Name: Tehreem Amna

Internship Title: SOC Intern - Team PI

Task Title: Firewall Monitoring with Wazuh

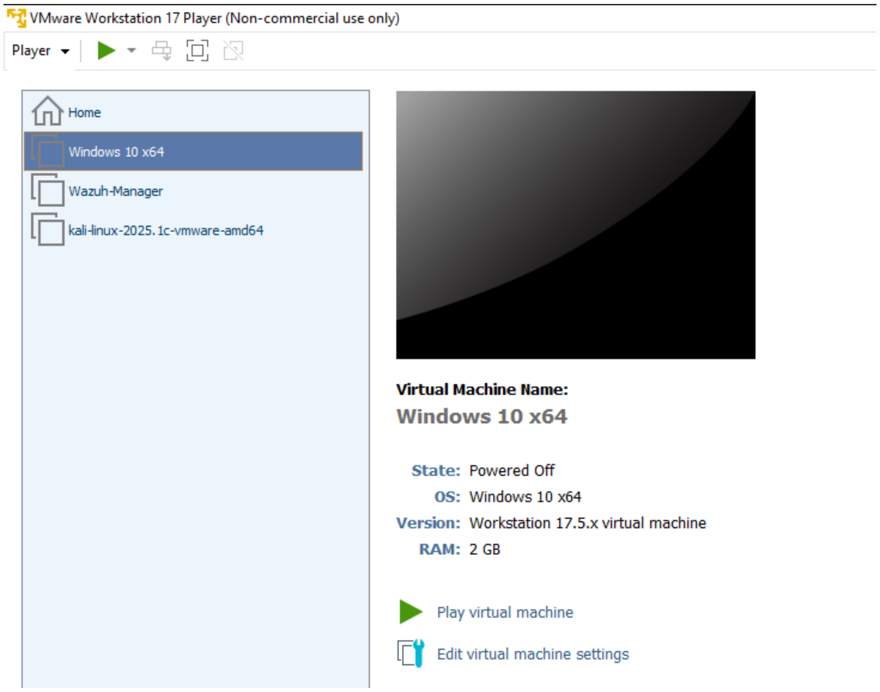
Date: 15 August 2025

Task Objective:

The goal of this lab was to create a safe, isolated network where a Windows 10 VM acts as both a firewall and Wazuh agent, and a Wazuh Manager VM collects and analyzes its logs. We also wanted to test site blocking, firewall logging, and policy monitoring.

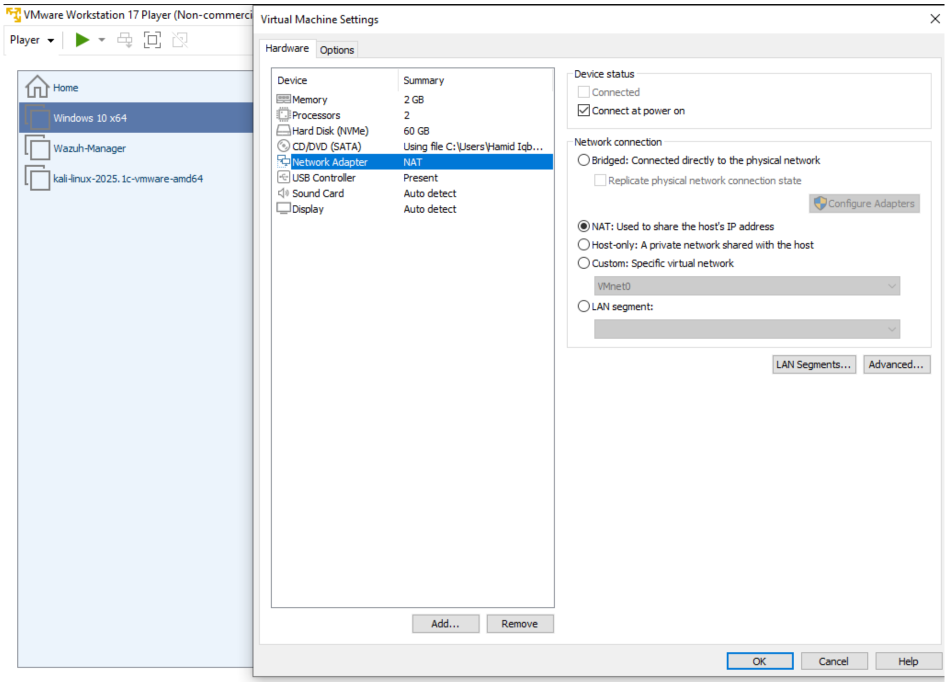
Step 1: Set up VMware Networks

VMware can create virtual adapters even if we have only one physical Ethernet.


