

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 configrtation**

MANUUR

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.

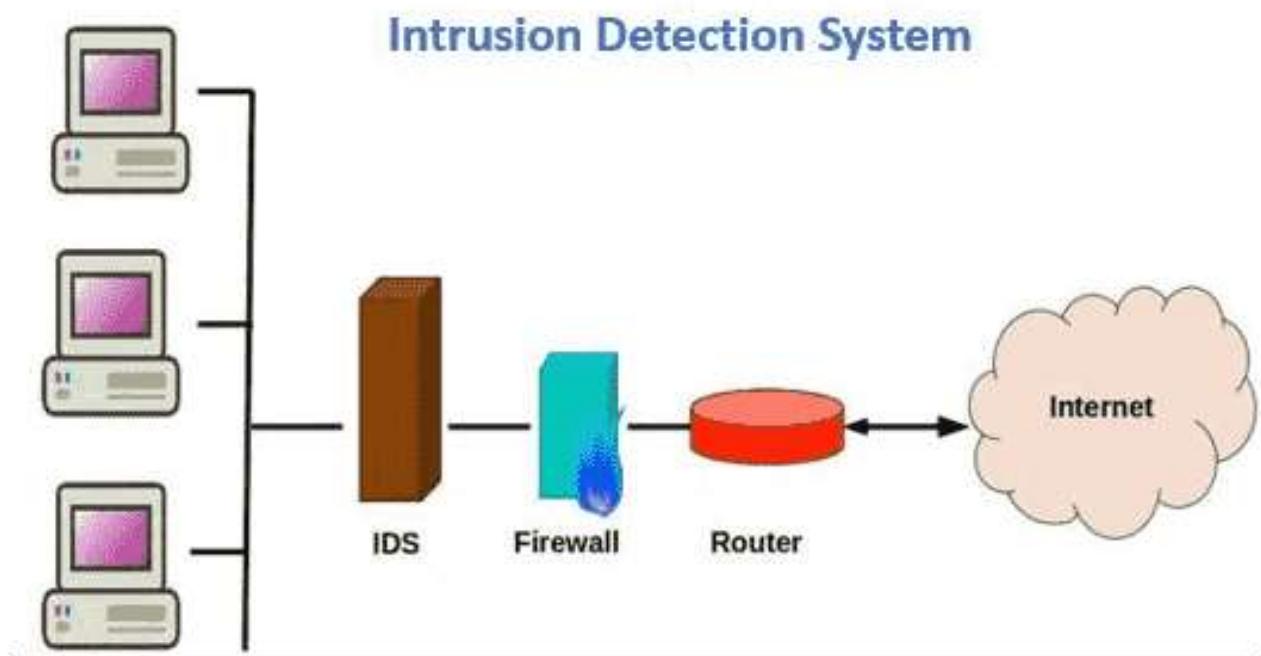
9. Analyze Past Attacks

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.

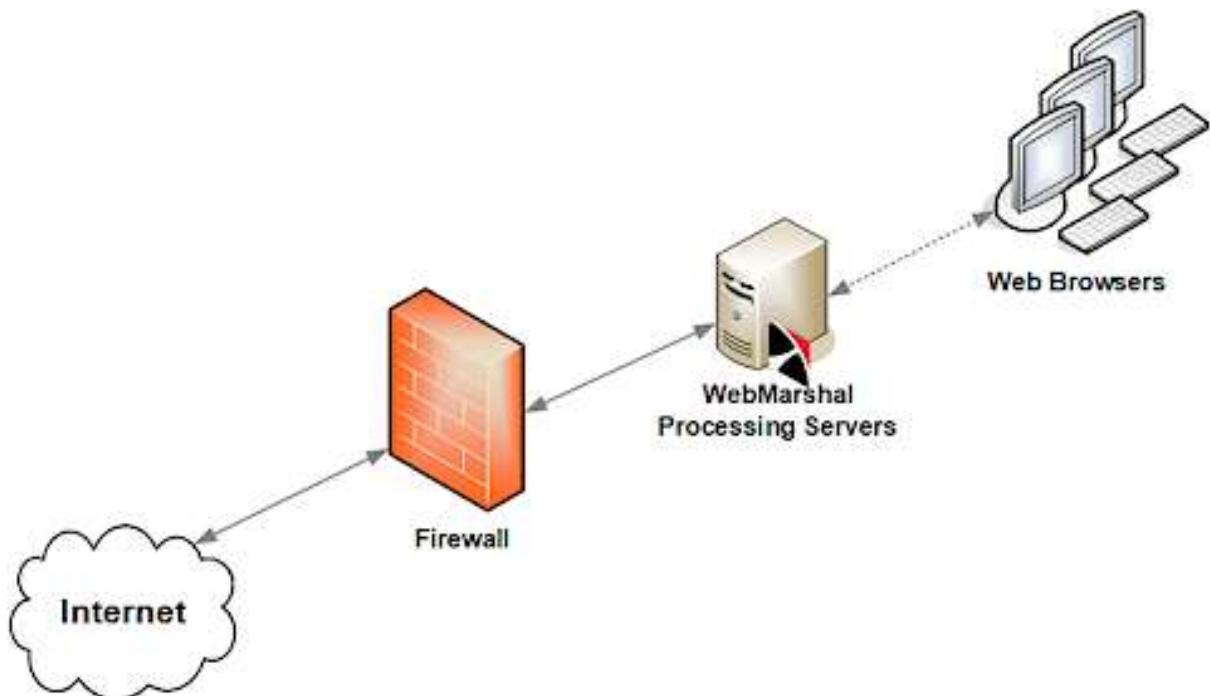
Types of password

- 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

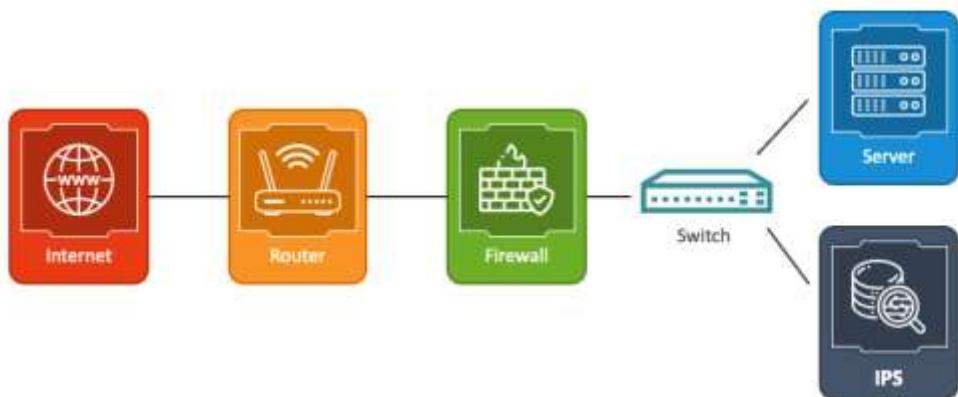
- Stops threats early, minimizing potential **downtime, data loss, or breaches.**

✓ 9. Alerts and Logs for Forensics

- Logs events for later analysis or investigation.

How does work IPS

INTRUSION PREVENTION SYSTEM



Source : www.thesecuritybuddy.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

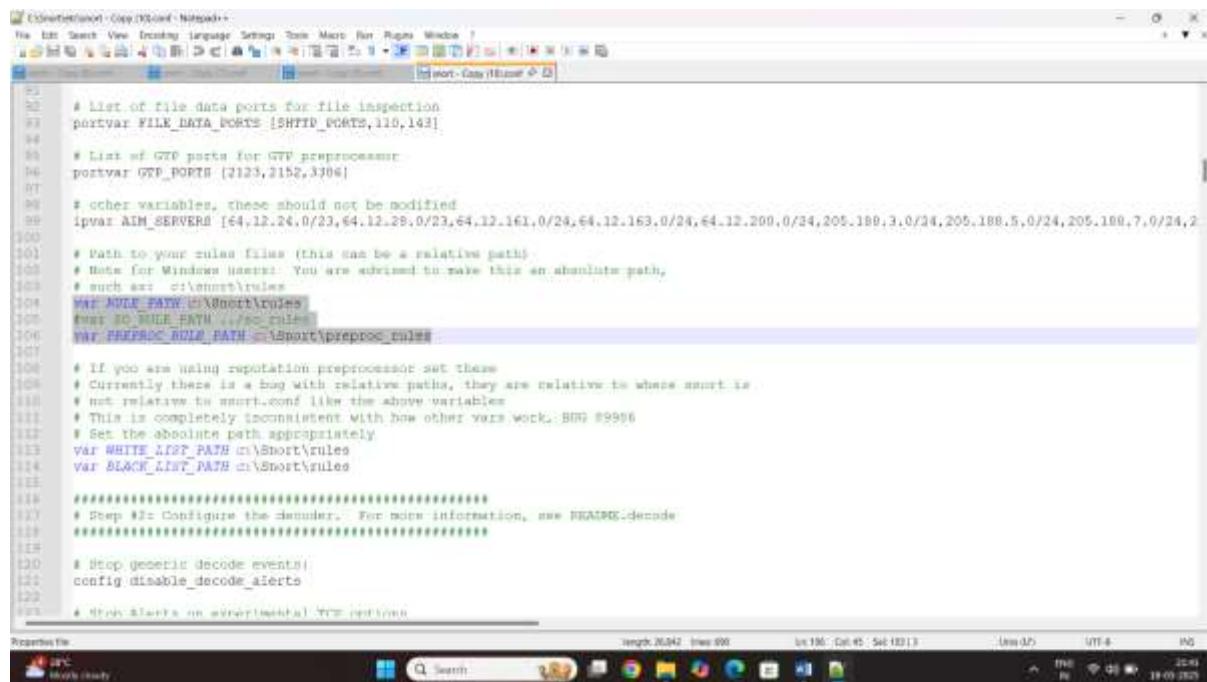
```
# Configure the base detection engine
# Configure dynamic loaded libraries
# Configure preprocessor
# Configure output pipeline
# Customize your rule set
# Customize preprocessor and decoder rule set
# Customize shared object rule set
#####
#
# Step #2: Set the network variables. For more information, see README.variables
#
# Setup the network addresses you are protecting
$PVIZ_HOME_NET 192.168.1.0/24
#
# Set up the external network addresses. Leave as "any" in most situations
$PVIZ_EXTERNAL_NET (SHOME_NET
#
# List of DNS servers on your network
$PVIZ_DNS_SERVERS SHOME_NET
#
# List of SMTP servers on your network
$PVIZ_SMTP_SERVERS SHOME_NET
#
# List of web servers on your network
$PVIZ_HTTP_SERVERS SHOME_NET
#
# List of sql servers on your network
$PVIZ_SQL_SERVERS SHOME_NET
#
# List of telnet servers on your network
$PVIZ_TELNET_SERVERS SHOME_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 [SHFTTD_PORTS,110,143]
# List of GTP ports for GTP preprocessor
$portvar GTP_PORTS [2123,2152,3306]
# other variables, these should not be modified
$ipvar AIM_SERVERS [64.12.24.0/23,64.12.29.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.189.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.8.0/24]
# 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 ED_RULE_PATH ..\..\rules
$var PREPROC_RULE_PATH ..\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 REAMDE-decode
#####
# Stop generic decode events
$config disable_decode_alerts
# Only starts on experimental TCP options
```

