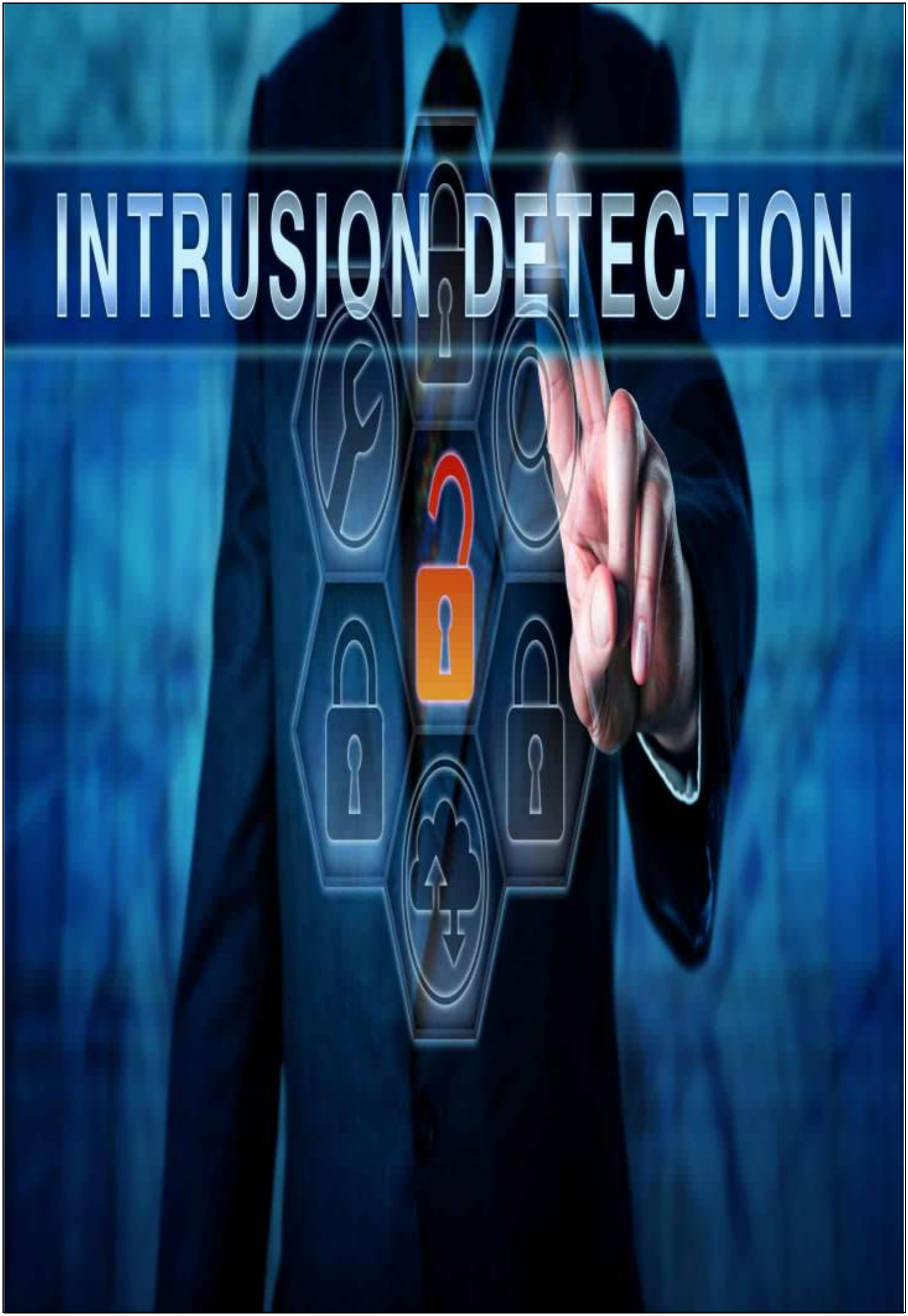

INTRUSION DETECTION

Module 12 evading IDS,IPS firewall and honeypots

Index

- Bastion host
- Screened subnet/dmz/popular
- Multi-home firewall

6 What is ips

- Why are use ips
- How does work ips

Task1 How to configuration Intrusion Detection tool Snort

Task2 How to configuration Windows firewall

How to windows firewall configuration outbound traffic rule

How to windows firewall configuration inbound traffic rule

7 types of security controls

Security guards detection honeypot

Extra activity using zone alarm how to configrtaion

What is IDS

An **Intrusion Detection System (IDS)** is a cybersecurity tool used to detect unauthorized access or malicious activities in a computer system or network.
Its main purpose is to monitor and analyze traffic for signs of suspicious behavior.
Unlike firewalls, which block traffic, IDS only detects and alerts.

Way are use ids

1. **Detect Unauthorized Access**
   IDS helps identify when someone tries to break into a system or network.

2. **Monitor Network Traffic**
   It watches data moving through the network to find suspicious patterns.

3. **Alert on Threats**
   When something unusual or dangerous is found, IDS sends an alert.

4. **Protect Sensitive Data**
   It helps prevent attackers from stealing or damaging important information.

5. **Identify Malware and Attacks**
   IDS can detect known malware, viruses, and hacking attempts.
6. **Support Incident Response**
   It provides logs and details to help security teams respond quickly.

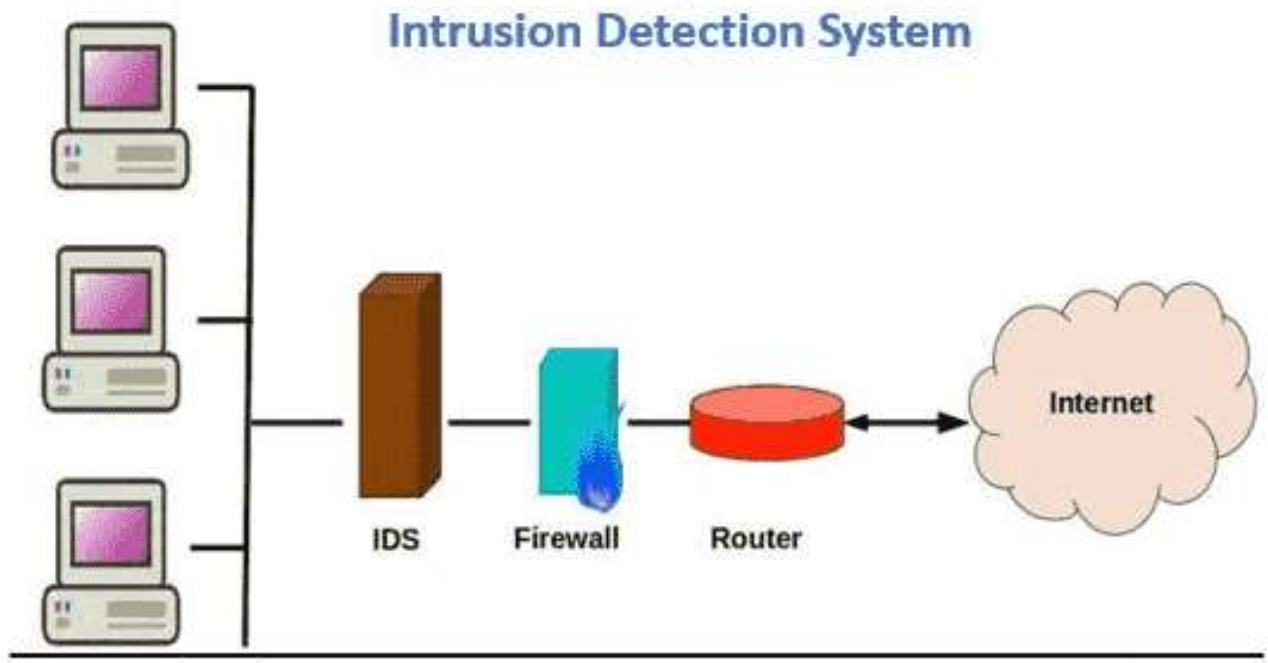
7. **Compliance Requirements**
   Many laws and regulations (like HIPAA, PCI-DSS) require monitoring tools like IDS.

8. **Improve Security Awareness**
   It gives visibility into what's happening in your systems and networks.

9. **Analyze Past Attacks**
   IDS logs can help understand how attacks happened and prevent them in the future.

10. **Work With Other Tools**
    IDS works alongside firewalls, antivirus, and other security systems for stronger protection.

How does ids work



1. **Monitors Traffic or System Activity**
   IDS watches data that flows through a network or activity on a computer system.

2. **Collects Data**
   It gathers information from network packets, system logs, or files.

3. **Analyzes Behavior**
   The system looks at the data to find anything strange or harmful.

4. **Uses Detection Methods**
   IDS can detect threats in two main ways:
   - **Signature-based Detection**: Looks for known attack patterns (like a virus signature).
   - **Anomaly-based Detection**: Looks for unusual behavior that doesn't match normal activity.

5. **Compares with Rules or Baselines**
   IDS compares current activity to a set of rules or what's considered "normal" behavior.

6. **Raises an Alert**
   If something suspicious is found, the IDS alerts the system administrator.

7. **Logs the Event**
   It records details about what happened for future investigation.

8. **No Action (Detection Only)**
   IDS does **not** block or stop the attack — it only reports it (unlike IPS, which can block).

Type of IDS

1. **NIDS (Network-based IDS)**
   - Monitors network traffic in real-time.
   - Placed at strategic points (e.g., near a firewall or router).

- Detects attacks like DDoS, port scanning, or unauthorized access.
- Example: Snort, Suricata.

2. **HIDS (Host-based IDS)**
   - Installed on individual devices or servers.
   - Monitors system files, logs, and application activity.
   - Detects changes in files, unauthorized logins, or malware behavior.
   - Example: OSSEC, Tripwire.

3. **SIDS (Signature-based IDS)**
   - Detects threats by matching patterns (signatures) of known attacks.
   - Very effective against known threats.
   - Needs regular updates to stay effective.

4. **AIDS (Anomaly-based IDS)**
   - Detects threats by identifying unusual behavior that differs from normal patterns.

- Can detect new or unknown attacks (zero-day threats).
- May produce false positives if not properly trained.

5. **Hybrid IDS**
   - Combines features of signature-based and anomaly-based systems.
   - Offers better detection accuracy and flexibility.
   - Balances speed and ability to detect both known and unknown threats.

Types of ids alert

When an Intrusion Detection System (IDS) detects suspicious activity, it can generate different types of alerts based on severity or type of threat:

---

1. True Positive (TP)

- **Meaning**: A real attack occurred and the IDS correctly identified it.

- ✅ **Good** – this is what we want from an IDS.

---

2. False Positive (FP)

- **Meaning**: The IDS thinks an attack occurred, but it was actually harmless activity.
- ⚠️ **Annoying** – can waste time and cause alert fatigue.

---

3. True Negative (TN)

- **Meaning**: No attack happened, and the IDS correctly ignored it.
- ✅ **Normal** – no alert needed.

---

4. False Negative (FN)

- **Meaning**: An actual attack happened, but the IDS failed to detect it.
- ❌ **Dangerous** – the threat goes unnoticed.

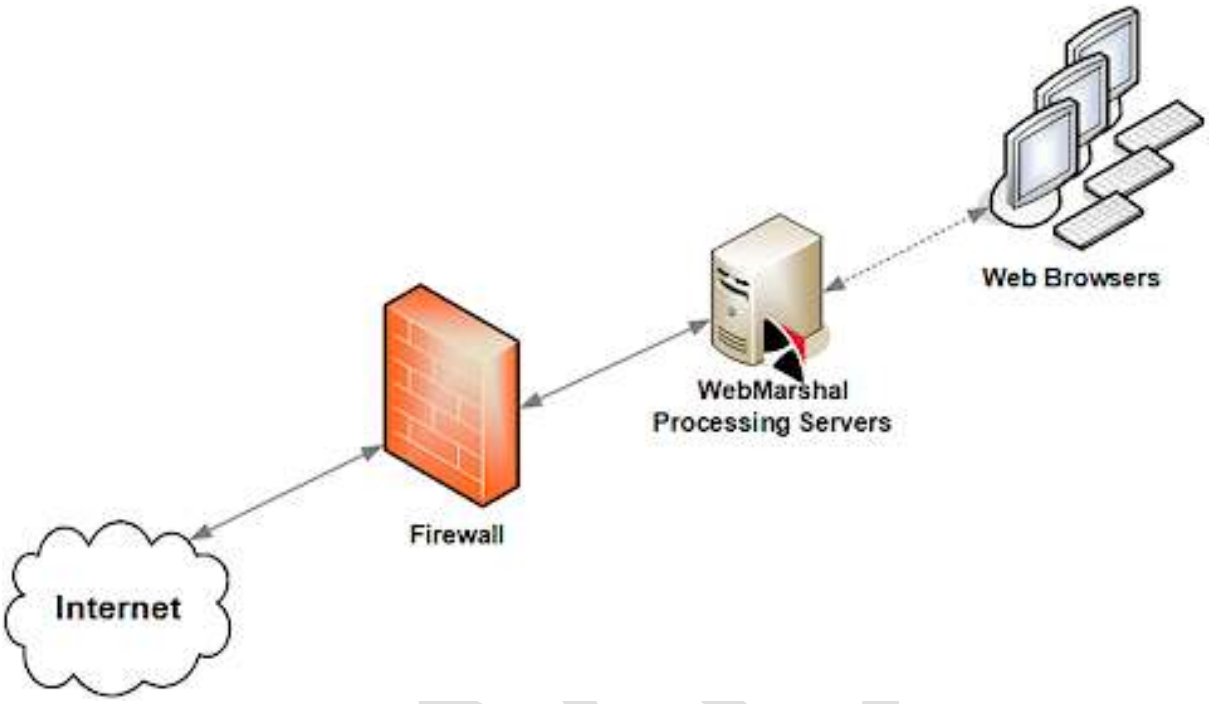
Types of password

- Text Passwords
- Biometric Passwords
- Application Passwords
- Default Passwords

what is firewall

A **firewall** is a **security system** that **monitors and controls incoming and outgoing network traffic** based on **predefined rules**. It acts like a **barrier** or **gatekeeper** between a **trusted network** (like your computer or internal network) and an **untrusted network** (like the internet).

How does work firewall



A firewall is a network security system 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, to prevent unauthorized access and potential threats

Way are use firewall

- **Block Unauthorized Access**

Prevents hackers or unknown users from entering your network or computer.

- **Protect Sensitive Data**

Helps safeguard personal, business, or financial information from being stolen.

- **Monitor Network Traffic**

Keeps track of all data going in and out of your system.

- **Prevent Malware & Viruses**

Blocks harmful software and known threats before they reach your device.

- **Control Internet Use**

Can restrict access to certain websites or online services (e.g., in schools or offices).

- **Stop Hacking Attempts**

Detects and blocks attempts like port scanning, brute-force attacks, or data theft.

- **Set Custom Security Rules**

Allows network admins to allow or block specific IPs, ports, or applications.

- **Protect Multiple Devices**

A single firewall can secure an entire network (home or business).

- **Improve Network Performance**

Reduces the risk of network overloads from malicious traffic.

Types of firewall

Packet-Filtering Firewall

- **Function:** Inspects packets individually based on IP addresses, ports, and protocols.
- **Pros:** Fast and simple.
- **Cons:** Doesn't inspect packet payloads, so limited protection.
- **Example:** Access Control Lists (ACLs) on routers.

---

2. Stateful Inspection Firewall (Dynamic Packet Filtering)

- **Function:** Tracks the state of active connections and makes decisions based on the context of traffic.

- **Pros:** More secure than packet-filtering; understands connection states.
- **Cons:** Slightly slower; more complex.

