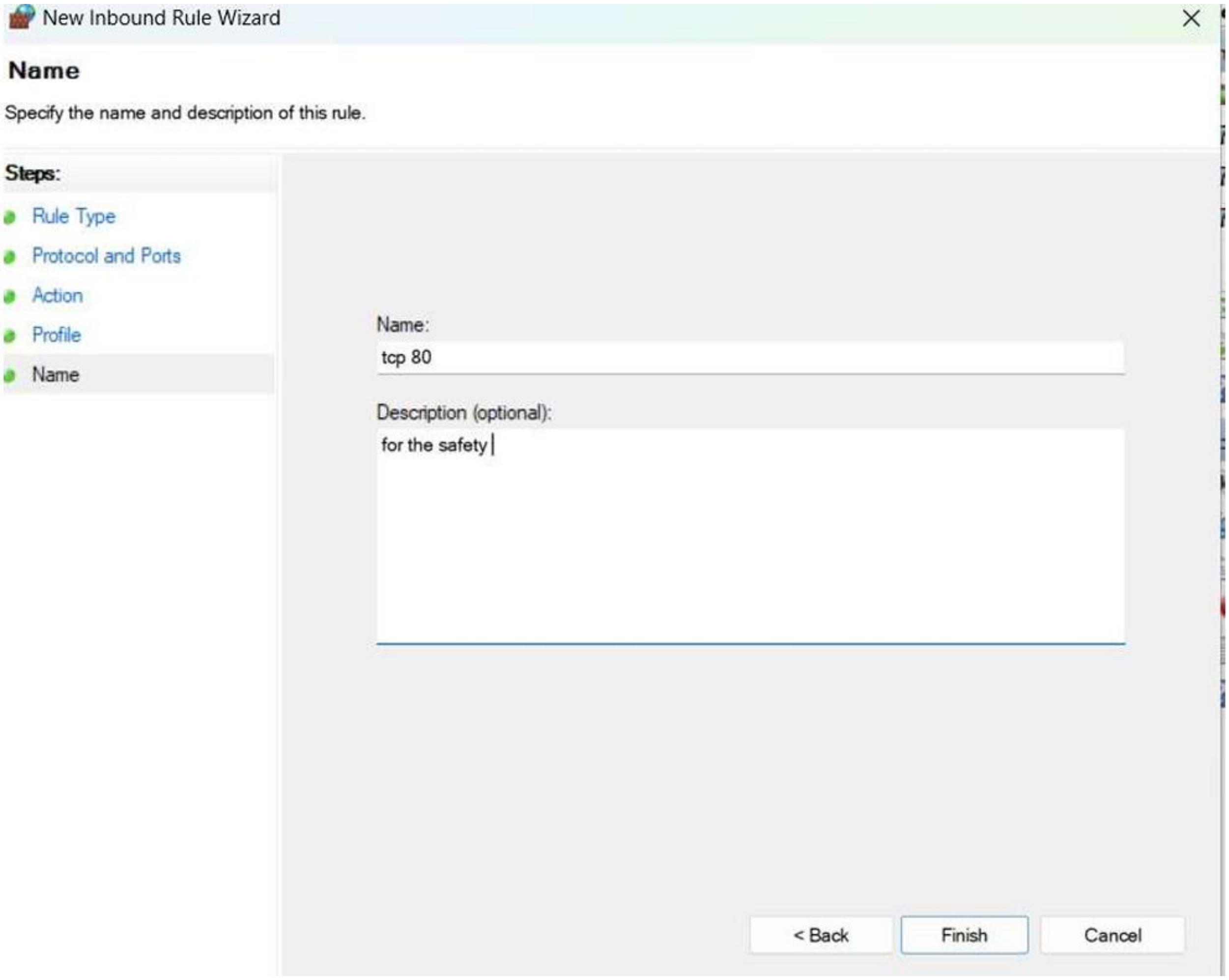
- Increased flexibility: Profiles provide flexibility in adapting your security measures to changing circumstances.

Example Use Cases:

- Home network: You might create a "Private" profile with relaxed rules for your home network, while using a "Public" profile with stricter rules when connecting to public Wi-Fi.

- Corporate network: Your company might have separate profiles for different departments or roles, with varying levels of access and permissions. By understanding and utilizing profiles effectively, you can enhance the security of your network and protect your sensitive data.