Step5: change line/104

Var RULE_PATH c:\snort\rules

Step6:change line/105

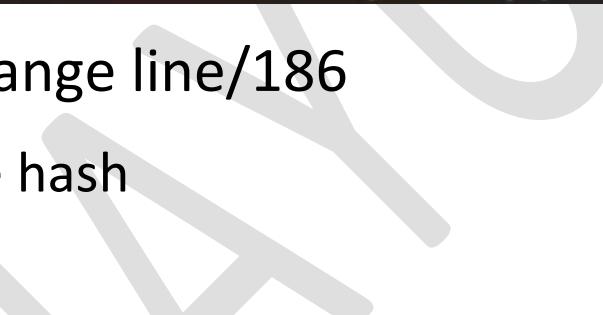
Remove hash

Step7: change line/

Var preproce_RULE_PATH
C:\snort\preproc_roles

Step8: change line/

var BLACK_LIST_PATH c:\Snort\rules



```
156 # <var> := arbitrary <name>-<value> passed to DAQ
157 # <dir> := path as to where to look for DAQ module so's
158
159 # Configure specific DAQ and DIB to run snort as after dropping privs. For more information see snort -h command line options
160 #
161 # config set_gid:
162 # config set_uid:
163
164 # Configure default snaplen. Snort defaults to MTU of in use-interface. For more information see README
165 #
166 # config snaplen:
167 #
168
169 # Configure default bpf_file to use for filtering what traffic reaches snort. For more information see snort -h command line options (-F)
170 #
171 # config bpf_file:
172 #
173
174 # Configure default log_directory for snort to log to. For more information see snort -h command line options (-l).
175 #
176 #config log_directory:snortlog
177
178 #####
179 # Step #3: Configure the main detection engine. For more information, see README.decode
180 #####
181
182 # Configure PCRE match limitations
183 config pcre_match_limit: 3500
184 config pcre_match_limit_recursion: 1500
185
186 # configure the detection engine. See the Snort Manual, Configuring Snort - Includes - config
187 config startaction: searchthreaded|af-sPLIT|searchconflict|no-new-pattern|len 20
```

Step8: change line/186

Remove the hash



```
156 #####
157 # Configure Perf Profiling for debugging
158 # For more information see README.PerfProfiling
159 #####
160
161 #config profile_rules: print all, sort avg_ticks
162 #config profile_preprocess: print all, sort avg_ticks
163
164 #####
165 # Configure pmtuclncktle: maxmflushing
166 # For more information see README.xmaxmflush
167 #####
168 config pmtu_max: 16000
169
170 #####
171 # Step #4: Configure dynamic loaded libraries.
172 # For more information, see Snort Manual, Configuring Snort - Dynamic Modules
173 #####
174
175 # path to dynamic preprocessor libraries
176 #dynamicpreprocessor:of directory C:\Snort\lib\x86\snort_dynamicpreprocessor/
177
178 # path to base preprocessor engine
179 #dynamicengine: c:\Snort\lib\x86\snort_dynamicengine\of_engine.dll
180
181 # path to dynamic rules libraries
182 #dynamicrulelibrary: directory C:\Snort\lib\x86\snort_dynamicrules/
183
184 #####
185 # Step #5: Configure preprocessors
186 # For more information, see the Snort Manual, Configuring Snort - Preprocessors
187 #####
188
```

Step9: change line/247

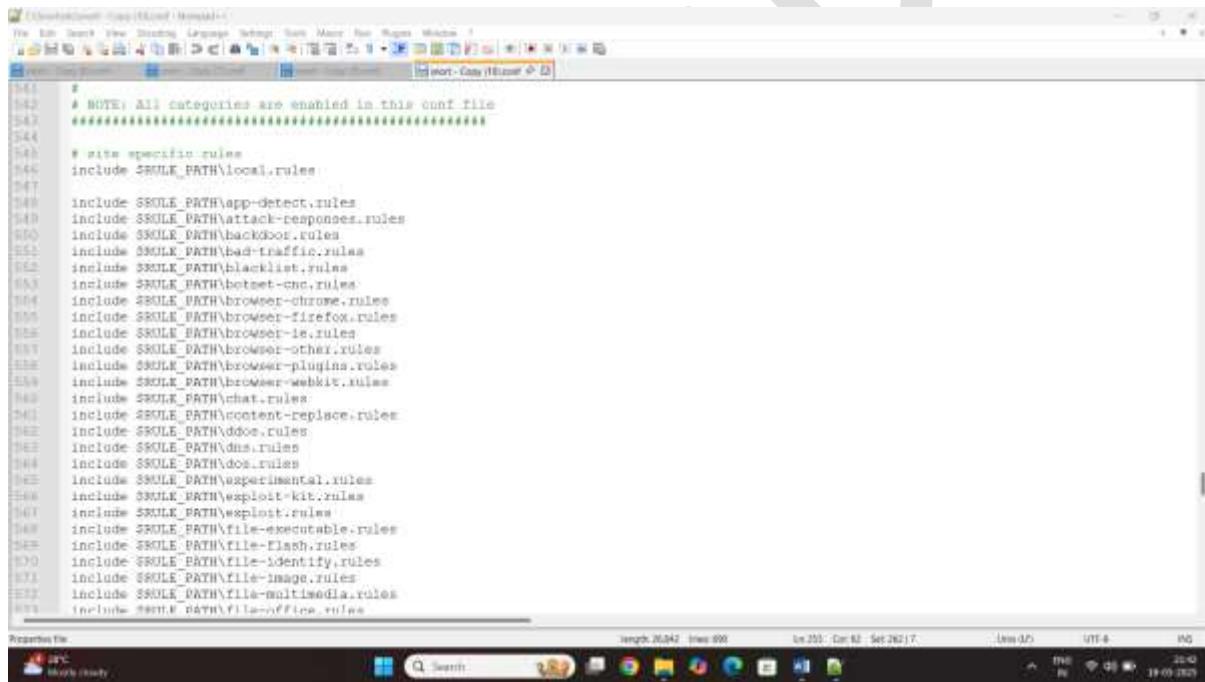
dynamicpreprocessor directory

c:\snort\lib\snort_dynamicpreprocessor/

Step10: change line/ 250

dynamicengine

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



```
141 #  
142 # NOTE: All categories are enabled in this conf file  
143 #####  
144  
145 # site specific rules  
146 include $RULE_PATH\local.rules  
147  
148 include $RULE_PATH\app-detect.rules  
149 include $RULE_PATH\attack-responses.rules  
150 include $RULE_PATH\backbot.rules  
151 include $RULE_PATH\bad-traffic.rules  
152 include $RULE_PATH\blacklist.rules  
153 include $RULE_PATH\botnet-cnc.rules  
154 include $RULE_PATH\browser-chrome.rules  
155 include $RULE_PATH\browser-firefox.rules  
156 include $RULE_PATH\browser-ie.rules  
157 include $RULE_PATH\browser-other.rules  
158 include $RULE_PATH\browser-plugins.rules  
159 include $RULE_PATH\browser-webkit.rules  
160 include $RULE_PATH\chat.rules  
161 include $RULE_PATH\content-replace.rules  
162 include $RULE_PATH\ddos.rules  
163 include $RULE_PATH\dns.rules  
164 include $RULE_PATH\dos.rules  
165 include $RULE_PATH\experimental.rules  
166 include $RULE_PATH\exploit-kit.rules  
167 include $RULE_PATH\exploits.rules  
168 include $RULE_PATH\file-executable.rules  
169 include $RULE_PATH\file-Flash.rules  
170 include $RULE_PATH\file-identify.rules  
171 include $RULE_PATH\file-image.rules  
172 include $RULE_PATH\file-multimedia.rules  
173 include $RULE_PATH\file-pdf.rules  
174 include $RULE_PATH\file-tiff.rules
```

Step11: change line/ 511

whitelist \$WHITE_LIST_PATH/whitelist.rules, \

Step12: change line/512

blacklist \$BLACK_LIST_PATH/blacklist.rules

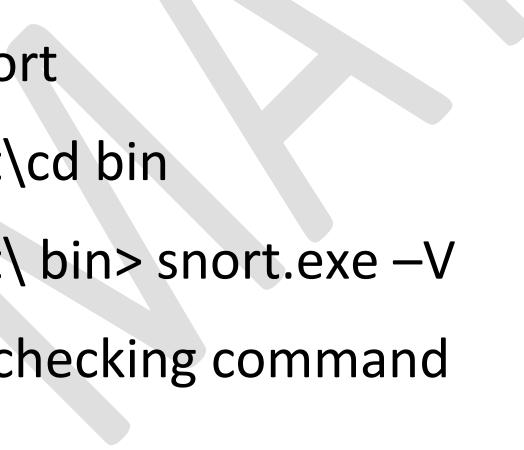


```
154 include $RULE_PATH\malware-cnc.rules
155 include $RULE_PATH\malware-other.rules
156 include $RULE_PATH\malware-tools.rules
157 include $RULE_PATH\misc.rules
158 include $RULE_PATH\multimedia.rules
159 include $RULE_PATH\mysql.rules
160 include $RULE_PATH\netbios.rules
161 include $RULE_PATH\ntp.rules
162 include $RULE_PATH\oracle.rules
163 include $RULE_PATH\os-linux.rules
164 include $RULE_PATH\os-other.rules
165 include $RULE_PATH\os-solaris.rules
166 include $RULE_PATH\os-windows.rules
167 include $RULE_PATH\other-ids.rules
168 include $RULE_PATH\pop3.rules
169 include $RULE_PATH\phishing-spam.rules
170 include $RULE_PATH\policy-multimedia.rules
171 include $RULE_PATH\policy-other.rules
172 include $RULE_PATH\policy.rules
173 include $RULE_PATH\policy-social.rules
174 include $RULE_PATH\policy-spam.rules
175 include $RULE_PATH\pop3.rules
176 include $RULE_PATH\pop3s.rules
177 include $RULE_PATH\protocol-finger.rules
178 include $RULE_PATH\protocol-ftp.rules
179 include $RULE_PATH\protocol-icmp.rules
180 include $RULE_PATH\protocol-icmp.rules
181 include $RULE_PATH\protocol-pop.rules
182 include $RULE_PATH\protocol-services.rules
183 include $RULE_PATH\protocol-voip.rules
184 include $RULE_PATH\pua-adware.rules
185 include $RULE_PATH\pua-other.rules
186 include $RULE_PATH\pua-jn.rules
```

