2025

Redynox

Intern: Uyor Chimdi Ebulu

Email: Chimdi2700@gmail.com

Objective:

Understand the basics of network security by learning about different types of network threats and how to implement basic security measures. This task will introduce you to the foundational concepts of securing a small network.

Skills: Basic Network Security, Threat Identification, Security Best Practices

Tools: Firewall (Windows Defender Firewall or a basic hardware firewall), Wireshark

[CYBER SECURITY INTERNSHIP]

TASK 1: Introduction to Network Security Basics

Network Security Concepts – Technical Summary

1 Network Threats: Types & Characteristics

Threat	Definition	Propagation	Techniques	Defense
Viruses	Malicious code that attaches to legitimate executable.	Infected files, email attachments, removable media.	Polymorphism, stealth techniques.	Antivirus/EDR, whitelisting, user awareness training.
Worms	Self-replicating malware spreading autonomously.	Network vulnerabilities (open ports, weak credentials).	Network scanning, credential stuffing.	Network scanning, credential stuffing.
Trojans	Malware disguised as legitimate software.	Social engineering, drive-by downloads.	Social engineering, drive-by downloads.	Sandboxing, behavioral analysis, traffic analysis.
Phishing	Social engineering to steal credentials or deliver malware	Emails, SMS, VoIP, social media.	Spoofed domains, malicious attachments.	Secure email gateways, DMARC/SPF/DKIM, awareness training.

1.2 Core Security Concepts

Firewalls

- **Function:** Enforce access control policies at network boundaries by inspecting packet headers (Layer 3/4) or payload (Layer 7).
- **Types:**
  - **Stateless (Packet Filtering):** Inspects individual packets.
  - **Stateful Inspection:** Tracks active connections, maintains state tables.
  - **Application-layer Firewalls (NGFW):** Deep Packet Inspection (DPI), SSL decryption, malware sandboxing.
- **Key Configurations:**
  - Default deny policies
  - Geo-blocking
  - Application control

Encryption

- **Purpose:** Ensure confidentiality, integrity, and authenticity of data.
- **Types:**
  - **Symmetric Encryption (Shared Key):** AES-256, ChaCha20 (fast, but key distribution challenges).
  - **Asymmetric Encryption (Public/Private Keys):** RSA, ECC (key exchange, digital signatures).
  - **Hybrid Encryption:** Used in TLS (session key exchanged via asymmetric, data encrypted via symmetric).
- **Protocols:**
  - TLS 1.3 (modern secure web communications)
  - IPsec (VPN tunneling)
  - PGP/GPG (email encryption)

Secure Network Configuration

- **Key Principles:**
  - **Least Privilege:** Minimal necessary access for users/services.
  - **Network Segmentation:** Isolating critical assets into VLANs/subnets.
  - **Zero Trust Architecture (ZTA):** Never trust, always verify — continuous authentication and micro-segmentation.
  - **Patch & Vulnerability Management:** Automated vulnerability scanning (e.g., Nessus, Qualys).
  - **Logging & Monitoring:** SIEM solutions for real-time alerting (e.g., Splunk, Elastic, Wazuh).
  - **Access Controls:** MFA, strong password policies, centralized IAM (Identity and Access Management).

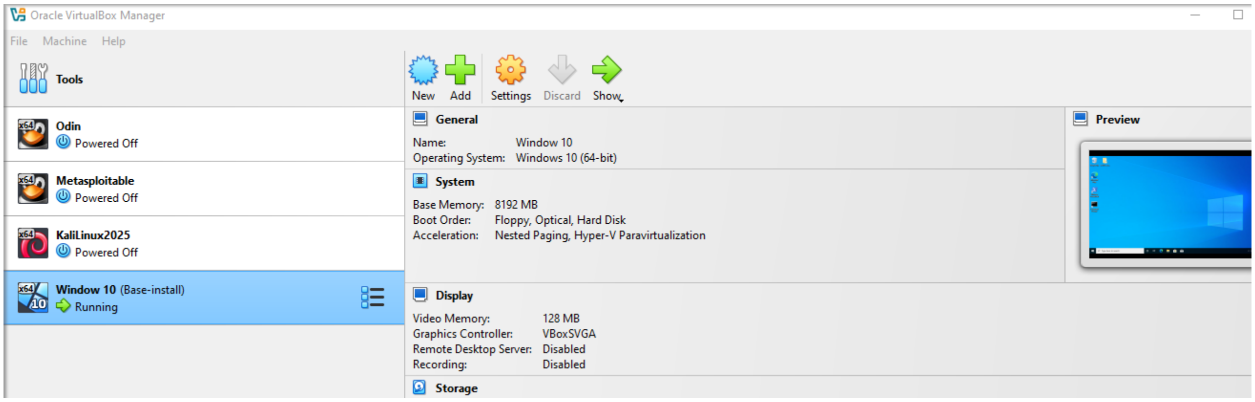
As a cybersecurity analyst, understanding both **technical controls** (firewalls, IDS, encryption) and **attack vectors** (phishing, malware variants) allows proactive defense, rapid incident response, and effective threat hunting. Continuous learning of TTPs (Tactics, Techniques & Procedures) via frameworks like MITRE ATT&CK enhances detection capability.

2. Implement Basic Security Measures:

2.1 Lab Setup and Firewall Configuration

Virtual Lab:

- Virtual router and three connected VMs (Windows 10, Kali Linux, Metasploitable).



Odin
Powered Off

Metasploitable
Powered Off

KaliLinux2025
Powered Off

Window 10 (Base-install)
Running

General

Name: Window 10
Operating System: Windows 10 (64-bit)

System

Base Memory: 8192 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization

Display

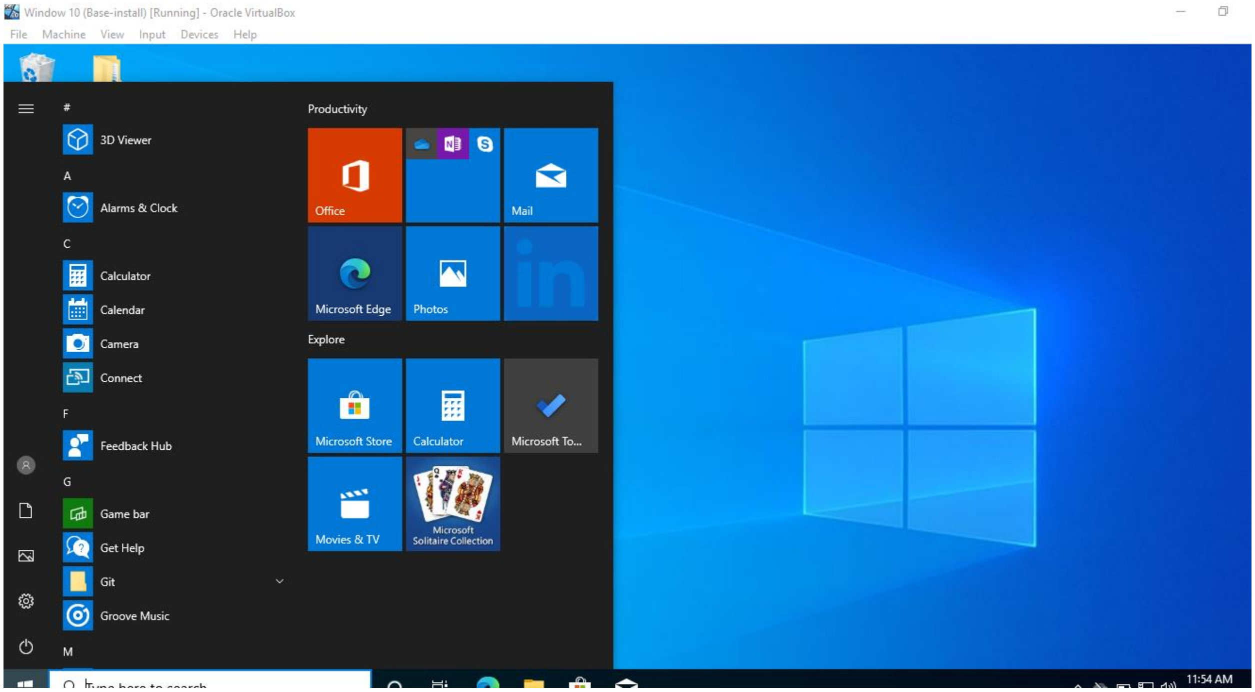
Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