VMware Workstation 17 Player (Non-commercial use only)
Player
Home
Windows 10 x64
Wazuh-Manager
kali-linux-2025.1c-vmware-amd64
Play virtual machine
Edit virtual machine settings

Virtual Machine Name:
Windows 10 x64

State: Powered Off
OS: Windows 10 x64
Version: Workstation 17.5.x virtual machine
RAM: 2 GB



VMware Workstation 17 Player (Non-commerci

Virtual Machine Settings

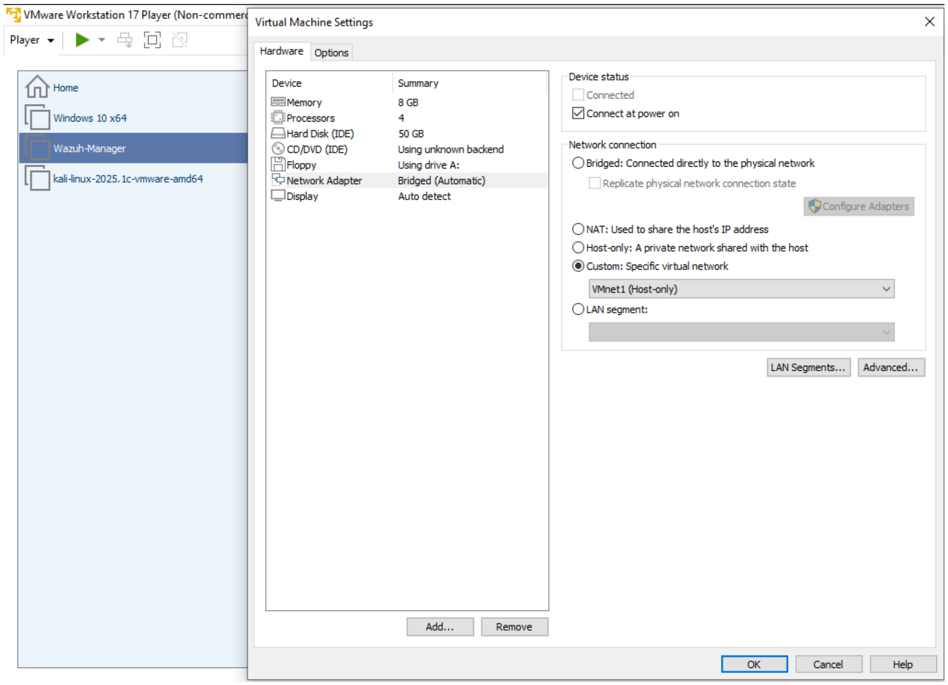
Device	Summary
Memory	2 GB
Processors	2
Hard Disk (NVMe)	60 GB
CD/DVD (SATA)	Using file C:\Users\Hamid Iqb...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

□ Connected
☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
● NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
○ Custom: Specific virtual network
VMnet0
○ LAN segment:



VMware Workstation 17 Player (Non-commerc

Virtual Machine Settings

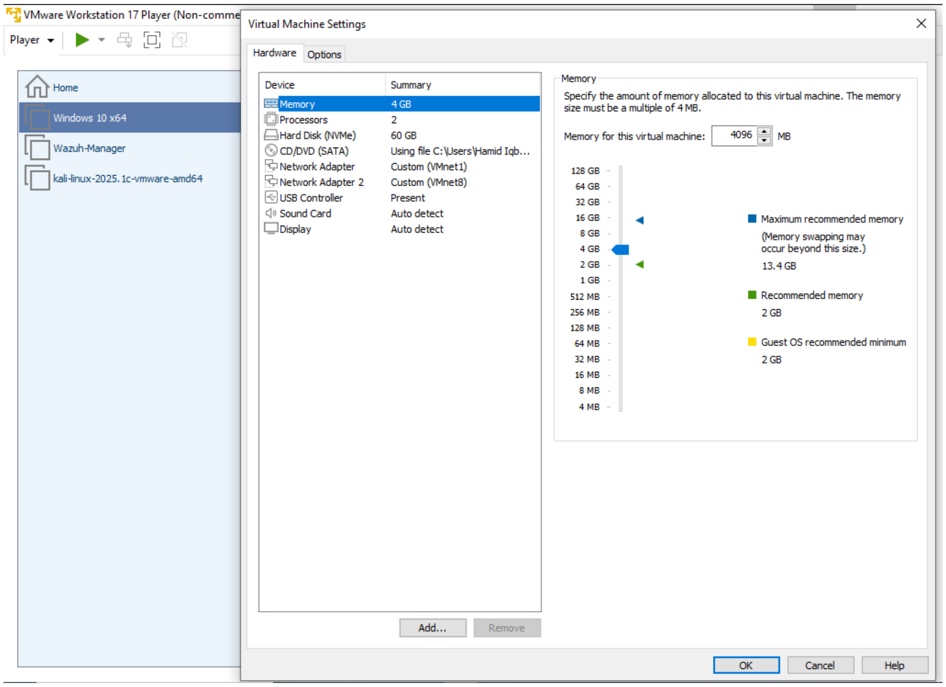
Device	Summary
Memory	8 GB
Processors	4
Hard Disk (IDE)	50 GB
CD/DVD (IDE)	Using unknown backend
Floppy	Using drive A:
Network Adapter	Bridged (Automatic)
Display	Auto detect