Step12: change line/
546 to 651 change /



```
155 include $RULE_PATH\web-coldfusion.rules
156 include $RULE_PATH\web-frontpage.rules
157 include $RULE_PATH\web-iis.rules
158 include $RULE_PATH\web-misc.rules
159 include $RULE_PATH\web-php.rules
160 include $RULE_PATH\all.rules
161
162 #####
163 # Step #8: Customize your preprocessor and decoder alerts
164 # For more information, see README.decoder_preproc_rules
165 #####
166
167 # decoder and preprocessor event rules
168 include $PREPROC_RULE_PATH\preprocessor.rules
169 include $PREPROC_RULE_PATH\decoder.rules
170 include $PREPROC_RULE_PATH\sensitive-data.rules
171
172 #####
173 # Step #9: Customize your Shared Object Smack Rules
174 # For more information, see http://rtf-ing-smart.org/2008/01/using-vrt-certified-shared-object-rules.html
175 #####
176
177 # dynamic library rules
178 # include $SO_RULE_PATH\bad-traffic.rules
179 # include $SO_RULE_PATH\chat.rules
180 # include $SO_RULE_PATH\dot.rules
181 # include $SO_RULE_PATH\exploit.rules
182 # include $SO_RULE_PATH\icmp.rules
183 # include $SO_RULE_PATH\imap.rules
184 # include $SO_RULE_PATH\misc.rules
185 # include $SO_RULE_PATH\multimedia.rules
186 # include $SO_RULE_PATH\netbios.rules
187 # include $SO_RULE_PATH\nntp.rules
```



```
[... Command Prompt ...]
Microsoft Windows [Version 10.0.22631.5335]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>.
C:\Users\>cd ..
C:\>cd snort
C:\Snort>cd bin
C:\Snort\bin>snort.exe -V
--> Snort! <-
[... ]>- Version 2.9.20-WIN64-GRE (Build 82)
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 2019-06-25
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:\> Command Prompt
C:\>cd snort
C:\>Snort\bin
C:\>Snort\bin\snort.exe -V
--> Snort! <-
0""> Version 2.9.20-WTM64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.18 2018-06-25
Using ZLIB version: 1.2.11

C:\>Snort\bin\snort.exe -W
--> Snort! <-
Version 2.9.20-WTM64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.18 2018-06-25
Using ZLIB version: 1.2.11

Index Physical Address IP Address Device Name Description
1 00:00:00:00:00:00 disabled \Device\NPF_{0005A29D-C9EA-4898-BF0D-002B05703402} NPF Miniport (Network Monitor)
2 00:00:00:00:00:00 disabled \Device\NPF_{1004D4462-1CE7-4696-BB9C-23852922D9} NPF Miniport (IPv6)
3 00:00:00:00:00:00 disabled \Device\NPF_{BCCB1807-C67F-43A3-9F38-E339F9E90E82} NPF Miniport (IP)
4 00:02:3E:00:F1:62 192.168.235.138 \Device\NPF_{0078A882-CED2-4863-BF7C-D7C9EFDC3AD7} Intel(R) Wireless-AC 9568 160MHz
5 00:59:56:C0:00:00 192.168.101.1 \Device\NPF_{15C9MF516-5A00-4B7A-AEC0A1E138C0} VMware Virtual Ethernet Adapter for VMnet8
6 00:59:56:C0:00:01 192.168.125.1 \Device\NPF_{1A9A04C7-2EFA-4062-9099-054B39A9FB71} VMware Virtual Ethernet Adapter for VMnet1
7 0A:07:3E:00:F1:62 169.254.226.54 \Device\NPF_{1E88AC887-4F68-4E20-B294-CC2E3FA62441} Microsoft Wi-Fi Direct Virtual Adapter #2
8 00:D2:3E:00:F1:63 169.254.183.248 \Device\NPF_{1E98B153C-6726-4F63-BB08-76AA2C4306E7} Microsoft Wi-Fi Direct Virtual Adapter
9 0A:00:27:00:00:00 192.168.56.1 \Device\NPF_{1E93B098-2586-4E7c-AE1D-877C0B88869B} 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:50:00:C0:26 169.254.32.216 \Device\NPF_{1E956C02E-C167-0F21-B49B-6C8C07715264} HotspotShield TAP-Windows Adapter V9
12 00:59:C2:37:82:B8 169.254.136.37 \Device\NPF_{12A7A883C-1030-4656-80D9-9B880F0326F} Intel(R) Ethernet Connection (6) I219-LM

C:\>Snort\bin\snort

```

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

Interface checking command

```

C:\> Command Prompt
C:\> Windows PowerShell
C:\> 2 byte states : 19.86
C:\> 4 byte states : 137.47
[ Number of patterns truncated to 20 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_{0078A882-CED2-4863-BF7C-D7C9EFDC3AD7}".

--> Initialization Complete <-
--> Snort! <-
0""> Version 2.9.20-WTM64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.18 2018-06-25
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE, Version 3.2 <Build 1>
Preprocessor Object: SF_SQLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 7>
Preprocessor Object: SF_SMB Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDP 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 1.1 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET 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_DCERPC2 Version 1.0 <Build 3>

Total snort Fixed Memory Cost = MaxRas:548352072
Snort successfully validated the configuration!
Snort exiting.

C:\>Snort\bin\snort

```

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

This command testing snort configurtaiion

```
Command Prompt      Windows Reserved      - + X
--tsval-drop-as-alert          Converts drop, adrop, and reject rules into alert rules during startup.
--tsval-drop-as-ignore         Use drop, adrop, 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 detection 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 <tf>             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 -x.
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 (ip4v, ip6v, ethernet) that is encapsulated by MPLS
--require-rule-sid            Require that all smart rules have SID specified
--daq <type>                 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.
--suppress-config-log         Suppress configuration information output.

C:\Snort\bin>
```

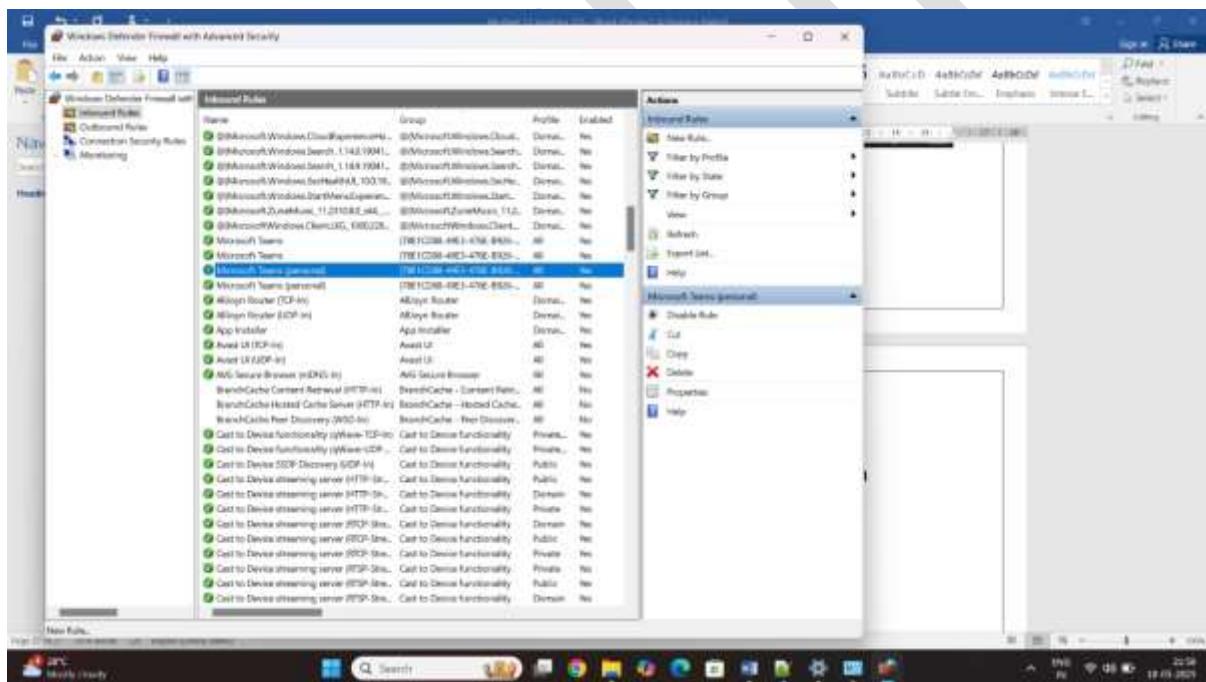
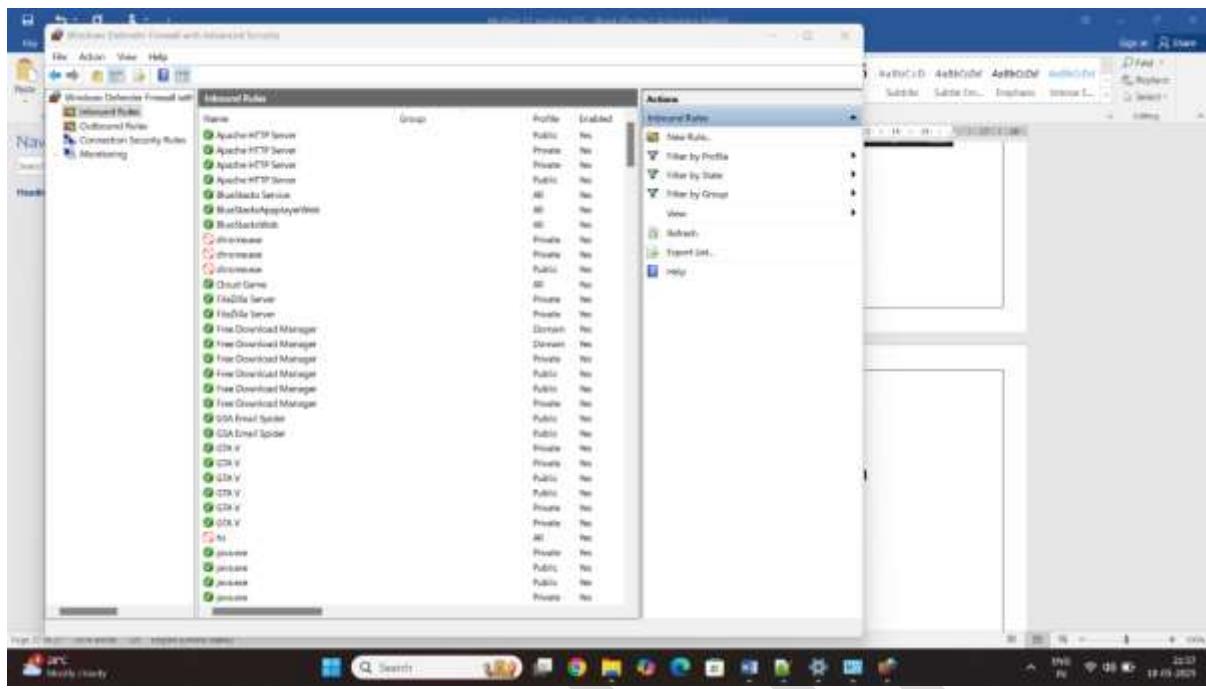
C:\ snort\ bin> snort | 5 –c c:\snort\etc\snort\conf
–W