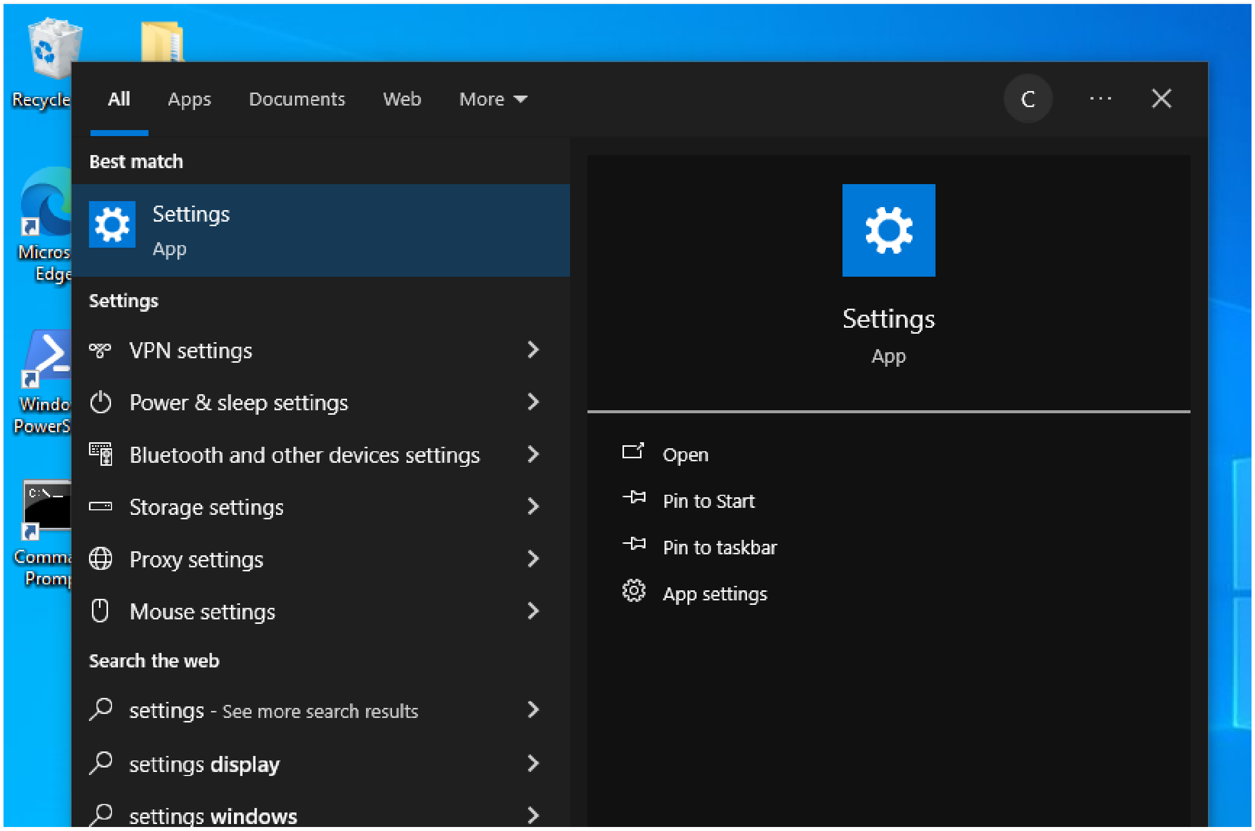
Windows Defender Firewall Configuration:

- Enable and configure a basic firewall (e.g., Windows Defender Firewall) to block unauthorized access.

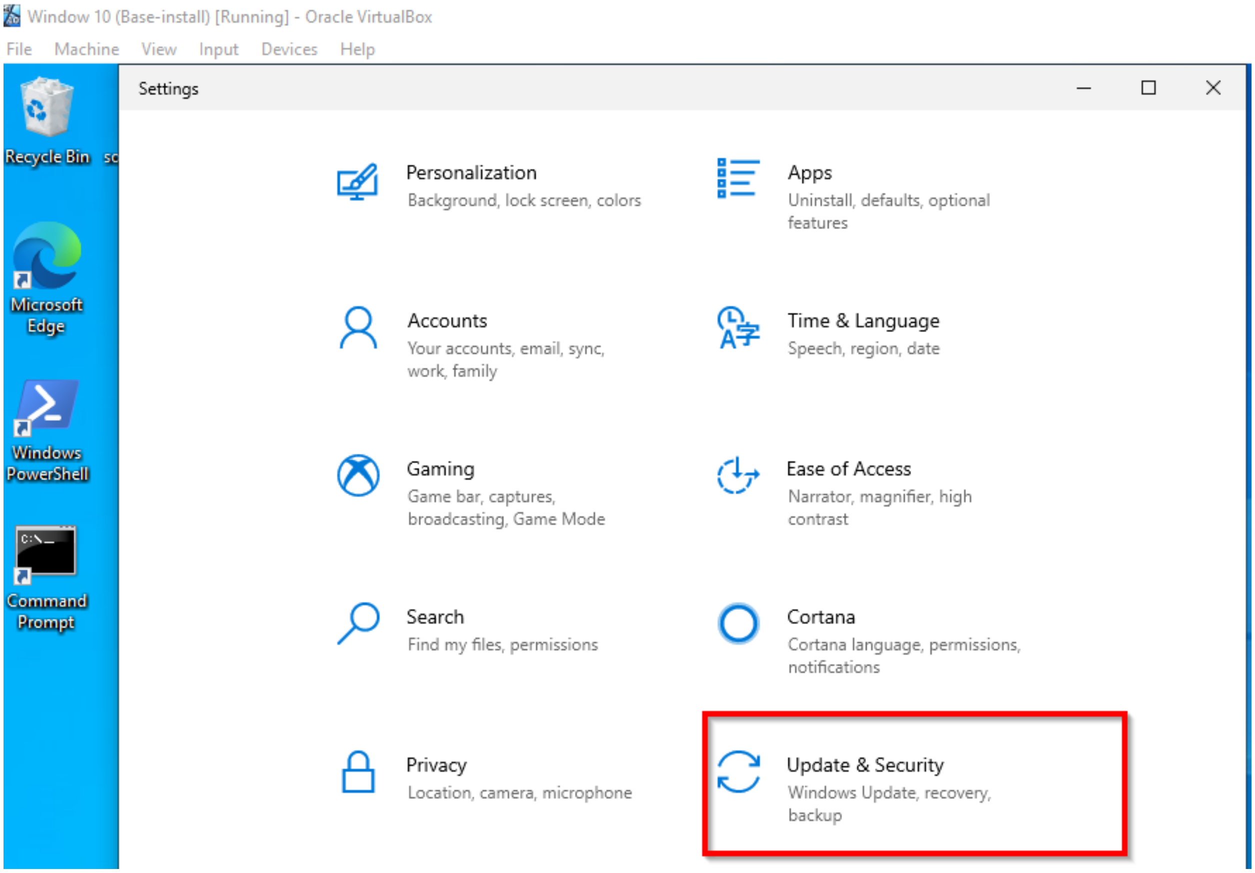
Step 1: Launch start from the taskbar.