- **Then click on next**



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

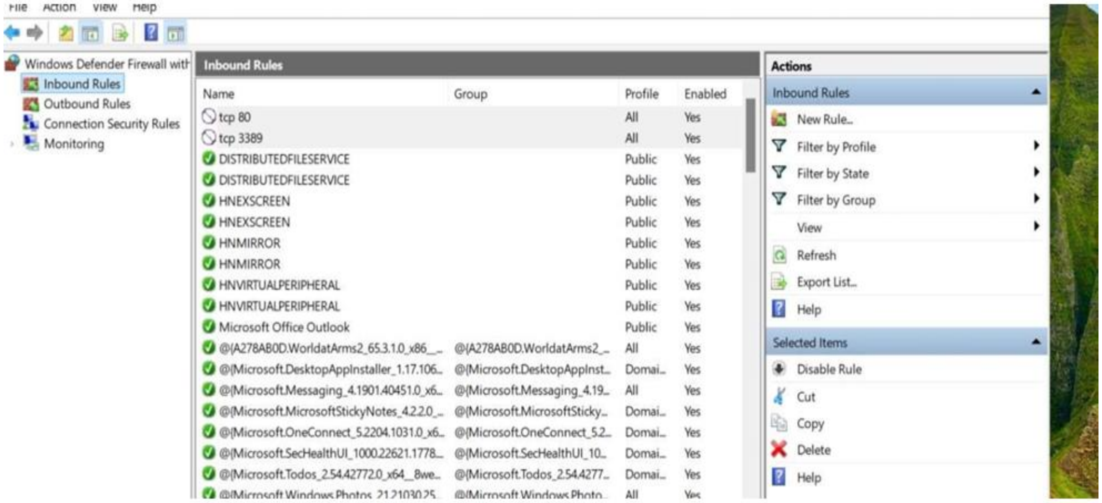
Name:

tcp 80

Description (optional):

for the safety

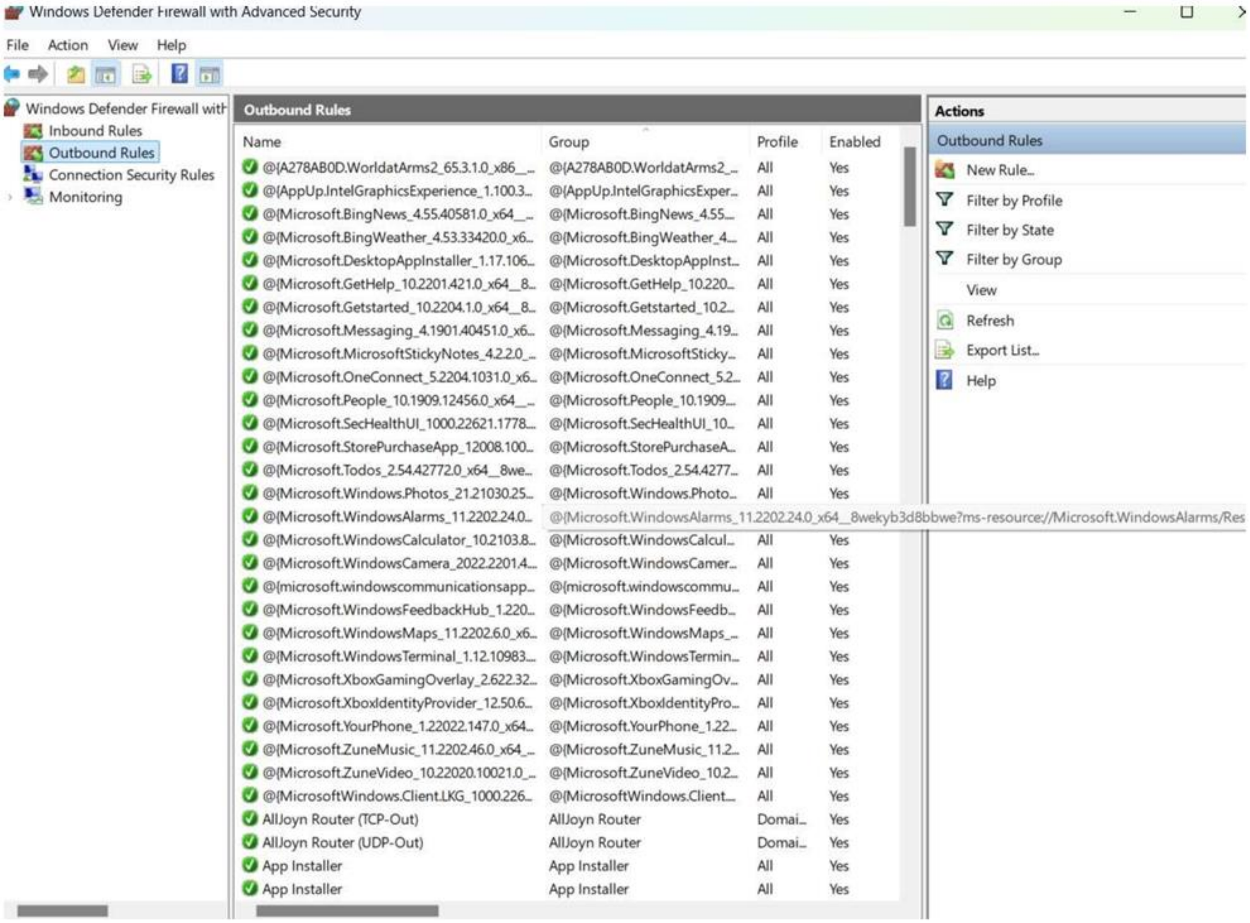
- **Give the name to the rule and description to it, so that you can search the rule easily and click on finish**.