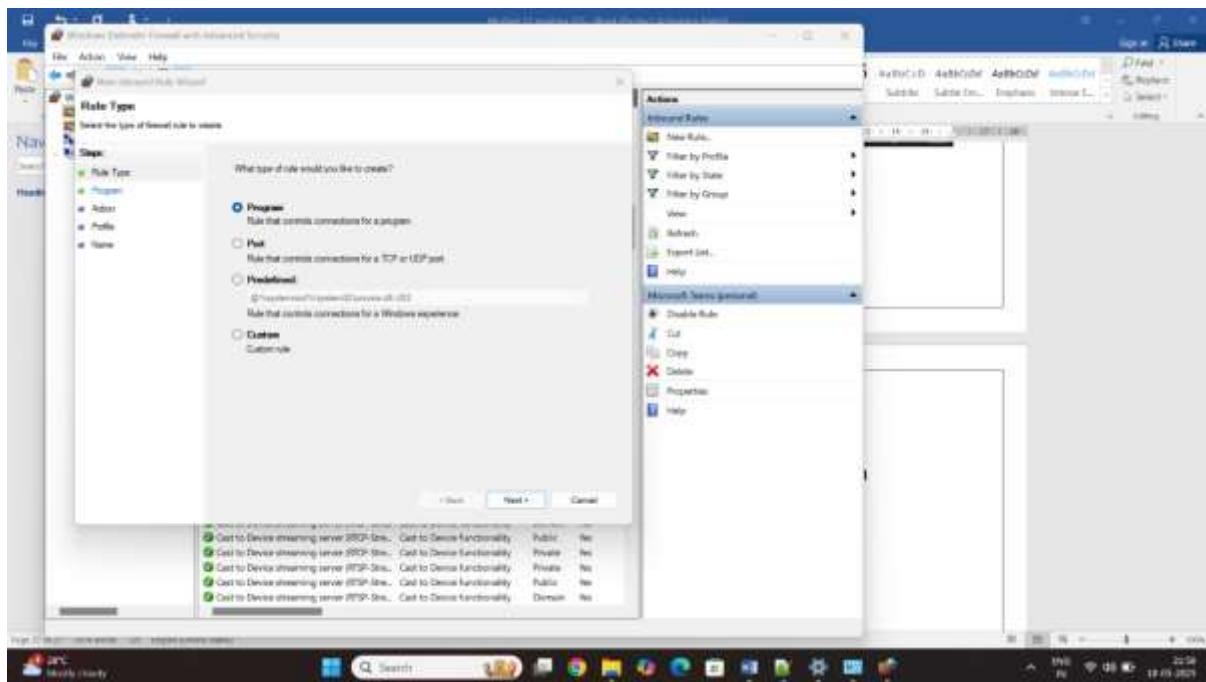
This command are monitoring mode use

How to windows firewall configuration in bound traffic rule

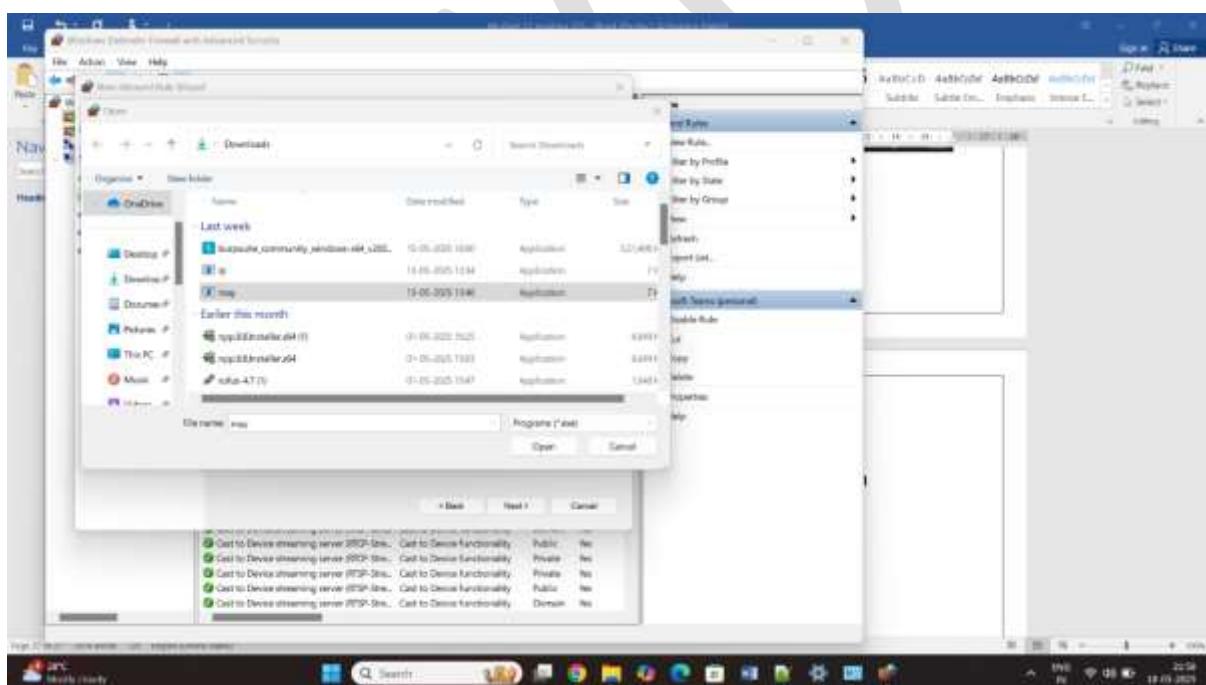
Step1: go to setting and select the option windows defender

Step2 choice the option inbound

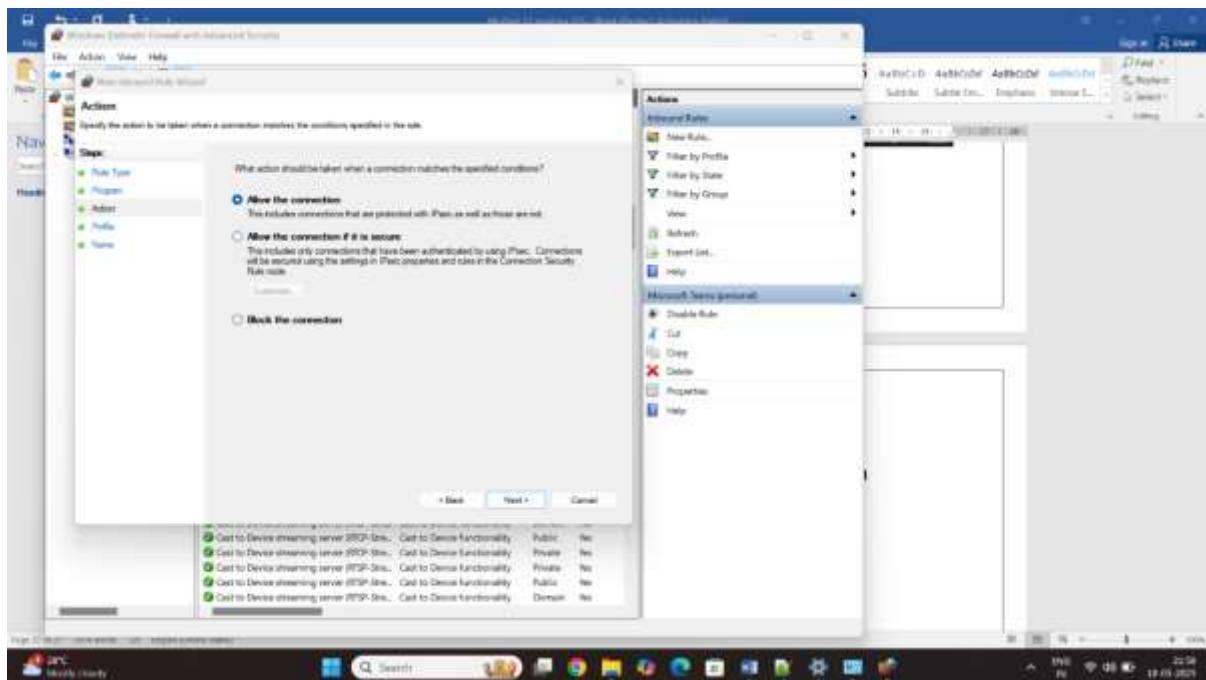




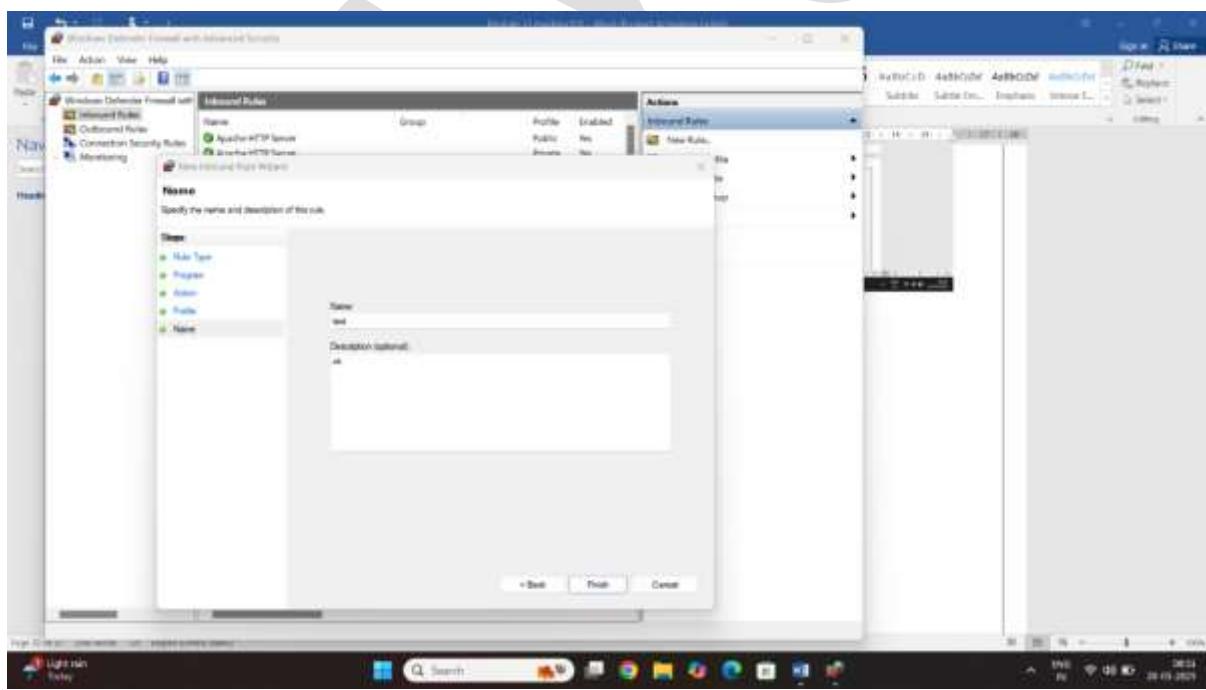
Step3:select the program option



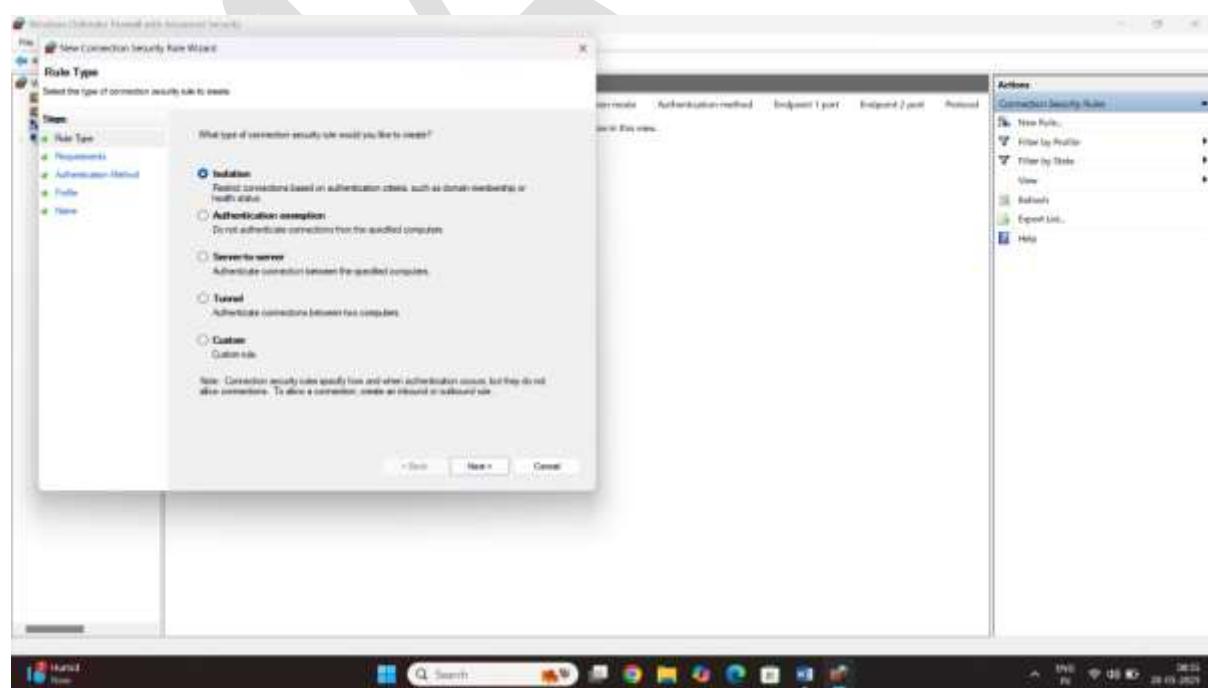
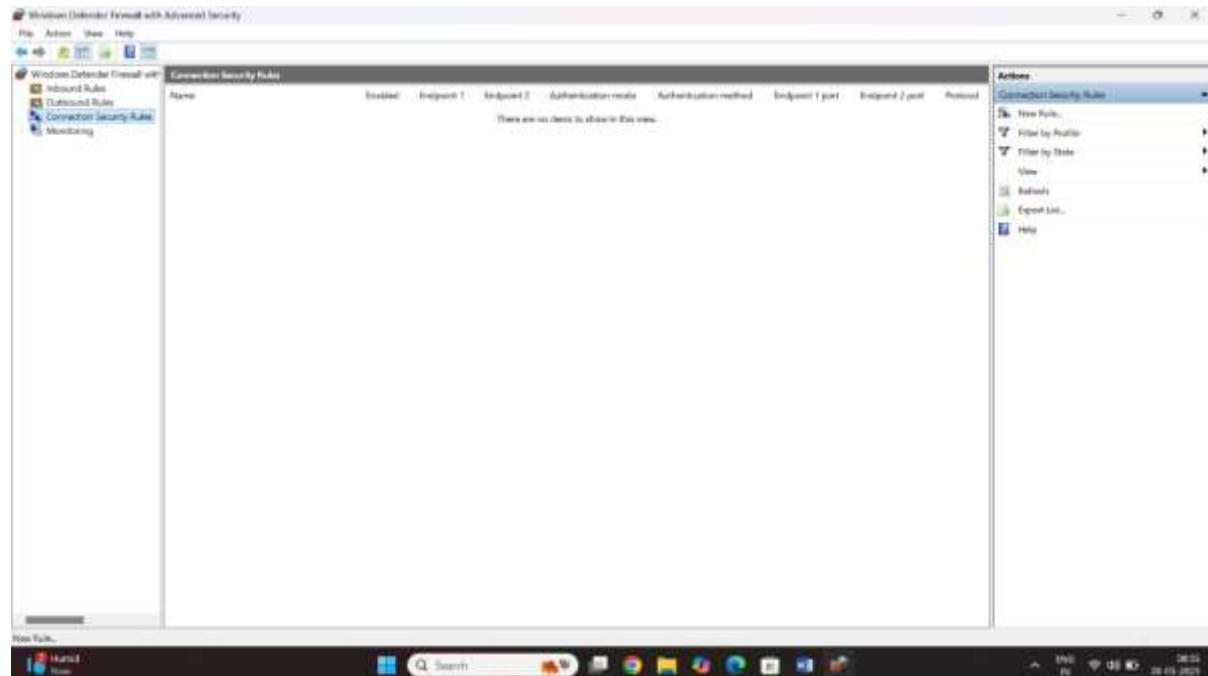
Step4: click on browser choice the block activity