Step 2: Search “Settings” in the search bar



Step 3: In the left pane of Settings, click Update & security



Settings

Personalization
Background, lock screen, colors

Apps
Uninstall, defaults, optional features

Accounts
Your accounts, email, sync, work, family

Time & Language
Speech, region, date

Gaming
Game bar, captures, broadcasting, Game Mode

Ease of Access
Narrator, magnifier, high contrast

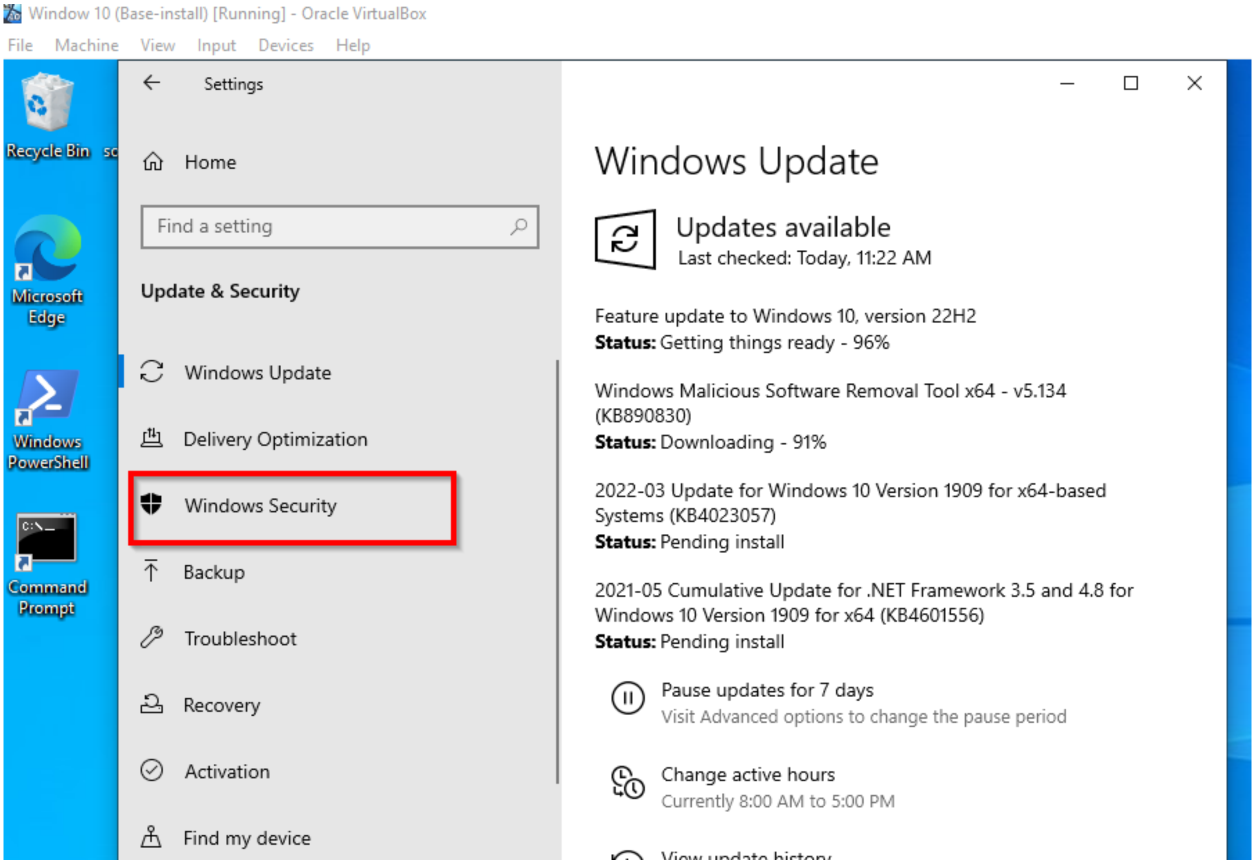
Search
Find my files, permissions

Cortana
Cortana language, permissions, notifications

Privacy
Location, camera, microphone

Update & Security
Windows Update, recovery, backup

Step 4: Click Window Security option in Update & Security



Windows Update

Updates available
Last checked: Today, 11:22 AM

Feature update to Windows 10, version 22H2
Status: Getting things ready - 96%

Windows Malicious Software Removal Tool x64 - v5.134 (KB890830)
Status: Downloading - 91%

2022-03 Update for Windows 10 Version 1909 for x64-based Systems (KB4023057)
Status: Pending install

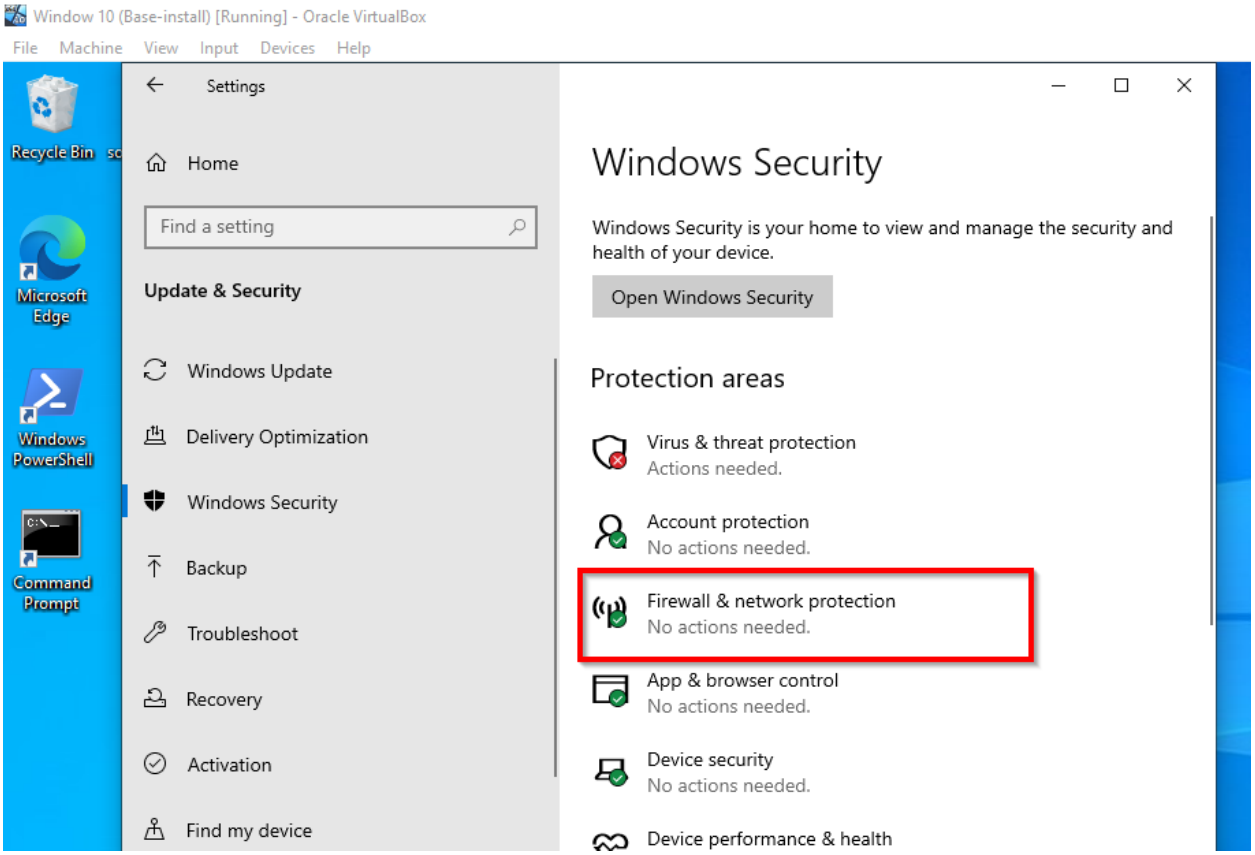
2021-05 Cumulative Update for .NET Framework 3.5 and 4.8 for Windows 10 Version 1909 for x64 (KB4601556)
Status: Pending install

Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 8:00 AM to 5:00 PM

View update history

Step 5: Select Firewall & network protection.



Windows Security

Windows Security is your home to view and manage the security and health of your device.

Protection areas

Virus & threat protection
Actions needed.

Account protection
No actions needed.

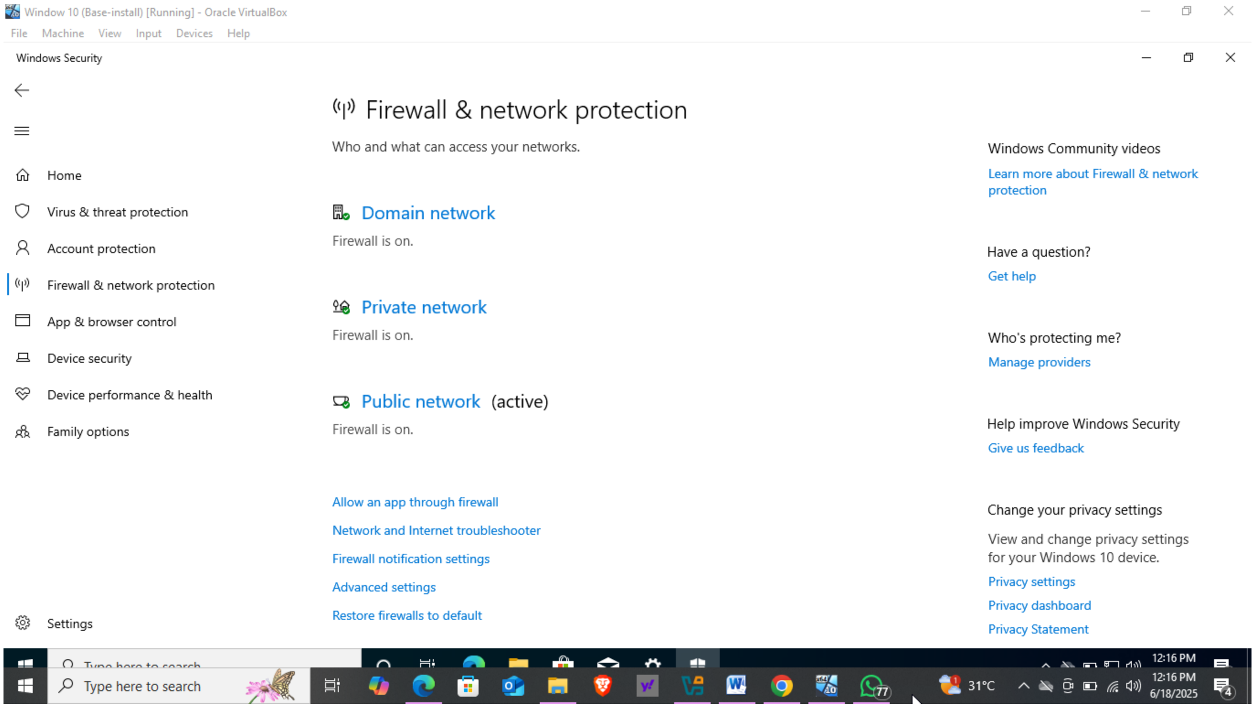
Firewall & network protection
No actions needed.

