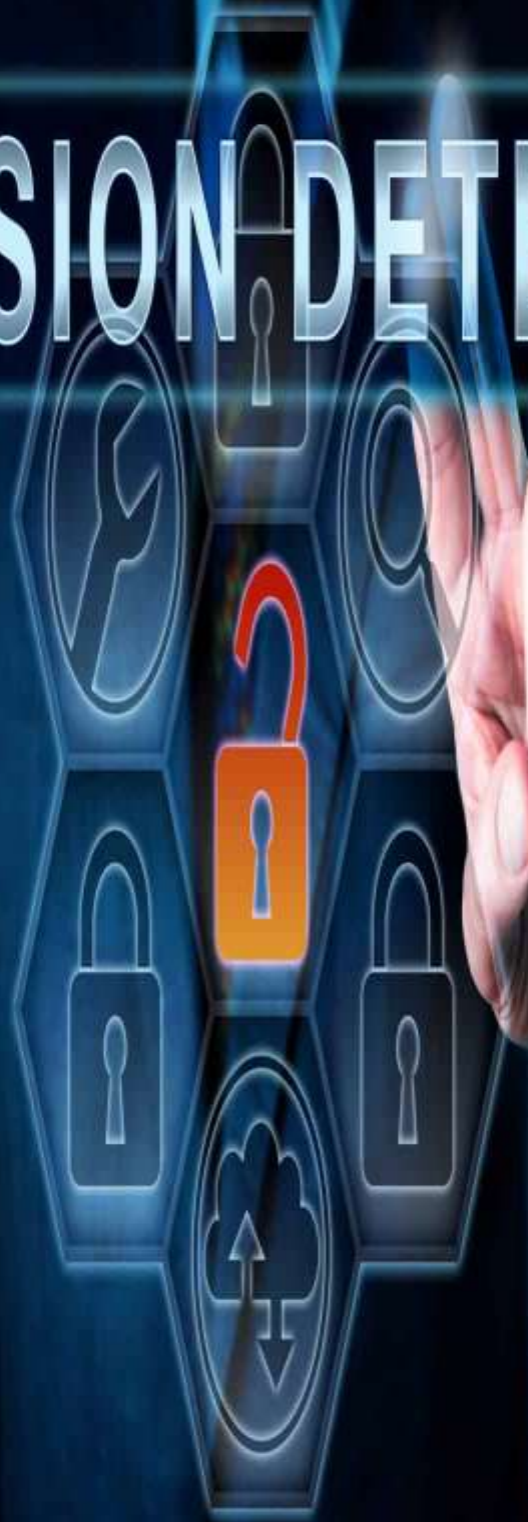


INTRUSION DETECTION



Module 12 evading IDS,IPS firewall and honeypots

Index

1 What is IDS

- Way are use ids
- How does ids work
- **Type of ids**
 - Network-Based IDS (NIDS)
 - Host-Based IDS (HIDS)

2 type of ids alert

3 types of password

4 what is firewall

- Way are use firewall
- How does work firewall
- Types of firewall

5 type of firewall Architectures

- 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 configtaion

MAYUR

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.

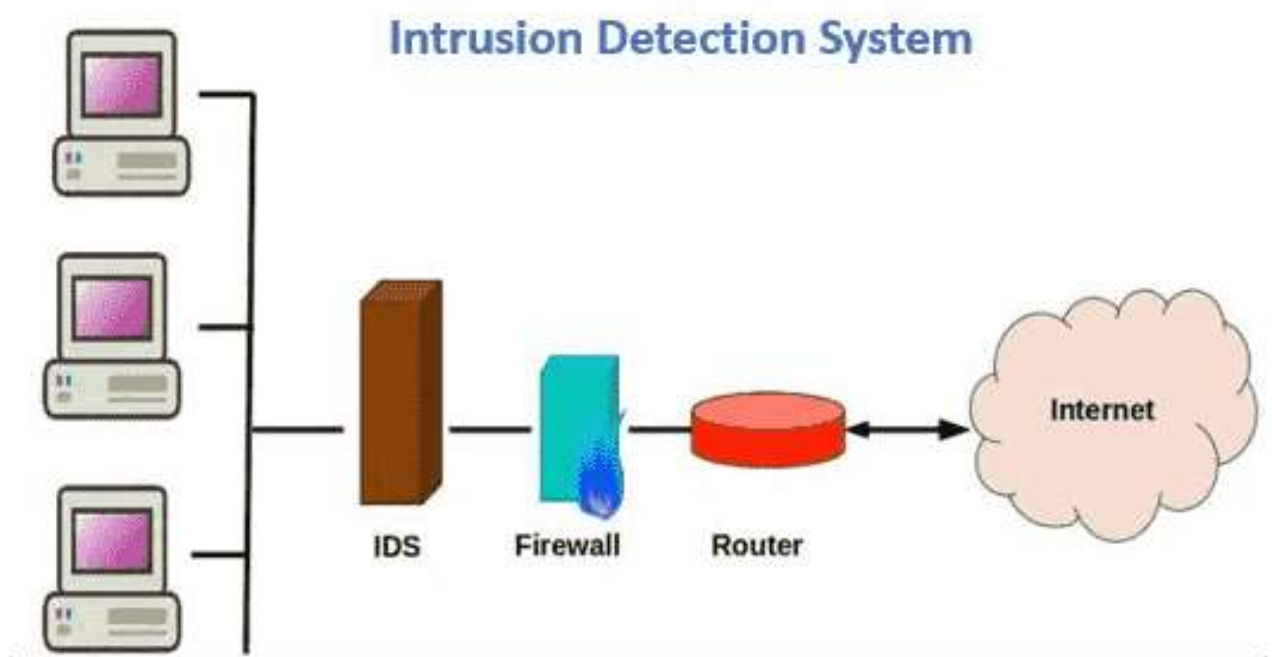
9. Analyze Past Attacks

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.

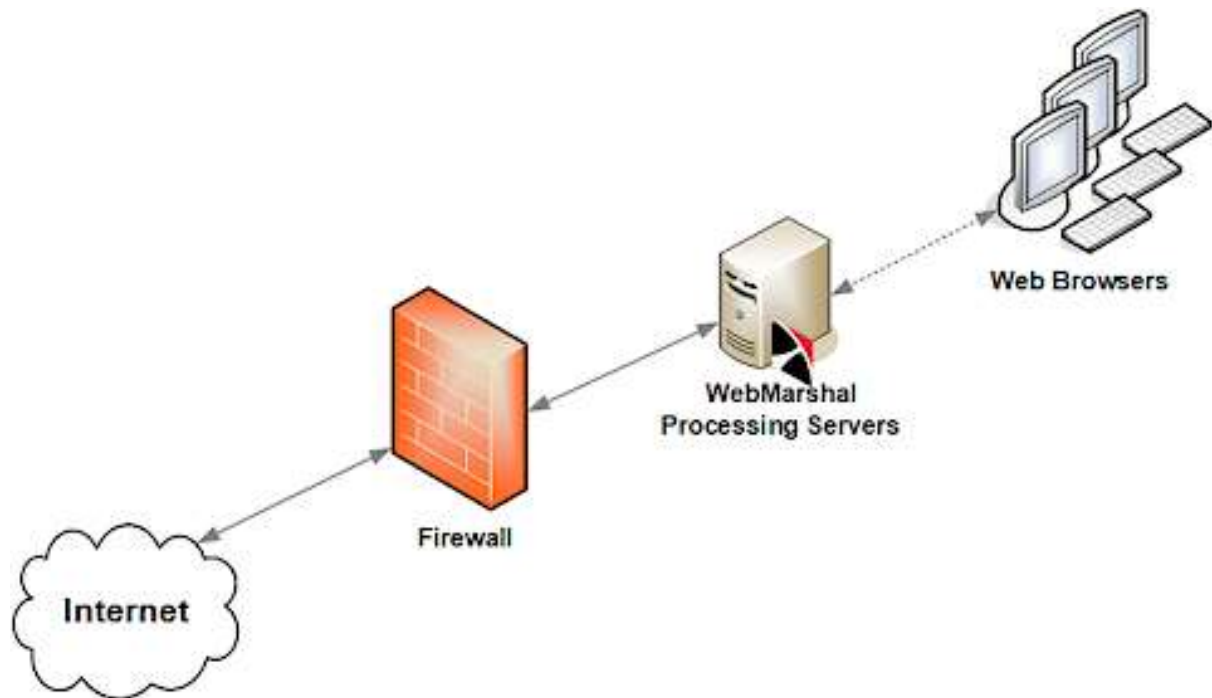
Types of password

- 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

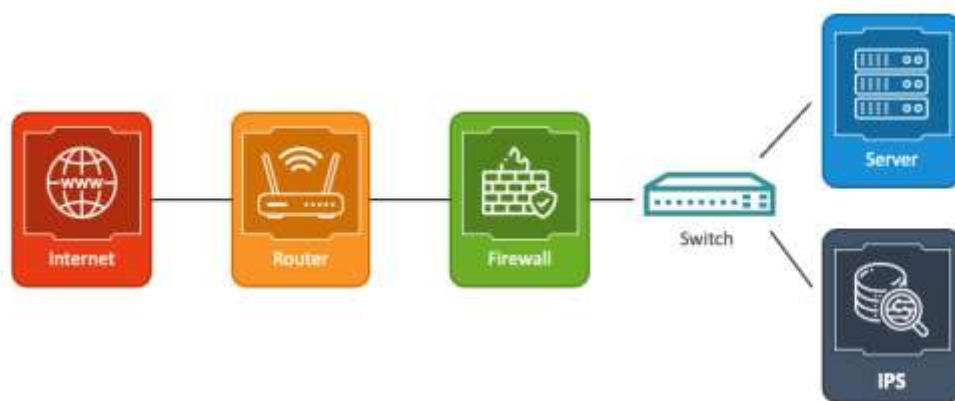
- Stops threats early, minimizing potential **downtime, data loss, or breaches.**

✓ 9. Alerts and Logs for Forensics

- Logs events for later analysis or investigation.

How does work IPS

INTRUSION PREVENTION SYSTEM



Source : www.thesecuritybuffly.com

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.