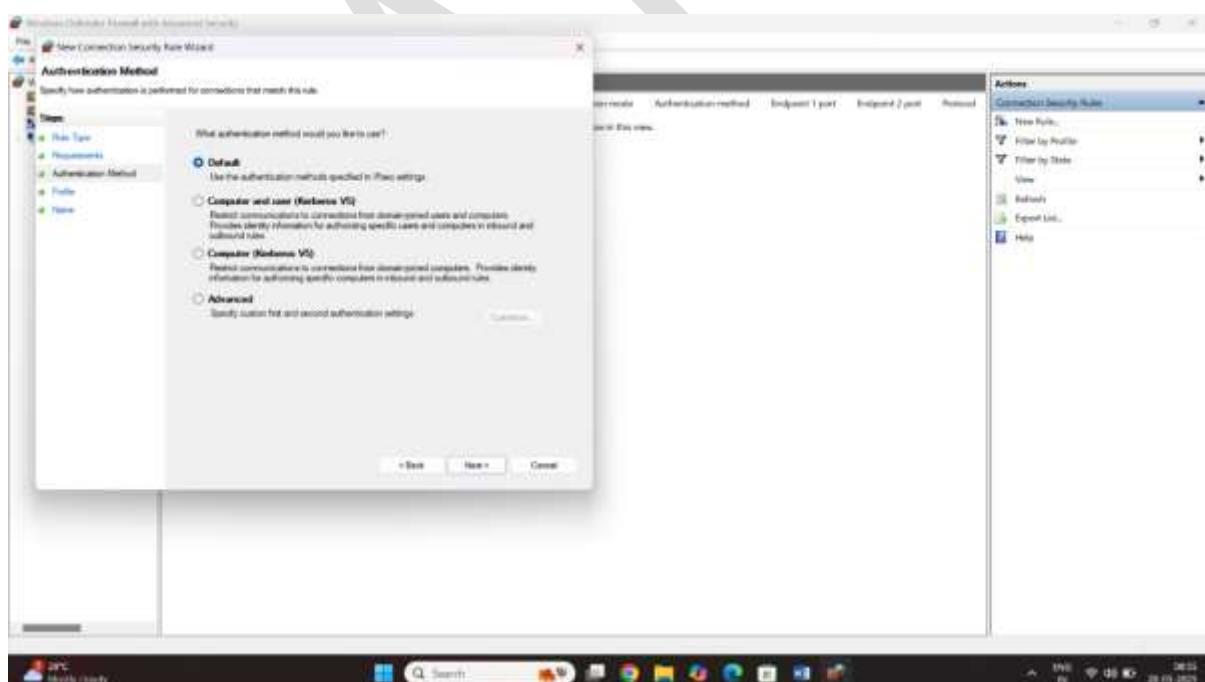
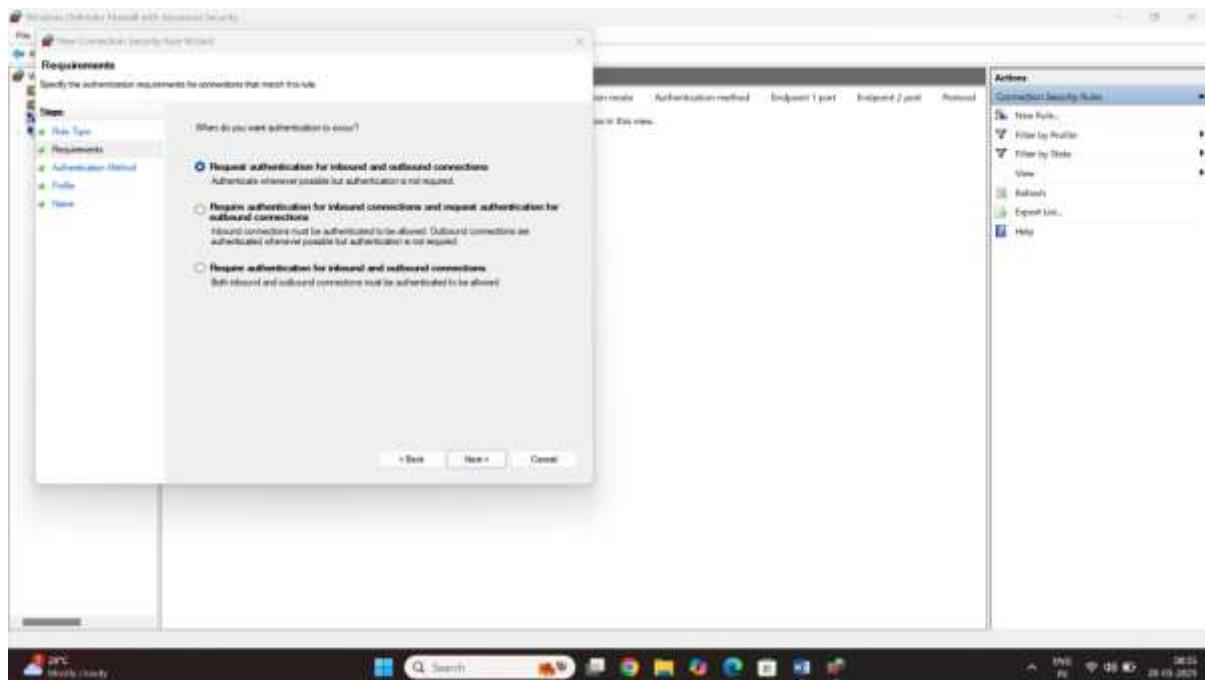