Inbound Rules

Name	Group	Profile	Enabled
⊘ tcp 80		All	Yes
⊘ tcp 3389		All	Yes
✓ DISTRIBUTEDFILESERVICE		Public	Yes
✓ DISTRIBUTEDFILESERVICE		Public	Yes
✓ HNEXSCREEN		Public	Yes
✓ HNEXSCREEN		Public	Yes
✓ HNMIRROR		Public	Yes
✓ HNMIRROR		Public	Yes
✓ HNVIRTUALPERIPHERAL		Public	Yes
✓ HNVIRTUALPERIPHERAL		Public	Yes
✓ Microsoft Office Outlook		Public	Yes
✓ @{A278AB0D.WorldatArms2_65.3.1.0_x86__...	@{A278AB0D.WorldatArms2_...	All	Yes
✓ @{Microsoft.DesktopAppInstaller_1.17.106...	@{Microsoft.DesktopAppInst...	Domai...	Yes
✓ @{Microsoft.Messaging_4.1901.40451.0_x6...	@{Microsoft.Messaging_4.19...	All	Yes
✓ @{Microsoft.MicrosoftStickyNotes_4.2.2.0_...	@{Microsoft.MicrosoftSticky...	Domai...	Yes
✓ @{Microsoft.OneConnect_5.2204.1031.0_x6...	@{Microsoft.OneConnect_5.2...	Domai...	Yes
✓ @{Microsoft.SecHealthUI_1000.22621.1778...	@{Microsoft.SecHealthUI_10...	Domai...	Yes
✓ @{Microsoft.Todos_2.54.42772.0_x64__8we...	@{Microsoft.Todos_2.54.4277...	Domai...	Yes
✓ @{Microsoft.Windows.Photos_21.21030.25...	@{Microsoft.Windows.Photo...	All	Yes

- **As you can see the rules are created and you can even delete them by clicking on the rule and click on delete op on shown on the right side.**



Outbound Rules

Name	Group	Profile	Enabled
@{A278AB0D.WorldatArms2_65.3.1.0_x86__...	@{A278AB0D.WorldatArms2_...	All	Yes
@{AppUp.IntelGraphicsExperience_1.100.3...	@{AppUp.IntelGraphicsExper...	All	Yes
@{Microsoft.BingNews_4.55.40581.0_x64__...	@{Microsoft.BingNews_4.55...	All	Yes
@{Microsoft.BingWeather_4.53.33420.0_x6...	@{Microsoft.BingWeather_4...	All	Yes
@{Microsoft.DesktopAppInstaller_1.17.106...	@{Microsoft.DesktopAppInst...	All	Yes
@{Microsoft.GetHelp_10.2201.421.0_x64__8...	@{Microsoft.GetHelp_10.220...	All	Yes
@{Microsoft.Getstarted_10.2204.1.0_x64__8...	@{Microsoft.Getstarted_10.2...	All	Yes
@{Microsoft.Messaging_4.1901.40451.0_x6...	@{Microsoft.Messaging_4.19...	All	Yes
@{Microsoft.MicrosoftStickyNotes_4.2.2.0_...	@{Microsoft.MicrosoftSticky...	All	Yes
@{Microsoft.OneConnect_5.2204.1031.0_x6...	@{Microsoft.OneConnect_5.2...	All	Yes
@{Microsoft.People_10.1909.12456.0_x64__...	@{Microsoft.People_10.1909...	All	Yes
@{Microsoft.SecHealthUI_1000.22621.1778...	@{Microsoft.SecHealthUI_10...	All	Yes
@{Microsoft.StorePurchaseApp_12008.100...	@{Microsoft.StorePurchaseA...	All	Yes
@{Microsoft.Todos_2.54.42772.0_x64__8we...	@{Microsoft.Todos_2.54.4277...	All	Yes
@{Microsoft.Windows.Photos_21.21030.25...	@{Microsoft.Windows.Photo...	All	Yes
@{Microsoft.WindowsAlarms_11.2202.24.0...	@{Microsoft.WindowsAlarms_11.2202.24.0_x64__8wekyb3d8bbwe?ms-resource://Microsoft.WindowsAlarms/Res		
@{Microsoft.WindowsCalculator_10.2103.8...	@{Microsoft.WindowsCalcul...	All	Yes
@{Microsoft.WindowsCamera_2022.2201.4...	@{Microsoft.WindowsCamer...	All	Yes
@{microsoft.windowscommunicationsapp...	@{microsoft.windowscommu...	All	Yes
@{Microsoft.WindowsFeedbackHub_1.220...	@{Microsoft.WindowsFeedb...	All	Yes
@{Microsoft.WindowsMaps_11.2202.6.0_x6...	@{Microsoft.WindowsMaps_...	All	Yes
@{Microsoft.WindowsTerminal_1.12.10983...	@{Microsoft.WindowsTermin...	All	Yes
@{Microsoft.XboxGamingOverlay_2.622.32...	@{Microsoft.XboxGamingOv...	All	Yes
@{Microsoft.XboxIdentityProvider_12.50.6...	@{Microsoft.XboxIdentityPro...	All	Yes
@{Microsoft.YourPhone_1.22022.147.0_x64...	@{Microsoft.YourPhone_1.22...	All	Yes
@{Microsoft.ZuneMusic_11.2202.46.0_x64_...	@{Microsoft.ZuneMusic_11.2...	All	Yes
@{Microsoft.ZuneVideo_10.22020.10021.0_...	@{Microsoft.ZuneVideo_10.2...	All	Yes
@{MicrosoftWindows.Client.LKG_1000.226...	@{MicrosoftWindows.Client...	All	Yes
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes
App Installer	App Installer	All	Yes
App Installer	App Installer	All	Yes

When you click on deleted, they will be deleted.