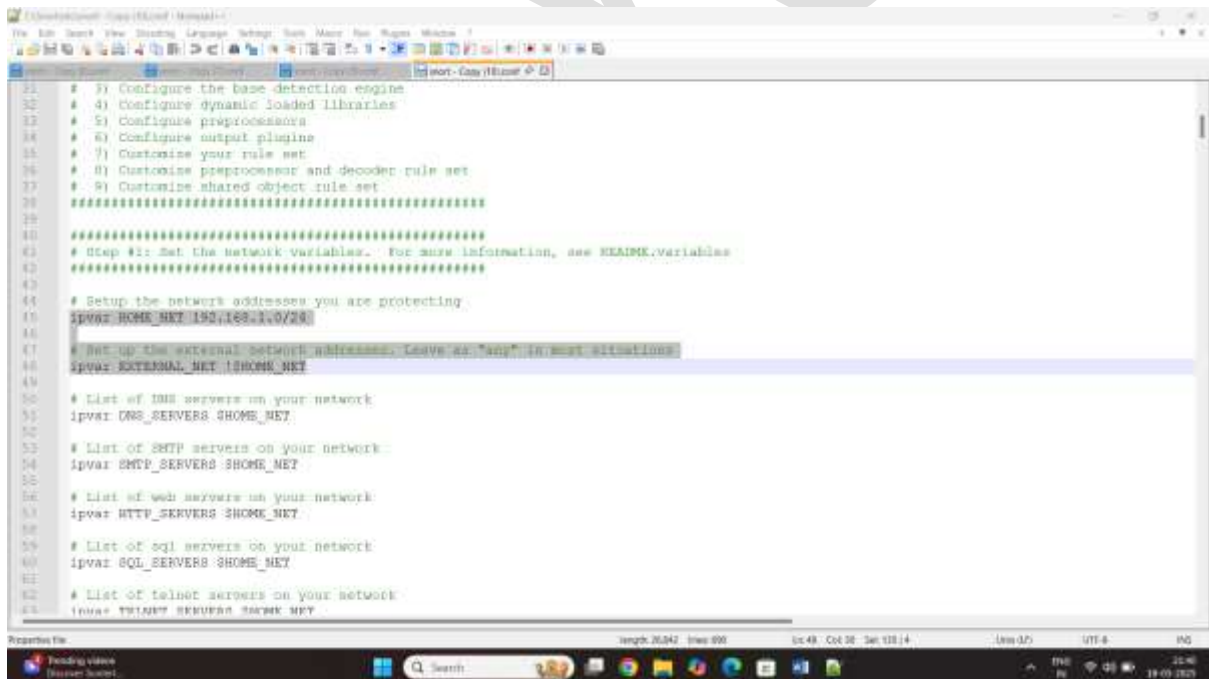
7. Updates & Learning

- 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



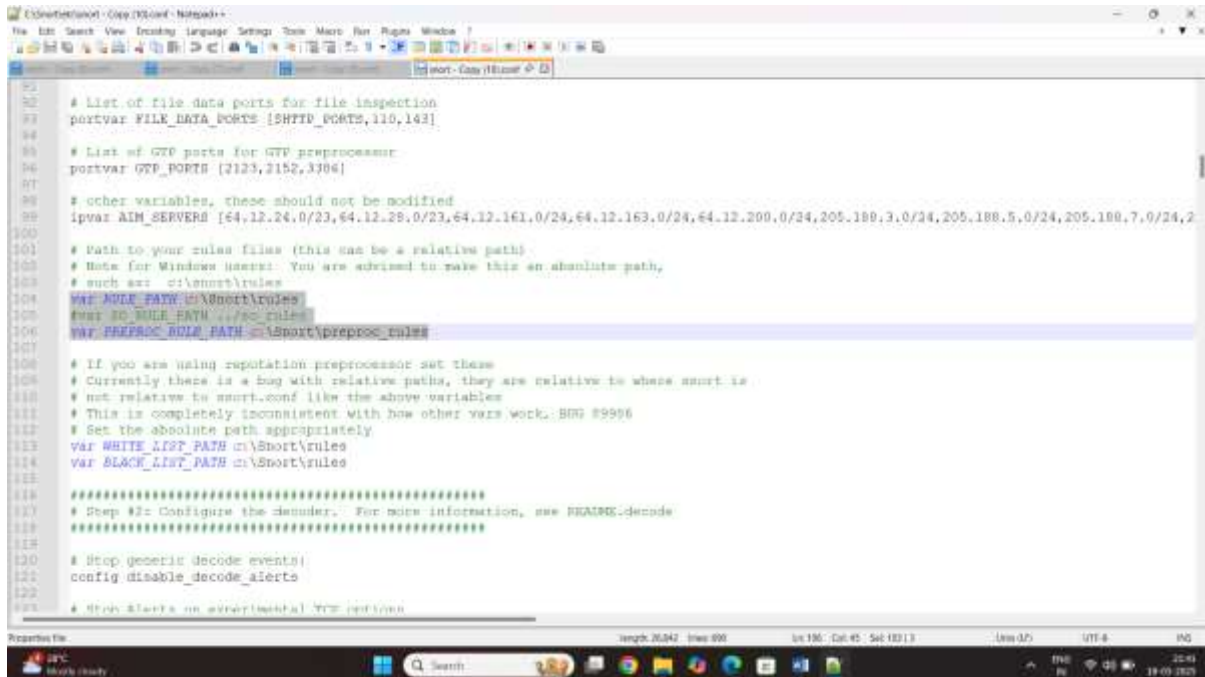
```
21 # 3) Configure the base detection engine
22 # 4) Configure dynamic loaded libraries
23 # 5) Configure preprocessors
24 # 6) Configure output plugins
25 # 7) Customize your rule set
26 # 8) Customize preprocessor and decoder rule set
27 # 9) Customize shared object rule set
28 #####
29
30 #####
31 # Step #1: Set the network variables. For more information, see README.variables
32 #####
33
34 # Setup the network addresses you are protecting
35 ipvar HOME_NET 192.168.1.0/24
36
37 # Set up the external network addresses. Leave as "any" in most situations
38 ipvar EXTERNAL_NET !$HOME_NET
39
40 # List of DNS servers on your network
41 ipvar DNS_SERVERS $HOME_NET
42
43 # List of SMTP servers on your network
44 ipvar SMTP_SERVERS $HOME_NET
45
46 # List of web servers on your network
47 ipvar HTTP_SERVERS $HOME_NET
48
49 # List of sql servers on your network
50 ipvar SQL_SERVERS $HOME_NET
51
52 # List of telnet servers on your network
53 ipvar TELNET_SERVERS $HOME_NET
```

Step3: change line/45

Ipvar HOME_NET 192.168.1.0/24

Step4: change line/47

Ip EXTERNAL_NET !\$ HOME_NET



```
# List of file data ports for file inspection
portvar FILE_DATA_PORTS [SMTP_PORTS,110,143]

# List of UDP ports for UDP preprocessor
portvar UDP_PORTS [2123,2152,3706]

# Other variables, these should not be modified
ipvar AIM_SERVERS [64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.209.0/24,205.189.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.11.0/24,205.188.13.0/24,205.188.15.0/24,205.188.17.0/24,205.188.19.0/24,205.188.21.0/24,205.188.23.0/24,205.188.25.0/24,205.188.27.0/24,205.188.29.0/24,205.188.31.0/24,205.188.33.0/24,205.188.35.0/24,205.188.37.0/24,205.188.39.0/24,205.188.41.0/24,205.188.43.0/24,205.188.45.0/24,205.188.47.0/24,205.188.49.0/24,205.188.51.0/24,205.188.53.0/24,205.188.55.0/24,205.188.57.0/24,205.188.59.0/24,205.188.61.0/24,205.188.63.0/24,205.188.65.0/24,205.188.67.0/24,205.188.69.0/24,205.188.71.0/24,205.188.73.0/24,205.188.75.0/24,205.188.77.0/24,205.188.79.0/24,205.188.81.0/24,205.188.83.0/24,205.188.85.0/24,205.188.87.0/24,205.188.89.0/24,205.188.91.0/24,205.188.93.0/24,205.188.95.0/24,205.188.97.0/24,205.188.99.0/24,205.188.101.0/24,205.188.103.0/24,205.188.105.0/24,205.188.107.0/24,205.188.109.0/24,205.188.111.0/24,205.188.113.0/24,205.188.115.0/24,205.188.117.0/24,205.188.119.0/24,205.188.121.0/24,205.188.123.0/24,205.188.125.0/24,205.188.127.0/24,205.188.129.0/24,205.188.131.0/24,205.188.133.0/24,205.188.135.0/24,205.188.137.0/24,205.188.139.0/24,205.188.141.0/24,205.188.143.0/24,205.188.145.0/24,205.188.147.0/24,205.188.149.0/24,205.188.151.0/24,205.188.153.0/24,205.188.155.0/24,205.188.157.0/24,205.188.159.0/24,205.188.161.0/24,205.188.163.0/24,205.188.165.0/24,205.188.167.0/24,205.188.169.0/24,205.188.171.0/24,205.188.173.0/24,205.188.175.0/24,205.188.177.0/24,205.188.179.0/24,205.188.181.0/24,205.188.183.0/24,205.188.185.0/24,205.188.187.0/24,205.188.189.0/24,205.188.191.0/24,205.188.193.0/24,205.188.195.0/24,205.188.197.0/24,205.188.199.0/24,205.188.201.0/24,205.188.203.0/24,205.188.205.0/24,205.188.207.0/24,205.188.209.0/24,205.188.211.0/24,205.188.213.0/24,205.188.215.0/24,205.188.217.0/24,205.188.219.0/24,205.188.221.0/24,205.188.223.0/24,205.188.225.0/24,205.188.227.0/24,205.188.229.0/24,205.188.231.0/24,205.188.233.0/24,205.188.235.0/24,205.188.237.0/24,205.188.239.0/24,205.188.241.0/24,205.188.243.0/24,205.188.245.0/24,205.188.247.0/24,205.188.249.0/24,205.188.251.0/24,205.188.253.0/24,205.188.255.0/24]

# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH c:\snort\rules
# var SO_RULE_PATH c:\snort\rules
var PREPROC_RULE_PATH c:\snort\preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work. BUG #9996
# Set the absolute path appropriately
var WHITE_LIST_PATH c:\snort\rules
var BLACK_LIST_PATH c:\snort\rules

#####
# Step #2: Configure the decoder. For more information, see README.decode
#####

# Stop generic decode events
config disable_decode_alerts

# Stop alerts on experimental TCP options
```