---

3. Proxy Firewall (Application-Level Gateway)

- **Function:** Acts as an intermediary between internal users and the internet, inspecting traffic at the application layer.
- **Pros:** Strong filtering and anonymity; can inspect data payloads.
- **Cons:** Slower due to deeper inspection; can be resource-intensive.

---

4. Next-Generation Firewall (NGFW)

- **Function:** Combines traditional firewall functions with advanced features like intrusion prevention, deep packet inspection, and application awareness.
- **Pros:** Comprehensive protection against modern threats.
- **Cons:** High cost and complexity.

---

5. Network Address Translation (NAT) Firewall

- **Function:** Masks internal IP addresses by converting them into a single public IP address.
- **Pros:** Adds a layer of privacy and protection.
- **Cons:** Limited inspection; not a standalone security solution.

---

6. Web Application Firewall (WAF)

- **Function:** Specifically protects web applications by monitoring HTTP traffic.
- **Pros:** Protects against web-based attacks like SQL injection and cross-site scripting (XSS).
- **Cons:** Limited to web apps only.

---

7. Cloud-Based Firewall (Firewall as a Service - FWaaS)

- **Function:** Firewall hosted in the cloud, protecting cloud infrastructure and remote users.
- **Pros:** Scalable, easy to deploy for distributed environments.

- **Cons:** Dependent on internet connectivity and third-party service reliability.

---

8. Hardware vs. Software Firewalls

- **Hardware Firewalls:** Physical devices placed between a network and the gateway (e.g., routers with firewall features).
- **Software Firewalls:** Programs installed on individual systems (e.g., Windows Firewall).

Types of Firewall Architectures

Firewall architecture refers to how firewalls are structured and deployed within a network to control and filter traffic. Here are the main types of **firewall architectures**:

---

1. Bastion Host Architecture

- **Definition:** A single, hardened system placed on the network perimeter.
- **Usage:** Acts as the sole point of contact between internal and external networks.
- **Pros:** Simple to implement.

- **Cons:** Single point of failure; limited protection.

---

2. Screened Subnet Architecture (DMZ - Demilitarized Zone)

- **Definition:** Uses two firewalls or a three-legged firewall to create a **DMZ** between the internal network and the internet.
- **Components:**
  - **External firewall:** Between internet and DMZ.
  - **Internal firewall:** Between DMZ and internal network.
  - **DMZ:** Hosts public-facing services (e.g., web, mail servers).
- **Pros:** Strong security, isolation of public services.
- **Cons:** More complex and expensive.

---

3. Screened Host Architecture

- **Definition:** Combines a **bastion host** and a **screening router**.
- **How it works:** The router filters traffic and forwards legitimate traffic to the bastion host.

- **Pros:** More secure than a single firewall.
- **Cons:** Still vulnerable if the bastion host is compromised.

---

4. Dual-Homed Host Architecture

- **Definition:** A single system with two network interfaces — one for internal, one for external connections.
- **How it works:** Acts as a firewall by not forwarding packets between interfaces unless specifically configured.
- **Pros:** Offers control over traffic routing.
- **Cons:** Not scalable for large networks.

---

5. Multi-Homed Firewall Architecture

- **Definition:** A firewall with three or more interfaces (e.g., internal, external, DMZ).
- **How it works:** Separates different network zones with strict rules.
- **Pros:** Highly flexible and secure.
- **Cons:** Complex to configure and maintain.

---

6. Distributed Firewall Architecture

- **Definition:** Firewalls are deployed across multiple points in the network (e.g., endpoints, cloud, gateways).
- **How it works:** Managed centrally, but filtering occurs at various network points.
- **Pros:** Scalable and effective for modern, decentralized networks.
- **Cons:** Requires centralized management tools and policy consistency.

What is IPS

- **IPS** stands for **Intrusion Prevention System**.
- It is a **network security technology**.
- IPS **monitors traffic** in real time.
- It detects and blocks **suspicious or malicious activity**.
- IPS works at the **network or host level**.
- It uses **signatures**, **anomaly detection**, or **behavior analysis**.
- IPS can **drop packets**, **block IPs**, or **reset connections**.

- It provides **proactive protection** unlike IDS (which only detects).
- IPS is often placed **behind the firewall**.
- It inspects traffic **before it reaches the internal network**.
- There are different types: **Network-based (NIPS)**, **Host-based (HIPS)**, etc.
- NIPS secures the entire network.
- HIPS protects individual computers or servers.
- IPS helps prevent **DDoS attacks, worms, malware**, and **exploits**.
- It generates **logs and alerts** for administrators.
- It must be **regularly updated** to detect new threats.
- False positives can occur and need **fine-tuning**.

Why are use IPS

An **IPS** is used to **enhance network and system security** by actively preventing threats. Here are the main reasons we use IPS:

✅ 1. Real-Time Threat Prevention

- Automatically blocks malicious traffic **before it reaches the target**.
- Protects against worms, viruses, exploits, and hackers.

✅ 2. Detects and Stops Known Attacks

- Uses **signature-based detection** to identify known threats.
- Blocks them instantly without waiting for admin action.

✅ 3. Stops Unknown or Suspicious Behavior

- With **anomaly and behavior-based detection**, it can stop zero-day or new attacks.

✅ 4. Reduces Human Error

- Works automatically; doesn’t rely solely on human monitoring or manual intervention.

✅ 5. Enhances Network Visibility

- Monitors all incoming and outgoing traffic.
- Helps identify weak points or misuse within the network.

✅ 6. Supports Compliance Requirements

- Helps meet **regulatory standards** (e.g., GDPR, HIPAA, PCI-DSS) by improving security controls.

✅ 7. Complements Other Security Tools

- Works alongside **firewalls, antivirus, and SIEM systems** for layered defense.

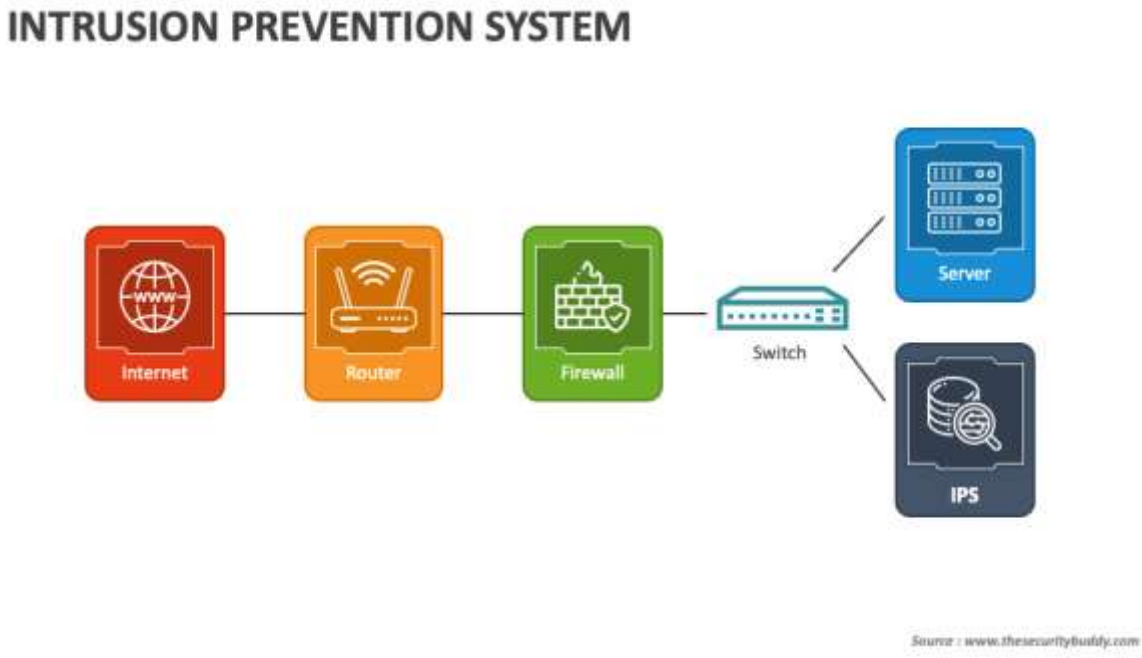
✅ 8. Reduces Damage from Attacks

- Stops threats early, minimizing potential **downtime, data loss, or breaches**.

✅ 9. Alerts and Logs for Forensics

- Logs events for later analysis or investigation.

How does work IPS



An **Intrusion Prevention System (IPS)** protects networks and systems by actively monitoring and

blocking malicious traffic in **real time**. Here's how it works, step by step:

⚙ Step-by-Step Working of IPS:

1. **Traffic Monitoring**
   - IPS constantly **monitors network traffic** (incoming and outgoing) between devices.

2. **Deep Packet Inspection (DPI)**
   - It examines the **content of packets** — not just headers — to detect threats hidden in the data.

3. **Threat Detection**
   - Uses various methods:
     - **Signature-based detection** – compares traffic to a database of known attack patterns.
     - **Anomaly-based detection** – identifies deviations from normal behavior.

- **Policy-based detection** – follows rules defined by the network administrator.

4. **Decision Making**
   - IPS determines if the traffic is:
     - **Legitimate** → Allow it.
     - **Malicious or suspicious** → Take action.

5. **Prevention/Action**
   - If a threat is detected, IPS can:
     - **Drop the malicious packets**
     - **Block the source IP address**
     - **Reset the connection**
     - **Quarantine the threat**
     - **Alert the administrator**

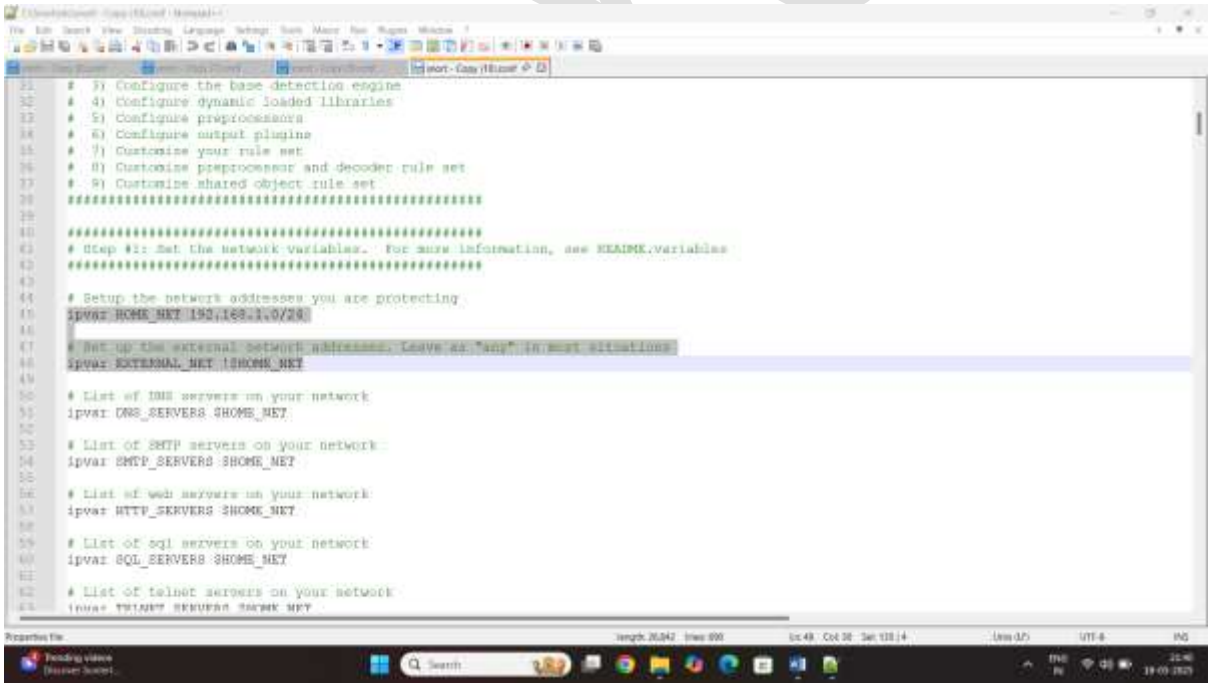
6. **Logging and Reporting**
   - Records the event in logs for review, analysis, or forensic investigation.
7. **Updates & Learning**

- Regular updates are applied to signature databases.
- Some IPS systems use **machine learning** to improve over time.