This is how you create or add a new rule to the firewall and remove a rule from the firewall.

We saw the ways to implement rules, now which ports and profiles should be closed for better security?

While the default rules provided by Windows Firewall offer a basic level of protection, creating custom rules can significantly enhance your network security by allowing you to tailor the firewall's behaviour to your specific needs.

Here are some examples of custom rules you can create, along with explanations for their purpose:

Inbound Rules

- Block all incoming traffic on specific ports:

Ports: 139, 445 (SMB), 23 (Telnet), 20, 21 (FTP)

Purpose: These ports are commonly used for file sharing and remote administration. Blocking them can help prevent unauthorized access to your system.

- Allow only specific incoming connections:

Ports: 80 (HTTP), 443 (HTTPS), 22 (SSH), 3389 (RDP)

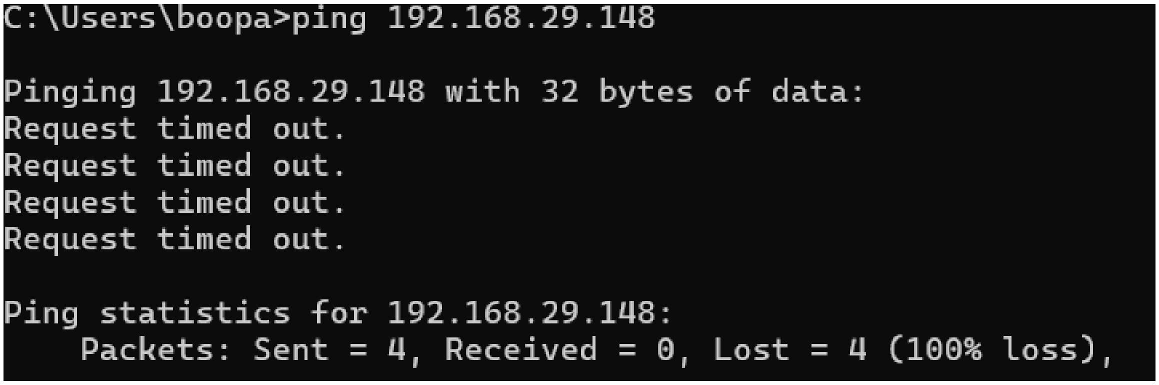
Purpose: These ports are typically used for legitimate web traffic, secure connections, and remote administration. Allow only connections from trusted sources to prevent unauthorized access.

Remember to consider the following factors when creating custom rules:

- **Impact on functionality:** Ensure that the rules you create do not interfere with legitimate network traffic or applications.
- **Security risks:** Evaluate the potential security risks associated with allowing or blocking certain traffic.
- **Testing:** Test your custom rules to ensure they are working as intended and do not cause any unexpected issues.