Step5: change line/104

Var RULE_PATH c:\snort\rules

Step6:change line/105

Remove hash

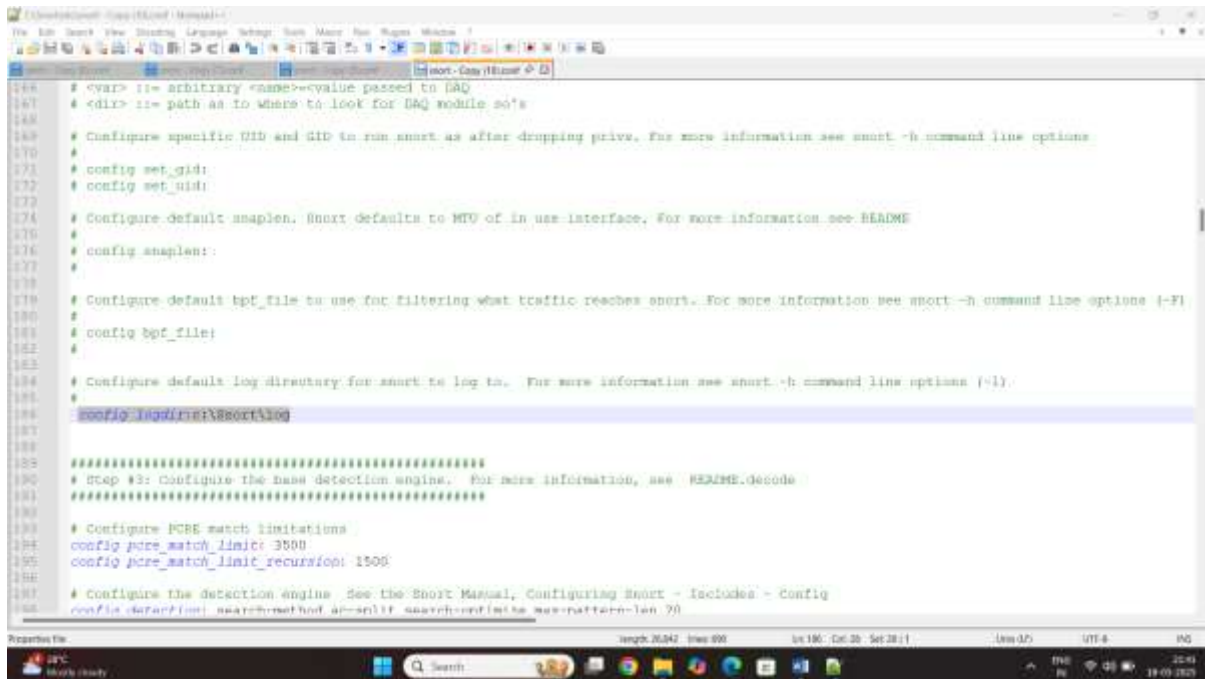
Step7: change line/

Var preproc_RULE_PATH

C:\snort\preproc_roles

Step8: change line/

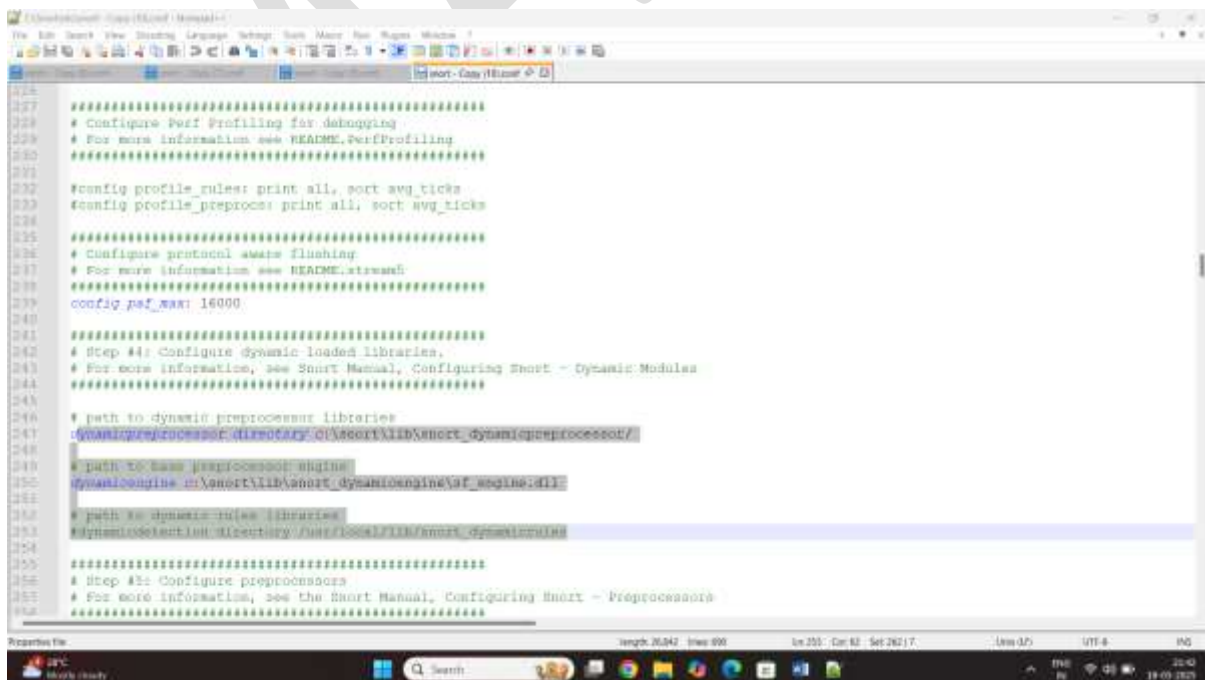
var BLACK_LIST_PATH c:\Snort\rules



```
164 # <var> == arbitrary <name>=<value passed to <dir>
165 # <dir> == path as to where to look fordaq module so's
166
167 # Configure specific UID and GID to run snort as after dropping privs. For more information see snort -h command line options
168 #
169 # config set_gid:
170 # config set_uid:
171
172 # Configure default snmpen. Snort defaults to MIB of In use interface. For more information see README
173 #
174 # config snmpen::
175 #
176 # Configure default bpf_file to use for filtering what traffic reaches snort. For more information see snort -h command line options (-F)
177 #
178 # config bpf_file:
179 #
180 # Configure default log directory for snort to log to. For more information see snort -h command line options (-l).
181 #
182 # config logdir::c:\snort\log
183
184 #####
185 # Step #3: Configure the base detection engine. For more information, see README.decode
186 #####
187
188 # Configure PCRE match limitations
189 config pcre_match_limit: 3500
190 config pcre_match_limit_recursion: 1500
191
192 # Configure the detection engine. See the Snort Manual, Configuring Snort - Includes - Config
193 config detection: search-method ap-sqlite search-runtime max-pattern-len 70
```

Step8: change line/186

Remove the hash



```
227 #####
228 # Configure Perf Profiling for debugging
229 # For more information see README.PerfProfiling
230 #####
231
232 #config profile_rules: print all, sort avg_ticks
233 #config profile_preprocs: print all, sort avg_ticks
234
235 #####
236 # Configure protocol aware flushing
237 # For more information see README.kitware
238 #####
239 config paf_max: 16000
240
241 #####
242 # Step #4: Configure dynamic loaded libraries,
243 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
244 #####
245
246 # path to dynamic preprocessor libraries
247 dynamicpreprocessor_directory c:\snort\lib\snort_dynamicpreprocessor\
248
249 # path to base preprocessor engine
250 dynamicengine c:\snort\lib\snort_dynamicengine\af_engine.dll
251
252 # path to dynamic rules libraries
253 dynamicruleset_directory c:\snort\lib\snort_dynamicruleset\
254
255 #####
256 # Step #5: Configure preprocessors
257 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
258 #####
```

Step9: change line/247

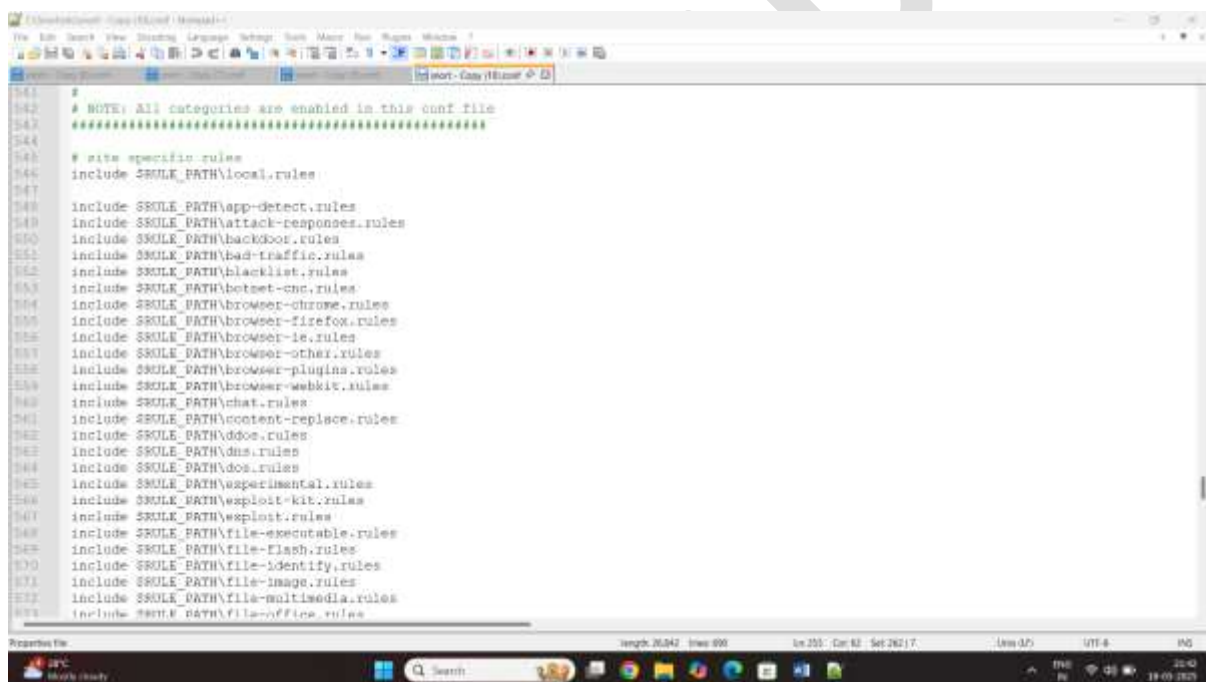
dynamicpreprocessor directory

c:\snort\lib\snort_dynamicpreprocessor/

Step10: change line/ 250

dynamicengine

c:\snort\lib\snort_dynamicengine\sfe_engine.dll



```
241 #
242 # NOTE: All categories are enabled in this conf file
243 #
244 #
245 # site specific rules
246 include $RULE_PATH/local.rules
247
248 include $RULE_PATH/app-detect.rules
249 include $RULE_PATH/attack-responses.rules
250 include $RULE_PATH/backdoor.rules
251 include $RULE_PATH/bad-traffic.rules
252 include $RULE_PATH/blacklist.rules
253 include $RULE_PATH/botnet-cnc.rules
254 include $RULE_PATH/browser-chrome.rules
255 include $RULE_PATH/browser-firefox.rules
256 include $RULE_PATH/browser-ie.rules
257 include $RULE_PATH/browser-other.rules
258 include $RULE_PATH/browser-plugins.rules
259 include $RULE_PATH/browser-webkit.rules
260 include $RULE_PATH/chat.rules
261 include $RULE_PATH/content-replace.rules
262 include $RULE_PATH/ddos.rules
263 include $RULE_PATH/dns.rules
264 include $RULE_PATH/dos.rules
265 include $RULE_PATH/experimental.rules
266 include $RULE_PATH/exploit-kit.rules
267 include $RULE_PATH/exploit.rules
268 include $RULE_PATH/file-executable.rules
269 include $RULE_PATH/file-flash.rules
270 include $RULE_PATH/file-identify.rules
271 include $RULE_PATH/file-image.rules
272 include $RULE_PATH/file-multimedia.rules
273 include $RULE_PATH/file-office.rules
```

Step11: change line/ 511

whitelist \$WHITE_LIST_PATH/whitelist.rules, \

Step12: change line/512

blacklist \$BLACK_LIST_PATH/blacklist.rules


```
544 include $RULE_PATH\malware-cnc.rules
545 include $RULE_PATH\malware-other.rules
546 include $RULE_PATH\malware-tools.rules
547 include $RULE_PATH\misc.rules
548 include $RULE_PATH\multimedia.rules
549 include $RULE_PATH\mysql.rules
550 include $RULE_PATH\netbios.rules
551 include $RULE_PATH\nntp.rules
552 include $RULE_PATH\oracle.rules
553 include $RULE_PATH\os-linux.rules
554 include $RULE_PATH\os-other.rules
555 include $RULE_PATH\os-solaris.rules
556 include $RULE_PATH\os-windows.rules
557 include $RULE_PATH\other-ids.rules
558 include $RULE_PATH\p2p.rules
559 include $RULE_PATH\phishing-spam.rules
560 include $RULE_PATH\policy-multimedia.rules
561 include $RULE_PATH\policy-other.rules
562 include $RULE_PATH\policy.rules
563 include $RULE_PATH\policy-social.rules
564 include $RULE_PATH\policy-spam.rules
565 include $RULE_PATH\pop2.rules
566 include $RULE_PATH\pop3.rules
567 include $RULE_PATH\protocol-finger.rules
568 include $RULE_PATH\protocol-ftp.rules
569 include $RULE_PATH\protocol-icmp.rules
570 include $RULE_PATH\protocol-imap.rules
571 include $RULE_PATH\protocol-pop.rules
572 include $RULE_PATH\protocol-services.rules
573 include $RULE_PATH\protocol-voip.rules
574 include $RULE_PATH\pua-adware.rules
575 include $RULE_PATH\pua-other.rules
576 include $RULE_PATH\rsn-c7n.rules
```