App & browser control
No actions needed.

Device security
No actions needed.

Device performance & health

Step 6: Now Window's Security window will pop up window's. Here you can verify whether your Defender firewall is active or not.


Window 10 (Base-install) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Windows Security
Home
Virus & threat protection
Account protection
Firewall & network protection
App & browser control
Device security
Device performance & health
Family options
Settings
Type here to search
31°C
12:16 PM
6/18/2025

Firewall & network protection

Who and what can access your networks.

Domain network
Firewall is on.

Private network
Firewall is on.

Public network (active)
Firewall is on.

Allow an app through firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default

Windows Community videos
Learn more about Firewall & network protection

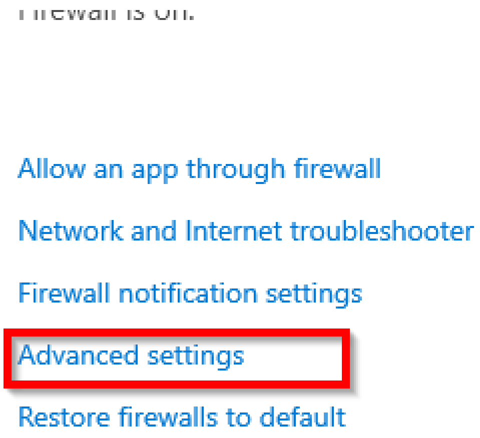
Have a question?
Get help

Who's protecting me?
Manage providers

Help improve Windows Security
Give us feedback

Change your privacy settings
View and change privacy settings for your Windows 10 device.
Privacy settings
Privacy dashboard
Privacy Statement

Step 7: Now to configure the firewall according to your requirement, click Advanced setting.


Firewall is on.

Allow an app through firewall

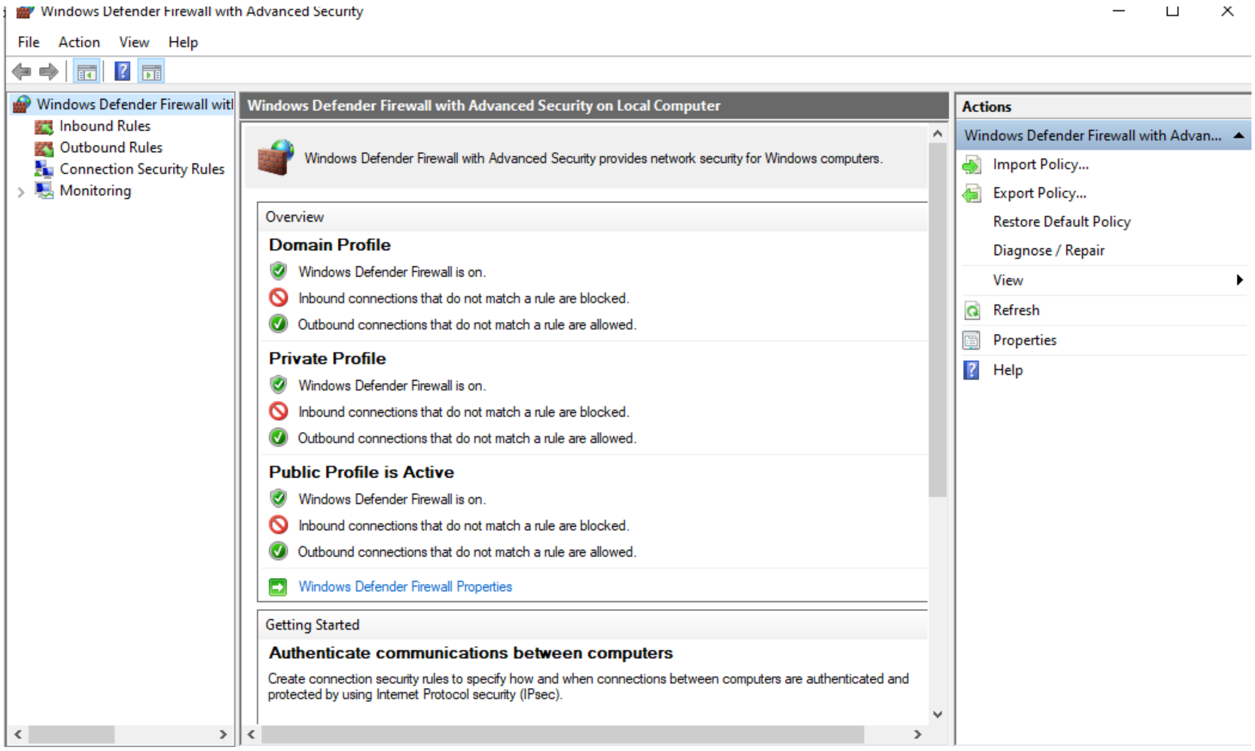
Network and Internet troubleshooter

Firewall notification settings

Advanced settings

Restore firewalls to default

Step 8: Windows Defender Firewall with Advanced Security window will launch after giving administrative permission.



Windows Defender Firewall with Advanced Security on Local Computer

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

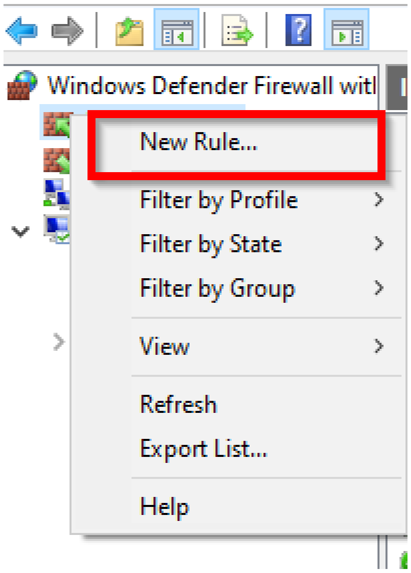
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Step 9: The left pane has several options:

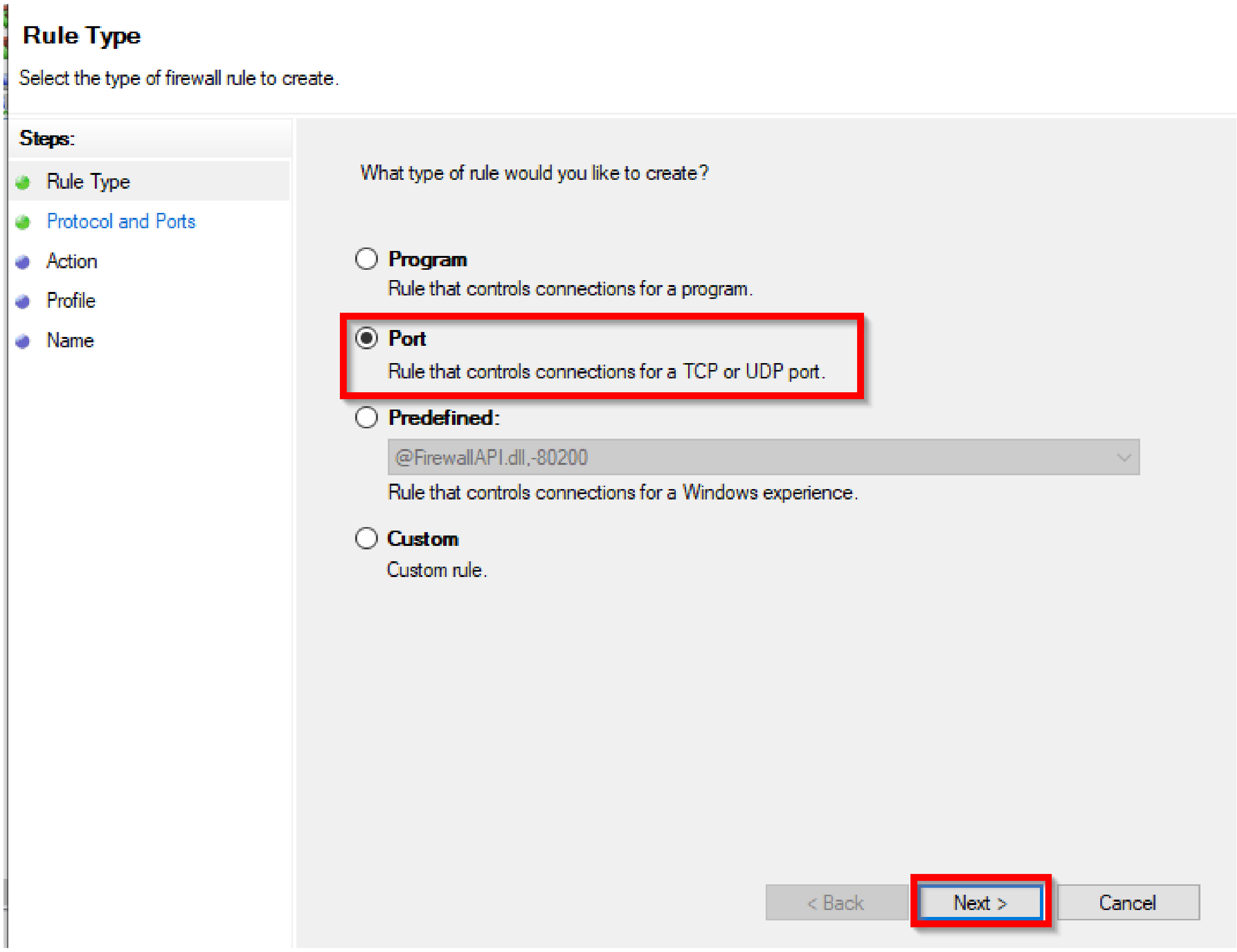
Inbound rules: Programs, processes, ports can be allowed or denied the incoming transmission of data within this inbound rules.