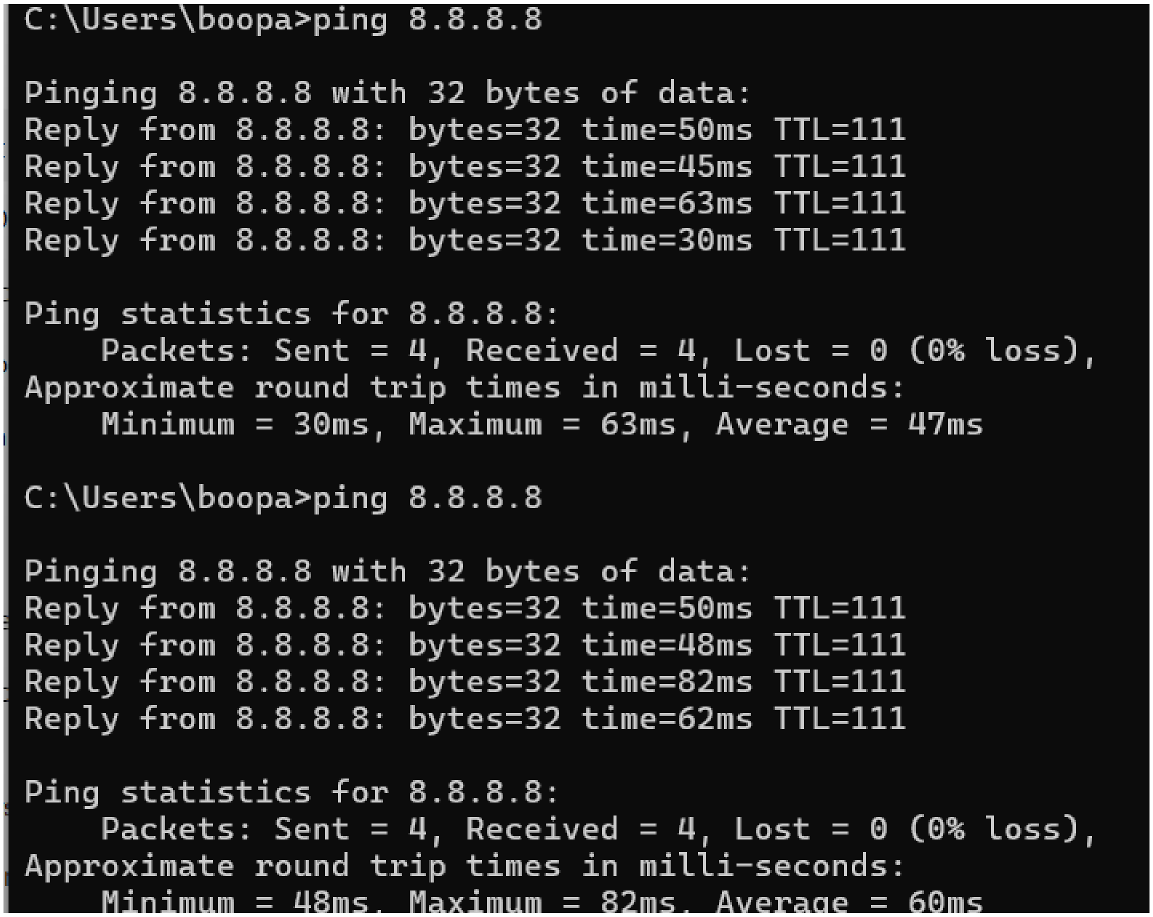
USING WIRESHARK TO PING THE OTHER DEVICE

- Open CMD and type the following command Ping by keeping the other device firewall on, you will see the connection request me out as it is blocking the request.



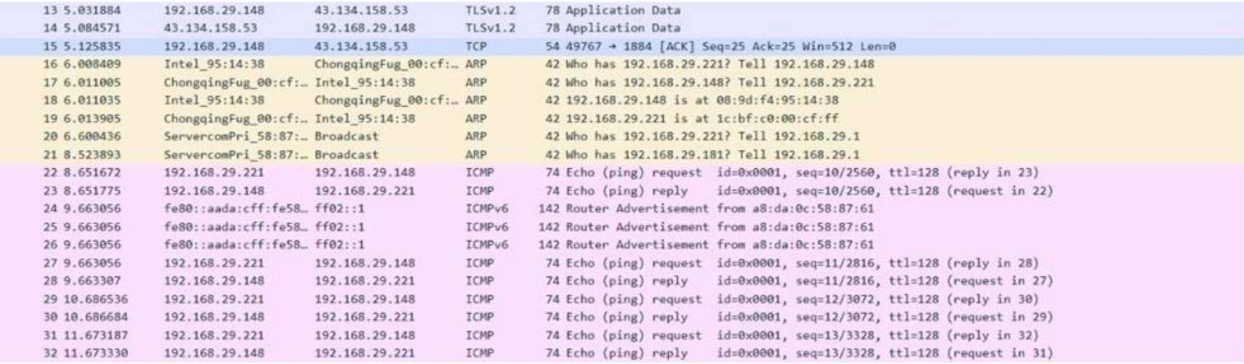
```
C:\Users\boopa>ping 192.168.29.148

Pinging 192.168.29.148 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.29.148:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Now switch off the fire wall of the other device and then type the same command again, you will see the following.



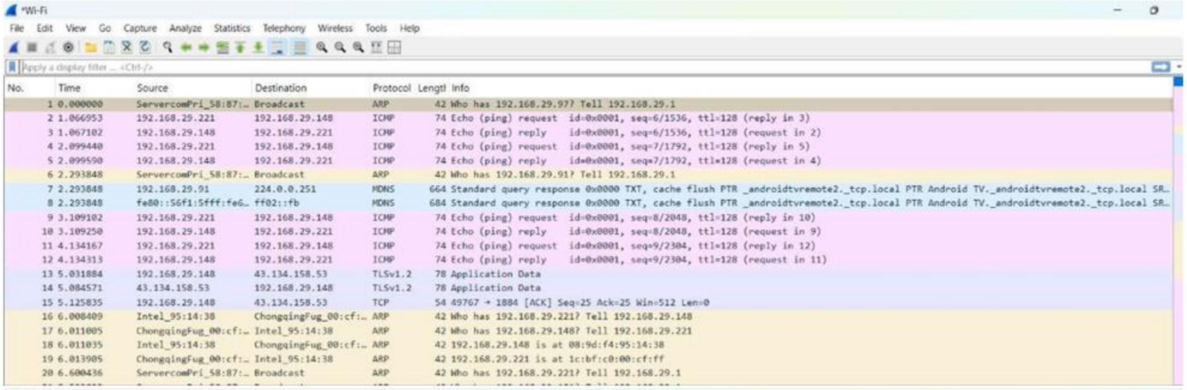
```
C:\Users\boopa>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=50ms TTL=111
Reply from 8.8.8.8: bytes=32 time=45ms TTL=111
Reply from 8.8.8.8: bytes=32 time=63ms TTL=111
Reply from 8.8.8.8: bytes=32 time=30ms TTL=111