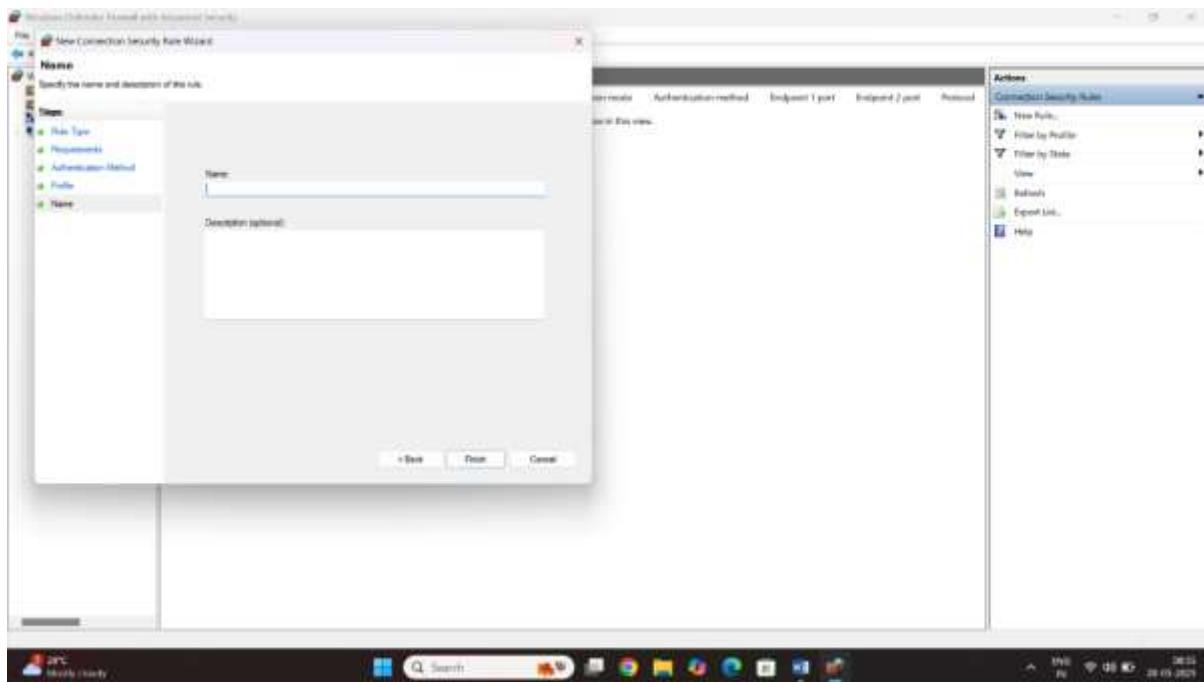
Step5: select the option all



Connection security rules



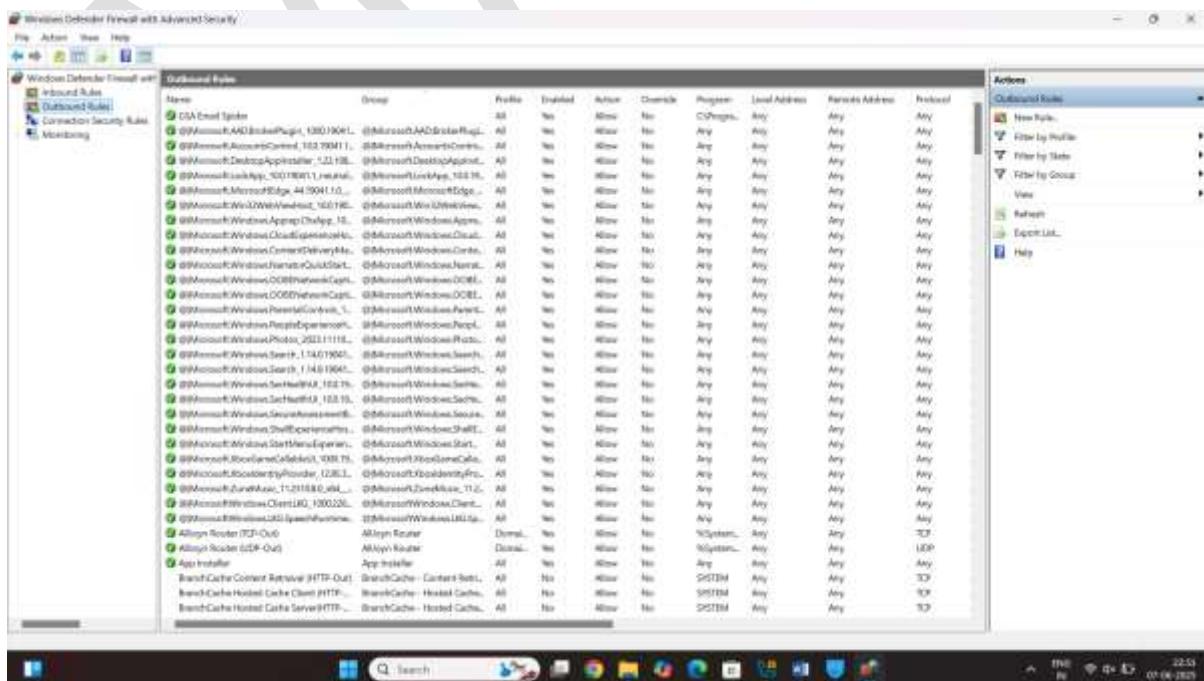


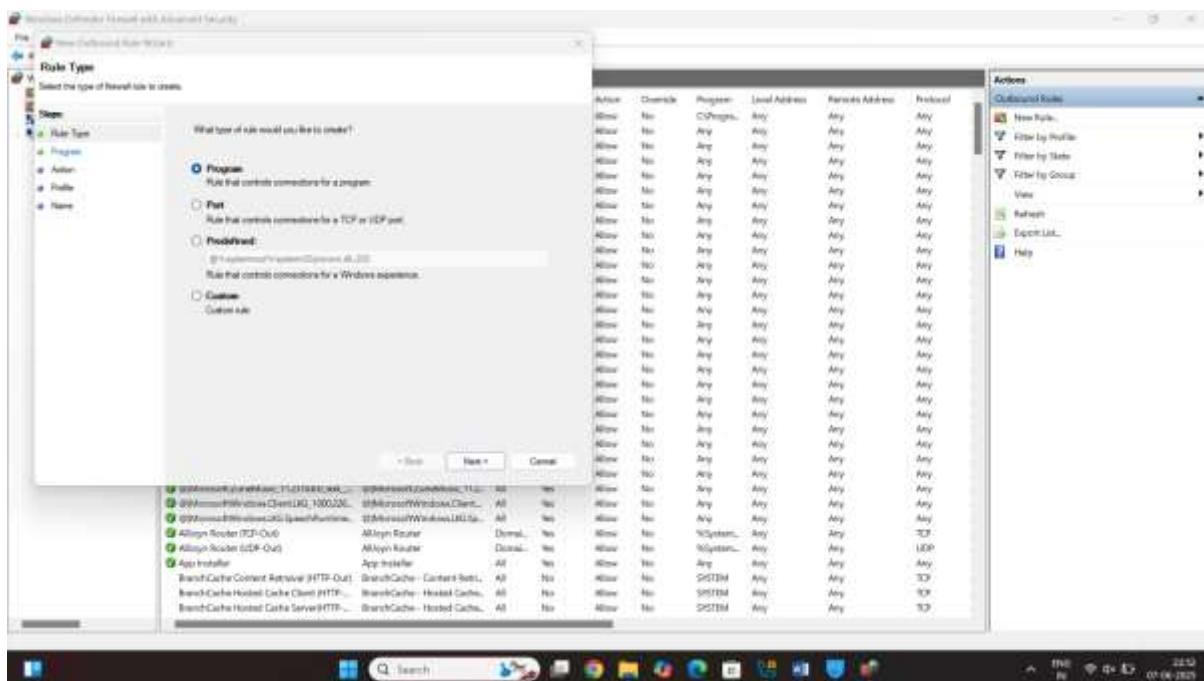


How to windows firewall configuration outbound traffic rule

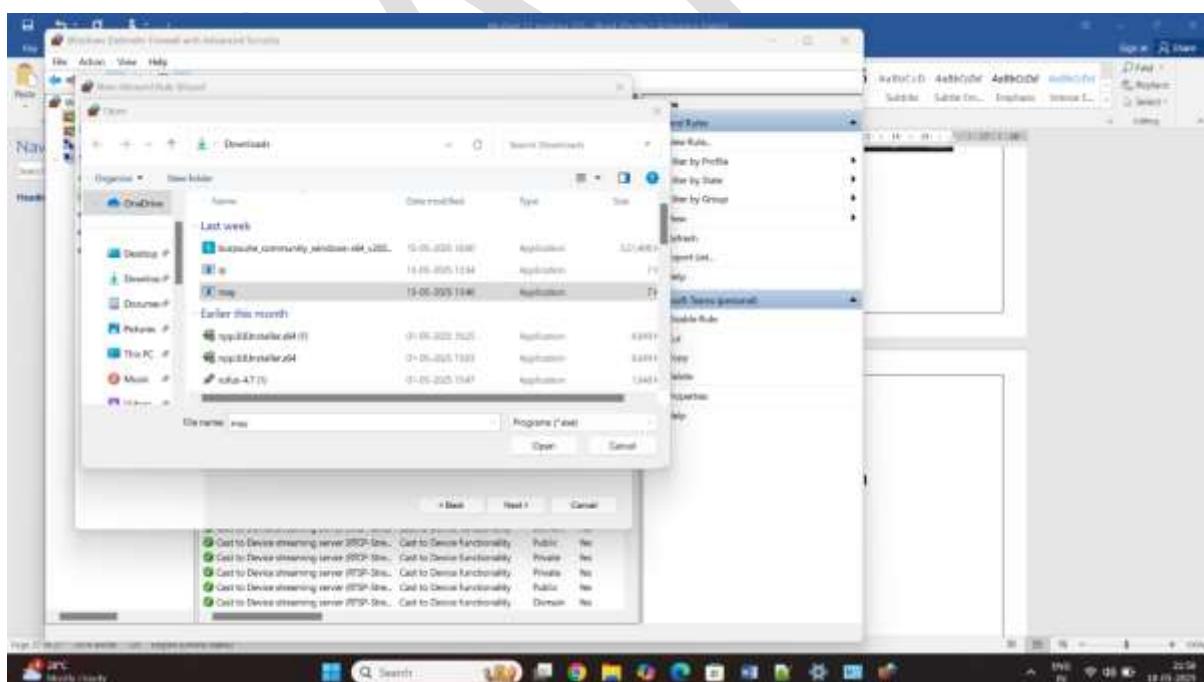
Step1: go to setting and select the option windows defender

Step2 choice the option oubound

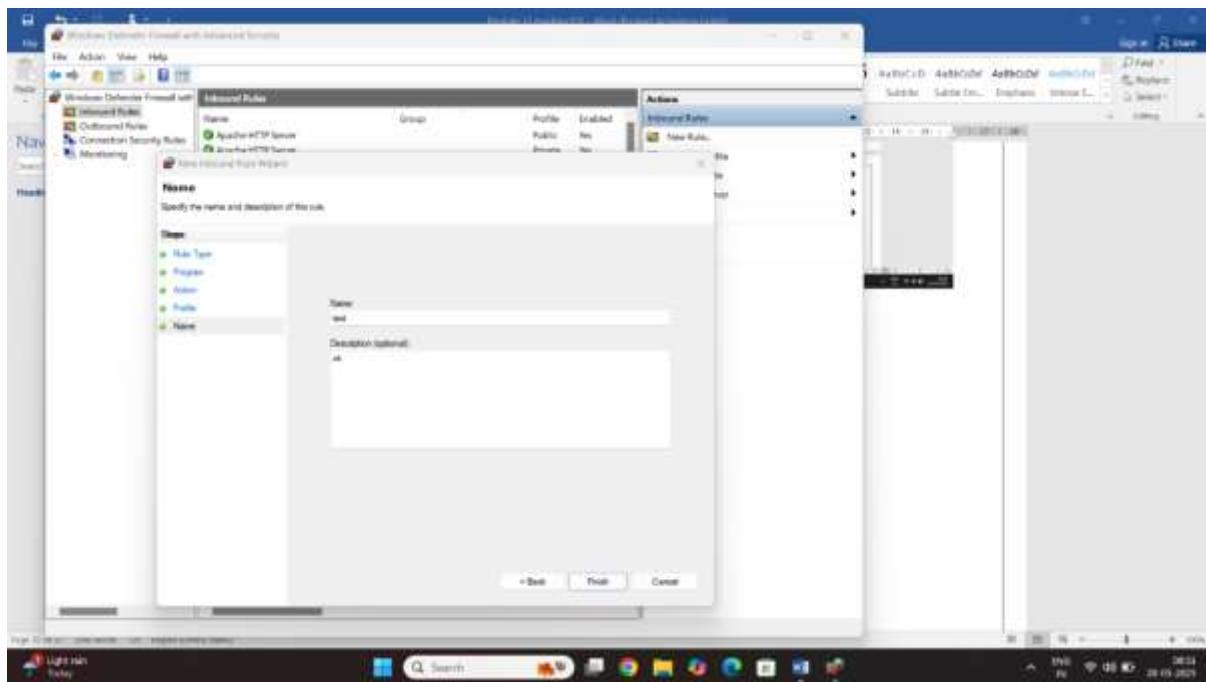




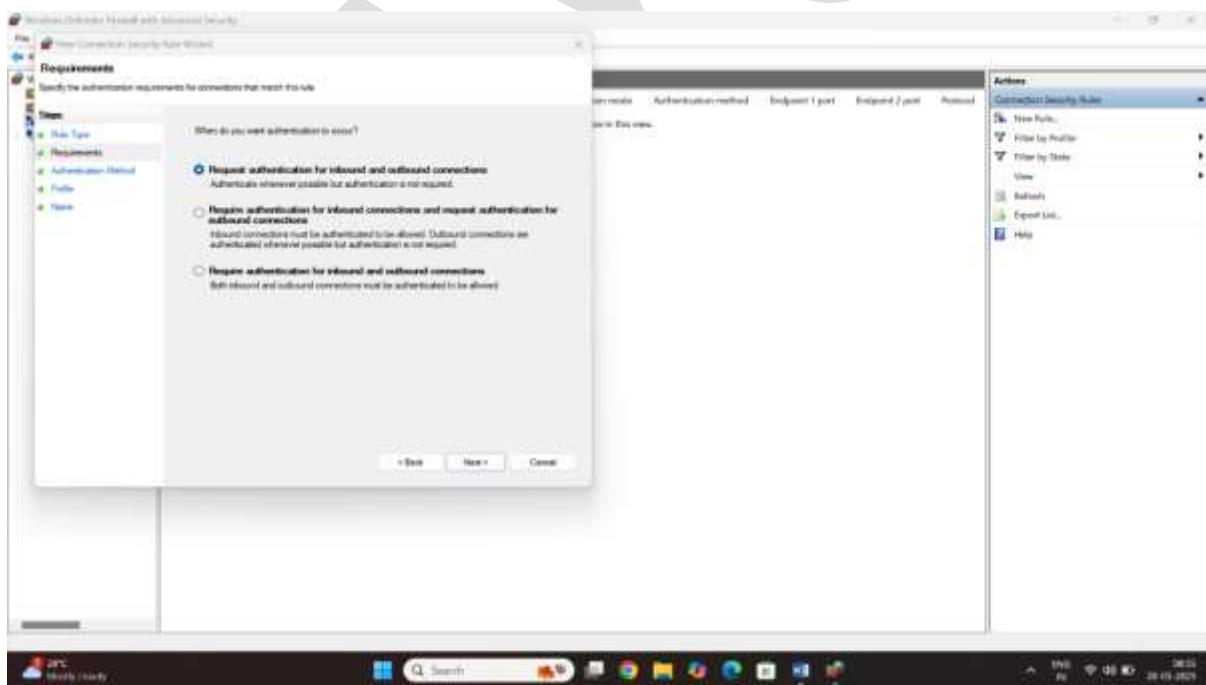
Step3:select the program option



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.