Outbound rules: Here we can specify whether data can be sent outwards by that program, process, or port.

Step 10: To add a new inbound rule, select Inbound Rules option, then click New Rule… from the right pane.



Step 11: Now we will configure an inbound rule for a network port. A New Inbound Rule Wizard window pops-up, select Port option and click next.



Rule Type

Select the type of firewall rule to create.

Steps:

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

What type of rule would you like to create?

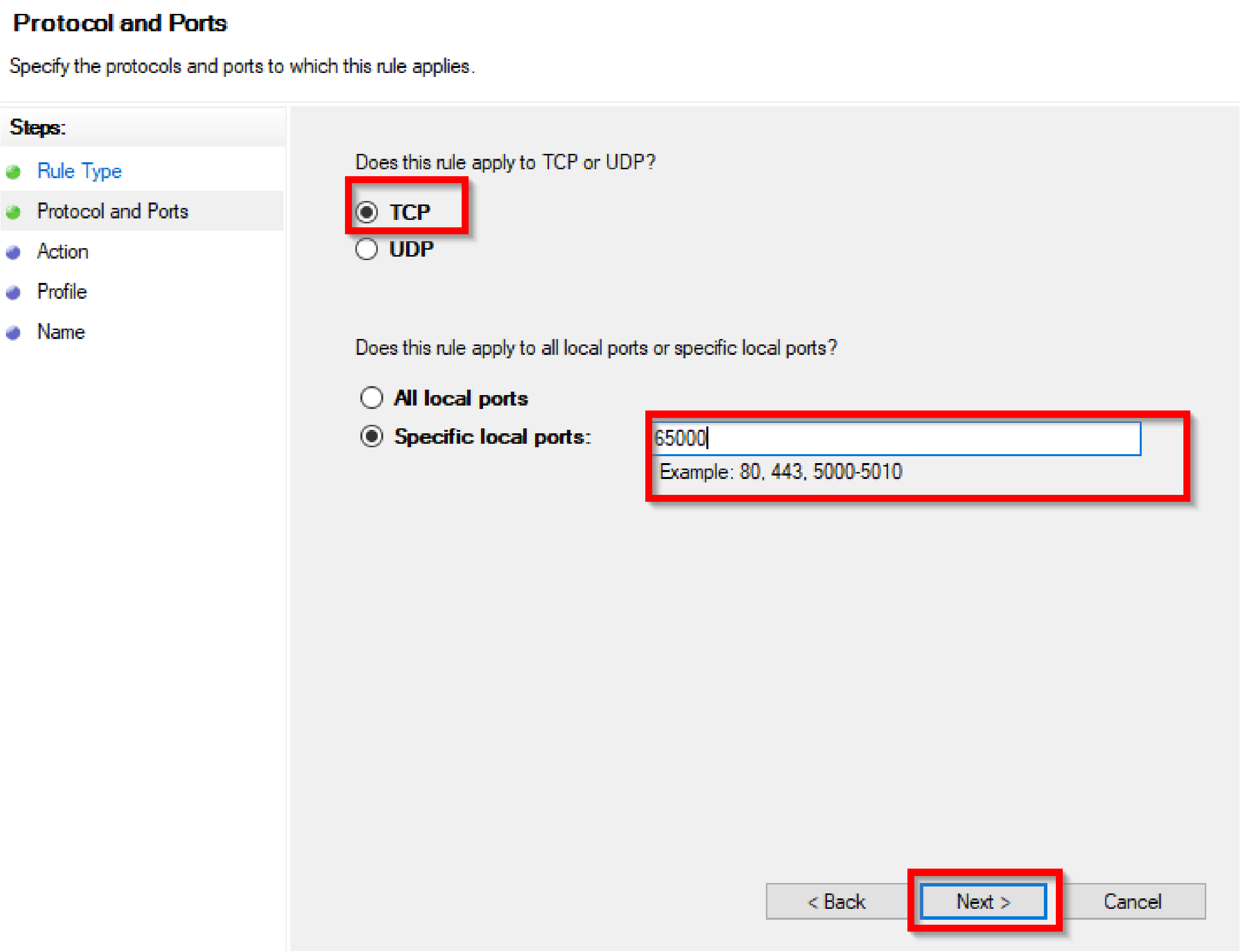
○ **Program**
Rule that controls connections for a program.

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

○ **Predefined:**
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Step 12: Now select TCP and specify port number 65000.



Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● TCP

○ UDP

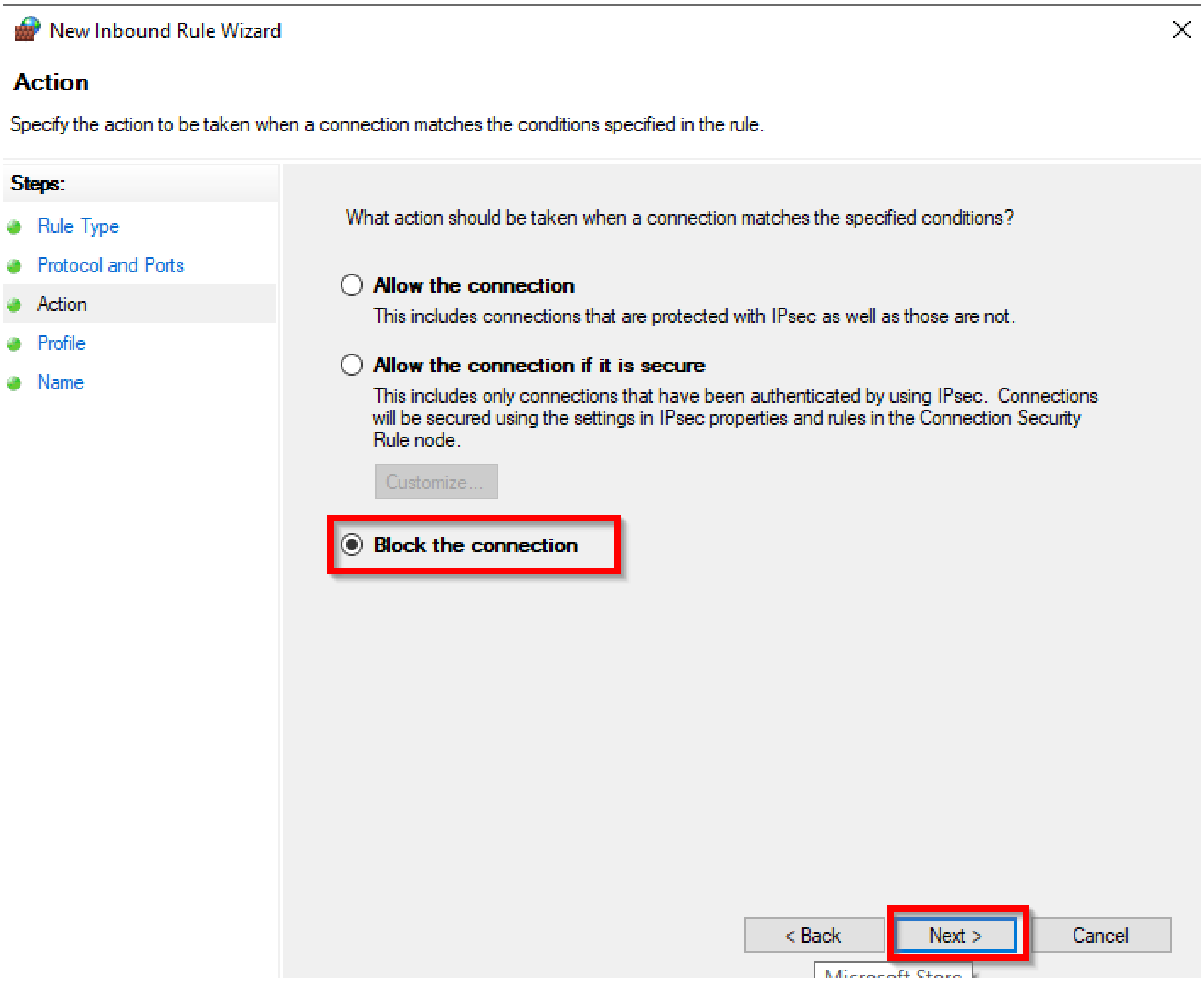
Does this rule apply to all local ports or specific local ports?