Step12: change line/
546 to 651 change /

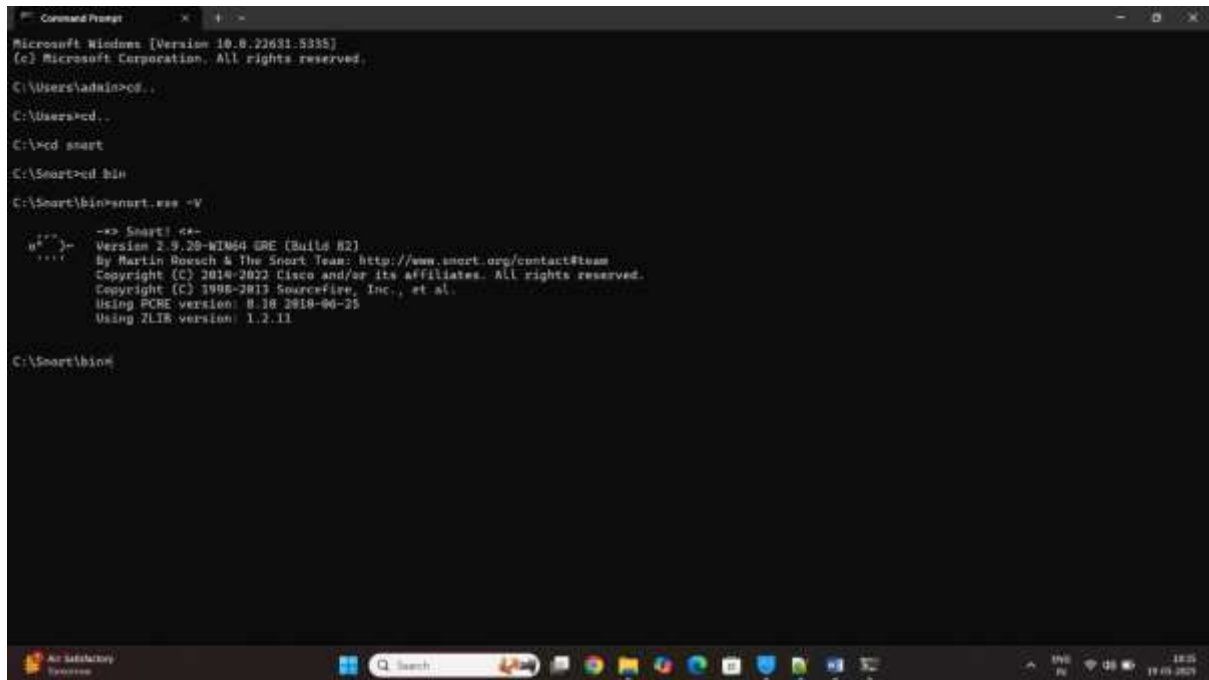
```
646 include $RULE_PATH\web-goldfusion.rules
647 include $RULE_PATH\web-frontpage.rules
648 include $RULE_PATH\web-iss.rules
649 include $RULE_PATH\web-misc.rules
650 include $RULE_PATH\web-php.rules
651 include $RULE_PATH\all.rules

#####
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
#####

# decoder and preprocessor event rules
include $PREPROC_RULE_PATH\preprocessor.rules
include $PREPROC_RULE_PATH\decoder.rules
include $PREPROC_RULE_PATH\sensitive-data.rules

#####
# Step #9: Customize your Shared Object Smart Rules
# For more information, see http://vrt-bing.munir.org/2009/01/using-vrt-certified-shared-object-rules.html
#####

# dynamic library rules
include $SO_RULE_PATH\bad-traffic.rules
include $SO_RULE_PATH\sha1.rules
include $SO_RULE_PATH\doh.rules
include $SO_RULE_PATH\expinit.rules
include $SO_RULE_PATH\icmp.rules
include $SO_RULE_PATH\imap.rules
include $SO_RULE_PATH\misc.rules
include $SO_RULE_PATH\multimedia.rules
include $SO_RULE_PATH\netbios.rules
include $SO_RULE_PATH\rsn.rules
```



```
Microsoft Windows [Version 10.0.22631.5355]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>cd ..
C:\Users>cd ..
C:\>cd snort
C:\snort>cd bin
C:\snort\bin>snort.exe -V

--> Snort! <*-
      )-
      *-
      *-
      *-
      Version 2.9.20-WIN64 GRE (Build B2)
      By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
      Copyright (C) 2010-2022 Cisco and/or its affiliates. All rights reserved.
      Copyright (C) 1998-2013 Sourcefire, Inc., et al.
      Using PCRE version: 8.38 2018-04-25
      Using ZLIB version: 1.2.11

C:\snort\bin>
```

C:\>cd snort

C:\>snort\cd bin

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

Version checking command

```

C:\>cd snort
C:\snort>cd bin
C:\snort\bin>snort.exe -V

--* Snort! *--
o" >-
****
Version 2.9.20-WIN64 GRE (Build 02)
By Martin Roesch & The Snort Team! http://www.snort.org/contactteam
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

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

--* Snort! *--
o" >-
****
Version 2.9.20-WIN64 GRE (Build 02)
By Martin Roesch & The Snort Team! http://www.snort.org/contactteam
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Index  Physical Address  IP Address  Device Name  Description
-----
1  00:00:00:00:00:00  disabled  \Device\NPF_{805A2905-C7EA-4B98-ADFD-002B85F70162}  WAN Miniport (Network Monitor)
2  00:00:00:00:00:00  disabled  \Device\NPF_{804D4462-1CE7-469E-BB9C-32865292CD9}  WAN Miniport (IPv6)
3  00:00:00:00:00:00  disabled  \Device\NPF_{5CCB1807-C67F-43A3-9F18-E336F9E9DE82}  WAN Miniport (IP)
4  00:02:3E:08:F1:62  192.168.235.118  \Device\NPF_{D678A802-CED2-4861-BF7C-D7C9EFD3AD7}  Intel(R) Wireless-AC 9560 160MHz
5  00:00:00:00:00:00  192.168.101.1  \Device\NPF_{5C8B3E16-5ABD-4BF1-BE7A-8EC6A1E138CB}  VMware Virtual Ethernet Adapter for VMnet8
6  00:00:00:00:00:00  192.168.125.1  \Device\NPF_{3A90A2C7-2EFA-4062-909F-80493A79F87}  VMware Virtual Ethernet Adapter for VMnet1
7  00:02:3E:08:F1:62  169.254.226.54  \Device\NPF_{E38AC287-4F68-4E2D-B384-CC1E3F36A73A}  Microsoft Wi-Fi Direct Virtual Adapter #2
8  00:02:3E:08:F1:62  169.254.183.248  \Device\NPF_{8F88133C-8726-4F63-BB08-76FAA2C0306E}  Microsoft Wi-Fi Direct Virtual Adapter
9  00:00:27:00:00:00  192.168.56.1  \Device\NPF_{6C38609B-2586-4EFC-AEFD-877CC88866B6}  VirtualBox Host-Only Ethernet Adapter
10  00:00:00:00:00:00  0000:0000:0000:0000:0000:0000  \Device\NPF_{Loopback}  Adapter for loopback traffic capture
11  00:FF:50:56:C4:2E  169.254.33.216  \Device\NPF_{5056C42E-C463-4F21-8A58-AC3C67735284}  HotspotShield TAP-Windows Adapter V9
12  00:50:C2:37:82:B4  169.254.136.37  \Device\NPF_{2A74883C-1838-465E-8D1D-96F8B0F032EF}  Intel(R) Ethernet Connection (6) I219-LM

C:\snort\bin>

```

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

Interface checking command

```

2 byte states : 19.06
4 byte states : 137.47

[ Number of patterns truncated to 28 bytes: 651 ]

MaxRas at the end of detection rules:17867872
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{0670A802-CED2-4861-BF7C-D7C9EFD3AD7}:".

--* Initialization Complete *--

--* Snort! *--
o" >-
****
Version 2.9.20-WIN64 GRE (Build 02)
By Martin Roesch & The Snort Team! http://www.snort.org/contactteam
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SMLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSM Version 1.1 <Build 7>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SOF Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.8 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FIPELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DMP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCEPCE2 Version 1.8 <Build 3>

Total snort Fixed Memory Cost = MaxRas:58532472
Snort successfully validated the configuration!
Snort exiting

C:\snort\bin>

```

C:\snort\bin> snort -l 5 -c c:\snort\etc\snort\conf -A

This command testing snort configuration

```

--treat-drop-as-alert      Converts drop, alert, and reject rules into alert rules during startup.
--treat-drop-as-ignore    Use drop, alert, and reject rules to ignore session traffic when not inline.
--process-all-events      Process all queued events (drop, alert,...), default stops after 1st action group.
--enable-inline-test      Enable Inline-Test Mode Operation
--dynamic-engine-lib <file> Load a dynamic detection engine
--dynamic-engine-lib-dir <path> Load all dynamic engines from directory
--dynamic-detection-lib <file> Load a dynamic rules library
--dynamic-detection-lib-dir <path> Load all dynamic rules libraries from directory
--dump-dynamic-rules <path> Creates stub rule files of all loaded rules libraries
--dynamic-preprocessor-lib <file> Load a dynamic preprocessor library
--dynamic-preprocessor-lib-dir <path> Load all dynamic preprocessor libraries from directory
--dynamic-output-lib <file> Load a dynamic output library
--dynamic-output-lib-dir <path> Load all dynamic output libraries from directory
--pcap-single <cf>       Same as -r.
--pcap-file <file>       File that contains a list of pcaps to read - read mode is implied.
--pcap-list <list>       a space separated list of pcaps to read - read mode is implied.
--pcap-loop <count>      this option will read the pcaps specified on command line continuously.
                        for <count> times. A value of 0 will read until Snort is terminated.
--pcap-reset             If reading multiple pcaps, reset Snort to post-configuration state before reading next pcap.
--pcap-show              print a line saying what pcap is currently being read.
--exit-check <count>     Signal termination after <count> callbacks from DAQ.Acquire(), showing the time it
                        takes from signaling until DAQ.Stop() is called.
--conf-error-out         Same as -v.
--enable-mpls-multicast  Allow multicast MPLS
--enable-mpls-overlapping-ip Handle overlapping IPs within MPLS clouds
--max-mpls-labelchain-len Specify the max MPLS label chain
--mpls-payload-type       Specify the protocol (ipv4, ipv6, ethernet) that is encapsulated by MPLS
--require-rule-sid        Require that all snort rules have SID specified.
--daq-type <mode>        Select packet acquisition module (default is pcap).
--daq-mode <mode>        Select the DAQ operating mode.
--daq-var <name=value>   Specify extra DAQ configuration variable.
--daq-dir <dir>          Tell snort where to find desired DAQ.
--daq-list [<dir>]        List packet acquisition modules available in dir. Default is static modules only.
--dirty-pig              Don't flush packets and release memory on shutdown.
--cs-dir <dir>           Directory to use for control socket.
--ha-peer               Activate live high-availability state sharing with peer.
--ha-out <file>         Write high-availability events to this file.
--ha-in <file>          Read high-availability events from this file on startup (warm-start).
--suppress-config-log    Suppress configuration information output.

C:\Snort\bin>

```

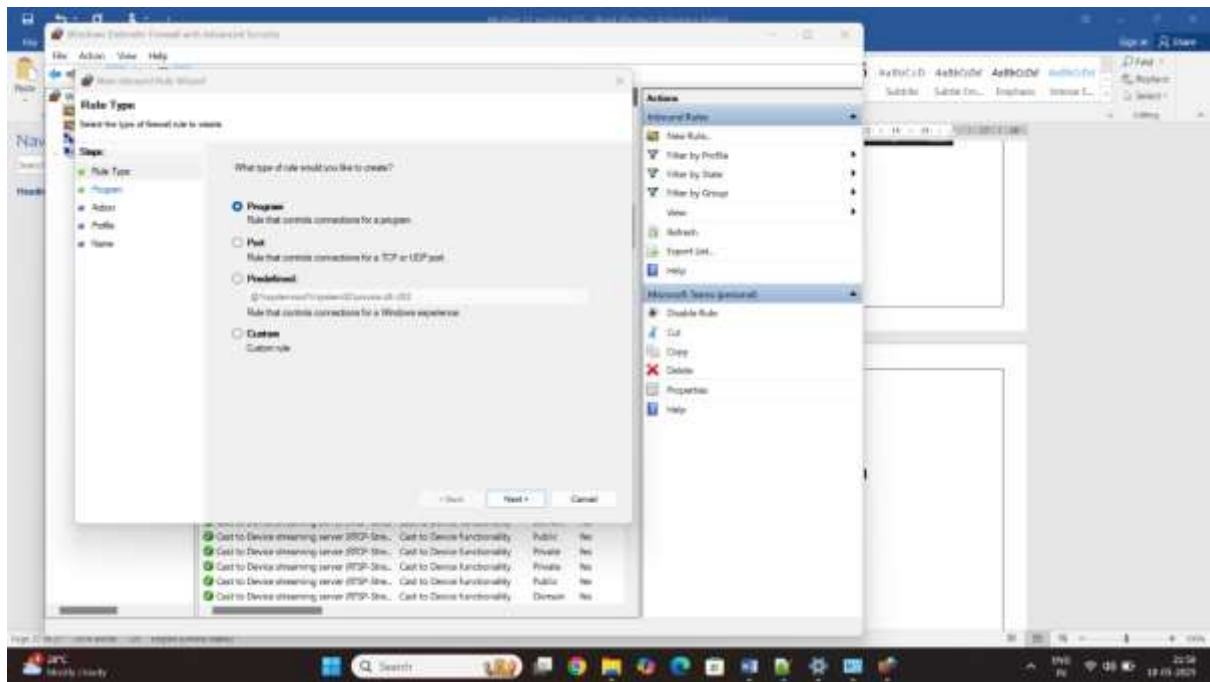
C:\snort\ bin> snort -l 5 -c c:\snort\etc\snort\conf -W