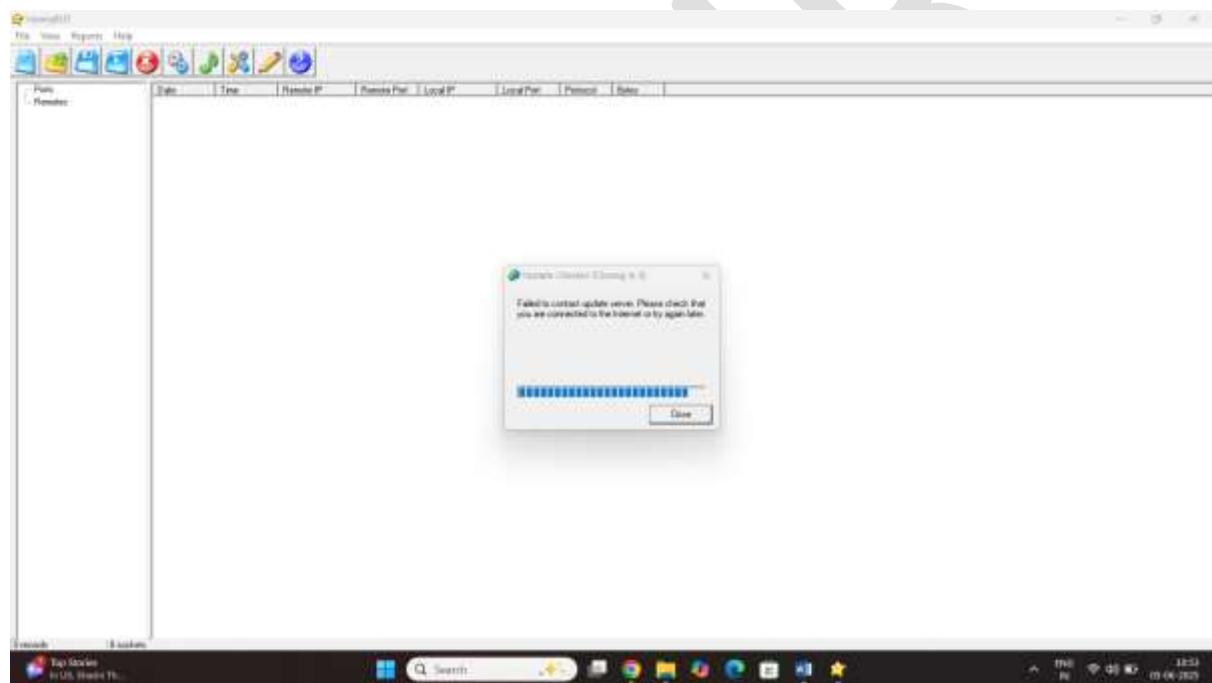
- **Examples:**

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

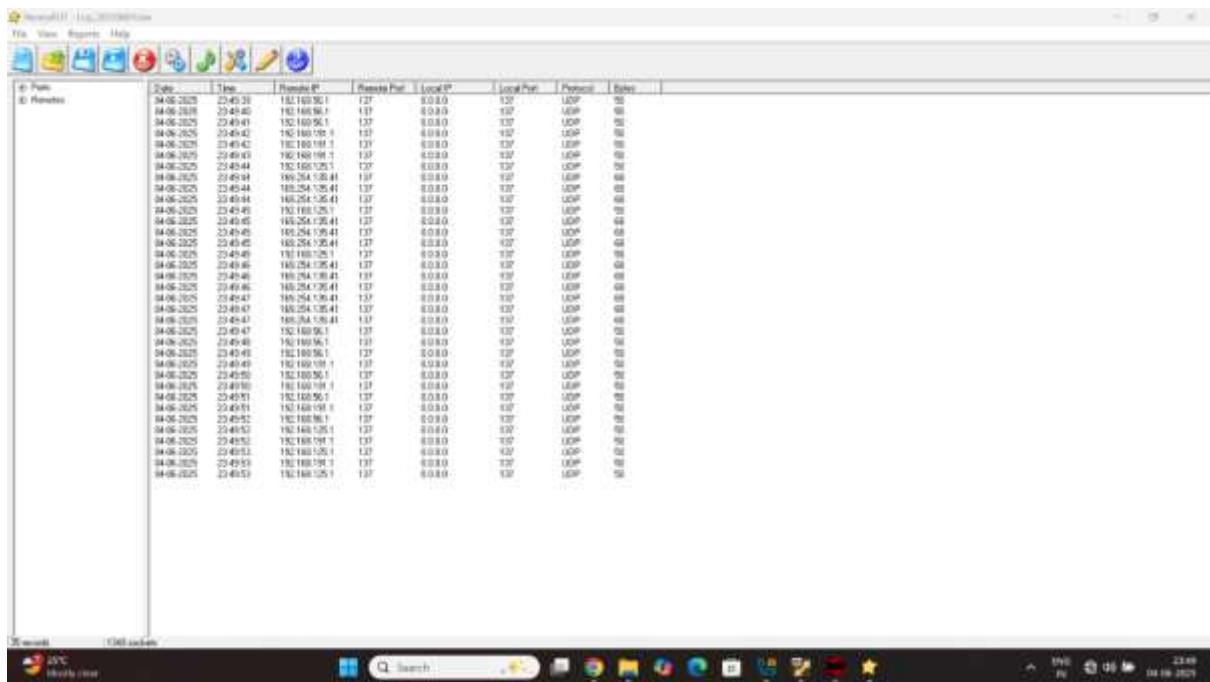
Security guards detection honeypot

Honeypot: is detection m

Step1: start the honeybot application



Click on all monetring option



Extra activity using zone alarm firewall how to configrtation

❓ What Is ZoneAlarm Firewall?

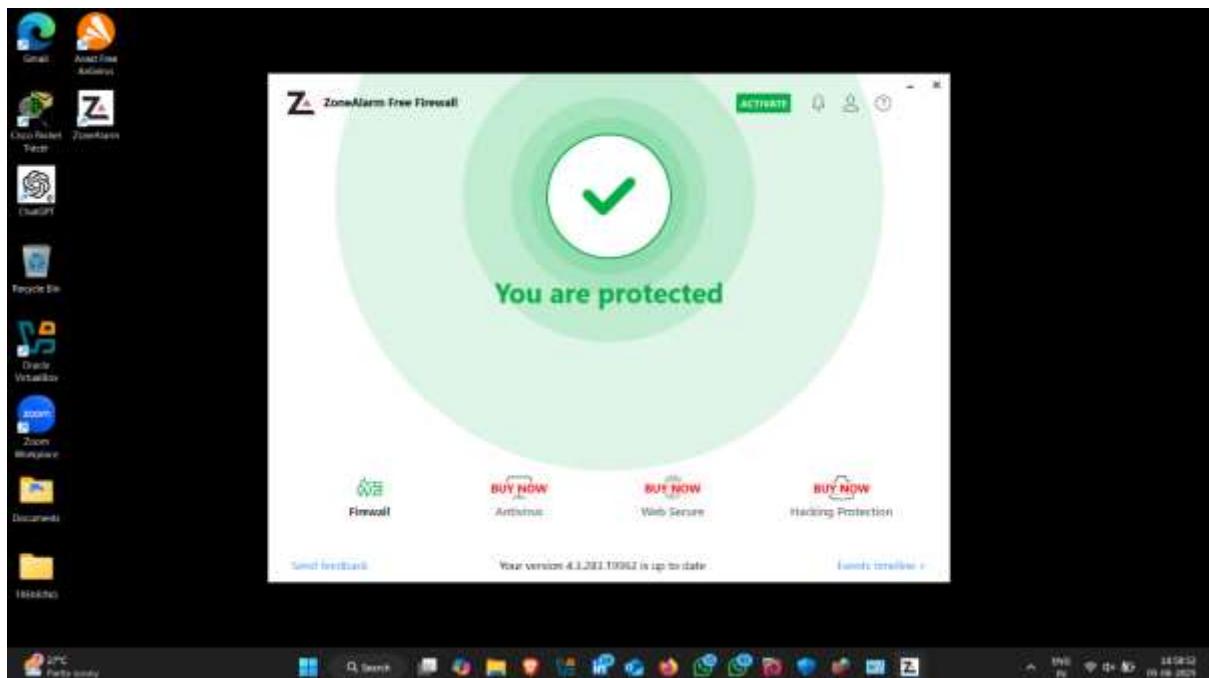
ZoneAlarm Firewall acts as a barrier between your computer and the internet, monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. It helps prevent unauthorized access to your computer and protects your data from malicious software.

⌚ Key Features

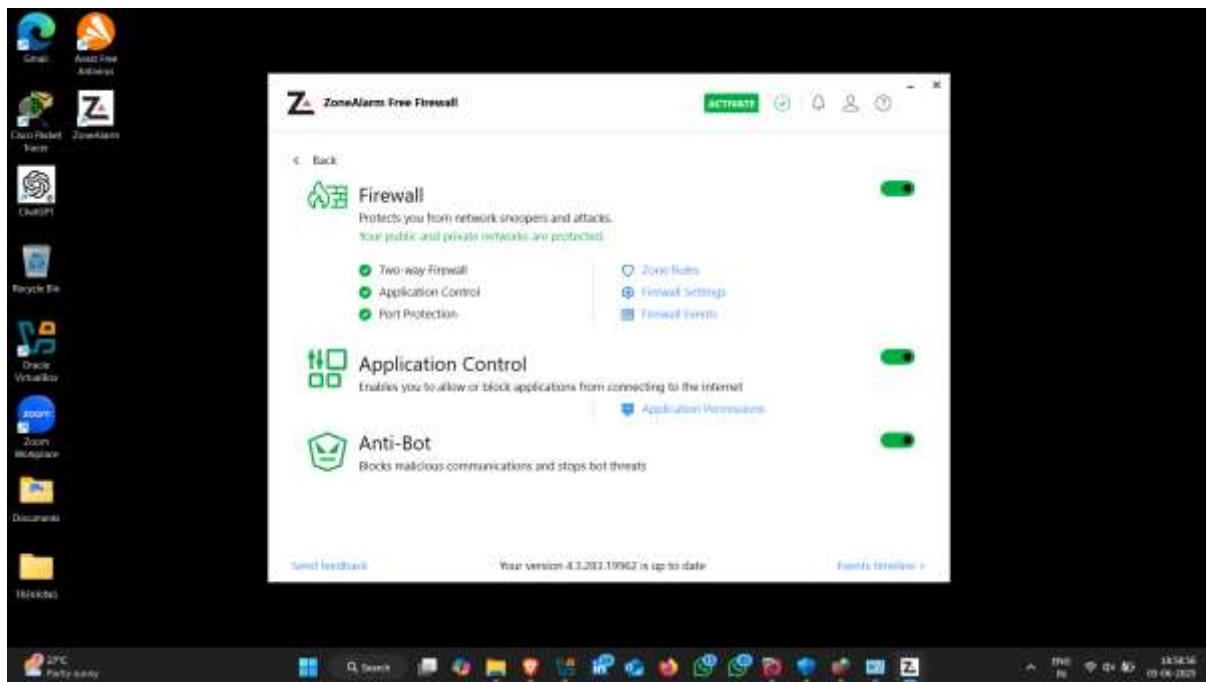
- **Two-Way Firewall Protection:** Monitors both inbound and outbound traffic, blocking unauthorized access and preventing malware from sending your data out.
- **Advanced Security Zones:** Defines three security zones—Trusted, Public, and Blocked—to apply appropriate security levels based on network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