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 63ms, Average = 47ms

C:\Users\boopa>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=50ms TTL=111
Reply from 8.8.8.8: bytes=32 time=48ms TTL=111
Reply from 8.8.8.8: bytes=32 time=82ms TTL=111
Reply from 8.8.8.8: bytes=32 time=62ms TTL=111

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 48ms, Maximum = 82ms, Average = 60ms
```

You can check the same using wire shark in the system that you are sending the packets

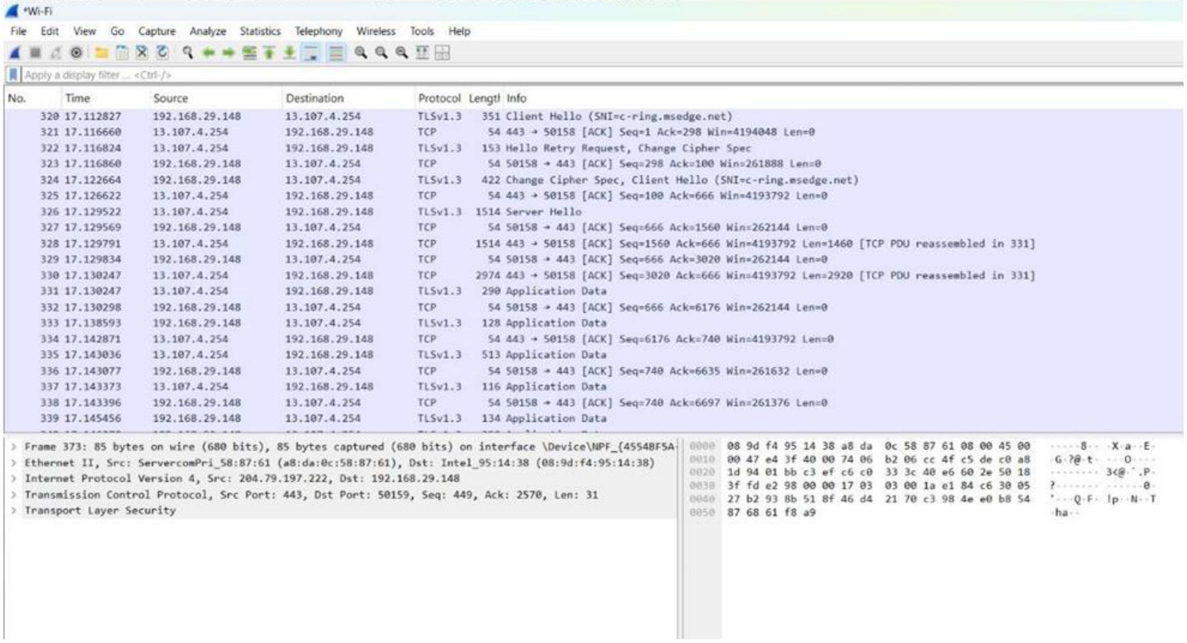