This command are monitoring mode use

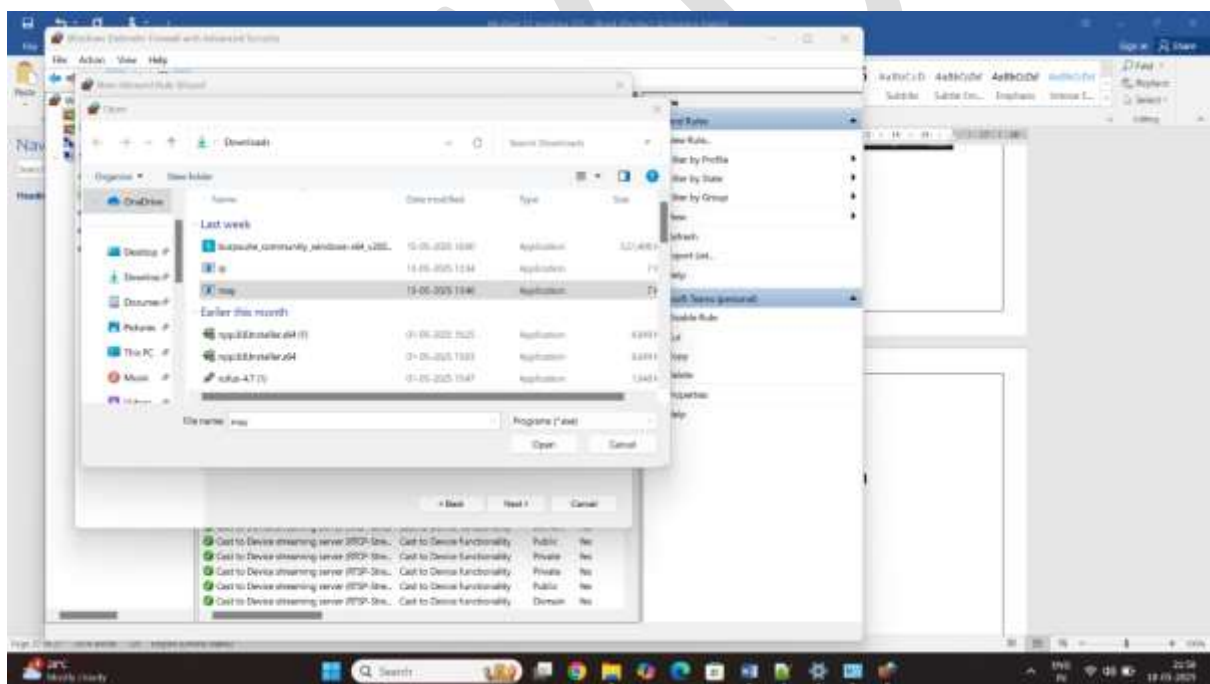
How to windows firewall configuration in bound traffic rule

Step1: go to setting and select the option windows defender

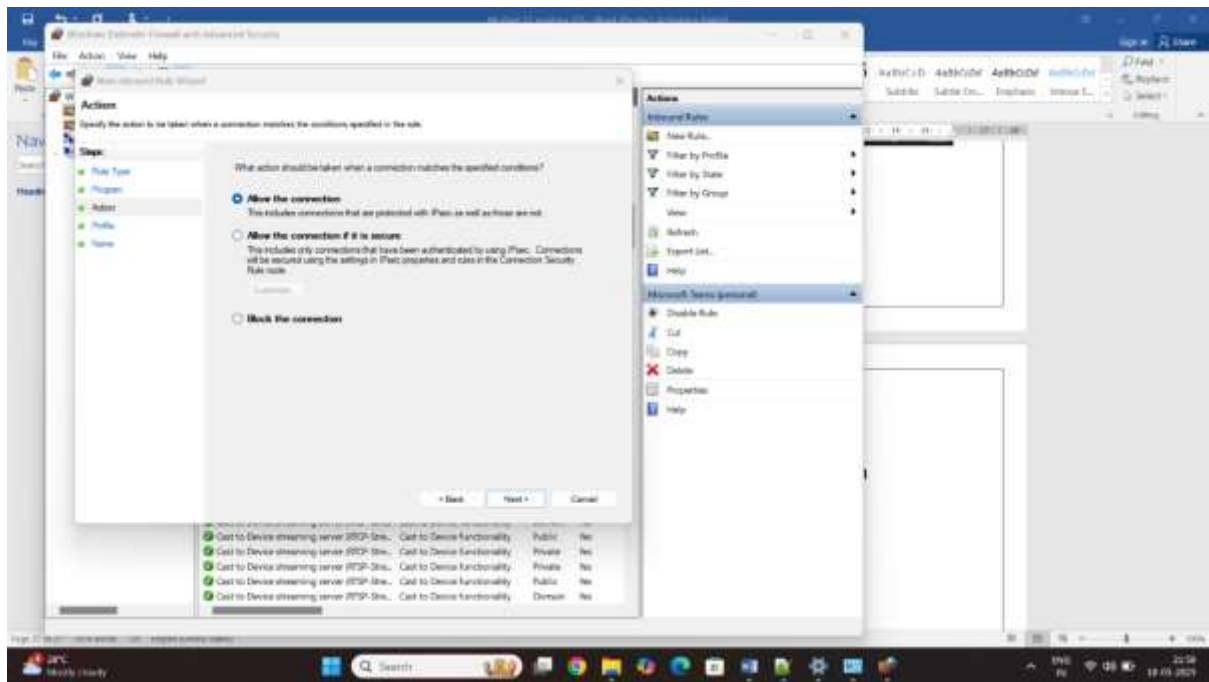
Step2 choice the option inbound



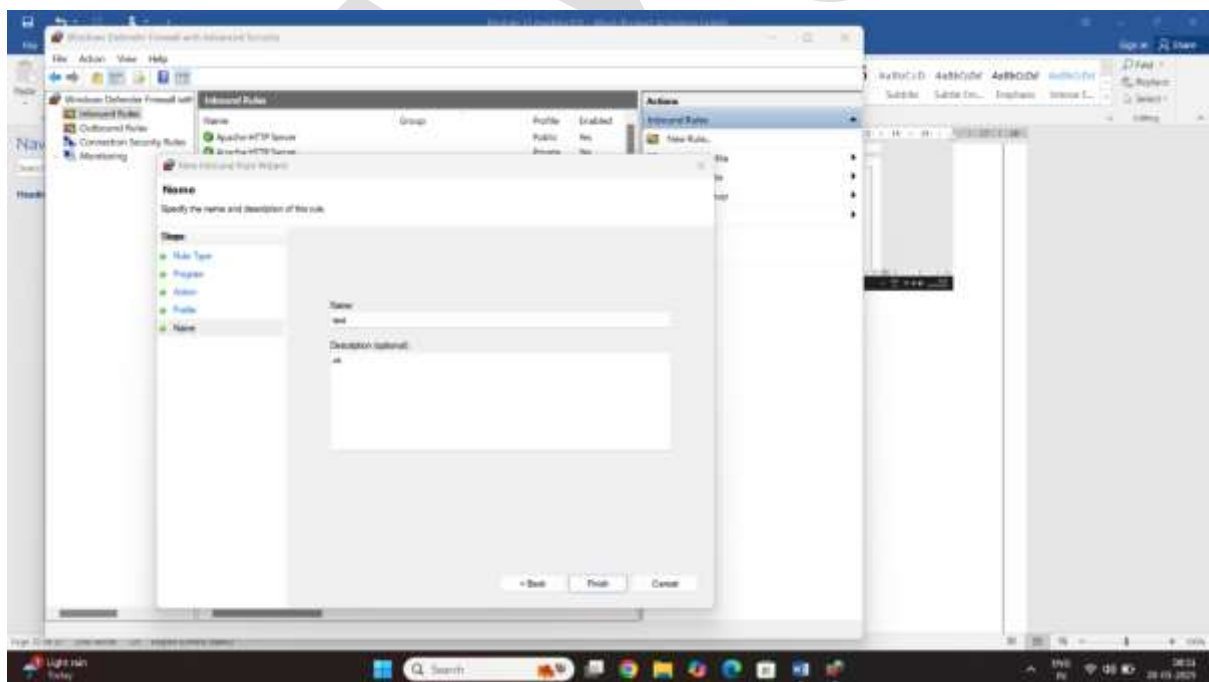
Step3:select the program option



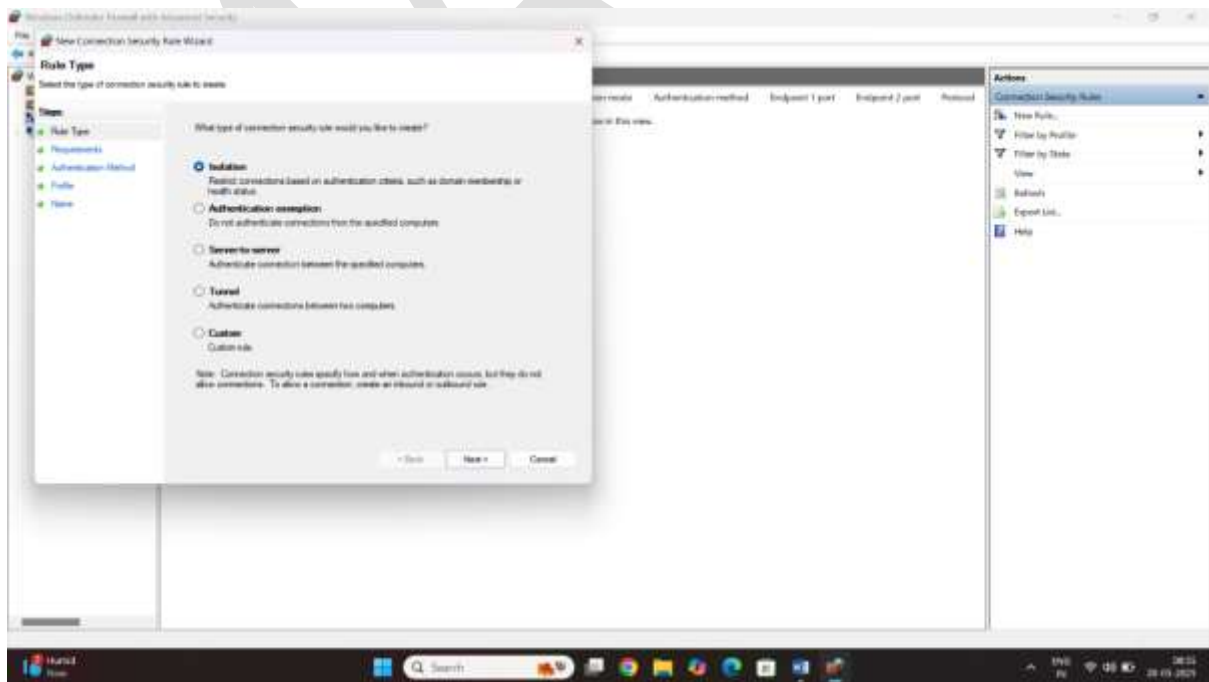
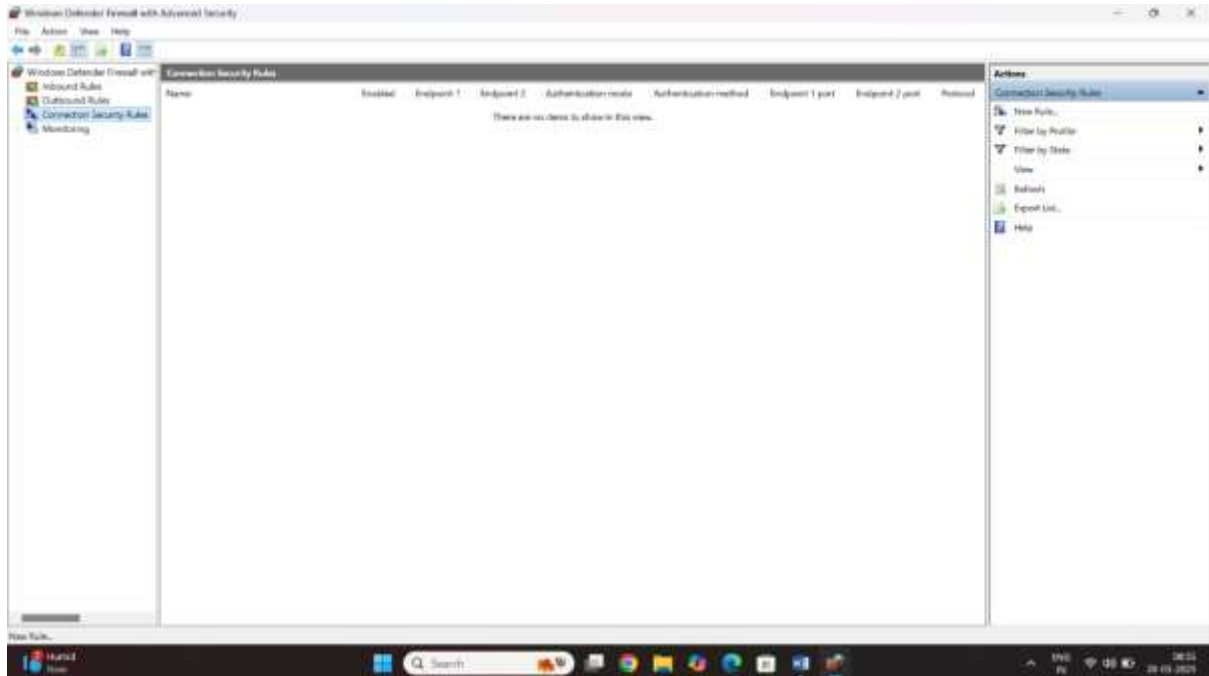
Step4: click on browser choice the block activity