How to configuration Intrusion Detection tool Snort

Step 1: open the Snort note++

Step2: insert the input ip testing network

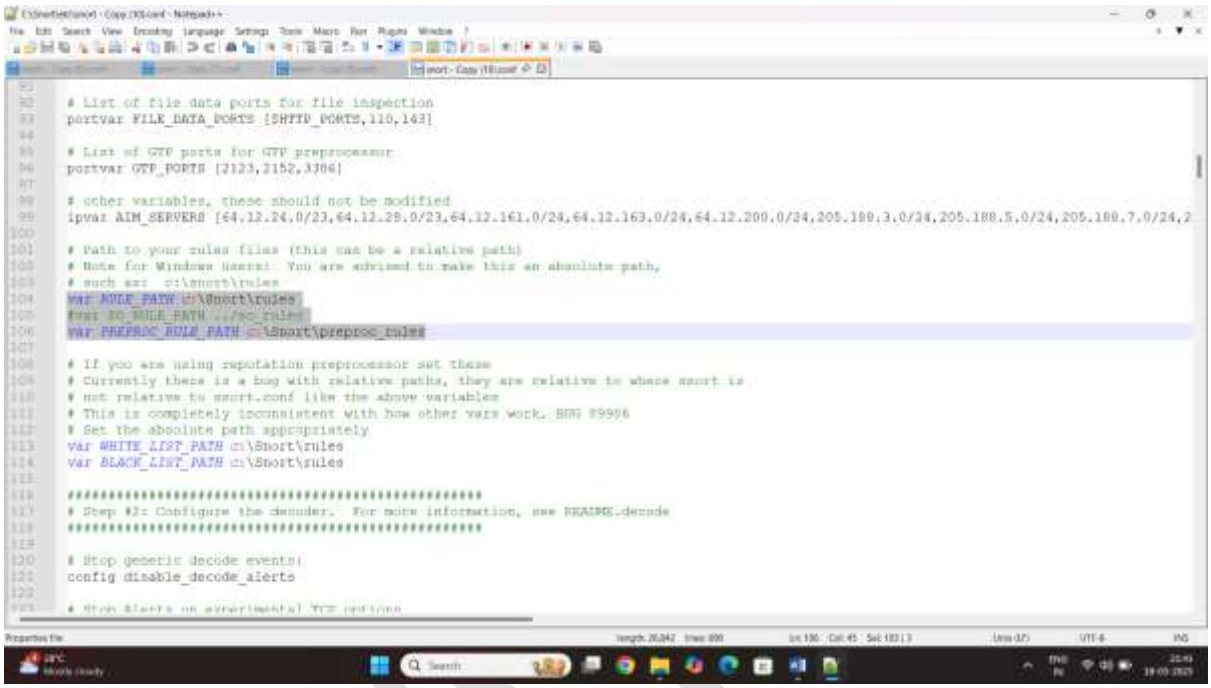


Step3: change line/45

Ipvar HOME_NET 192.168.1.0/24

Step4: change line/47

Ip EXTERNAL_NET !$ HOME_NET



Step5: change line/104

Var RULE_PATH c:\snort\rules

Step6:change line/105

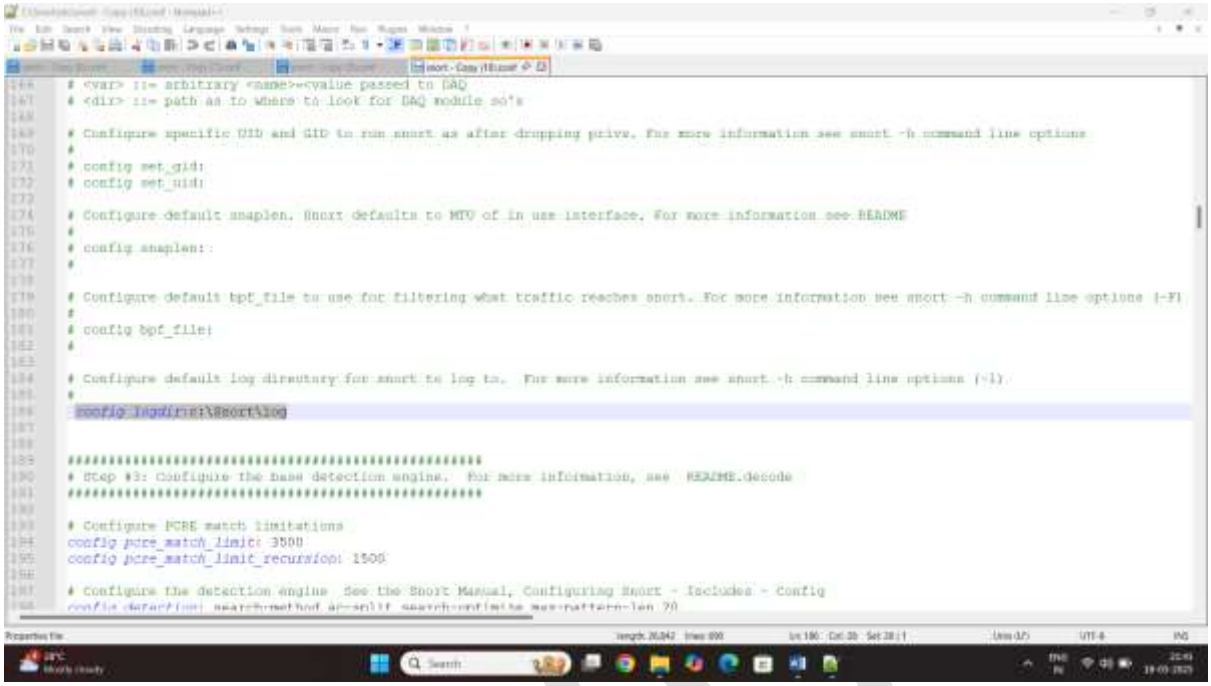
Remove hash

Step7: change line/

Var preproce_RULE_PATH
C:\snort\preproc_roles

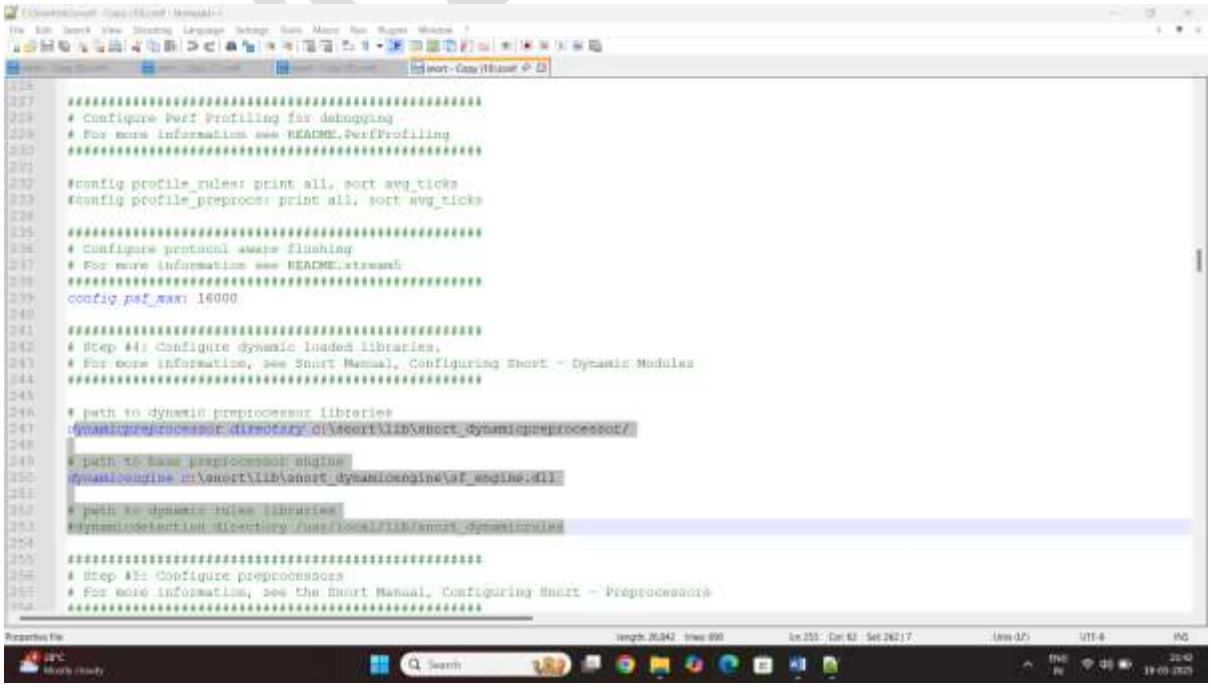
Step8: change line/

var BLACK_LIST_PATH c:\Snort\rules



Step8: change line/186

Remove the hash

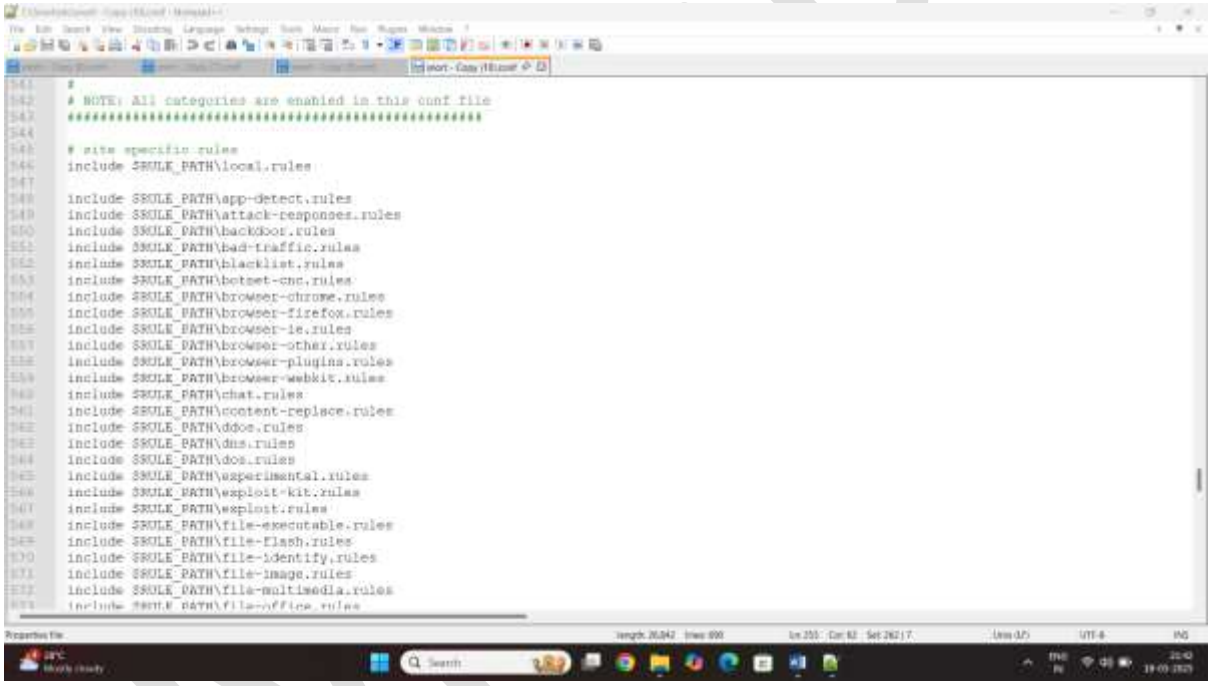


Step9: change line/247

dynamicpreprocessor directory c:\snort\lib\snort_dynamicpreprocessor/

Step10: change line/ 250

dynamicengine c:\snort\lib\snort_dynamicengine\sf_engine.dll

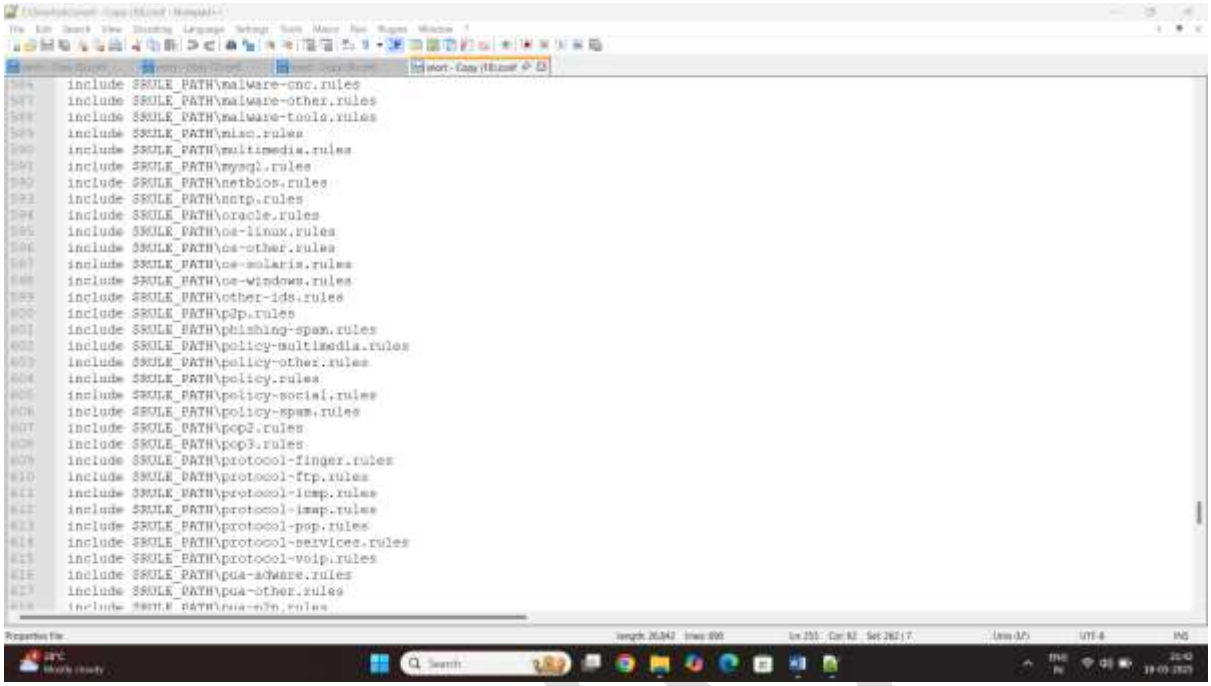


Step11: change line/ 511

whitelist $WHITE_LIST_PATH/whitelist.rules, \

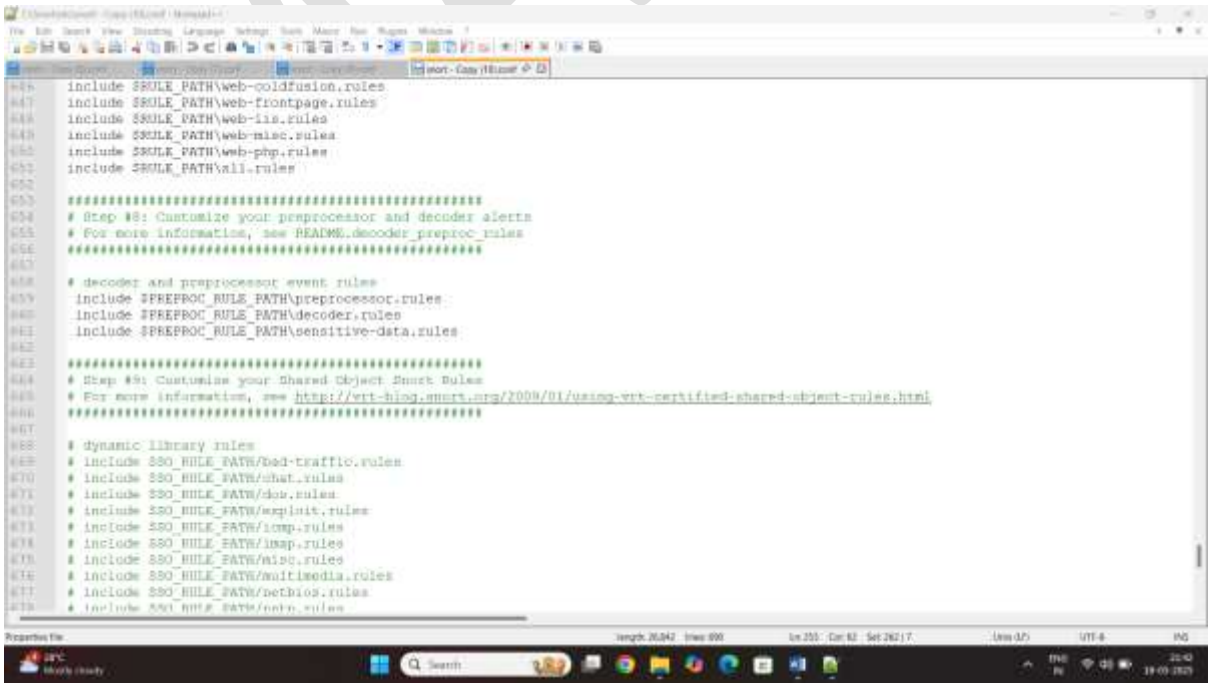
Step12: change line/512

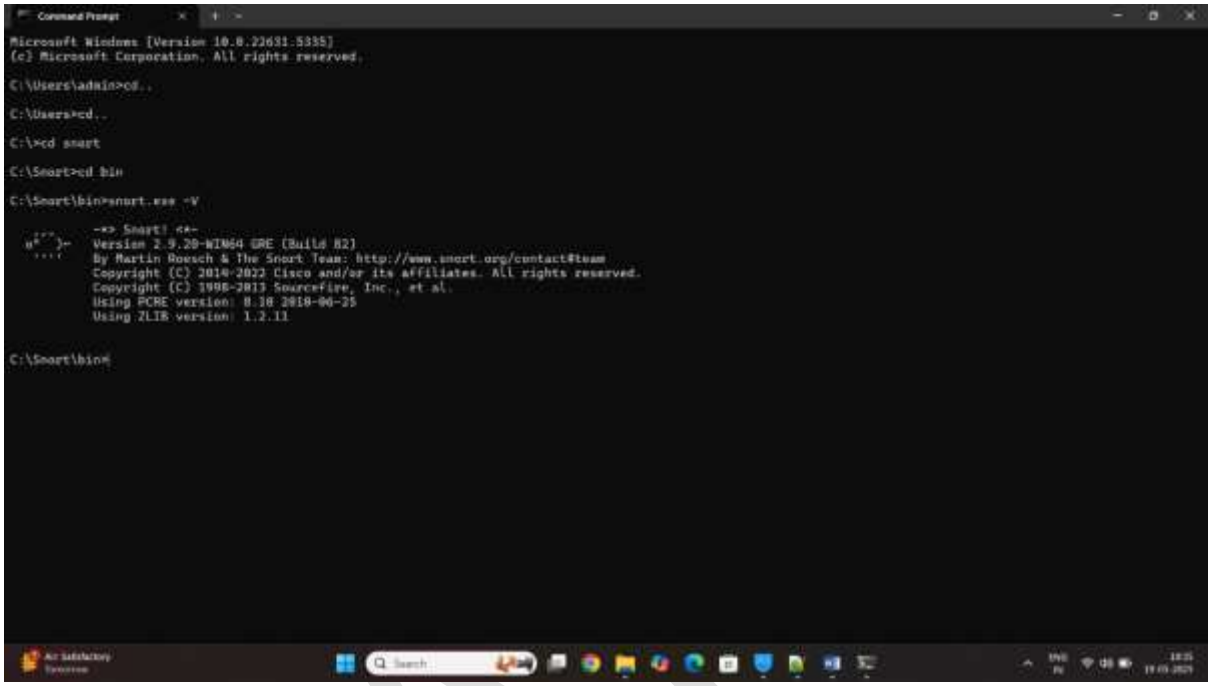
blacklist $BLACK_LIST_PATH/blacklist.rules