```
13 5.031884   192.168.29.148        43.134.158.53         TLSv1.2   78 Application Data
14 5.084571   43.134.158.53         192.168.29.148        TLSv1.2   78 Application Data
15 5.125835   192.168.29.148        43.134.158.53         TCP       54 49767 → 1884 [ACK] Seq=25 Ack=25 Win=512 Len=0
16 6.008409   Intel_95:14:38        ChongqingFug_00:cf:… ARP       42 Who has 192.168.29.221? Tell 192.168.29.148
17 6.011005   ChongqingFug_00:cf:… Intel_95:14:38        ARP       42 Who has 192.168.29.148? Tell 192.168.29.221
18 6.011035   Intel_95:14:38        ChongqingFug_00:cf:… ARP       42 192.168.29.148 is at 08:9d:f4:95:14:38
19 6.013905   ChongqingFug_00:cf:… Intel_95:14:38        ARP       42 192.168.29.221 is at 1c:bf:c0:00:cf:ff
20 6.600436   ServercomPri_58:87:… Broadcast             ARP       42 Who has 192.168.29.221? Tell 192.168.29.1
21 8.523893   ServercomPri_58:87:… Broadcast             ARP       42 Who has 192.168.29.181? Tell 192.168.29.1
22 8.651672   192.168.29.221        192.168.29.148        ICMP      74 Echo (ping) request  id=0x0001, seq=10/2560, ttl=128 (reply in 23)
23 8.651775   192.168.29.148        192.168.29.221        ICMP      74 Echo (ping) reply    id=0x0001, seq=10/2560, ttl=128 (request in 22)
24 9.663056   fe80::aada:cff:fe58… ff02::1               ICMPv6   142 Router Advertisement from a8:da:0c:58:87:61
25 9.663056   fe80::aada:cff:fe58… ff02::1               ICMPv6   142 Router Advertisement from a8:da:0c:58:87:61
26 9.663056   fe80::aada:cff:fe58… ff02::1               ICMPv6   142 Router Advertisement from a8:da:0c:58:87:61
27 9.663056   192.168.29.221        192.168.29.148        ICMP      74 Echo (ping) request  id=0x0001, seq=11/2816, ttl=128 (reply in 28)
28 9.663307   192.168.29.148        192.168.29.221        ICMP      74 Echo (ping) reply    id=0x0001, seq=11/2816, ttl=128 (request in 27)
29 10.686536  192.168.29.221        192.168.29.148        ICMP      74 Echo (ping) request  id=0x0001, seq=12/3072, ttl=128 (reply in 30)
30 10.686684  192.168.29.148        192.168.29.221        ICMP      74 Echo (ping) reply    id=0x0001, seq=12/3072, ttl=128 (request in 29)
31 11.673187  192.168.29.221        192.168.29.148        ICMP      74 Echo (ping) request  id=0x0001, seq=13/3328, ttl=128 (reply in 32)
32 11.673330  192.168.29.148        192.168.29.221        ICMP      74 Echo (ping) reply    id=0x0001, seq=13/3328, ttl=128 (request in 31)
```

All the purple line shows the echo ping from my system to the host system. If you are using wifi, as you start sniffing packets using wire shark you will see the handshake between your device and the wifi router you are using something like this


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time       Source                Destination     Protocol Lengtl Info
 1 0.000000   ServercomPri_58:87:… Broadcast       ARP       42 Who has 192.168.29.97? Tell 192.168.29.1
 2 1.066953   192.168.29.221        192.168.29.148  ICMP      74 Echo (ping) request  id=0x0001, seq=6/1536, ttl=128 (reply in 3)
 3 1.067102   192.168.29.148        192.168.29.221  ICMP      74 Echo (ping) reply    id=0x0001, seq=6/1536, ttl=128 (request in 2)
 4 2.099440   192.168.29.221        192.168.29.148  ICMP      74 Echo (ping) request  id=0x0001, seq=7/1792, ttl=128 (reply in 5)
 5 2.099590   192.168.29.148        192.168.29.221  ICMP      74 Echo (ping) reply    id=0x0001, seq=7/1792, ttl=128 (request in 4)
 6 2.293848   ServercomPri_58:87:… Broadcast       ARP       42 Who has 192.168.29.91? Tell 192.168.29.1
 7 2.293848   192.168.29.91         224.0.0.251     MDNS     664 Standard query response 0x0000 TXT, cache flush PTR _androidtvremote2._tcp.local PTR Android TV._androidtvremote2._tcp.local SR…
 8 2.293848   fe80::56f1:5fff:fe6… ff02::fb        MDNS     684 Standard query response 0x0000 TXT, cache flush PTR _androidtvremote2._tcp.local PTR Android TV._androidtvremote2._tcp.local SR…
 9 3.109102   192.168.29.221        192.168.29.148  ICMP      74 Echo (ping) request  id=0x0001, seq=8/2048, ttl=128 (reply in 10)
10 3.109250   192.168.29.148        192.168.29.221  ICMP      74 Echo (ping) reply    id=0x0001, seq=8/2048, ttl=128 (request in 9)
11 4.134167   192.168.29.221        192.168.29.148  ICMP      74 Echo (ping) request  id=0x0001, seq=9/2304, ttl=128 (reply in 12)
12 4.134313   192.168.29.148        192.168.29.221  ICMP      74 Echo (ping) reply    id=0x0001, seq=9/2304, ttl=128 (request in 11)
13 5.031884   192.168.29.148        43.134.158.53   TLSv1.2   78 Application Data
14 5.084571   43.134.158.53         192.168.29.148  TLSv1.2   78 Application Data
15 5.125835   192.168.29.148        43.134.158.53   TCP       54 49767 → 1884 [ACK] Seq=25 Ack=25 Win=512 Len=0
16 6.008409   Intel_95:14:38        ChongqingFug_00:cf:… ARP  42 Who has 192.168.29.221? Tell 192.168.29.148
17 6.011005   ChongqingFug_00:cf:… Intel_95:14:38  ARP       42 Who has 192.168.29.148? Tell 192.168.29.221
18 6.011035   Intel_95:14:38        ChongqingFug_00:cf:… ARP  42 192.168.29.148 is at 08:9d:f4:95:14:38
19 6.013905   ChongqingFug_00:cf:… Intel_95:14:38  ARP       42 192.168.29.221 is at 1c:bf:c0:00:cf:ff
20 6.600436   ServercomPri_58:87:… Broadcast       ARP       42 Who has 192.168.29.221? Tell 192.168.29.1
```