○ All local ports

● Specific local ports: 65000

Example: 80, 443, 5000-5010

Step 13: Now we can select the action we need to take on this port. We will block the inbound connection by selecting Block the connection option then click Next.



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

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

What action should be taken when a connection matches the specified conditions?

○ **Allow the connection**

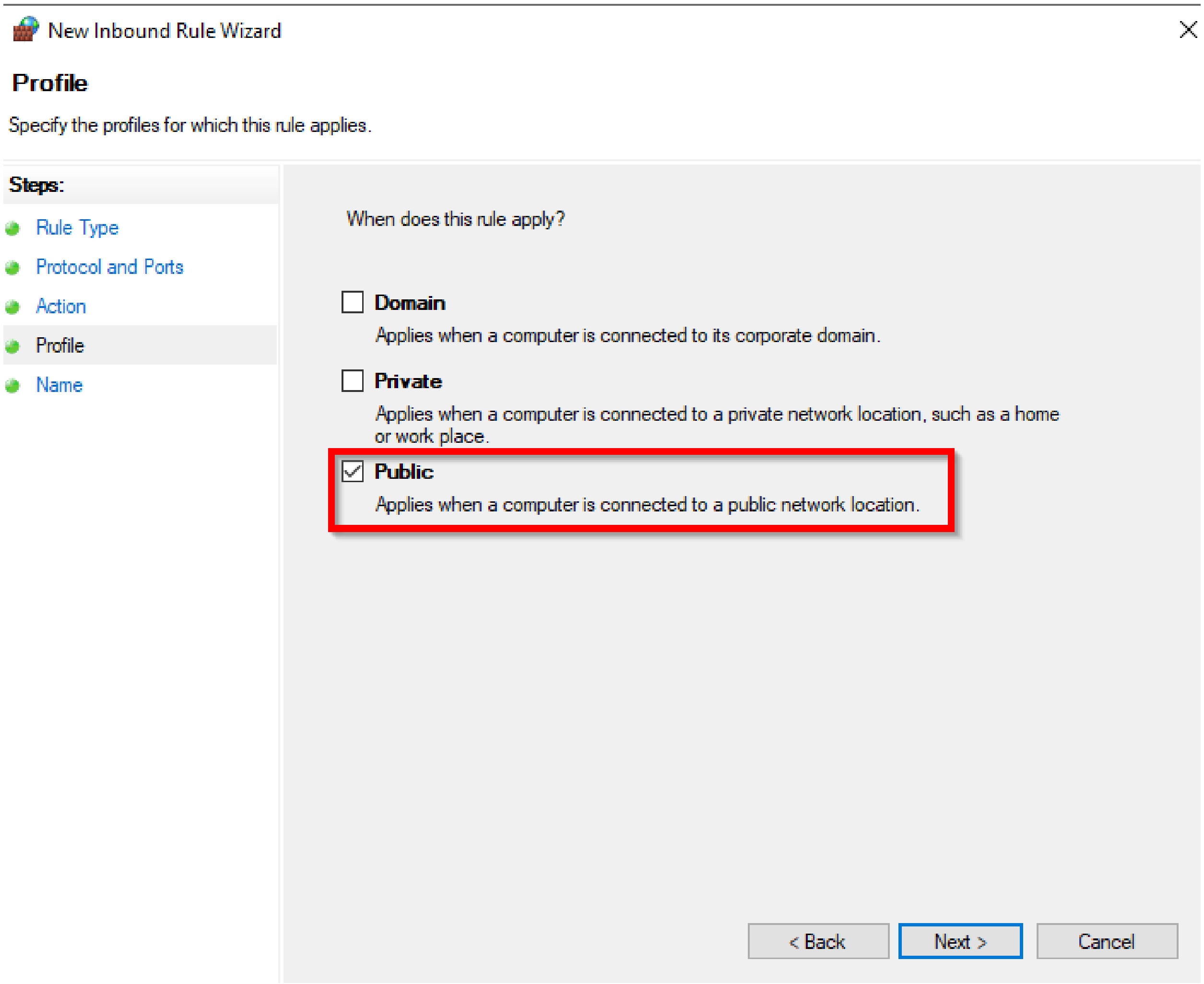
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**

Step 14: Here we can specify when should this rule come into action. We will keep only Public option selected and move Next.



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

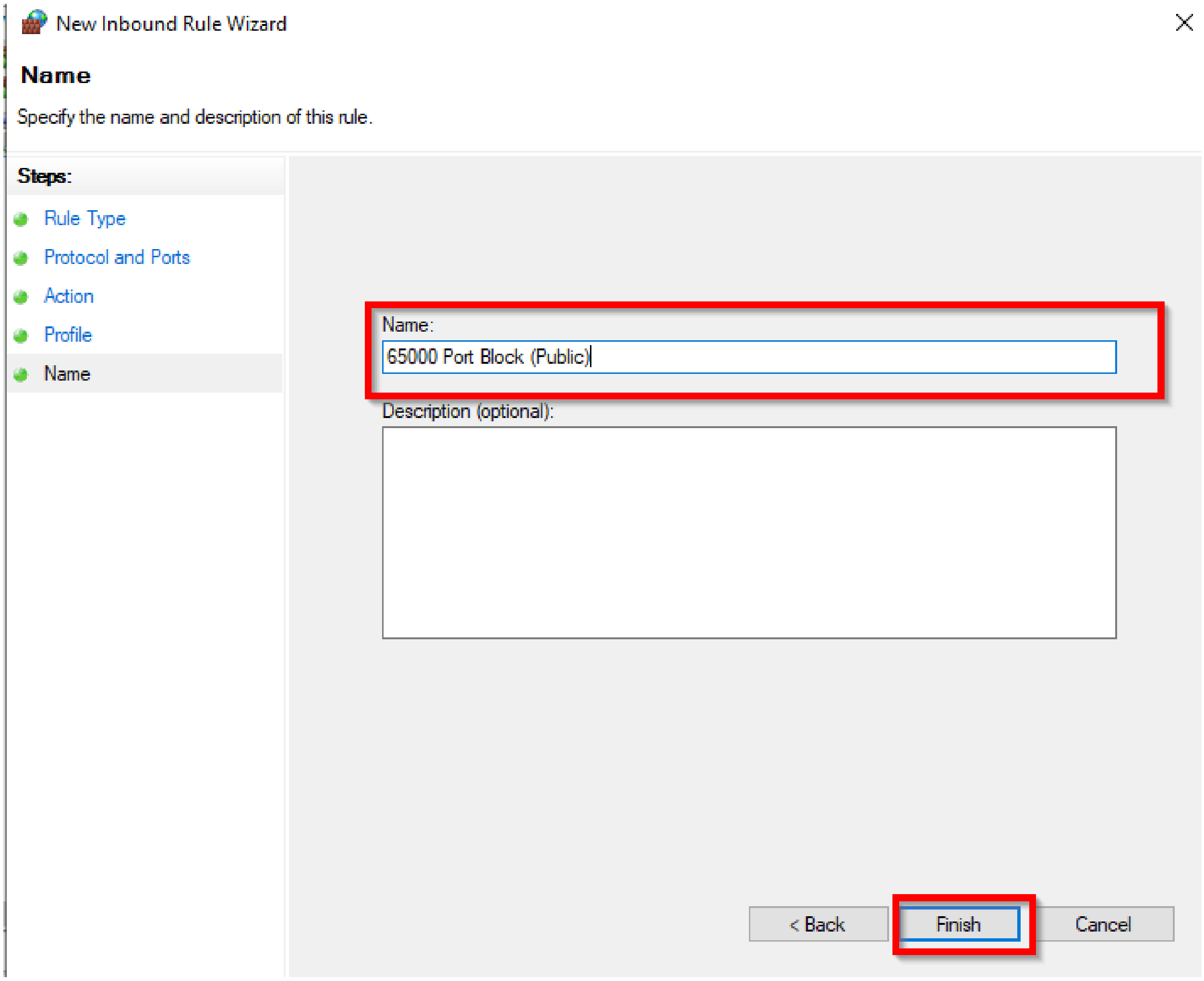
When does this rule apply?