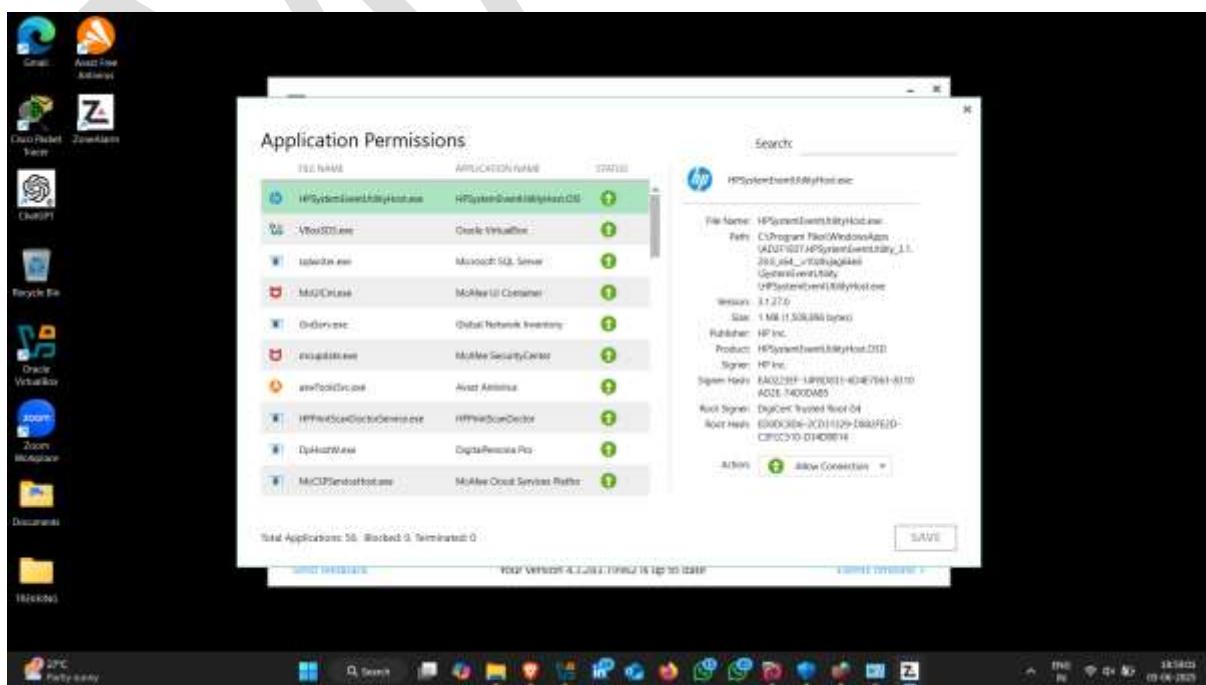
Configuration Zone alarm



Step1: click on zone alarm and start here

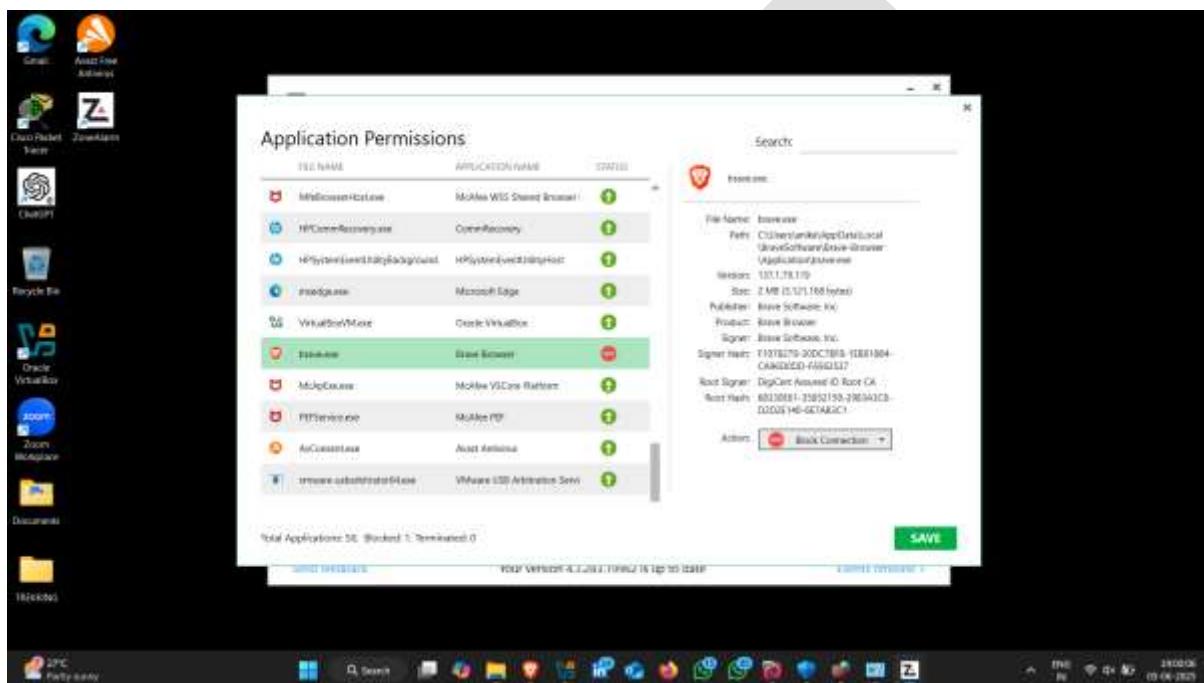


Step2 : select the all option allow permission

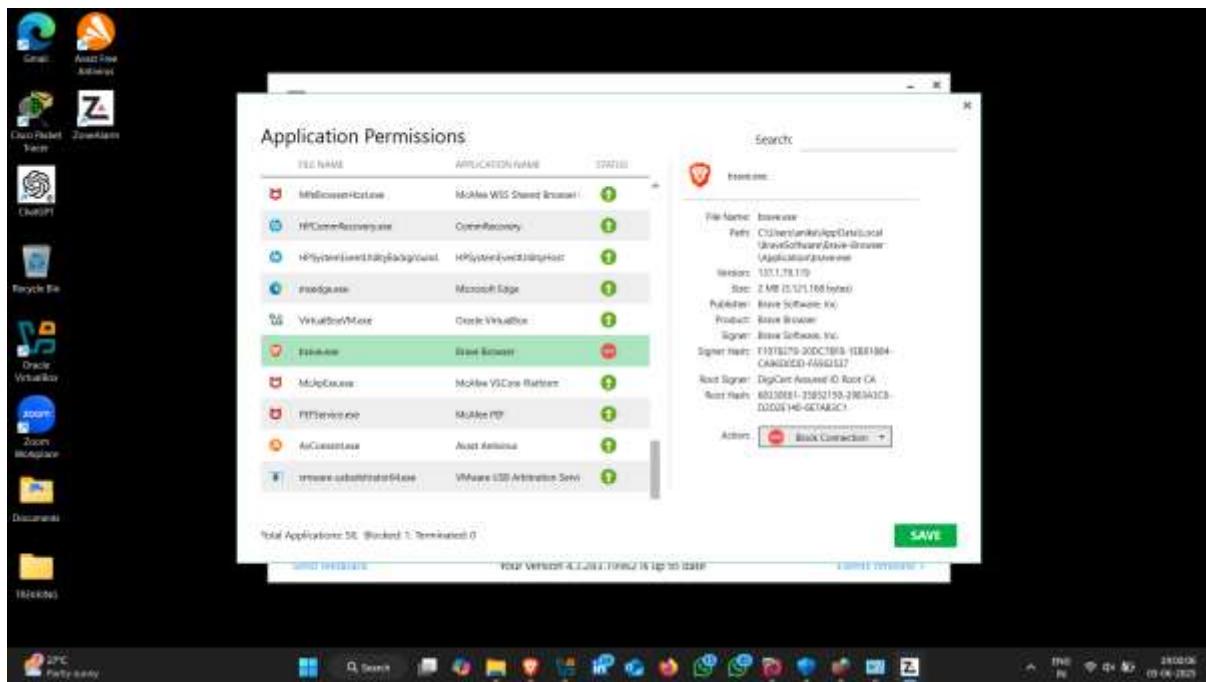


Step3 select application permission

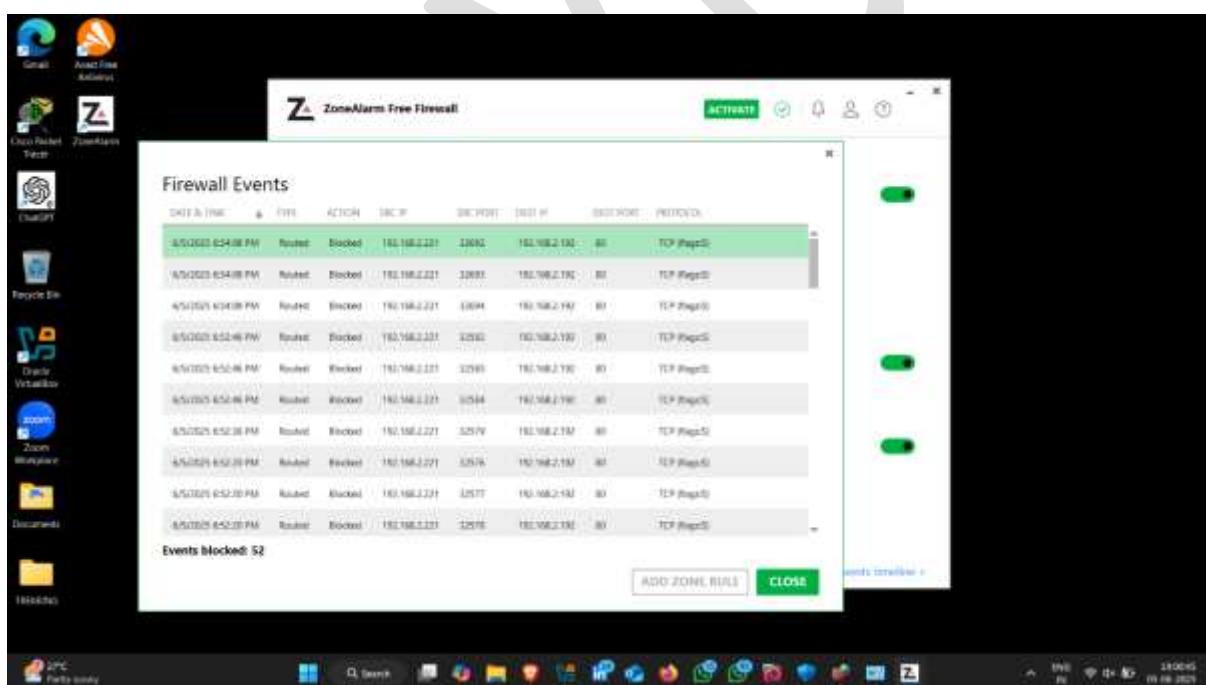
With set of rule



Step 4 I am choice the brave browser permission



Step5 Clicik on save and next



Step6 Complete the zone alarm configuration

MAYUR