Step12: change line/

546 to 651 change /



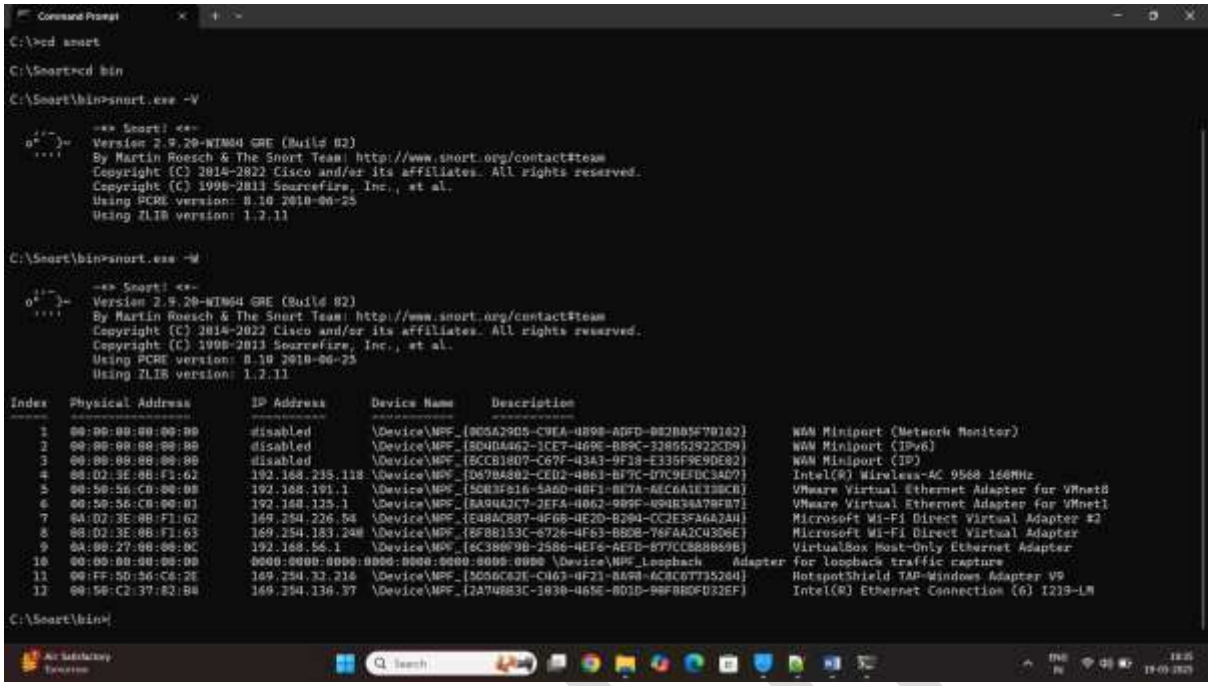


C:\cd snort

C:\ snort\cd bin

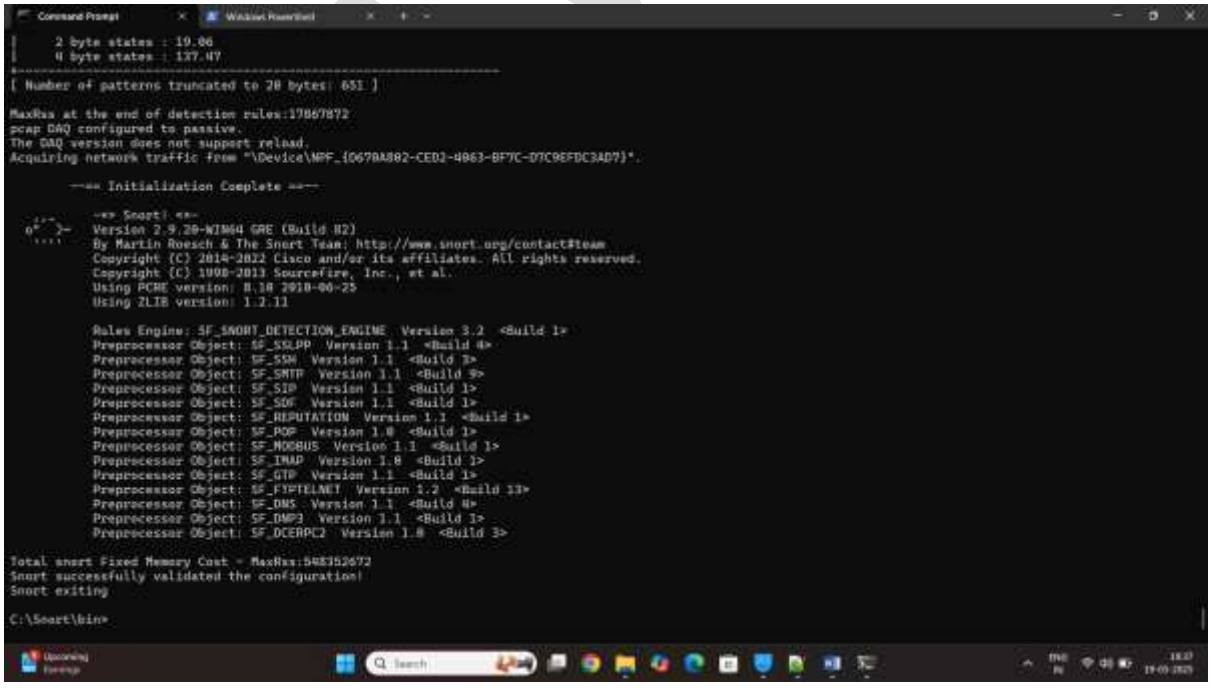
C:\ snort\ bin> snort.exe –V

Version checking command



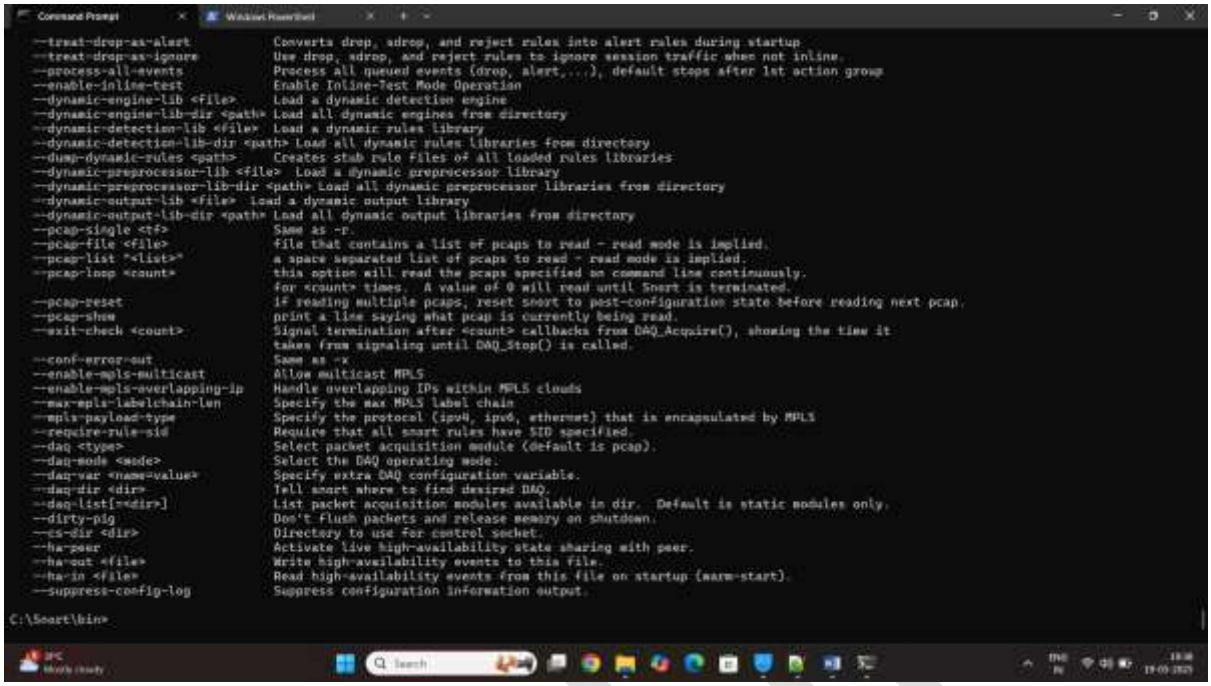
C:\ snort\ bin> snort.exe-W

Interface checking command



C:\ snort\ bin> snort I 5 –c c:\snort\etc\snort\conf –A

This command testing snort configurtaion



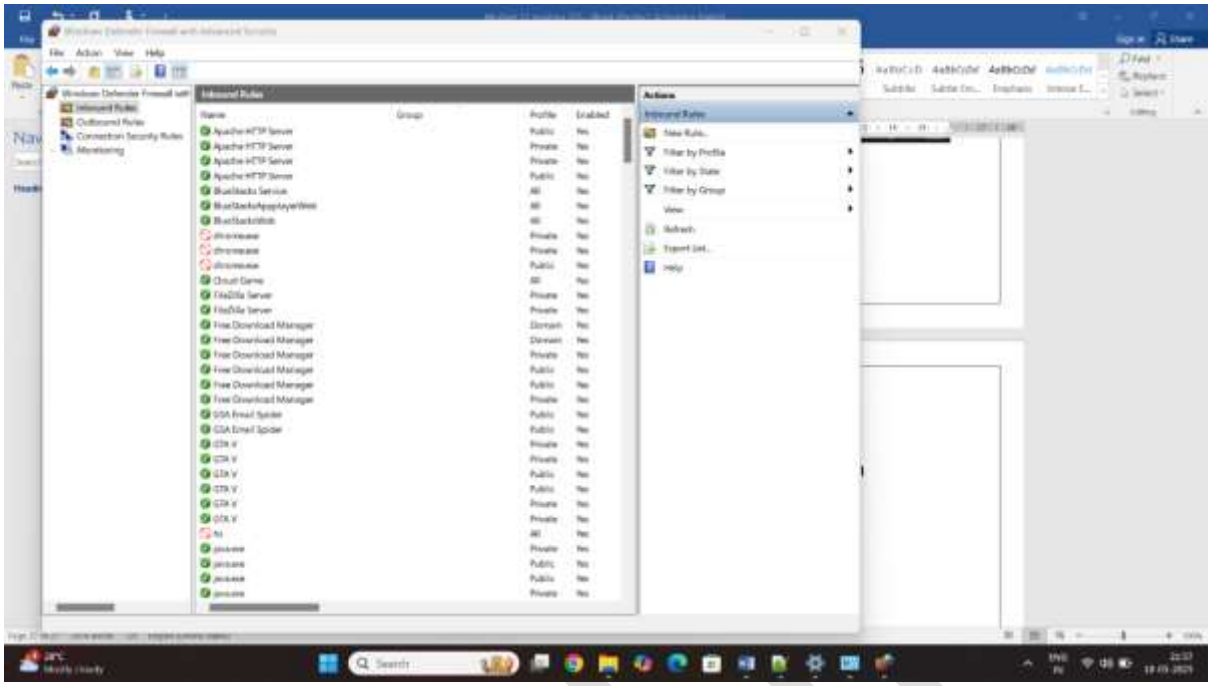
C:\ snort\ bin> snort I 5 –c c:\snort\etc\snort\conf –w

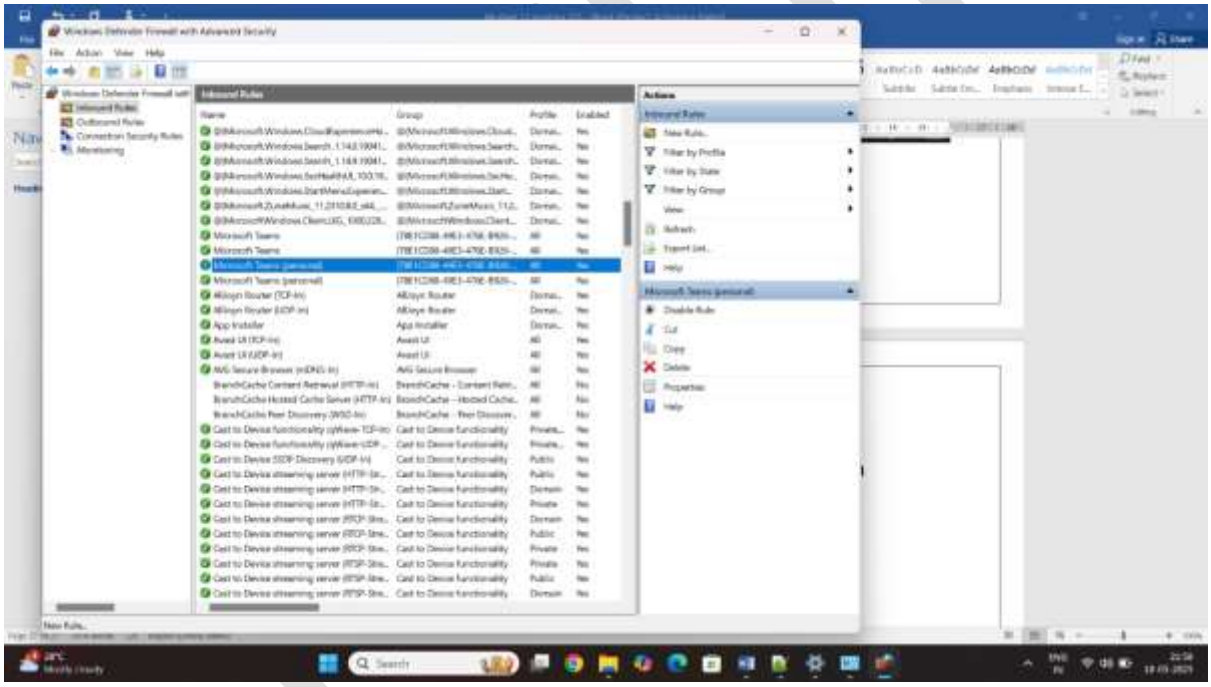
This command are mointering mode use

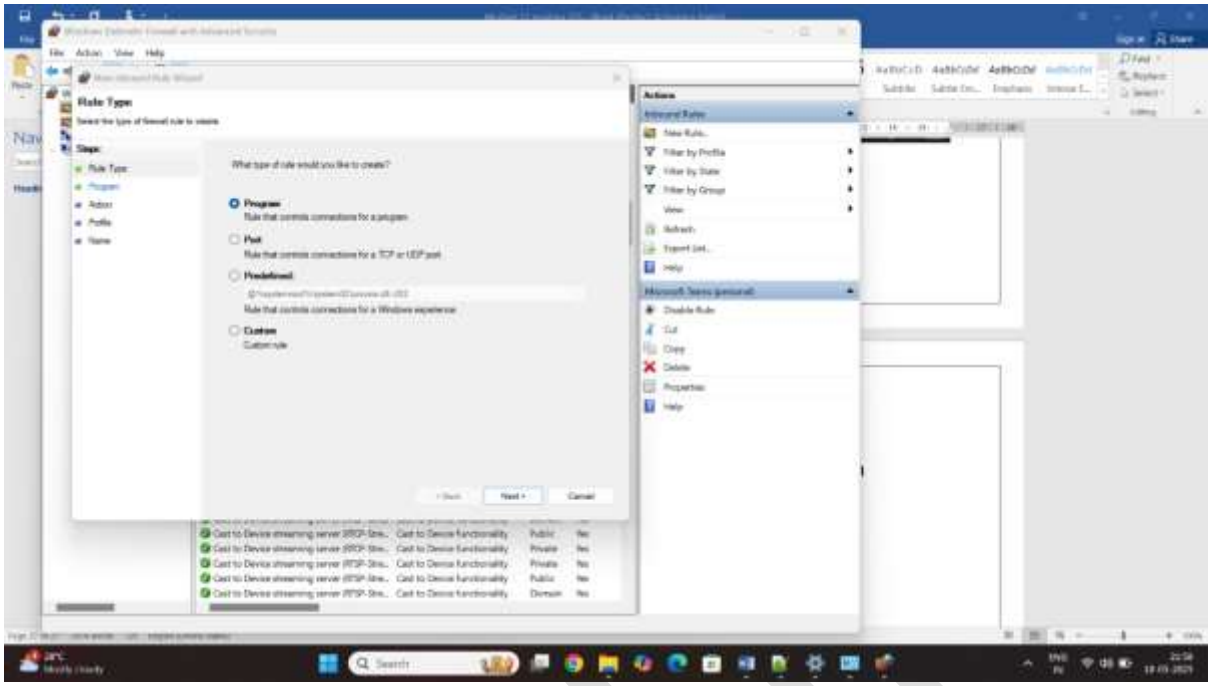
How to windows firewall configuration in bound traffic rule