☐ **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.

Step 15: This is the last step. Here we provide a name to this rule so that we can keep track of it later in the Inbound rules list. Write the name “65000 Port Block (Public)”. Click Finish.



New Inbound Rule Wizard

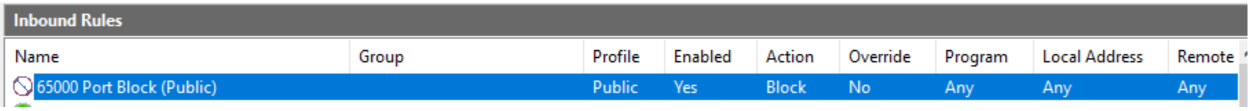
Name

Specify the name and description of this rule.

Name:
65000 Port Block (Public)

Description (optional):

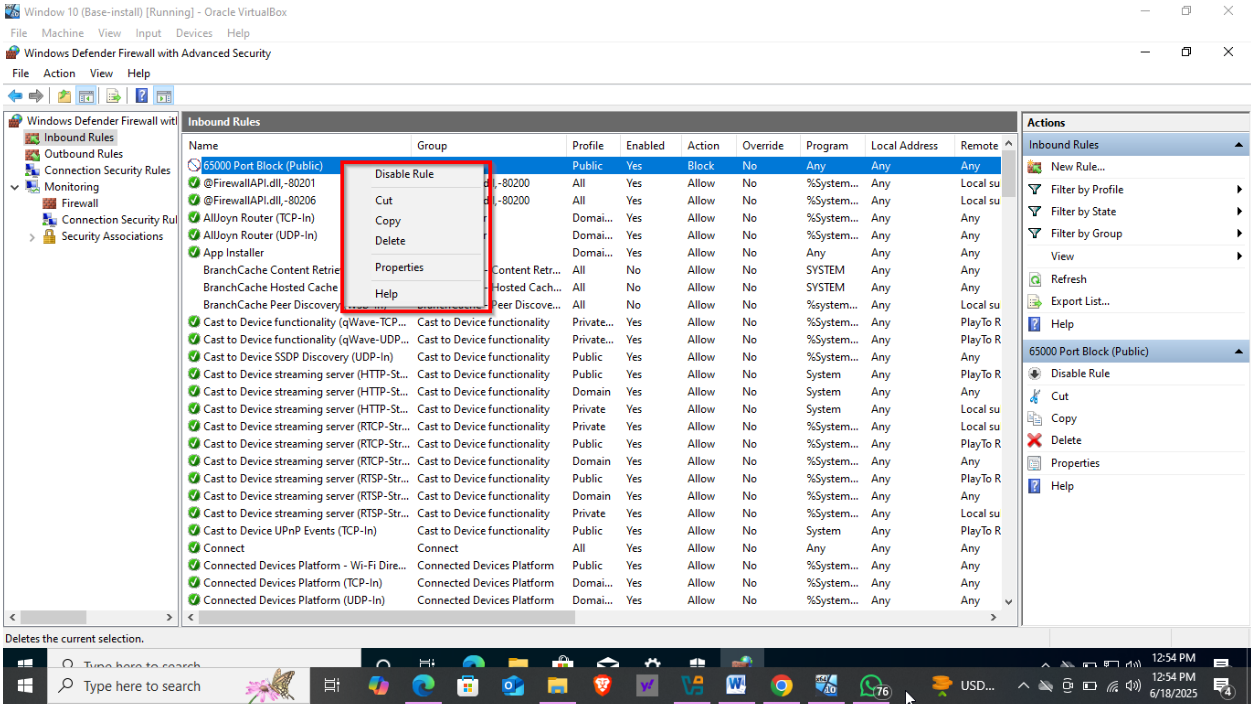
Step 16: The inbound rule is successfully created. We can find “65000 Port Block (Public)” in the Inbound rules list.



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote
65000 Port Block (Public)		Public	Yes	Block	No	Any	Any	Any

Step 17: Right-click the rule we just created and there are multiple options with which it can be Disabled or Deleted.

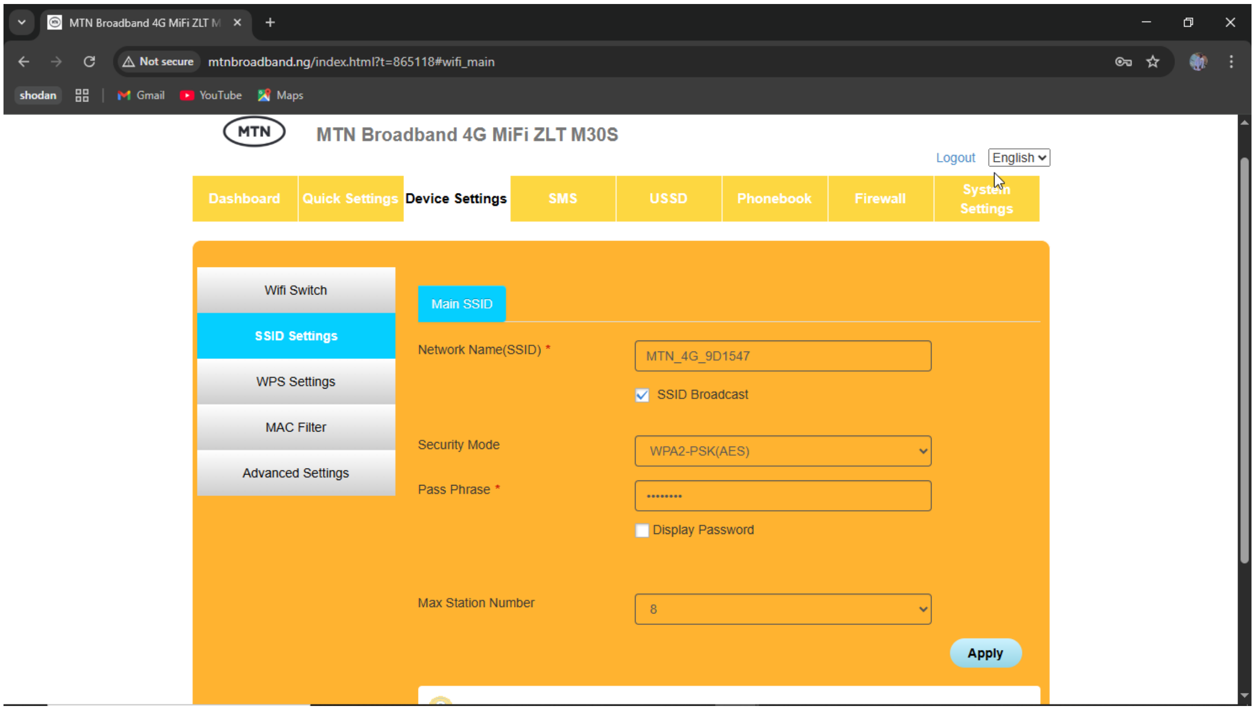


Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote
65000 Port Block (Public)		Public	Yes	Block	No	Any	Any	Any
@FirewallAPI.dll,-80201	dll,-80200	All	Yes	Allow	No	%System...	Any	Local su
@FirewallAPI.dll,-80206	dll,-80200	All	Yes	Allow	No	%System...	Any	Local su
AllJoyn Router (TCP-In)	r	Domai...	Yes	Allow	No	%System...	Any	Any
AllJoyn Router (UDP-In)	r	Domai...	Yes	Allow	No	%System...	Any	Any
App Installer		Domai...	Yes	Allow	No	Any	Any	Any
BranchCache Content Retrie	- Content Retr...	All	No	Allow	No	SYSTEM	Any	Any
BranchCache Hosted Cache	- Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any
BranchCache Peer Discovery	- Peer Discove...	All	No	Allow	No	%system...	Any	Local su
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo R
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo R
Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	Any
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayTo R
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes	Allow	No	System	Any	Any
Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes	Allow	No	System	Any	Local su
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local su
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo R
Cast to Device streaming server (RTCP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo R
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any
Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local su
Cast to Device UPnP Events (TCP-In)	Cast to Device functionality	Public	Yes	Allow	No	System	Any	PlayTo R
Connect	Connect	All	Yes	Allow	No	Any	Any	Any
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public	Yes	Allow	No	%System...	Any	Any
Connected Devices Platform (TCP-In)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any
Connected Devices Platform (UDP-In)	Connected Devices Platform	Domai...	Yes	Allow	No	%System...	Any	Any

Security Configurations:

- Changed default passwords on router and devices.
- Enabled WPA2 wireless encryption.