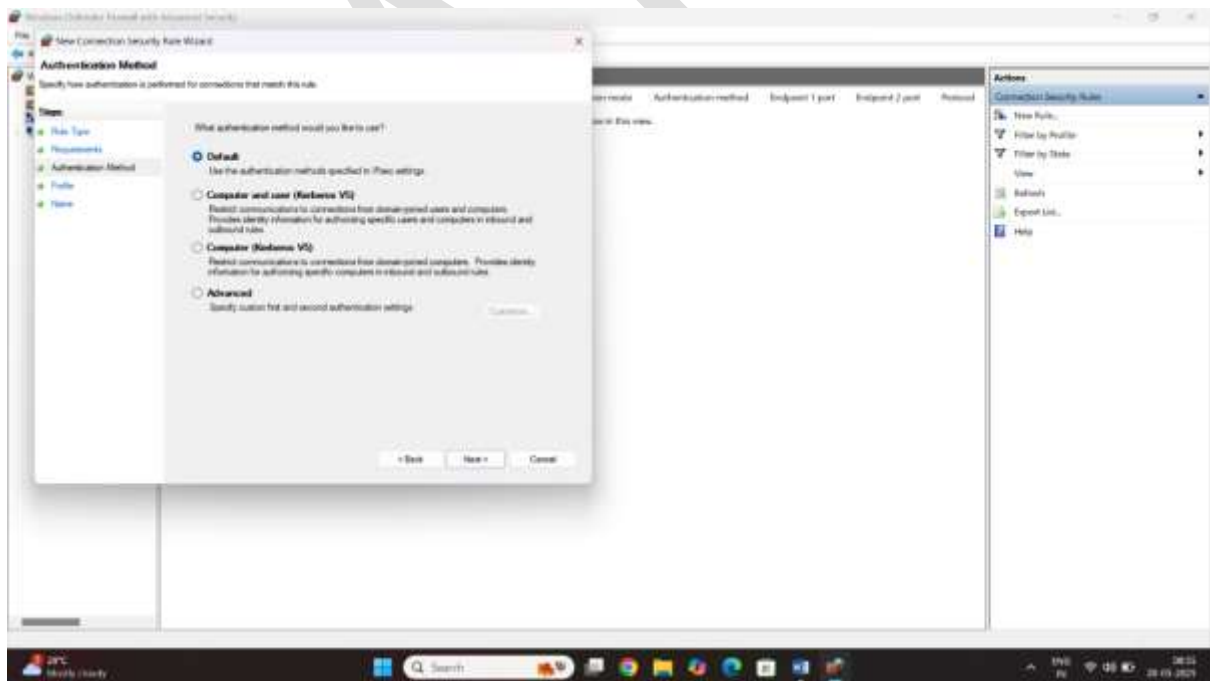
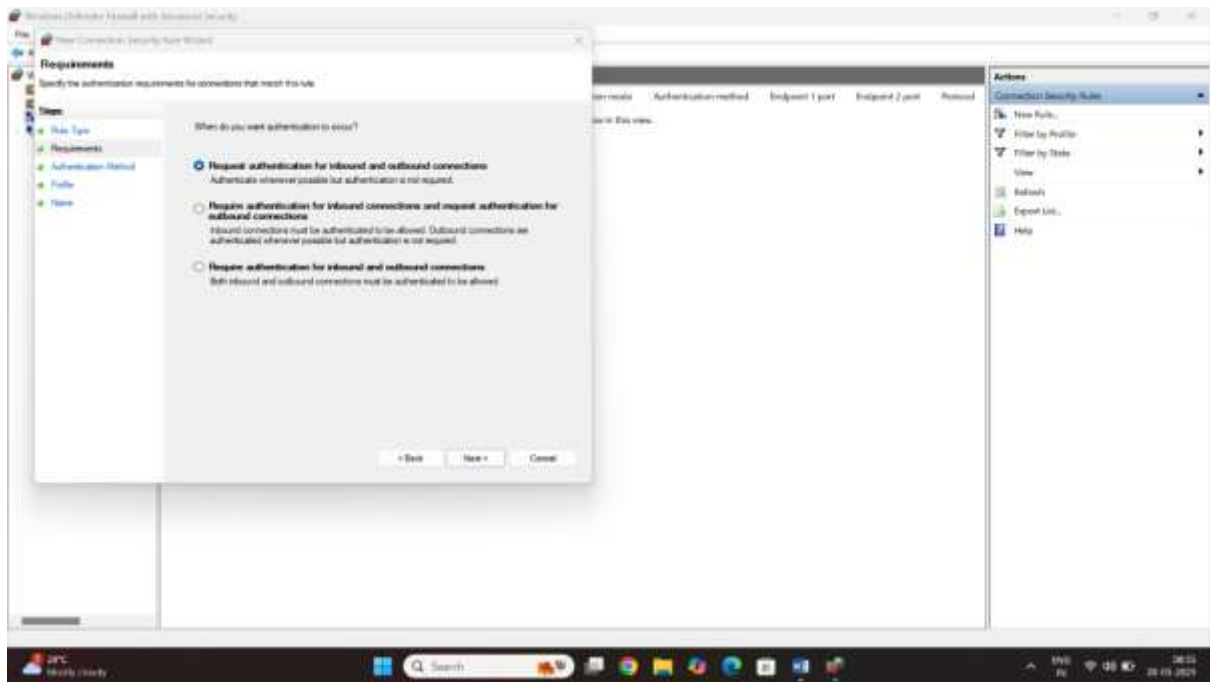