Step1: go to setting and select the option windows defender

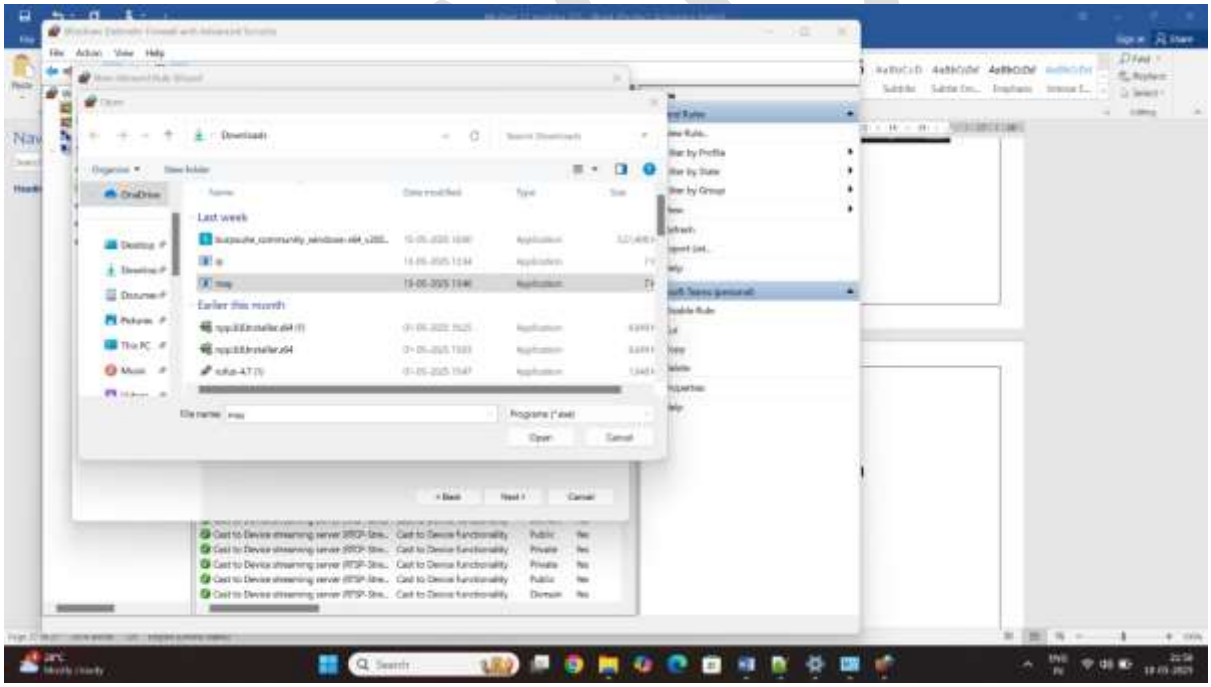
Step2 choice the option inbound



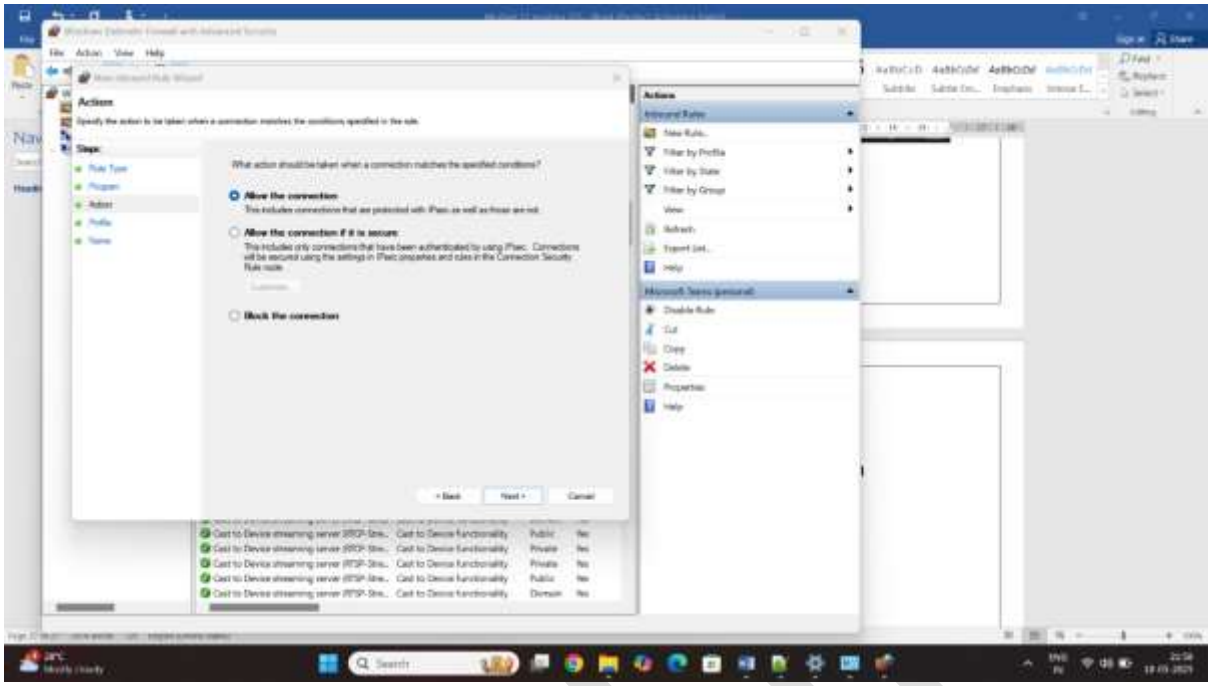




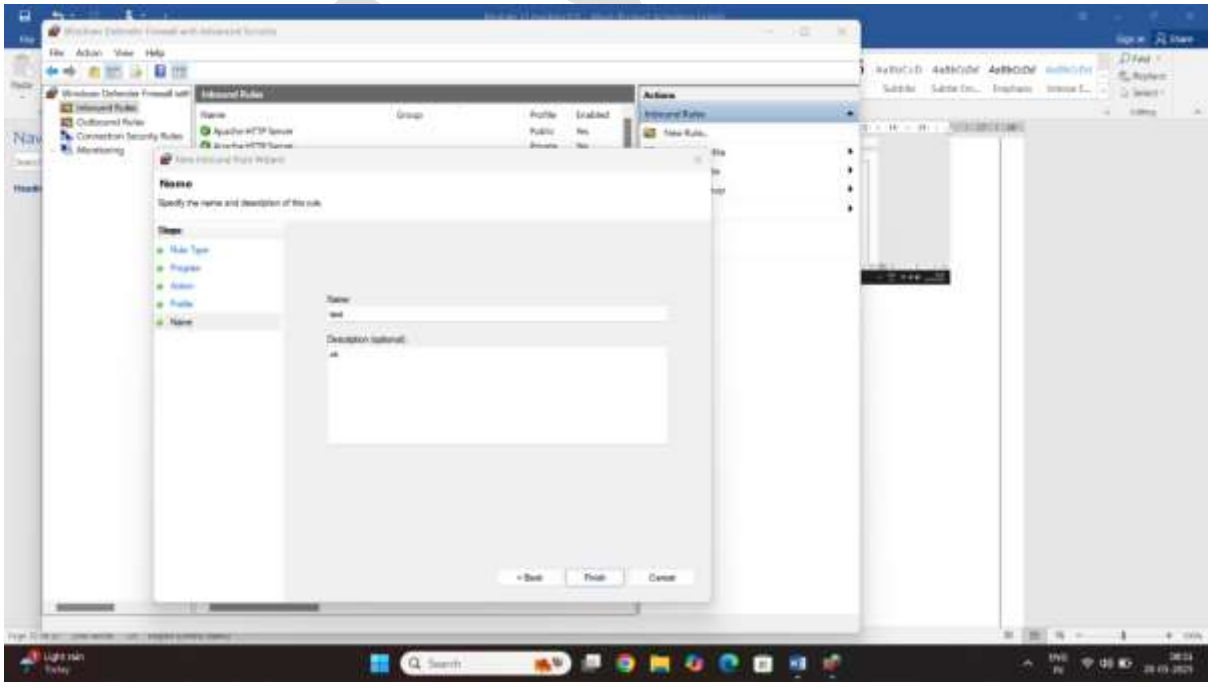
Step3:select the program option



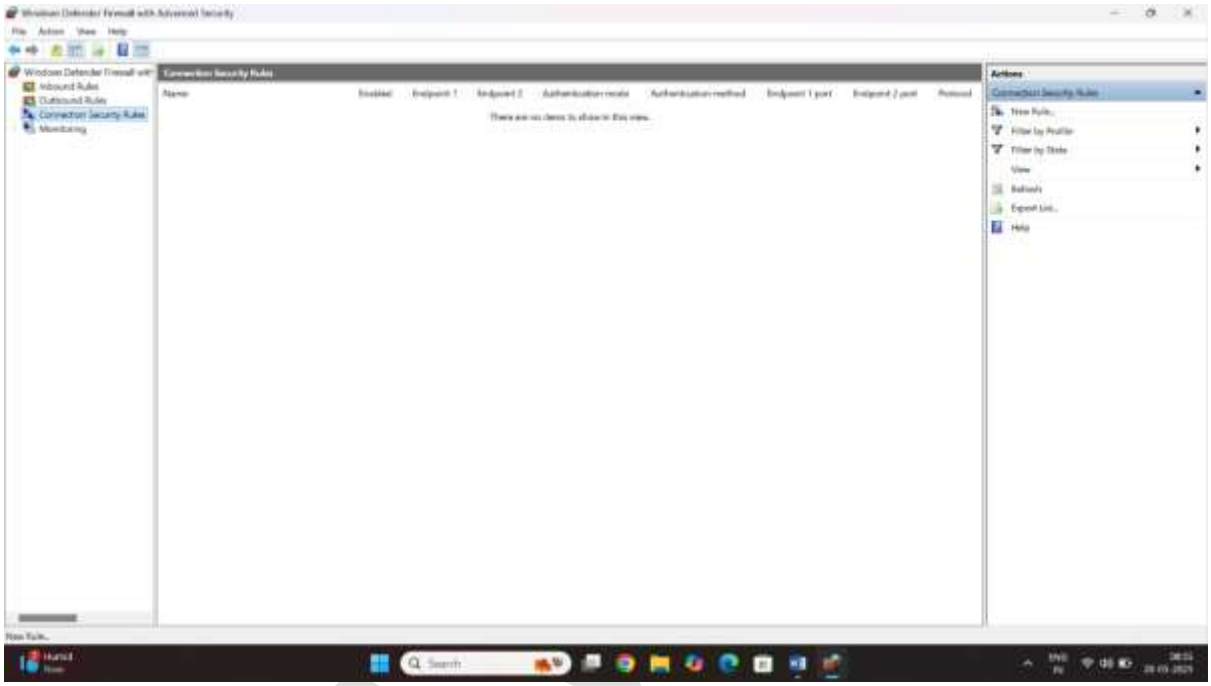
Step4: click on browser choice the block activity