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time        Source           Destination      Protocol Lengtl Info
320 17.112827  192.168.29.148   13.107.4.254     TLSv1.3   351 Client Hello (SNI=c-ring.msedge.net)
321 17.116660  13.107.4.254     192.168.29.148   TCP        54 443 → 50158 [ACK] Seq=1 Ack=298 Win=4194048 Len=0
322 17.116824  13.107.4.254     192.168.29.148   TLSv1.3   153 Hello Retry Request, Change Cipher Spec
323 17.116860  192.168.29.148   13.107.4.254     TCP        54 50158 → 443 [ACK] Seq=298 Ack=100 Win=261888 Len=0
324 17.122664  192.168.29.148   13.107.4.254     TLSv1.3   422 Change Cipher Spec, Client Hello (SNI=c-ring.msedge.net)
325 17.126622  13.107.4.254     192.168.29.148   TCP        54 443 → 50158 [ACK] Seq=100 Ack=666 Win=4193792 Len=0
326 17.129522  13.107.4.254     192.168.29.148   TLSv1.3  1514 Server Hello
327 17.129569  192.168.29.148   13.107.4.254     TCP        54 50158 → 443 [ACK] Seq=666 Ack=1560 Win=262144 Len=0
328 17.129791  13.107.4.254     192.168.29.148   TCP      1514 443 → 50158 [ACK] Seq=1560 Ack=666 Win=4193792 Len=1460 [TCP PDU reassembled in 331]
329 17.129834  192.168.29.148   13.107.4.254     TCP        54 50158 → 443 [ACK] Seq=666 Ack=3020 Win=262144 Len=0
330 17.130247  13.107.4.254     192.168.29.148   TCP      2974 443 → 50158 [ACK] Seq=3020 Ack=666 Win=4193792 Len=2920 [TCP PDU reassembled in 331]
331 17.130247  13.107.4.254     192.168.29.148   TLSv1.3   290 Application Data
332 17.130298  192.168.29.148   13.107.4.254     TCP        54 50158 → 443 [ACK] Seq=666 Ack=6176 Win=262144 Len=0
333 17.138593  192.168.29.148   13.107.4.254     TLSv1.3   128 Application Data
334 17.142871  13.107.4.254     192.168.29.148   TCP        54 443 → 50158 [ACK] Seq=6176 Ack=740 Win=4193792 Len=0
335 17.143036  13.107.4.254     192.168.29.148   TLSv1.3   513 Application Data
336 17.143077  192.168.29.148   13.107.4.254     TCP        54 50158 → 443 [ACK] Seq=740 Ack=6635 Win=261632 Len=0
337 17.143373  13.107.4.254     192.168.29.148   TLSv1.3   116 Application Data
338 17.143396  192.168.29.148   13.107.4.254     TCP        54 50158 → 443 [ACK] Seq=740 Ack=6697 Win=261376 Len=0
339 17.145456  192.168.29.148   13.107.4.254     TLSv1.3   134 Application Data
```

```
> Frame 373: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{4554BF5A-
> Ethernet II, Src: ServercomPri_58:87:61 (a8:da:0c:58:87:61), Dst: Intel_95:14:38 (08:9d:f4:95:14:38)
> Internet Protocol Version 4, Src: 204.79.197.222, Dst: 192.168.29.148
> Transmission Control Protocol, Src Port: 443, Dst Port: 50159, Seq: 449, Ack: 2570, Len: 31
> Transport Layer Security
```

```
0000  08 9d f4 95 14 38 a8 da  0c 58 87 61 08 00 45 00   ·····8·· ·X·a··E·
0010  00 47 e4 3f 40 00 74 06  b2 06 cc 4f c5 de c0 a8   ·G·?@·t· ···O····
0020  1d 94 01 bb c3 ef c6 c0  33 3c 40 e6 60 2e 50 18   ········ 3<@·`.P·
0030  3f fd e2 98 00 00 17 03  03 00 1a e1 84 c6 30 05   ?······· ······0·
0040  27 b2 93 8b 51 8f 46 d4  21 70 c3 98 4e e0 b8 54   '···Q·F· !p··N··T
0050  87 68 61 f8 a9                                     ·ha··
```

Three-way handshake

1. Request
2. Reply
3. ACK

If applications are exchanging data, then, there will be exchange of application data in the packets, you can click on that particular packet and see the exchange data request in the wire shark.

Here are some key points for educating others about the importance of network security:

1. **Data Protection**: Network security protects personal and sensitive data from theft or unauthorized access, safeguarding privacy.
2. **Preventing Financial Loss**: Cyber threats can lead to financial theft and fraud; network security reduces these risks.
3. **Securing Devices**: Every device connected to the internet, including phones and computers, can be a target for malware and hackers without security measures.
4. **Avoiding Service Disruptions**: Attacks like DDoS can disrupt services people rely on daily, from online banking to communication apps.
5. **Maintaining Privacy**: Strong security ensures that personal conversations, files, and activities stay private and are not exposed to unauthorized users.
6. **Raising Awareness**: Simple practices like using strong passwords, avoiding phishing scams, and updating software regularly can make a big difference.
7. **Protecting Businesses and Networks**: Even individual security habits contribute to overall network safety, affecting not only personal devices but workplaces and public networks.