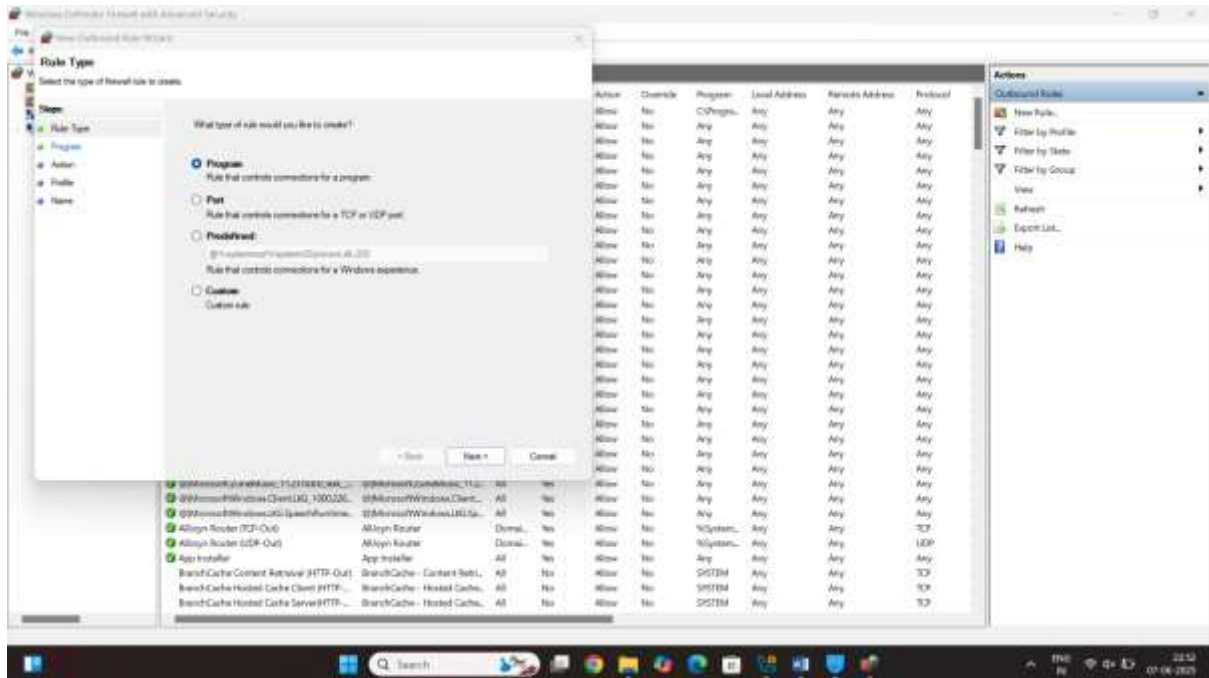
Step5: select the option all



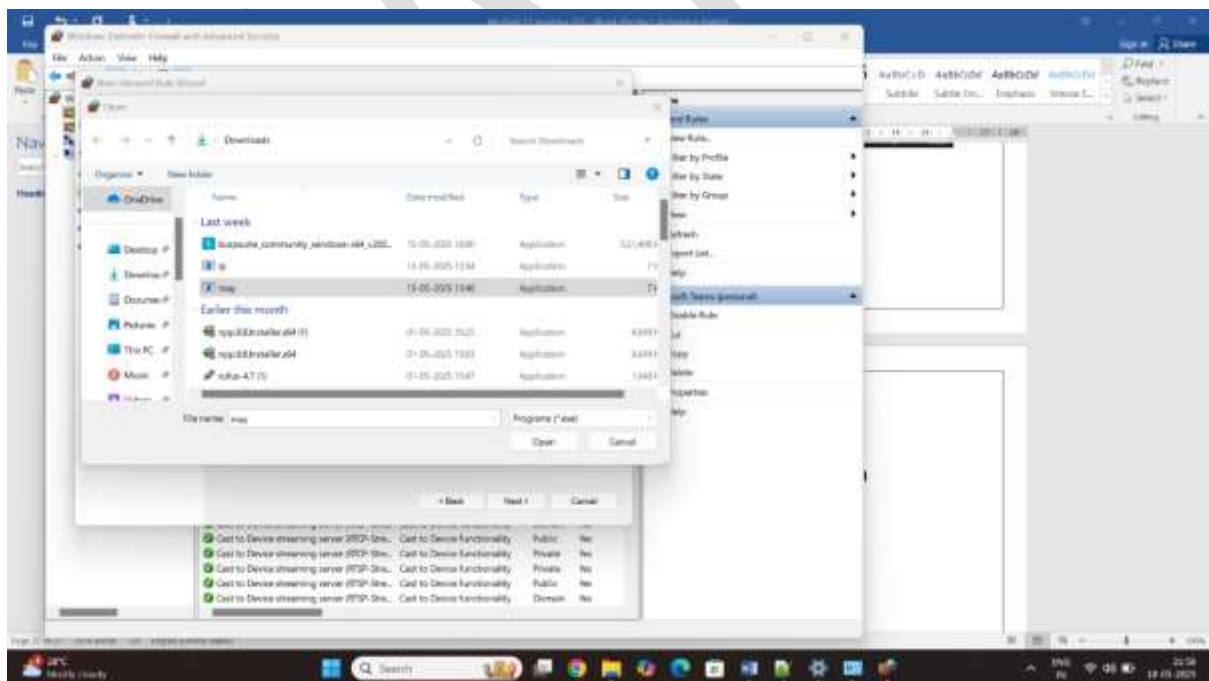
Connection security rules



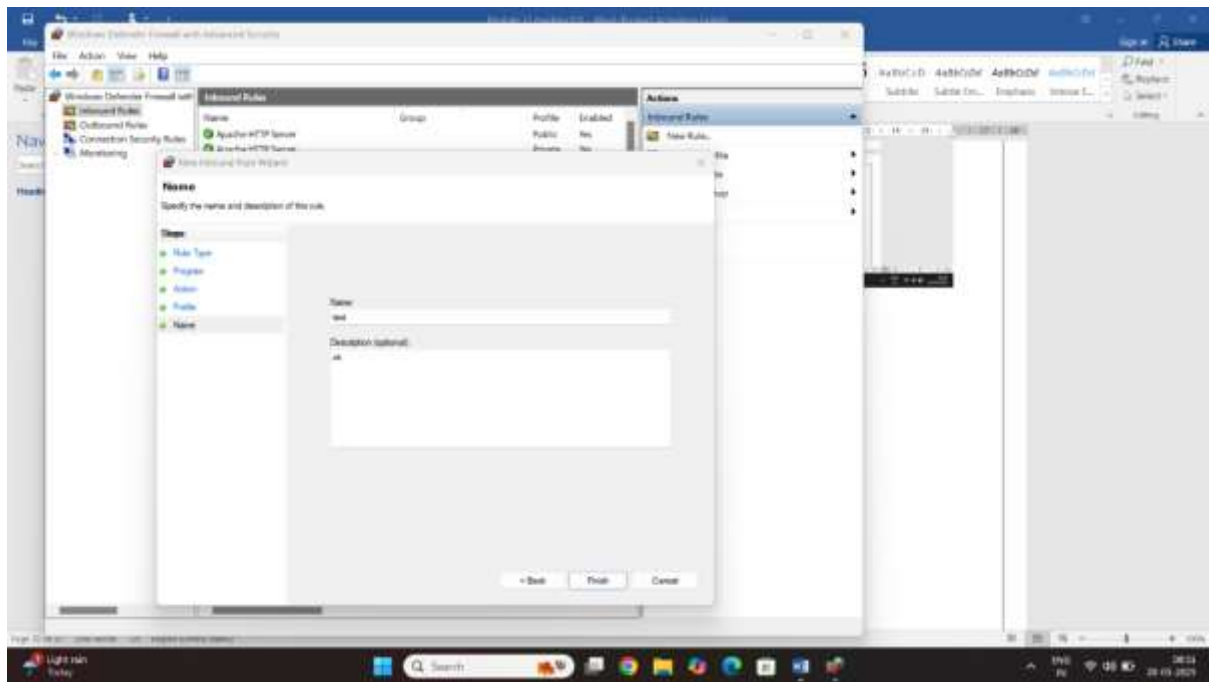




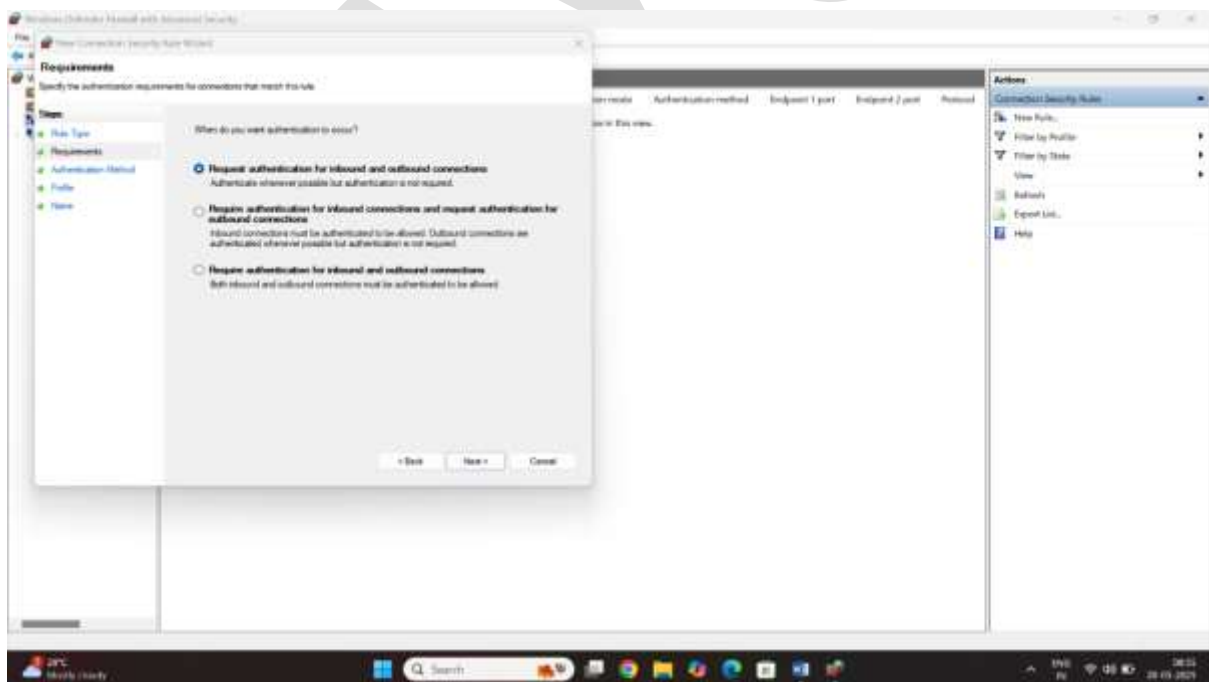
Step3:select the program option



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 configuration

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.

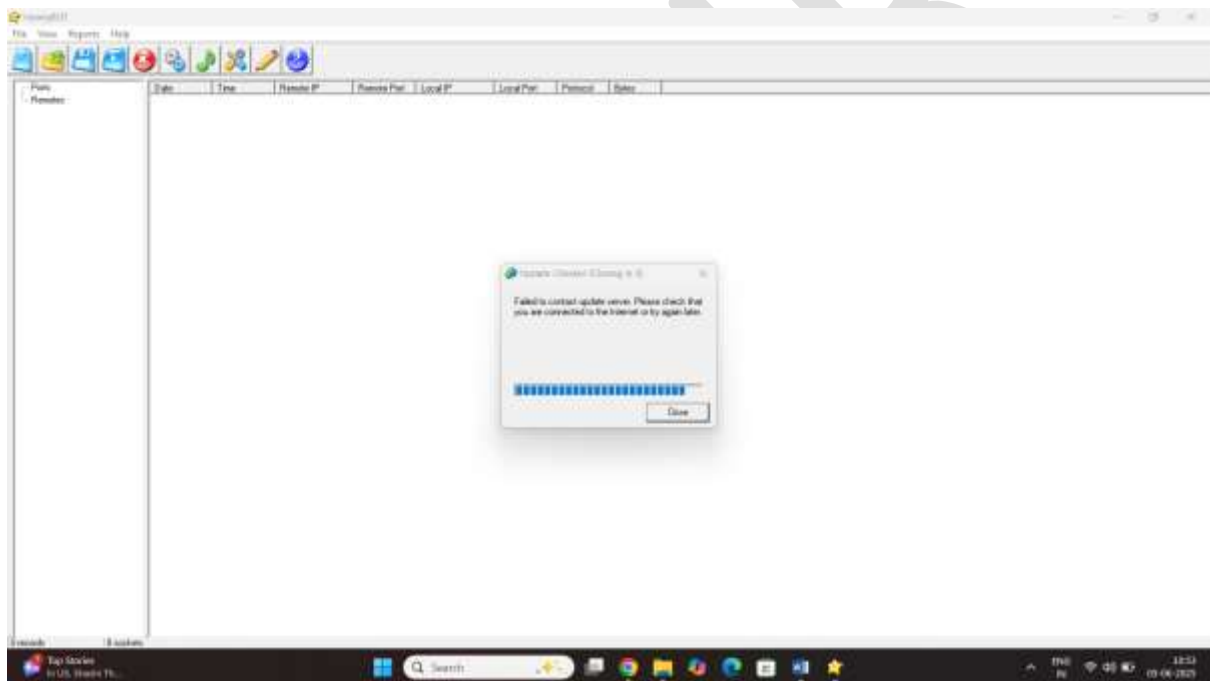
- **Examples:**

- 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



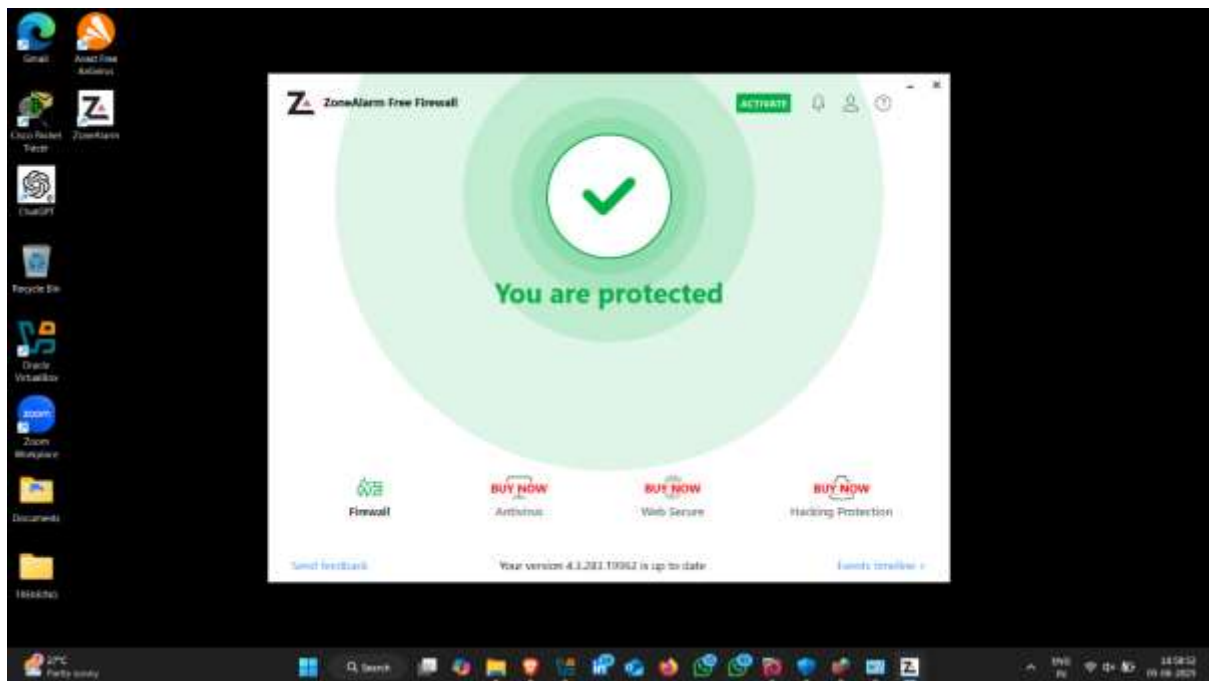
Click on all monetring option

⚙️ Key Features

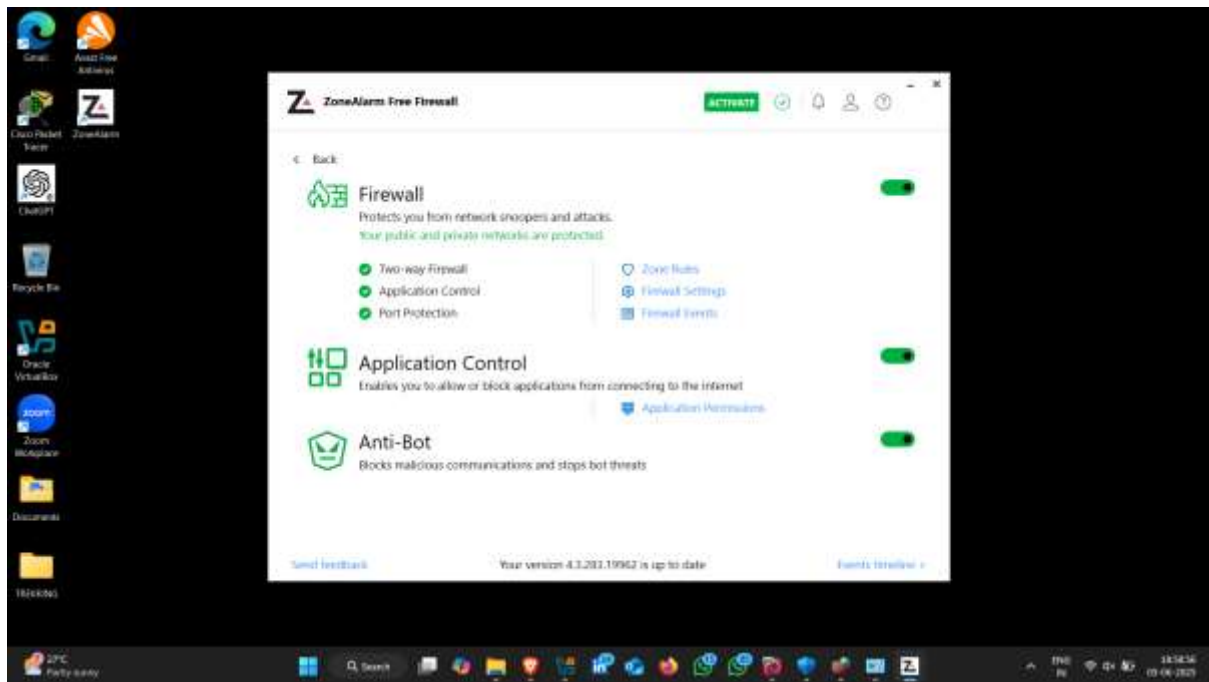
- **Two-Way Firewall Protection:** Monitors both inbound and outbound traffic, blocking unauthorized access and preventing malware from sending your data out.
- **Advanced Security Zones:** Defines three security zones—Trusted, Public, and Blocked—to apply appropriate security levels based on network 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.