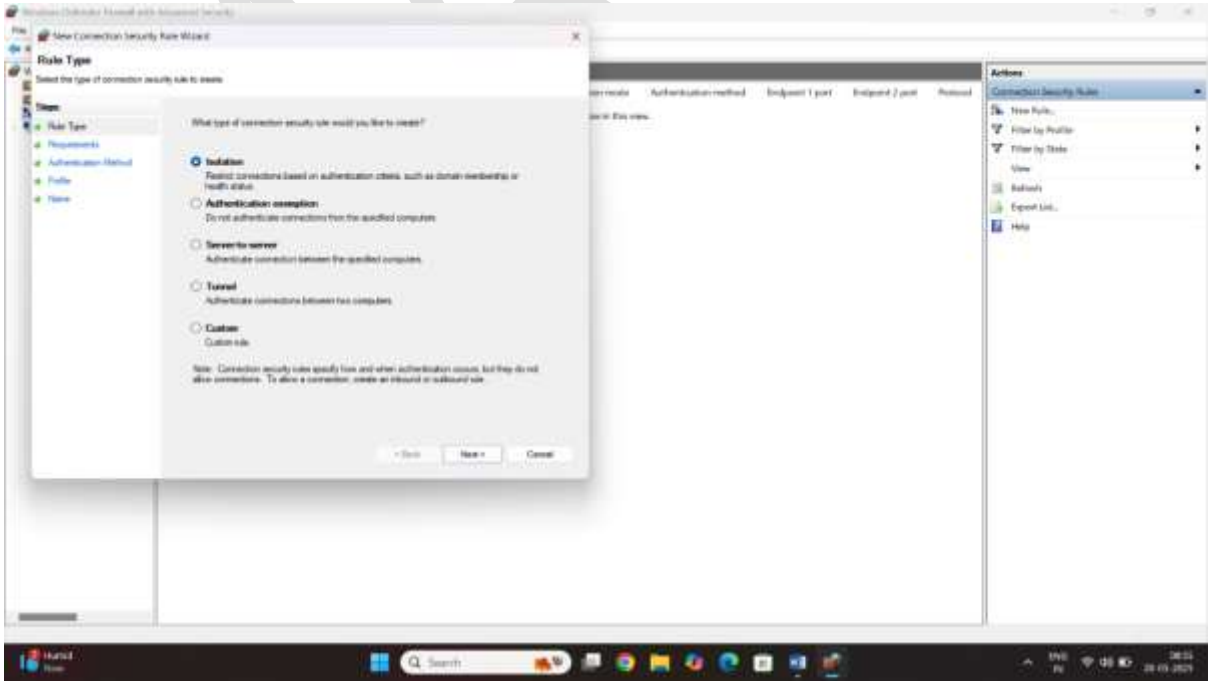


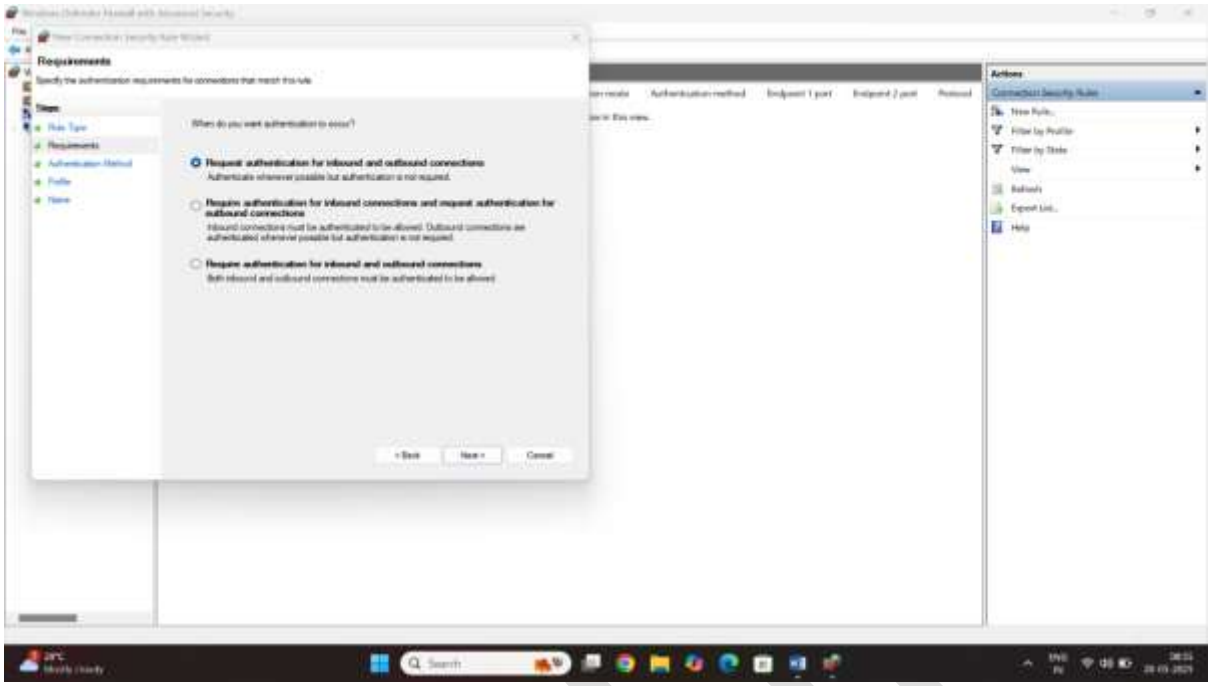
Step5: select the option all

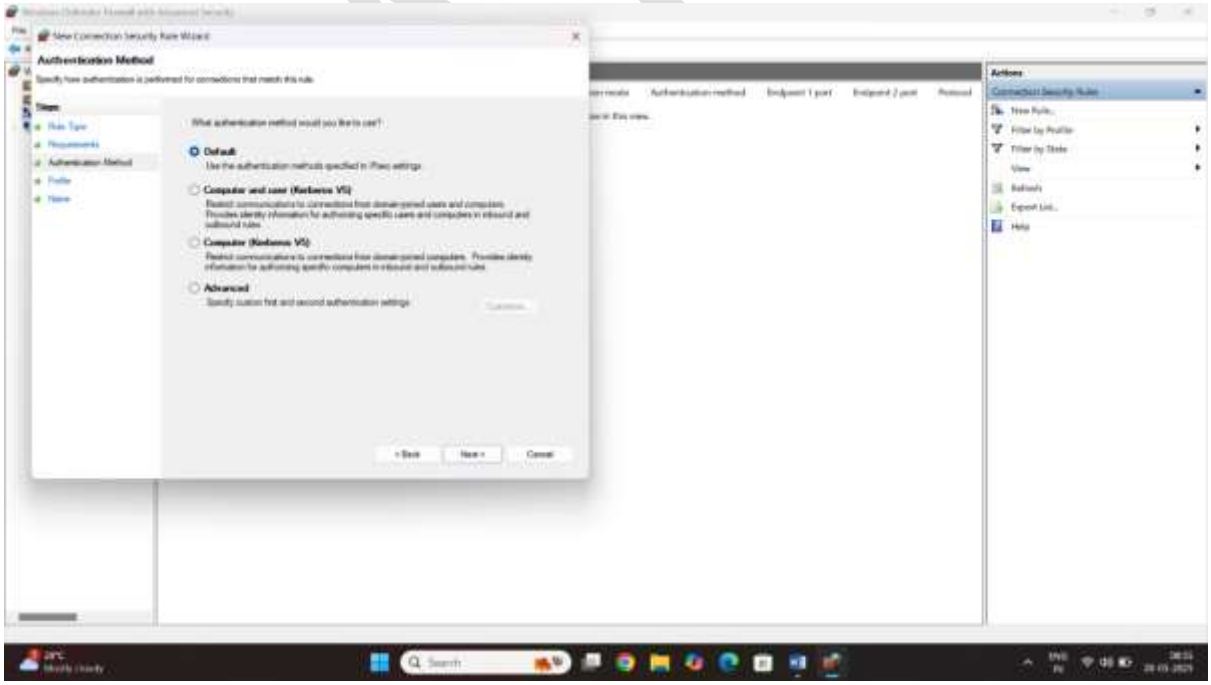


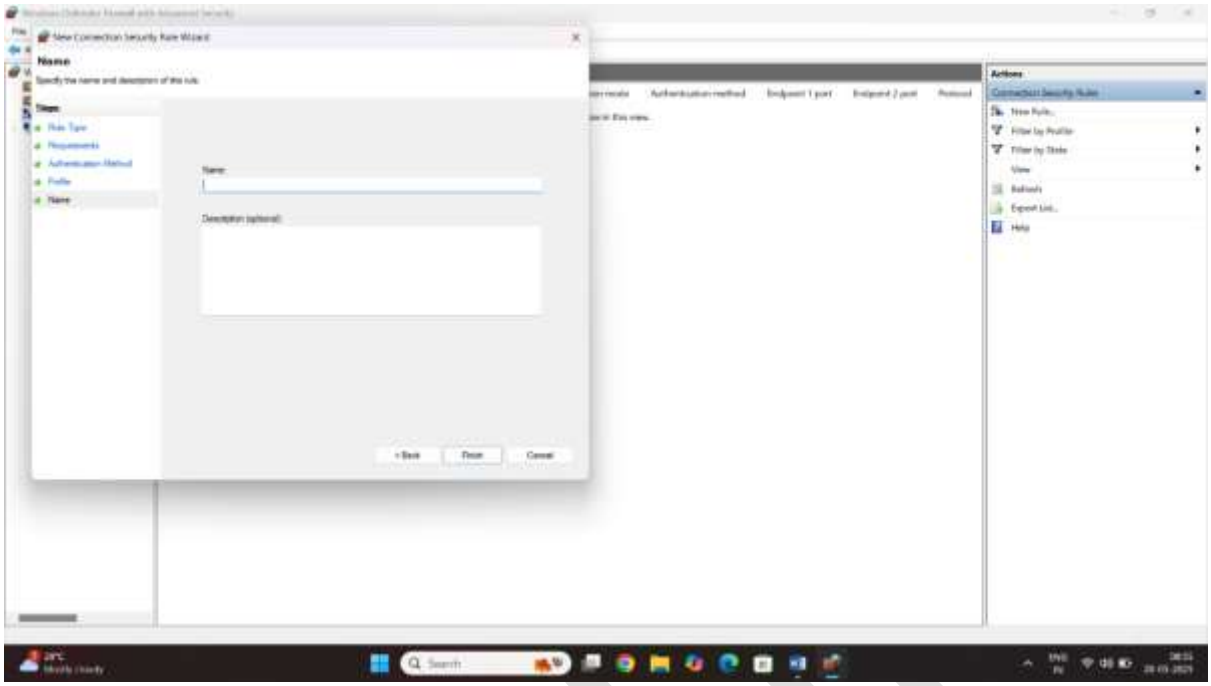
Connection security rules






Requirements
Specify the authentication requirements for connections that match this rule.
Steps:
Rule Type
Requirements
Authentication Method
Profile
Name
When do you want authentication to occur?
Request authentication for inbound and outbound connections
Authenticate whenever possible but authentication is not required.
Require authentication for inbound connections and request authentication for outbound connections
Inbound connections must be authenticated to be allowed. Outbound connections are authenticated whenever possible but authentication is not required.
Require authentication for inbound and outbound connections
Both inbound and outbound connections must be authenticated to be allowed.
< Back
Next >
Cancel
Actions
Connection Security Rules
New Rule...
Filter by Profile
Filter by State
View
Refresh
Export List...
Help

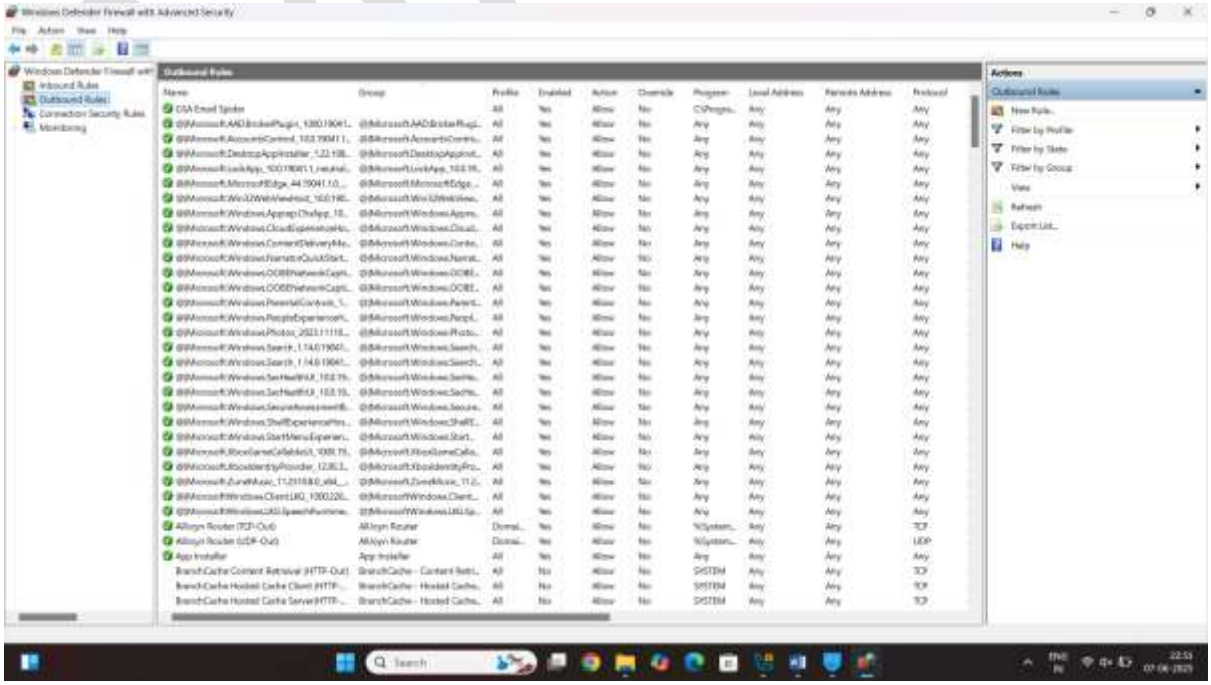

New Connection Security Rule Wizard
Authentication Method
Specify how authentication is performed for connections that match this rule.
Steps:
Rule Type
Requirements
Authentication Method
Profile
Name
What authentication method would you like to use?
Default
Use the authentication methods specified in IPsec settings.
Computer and user (Kerberos V5)
Computer (Kerberos V5)
Advanced
Specify custom first and second authentication settings.
< Back
Next >
Cancel
Actions
Connection Security Rules
New Rule...
Filter by Profile
Filter by State
View
Refresh
Export List...
Help

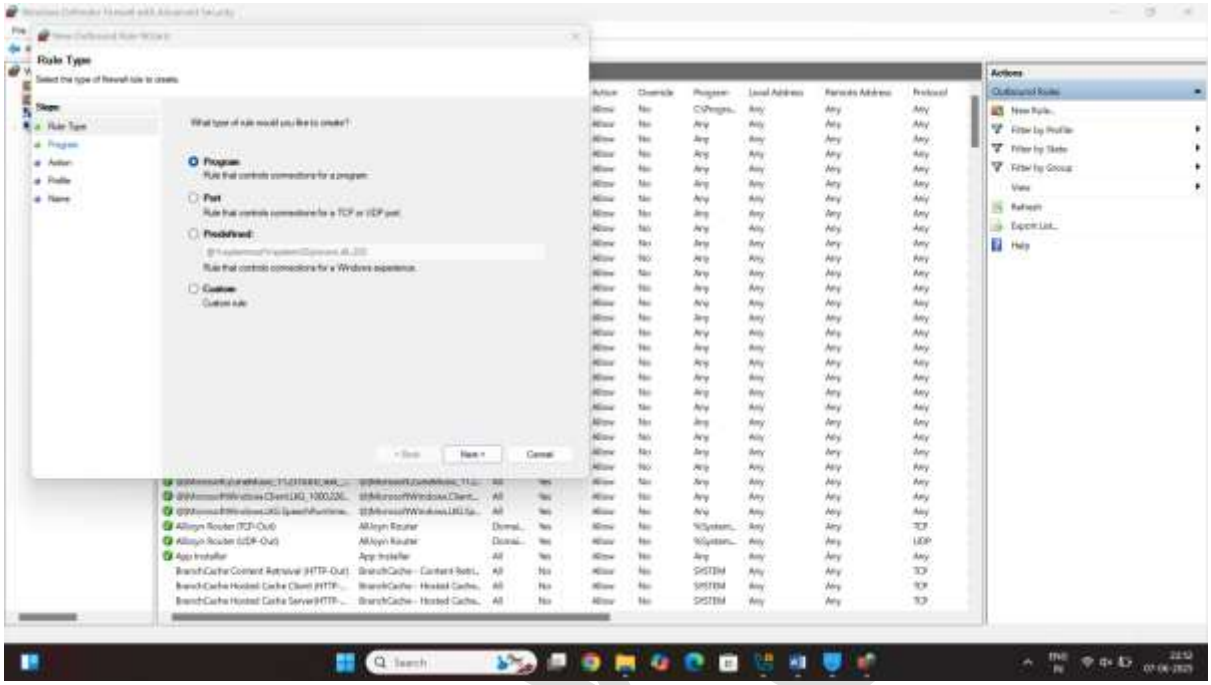


How to windows firewall configuration outbound traffic rule

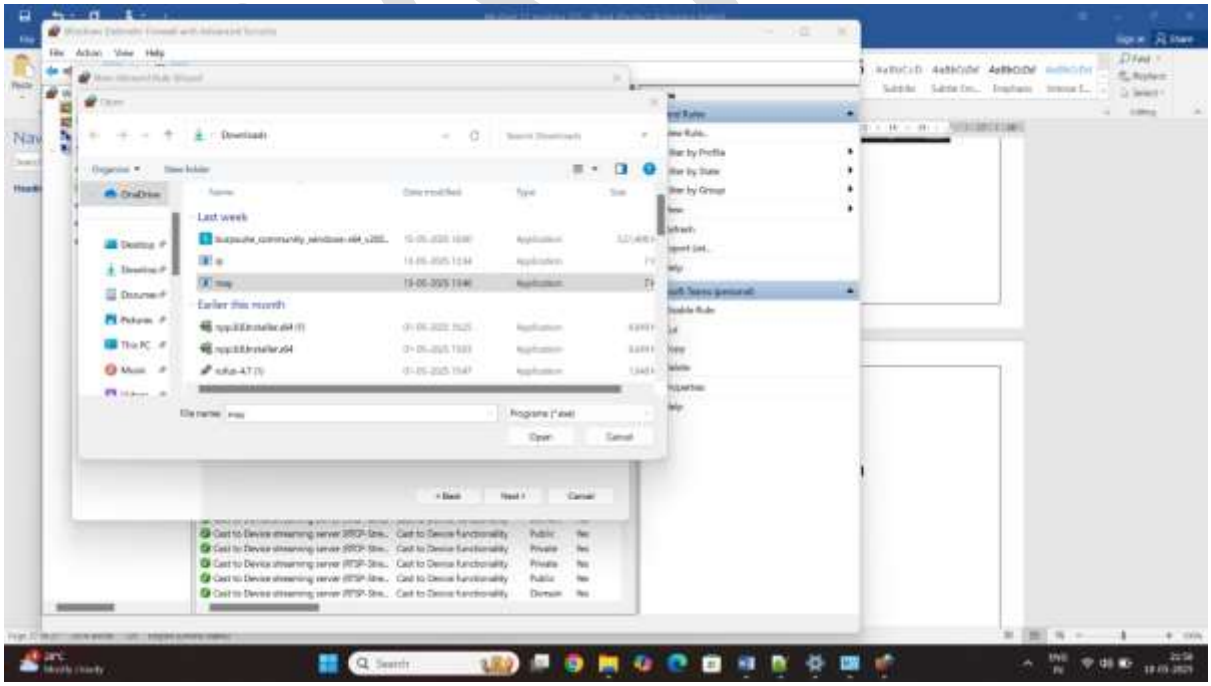
Step1: go to setting and select the option windows defender