mtnbroadband.ng/index.html?t=865118#wifi_main

MTN Broadband 4G MiFi ZLT M30S

Network Name(SSID) * MTN_4G_9D1547

☑ SSID Broadcast

Security Mode WPA2-PSK(AES)

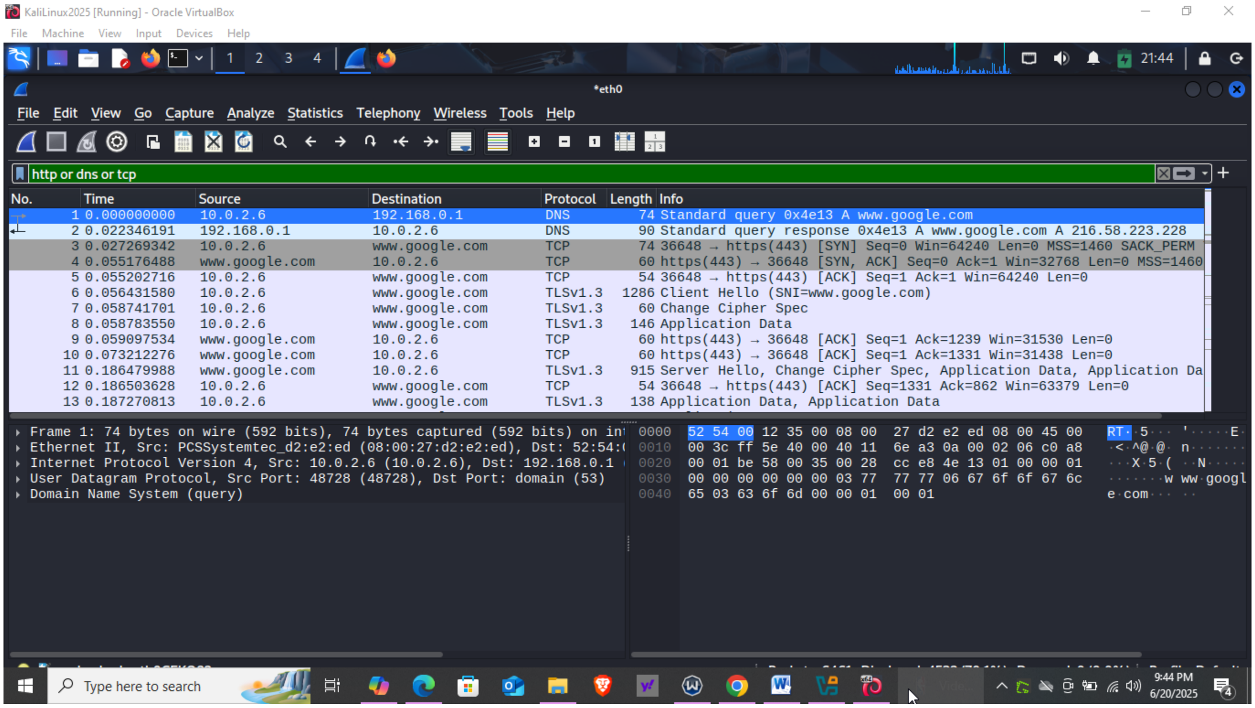
Pass Phrase * ••••••••

□ Display Password

Max Station Number 8

3. Monitor Network Traffic:

Tool Used: Wireshark



KaliLinux2025 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
21:44
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Type here to search
9:44 PM
6/20/2025

```
http or dns or tcp

No.  Time         Source          Destination     Protocol Length Info
   1 0.000000000  10.0.2.6        192.168.0.1     DNS         74 Standard query 0x4e13 A www.google.com
   2 0.022346191  192.168.0.1     10.0.2.6        DNS         90 Standard query response 0x4e13 A www.google.com A 216.58.223.228
   3 0.027269342  10.0.2.6        www.google.com  TCP         74 36648 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
   4 0.055176488  www.google.com  10.0.2.6        TCP         60 https(443) → 36648 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
   5 0.055202716  10.0.2.6        www.google.com  TCP         54 36648 → https(443) [ACK] Seq=1 Ack=1 Win=64240 Len=0
   6 0.056431580  10.0.2.6        www.google.com  TLSv1.3   1286 Client Hello (SNI=www.google.com)
   7 0.058741701  10.0.2.6        www.google.com  TLSv1.3     60 Change Cipher Spec
   8 0.058783550  10.0.2.6        www.google.com  TLSv1.3    146 Application Data
   9 0.059097534  www.google.com  10.0.2.6        TCP         60 https(443) → 36648 [ACK] Seq=1 Ack=1239 Win=31530 Len=0
  10 0.073212276  www.google.com  10.0.2.6        TCP         60 https(443) → 36648 [ACK] Seq=1 Ack=1331 Win=31438 Len=0
  11 0.186479988  www.google.com  10.0.2.6        TLSv1.3    915 Server Hello, Change Cipher Spec, Application Data, Application Da
  12 0.186503628  10.0.2.6        www.google.com  TCP         54 36648 → https(443) [ACK] Seq=1331 Ack=862 Win=63379 Len=0
  13 0.187270813  10.0.2.6        www.google.com  TLSv1.3    138 Application Data, Application Data

▸ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on in
▸ Ethernet II, Src: PCSSystemtec_d2:e2:ed (08:00:27:d2:e2:ed), Dst: 52:54:
▸ Internet Protocol Version 4, Src: 10.0.2.6 (10.0.2.6), Dst: 192.168.0.1
▸ User Datagram Protocol, Src Port: 48728 (48728), Dst Port: domain (53)
▸ Domain Name System (query)

0000  52 54 00 12 35 00 08 00  27 d2 e2 ed 08 00 45 00   RT··5···'·····E·
0010  00 3c ff 5e 40 00 40 11  6e a3 0a 00 02 06 c0 a8   ·<·^@·@·n·······
0020  00 01 be 58 00 35 00 28  cc e8 4e 13 01 00 00 01   ···X·5·(··N·····
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   ·······www·googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e·com·····
```

Protocol	Description	Observation
DNS	Domain Name System	Queries for `www.google.com`
TCP	Transmission Control Protocol	TCP handshake to `google.com` on port `443` (HTTPS)
TLSv1.3	Secure communication	TLS encryption established after TCP handshake

What This Traffic Means:

1. **DNS (Packets 1 & 2)**

- My system queries DNS to resolve `www.google.com`.
- DNS server responds with IP `216.58.223.228` (Google's server).

2. **TCP (Packets 3-5)**

- TCP three-way handshake starts:
  - `SYN` (start connection),
  - `SYN-ACK` (acknowledge),

    - `ACK` (confirm connection established).
- Target server: google.com on port `443` (HTTPS).

3. **TLSv1.3 (Packets 6+)**

- After TCP, encrypted communication starts.
- Client Hello packet (packet 6) includes SNI: www.google.com — this shows which domain you're connecting to (visible even in encrypted traffic).
- Then encryption begins (cipher negotiation, key exchange, encrypted data transfer).

No Suspicious Traffic

In my current capture:

- All observed traffic looks normal.
- I visited a legitimate site (`google.com`).
- No unusual IP addresses or unknown domains.
- No abnormal ports (standard HTTPS port `443` is used).

4. How These Security Measures Help Protect the Network

- **Firewall:** Prevents unauthorized external access by filtering traffic based on rules.
- **Strong Passwords:** Protect devices and accounts from brute force and credential stuffing attacks.
- **WPA3 Encryption:** Secures wireless communications, preventing eavesdropping.
- **Network Monitoring:** Allows early detection of unusual patterns or malicious traffic.

5: Reflection on Security Best Practices

1 Additional Security Measures for Complex Networks

- **Intrusion Detection and Prevention Systems (IDS/IPS):** Monitor and block suspicious activities in real-time.
- **Security Information and Event Management (SIEM):** Aggregate and analyze security logs across the network.
- **Zero Trust Architecture (ZTA):** Enforce continuous verification for users and devices.
- **Multi-Factor Authentication (MFA):** Strengthen access control.
- **Network Segmentation:** Isolate critical systems to contain breaches.
- **Patch and Vulnerability Management:** Ensure systems are regularly updated and vulnerabilities are remediated.

2 Educating Others on Network Security Importance

"In today's interconnected world, cybersecurity awareness is essential for everyone. I would educate others by simplifying complex concepts: showing how weak passwords, clicking unknown links, or using unprotected Wi-Fi can open doors to attackers. Simple steps like using strong passwords, enabling two-factor authentication, regularly updating devices, and being cautious with emails can significantly reduce personal and organizational risk."

Conclusion

This (Task 1) internship provided hands-on experience in identifying and mitigating network threats, configuring essential security controls, and analyzing real network traffic. The comprehensive exercise strengthened my understanding of fundamental cybersecurity principles and highlighted the importance of layered defense strategies.