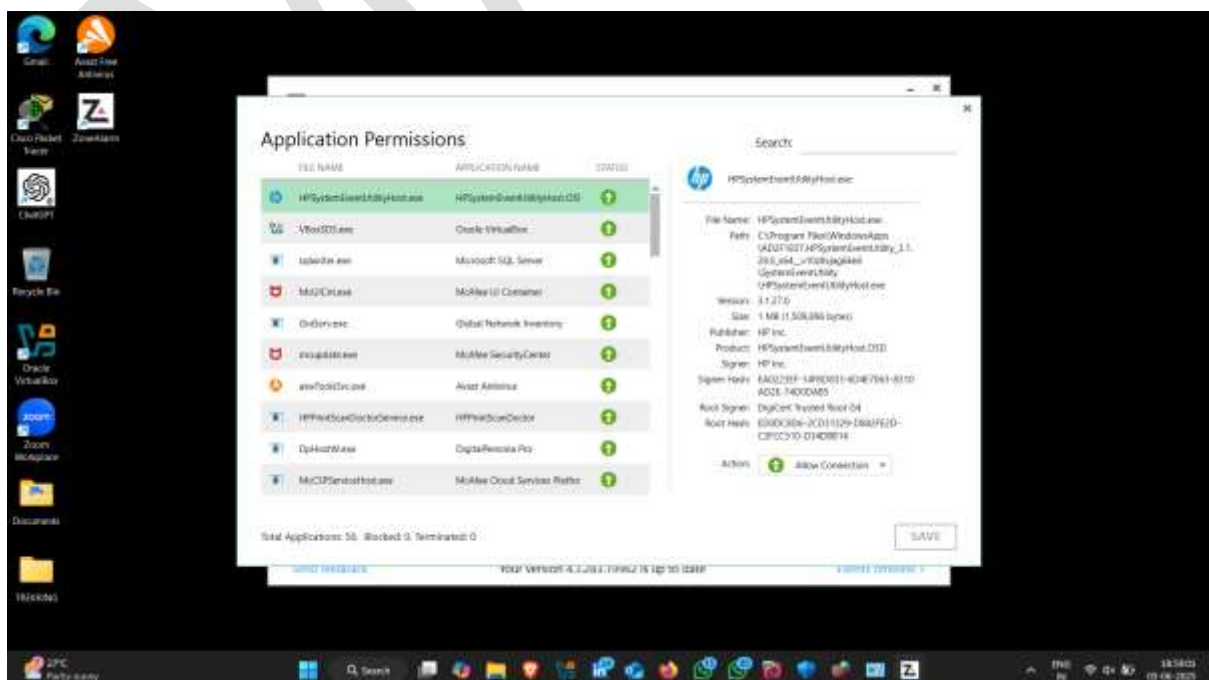
Configuration Zone alarm



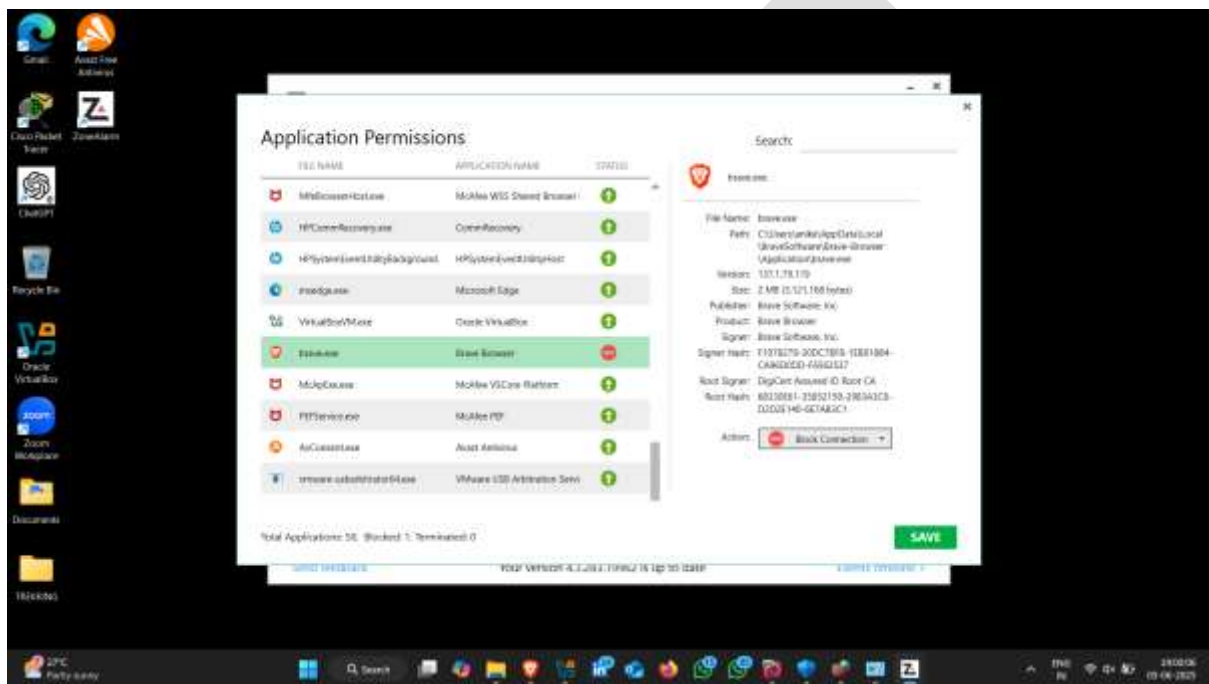
Step1: click on zone alarm and start here



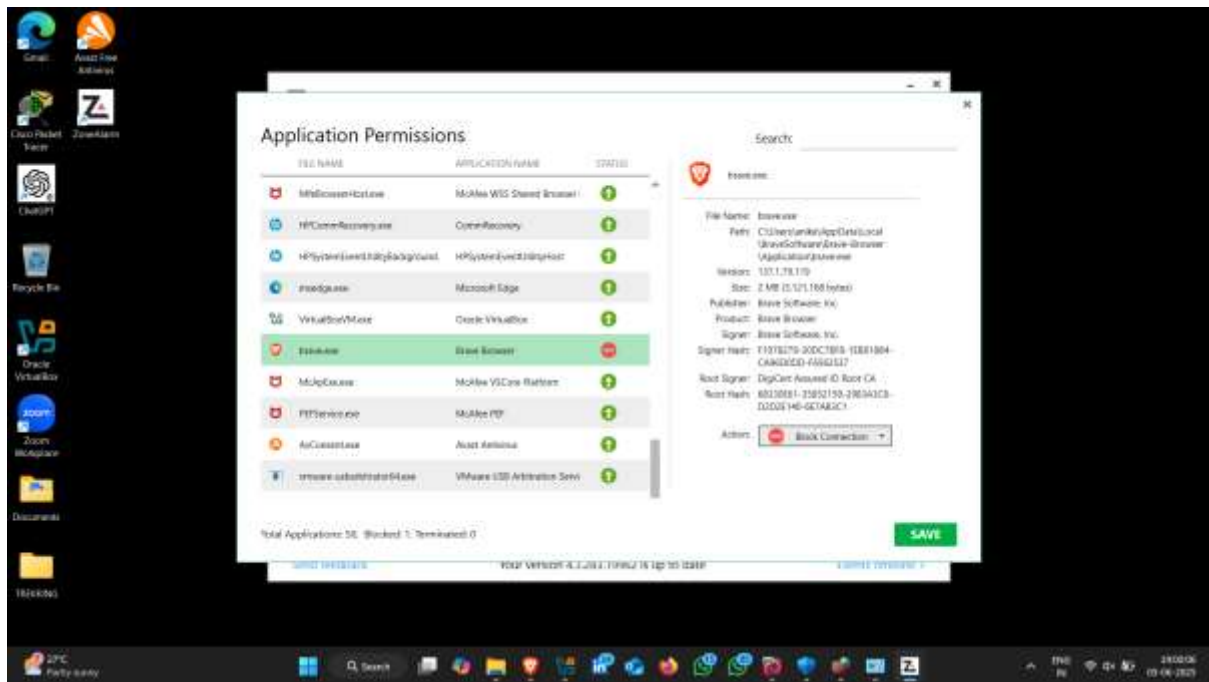
Step2 : select the all option allow permission



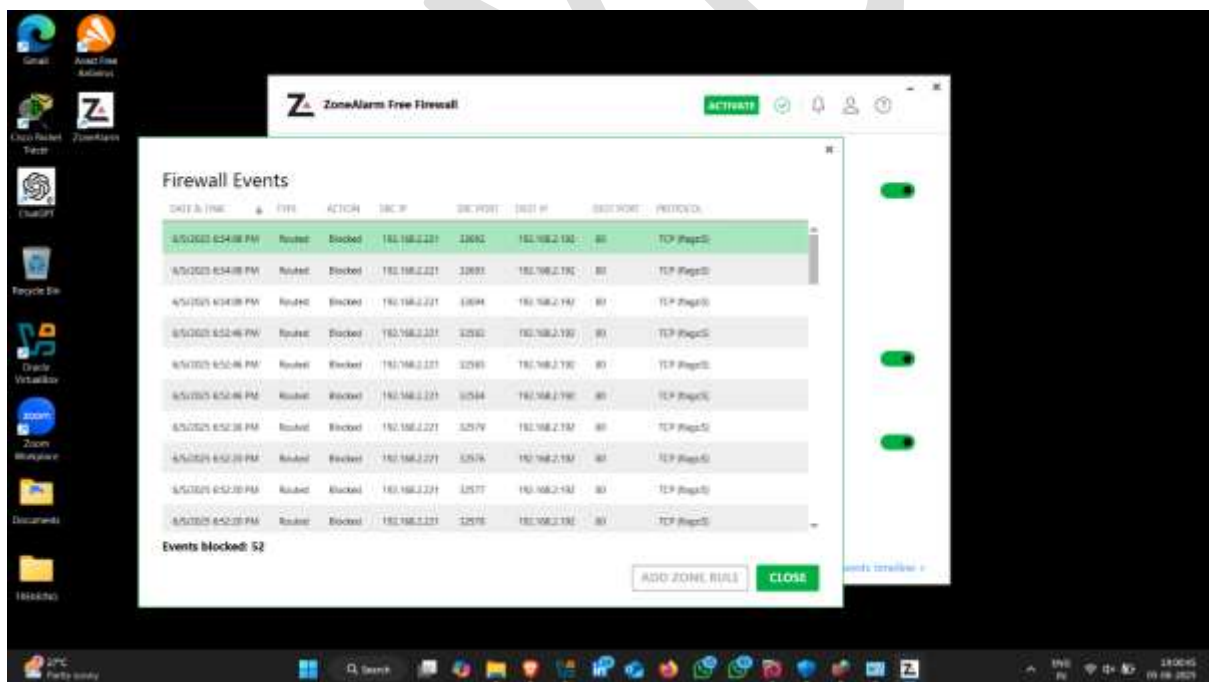
Step3 select application permission With set of rule



Step 4 I am choice the brave browser permission



Step5 Clicik on save and next



Step6 Complete the zone alarm configuration

MAYUR