Step2 choice the option oubound

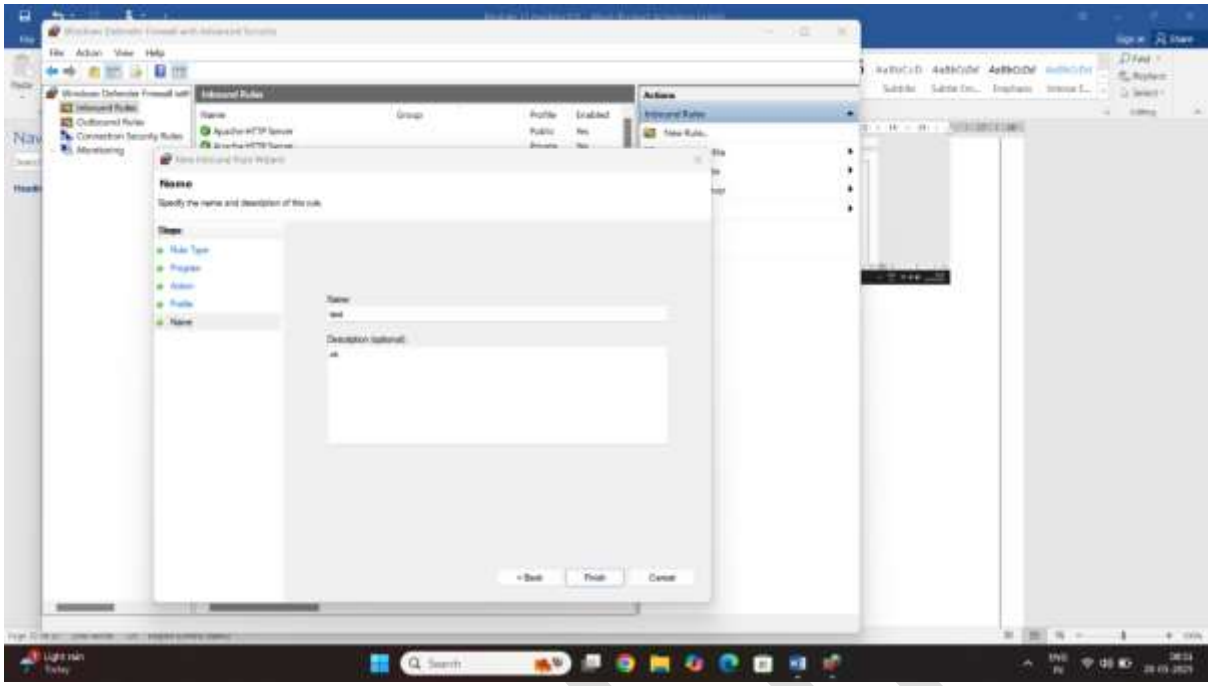




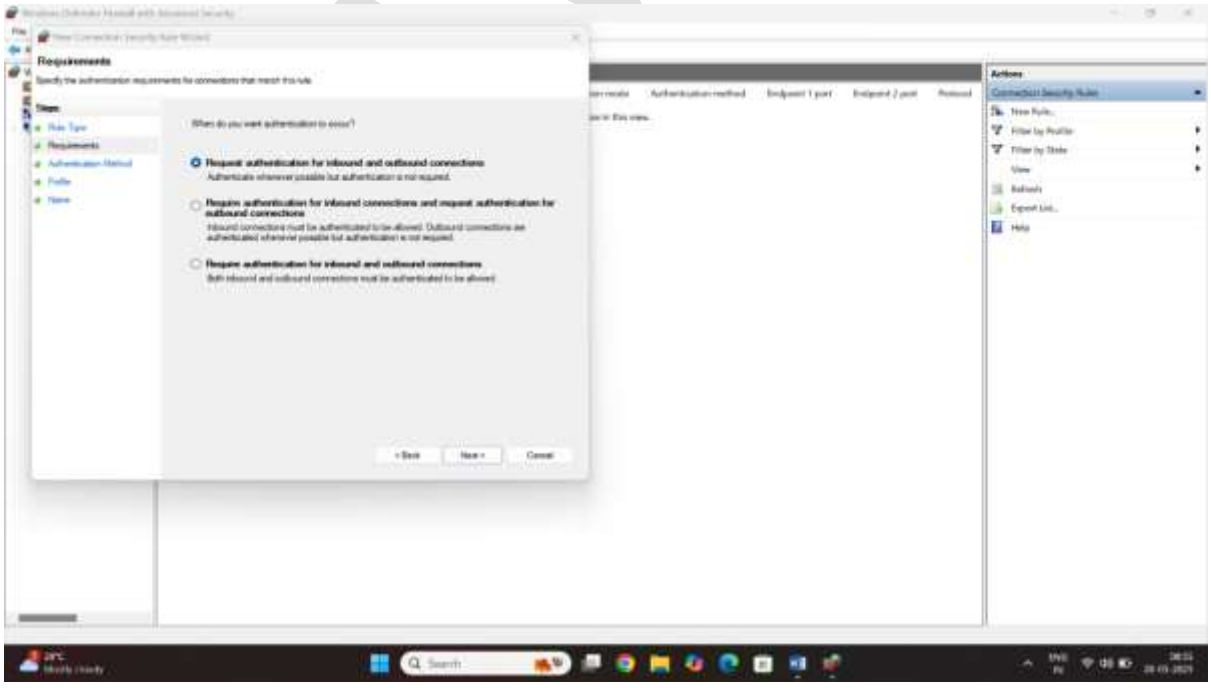
Step3:select the program option



Step4: click on browser choice the block activity



Step5: select the option all



Choice first option and select the out band rule

Click on next and complete the firewall out band configretion

Types of security controls

In cybersecurity, **security controls** are safeguards or countermeasures to detect, prevent, minimize, or respond to security risks. These controls can be categorized in different ways, but they generally fall into three main categories:

---

1. Administrative Controls (Management Controls)

These are policies, procedures, and regulations that guide how an organization manages security.

- **Examples:**
  - Security policies and procedures
  - Risk assessments
  - Security training and awareness programs
  - Incident response plans
  - Personnel background checks
  - Access control policies

---

2. Technical Controls (Logical Controls)

These are technology-based mechanisms used to protect systems and data.

- **Examples:**
  - Firewalls
  - Encryption
  - Antivirus and antimalware software
  - Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)
  - Multi-factor authentication (MFA)
  - Access control lists (ACLs)

---

3. Physical Controls

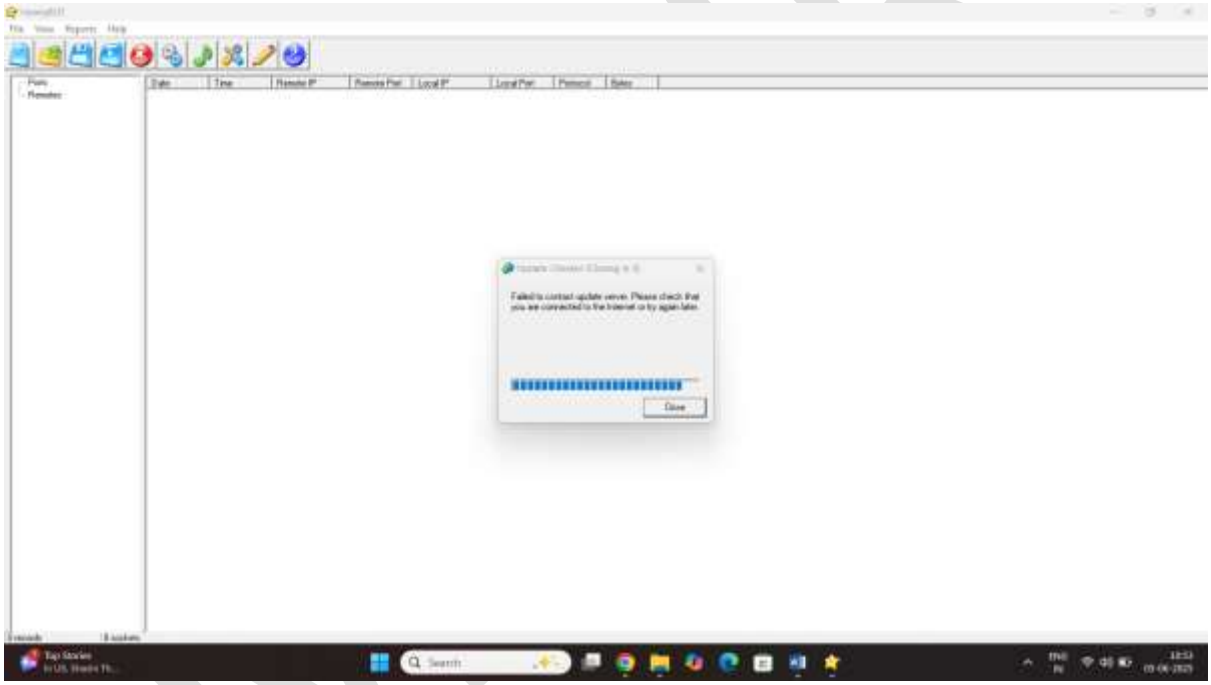
These are controls that prevent physical access to IT systems and infrastructure.

- **Examples:**
  - Security guards
  - Locked doors and cabinets
  - Video surveillance (CCTV)
  - Fencing and gates
  - Biometric access systems
  - Environmental controls (e.g., smoke detectors, fire suppression)

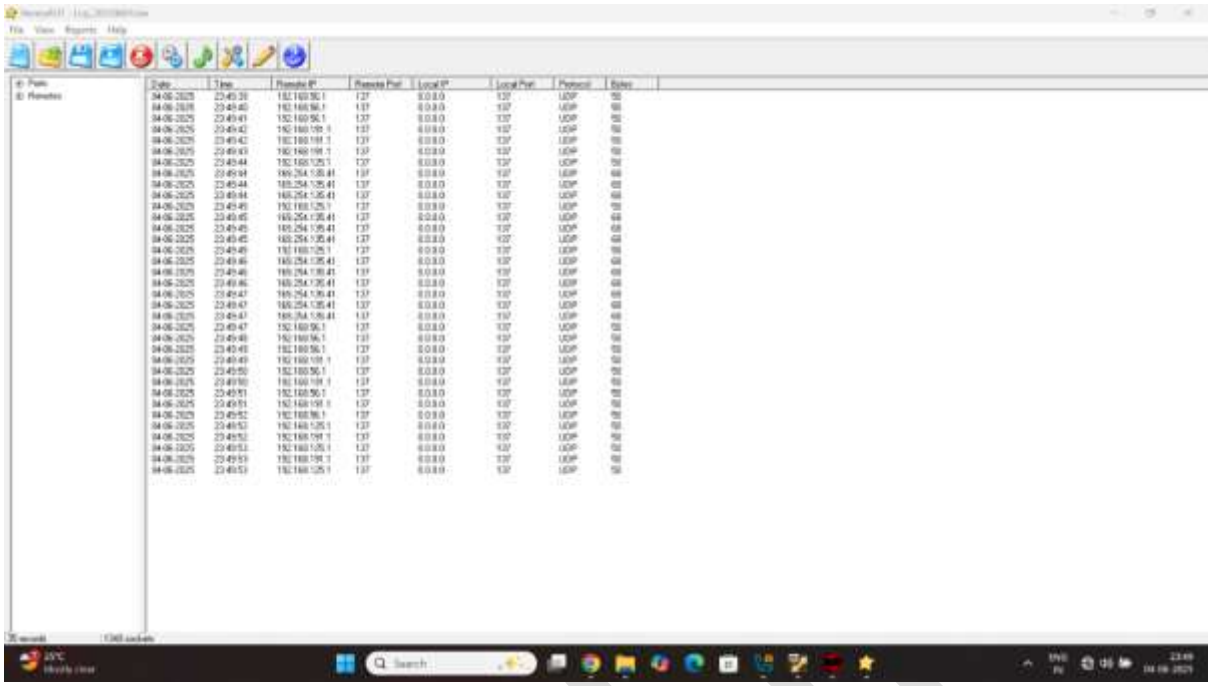
Security guards detection honeypot

Honeypot: is detection m

Step1: start the honeybot application



Click on all monetring option



Extra activity using zone alarm firewall how to configrtaion

🔐 What Is ZoneAlarm Firewall?

ZoneAlarm Firewall acts as a barrier between your computer and the internet, monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. It helps prevent unauthorized access to your computer and protects your data from malicious software.

⚙ Key Features

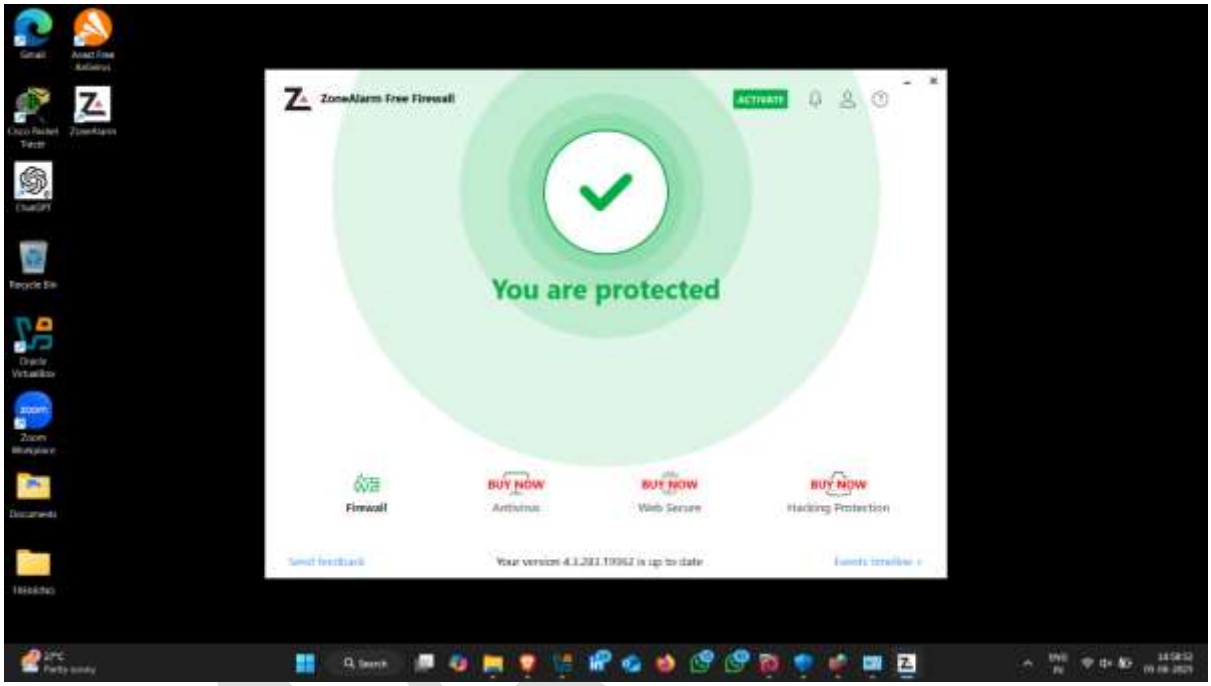
- **Two-Way Firewall Protection**: Monitors both inbound and outbound traffic, blocking unauthorized access and preventing malware from sending your data out.

- **Advanced Security Zones**: Defines three security zones—Trusted, Public, and Blocked—to apply appropriate security levels based on network trustworthiness.
- **Stealth Mode**: Makes your computer invisible to hackers by blocking unsolicited inbound traffic.

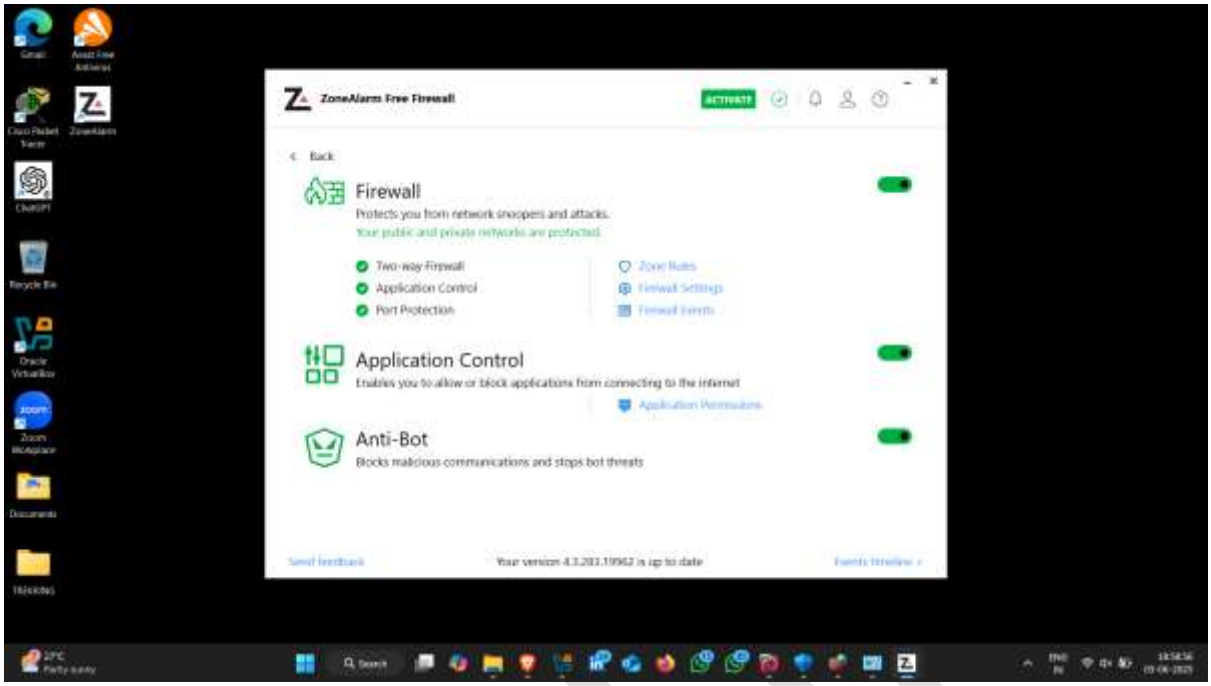
- **Application Control**: Monitors and controls which applications can access the internet, preventing unauthorized programs from communicating online.

- **Identity Protection Services**: Offers features like daily credit monitoring and fraud alerts to help protect against identity theft.

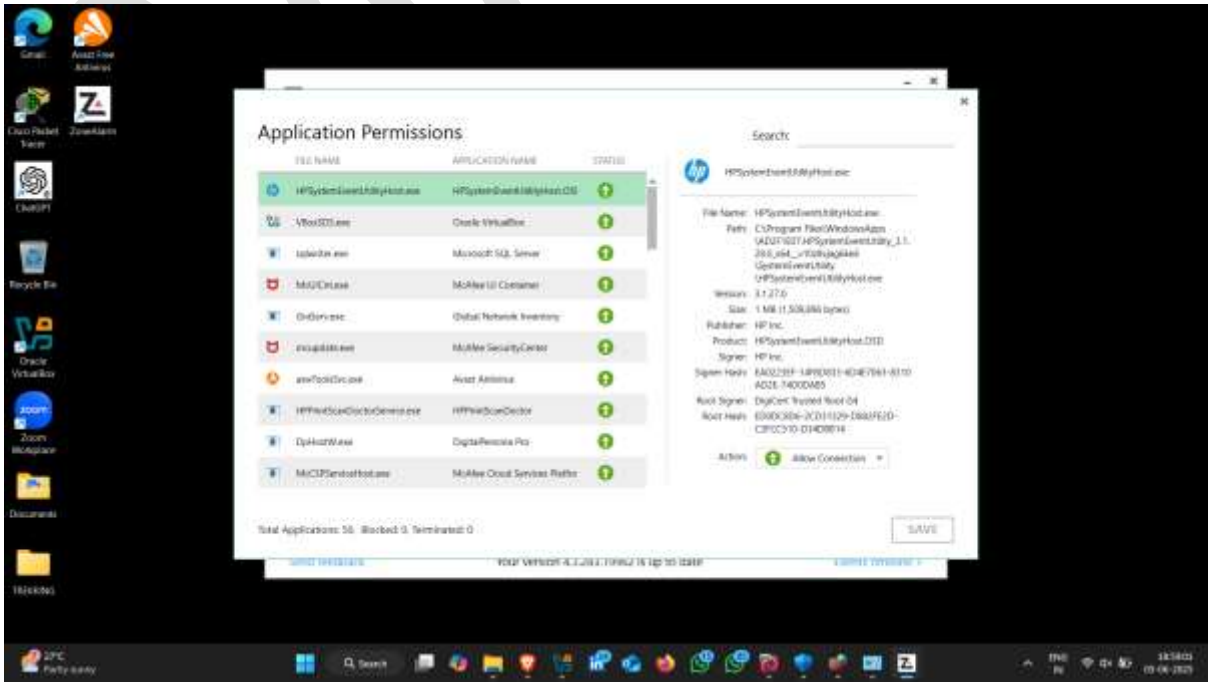
Configration Zone alarm



Step1: click on zone alarm and start here

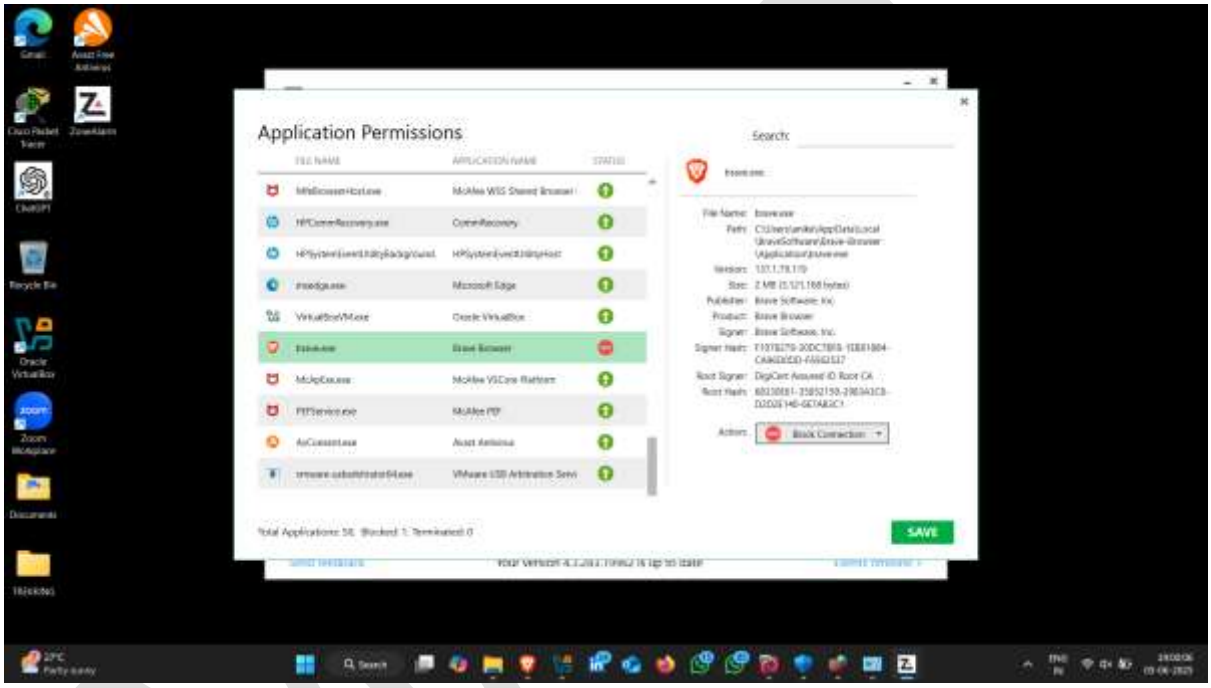


Step2 : select the all option allow permission

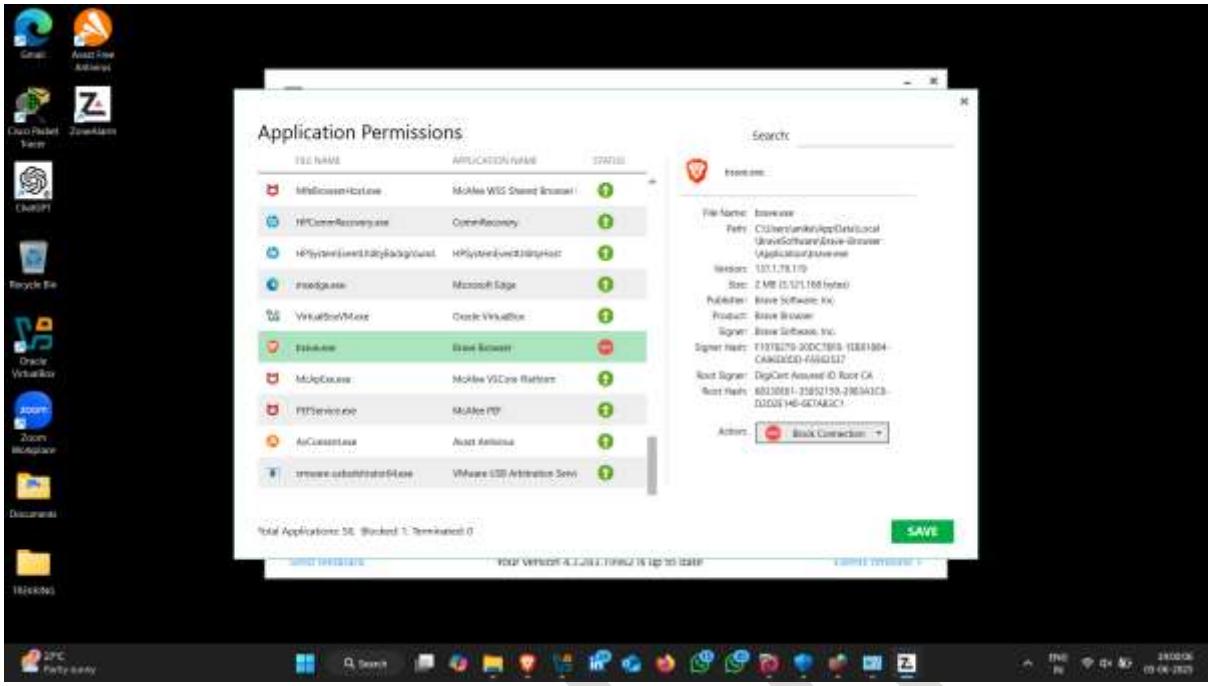


Step3 select application permission

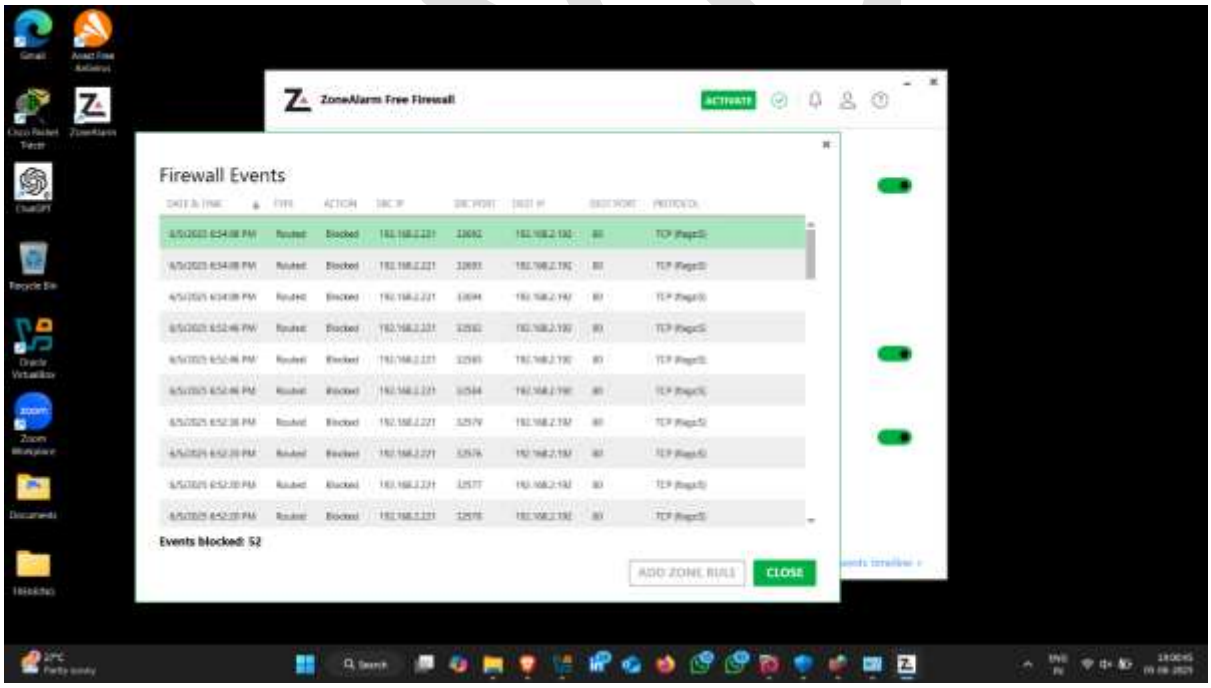
With set of rule



Step 4 I am choice the brave browser permission



Step5 Clicik on save and next



Step6 Complete the zone alarm configuration