Device status

□ Connected
☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network
□ Replicate physical network connection state
○ NAT: Used to share the host's IP address
○ Host-only: A private network shared with the host
● Custom: Specific virtual network
VMnet1 (Host-only)
○ LAN segment:



Device	Summary
Memory	4 GB
Processors	2
Hard Disk (NVMe)	60 GB
CD/DVD (SATA)	Using file C:\Users\Hamid Iqb...
Network Adapter	Custom (VMnet1)
Network Adapter 2	Custom (VMnet8)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: 4096 MB

🟦 Maximum recommended memory
(Memory swapping may occur beyond this size.)
13.4 GB

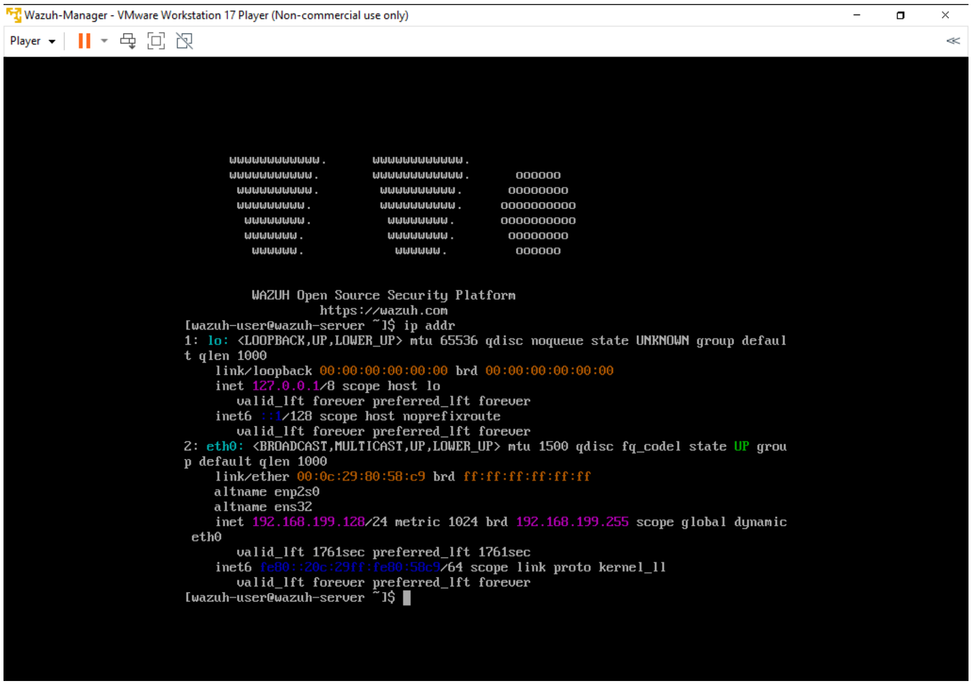
🟩 Recommended memory
2 GB

🟨 Guest OS recommended minimum
2 GB

Step 2: Checking Network

Wazuh Manager VM:

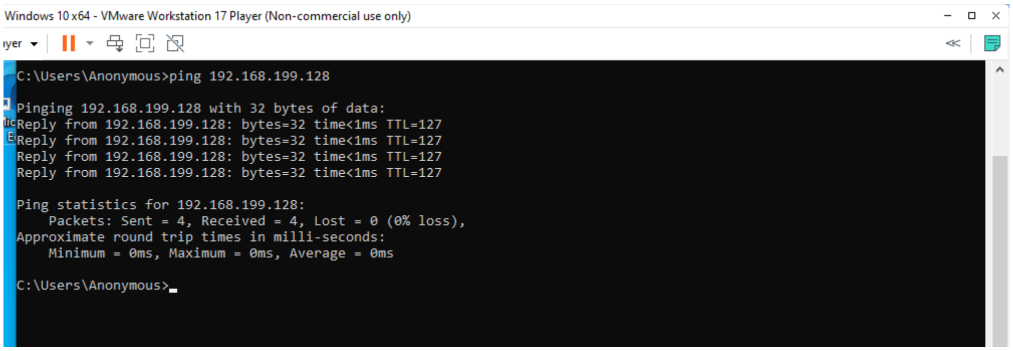
Checking IP on Host-Only network:


Wazuh-Manager - VMware Workstation 17 Player (Non-commercial use only)
Player

```
      wwwwwwwwwwww.      wwwwwwwwwwww.
      wwwwwwwwwww.       wwwwwwwwwwww.      oooooo
       wwwwwwwwww.        wwwwwwwwww.      oooooooo
       wwwwwwwww.         wwwwwwwwww.     oooooooooo
        wwwwwwww.          wwwwwwww.      oooooooooo
        wwwwwww.           wwwwwwww.       oooooooo
         wwwwww.            wwwwww.         oooooo


         WAZUH Open Source Security Platform
                  https://wazuh.com
[wazuh-user@wazuh-server ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether 00:0c:29:80:58:c9 brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    altname ens32
    inet 192.168.199.128/24 metric 1024 brd 192.168.199.255 scope global dynamic
 eth0
       valid_lft 1761sec preferred_lft 1761sec
    inet6 fe80::20c:29ff:fe80:58c9/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[wazuh-user@wazuh-server ~]$
```

Windows 10 VM:

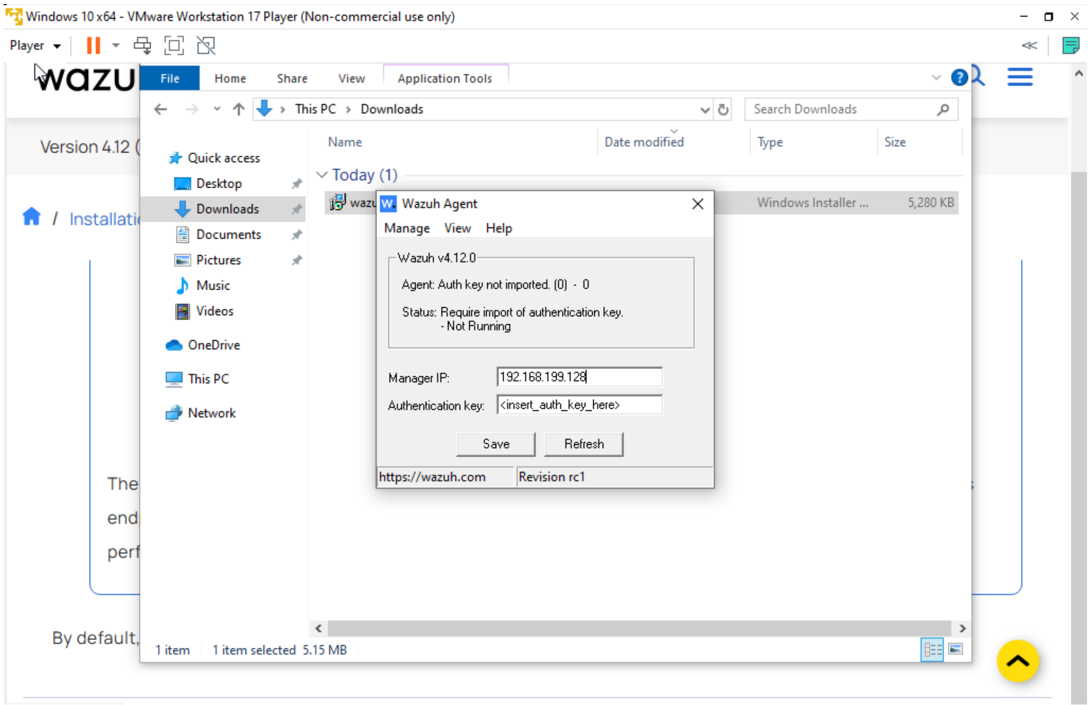
Testing connection to Wazuh Manager:



Windows 10 x64 - VMware Workstation 17 Player (Non-commercial use only)

```
C:\Users\Anonymous>ping 192.168.199.128

Pinging 192.168.199.128 with 32 bytes of data:
Reply from 192.168.199.128: bytes=32 time<1ms TTL=127
Reply from 192.168.199.128: bytes=32 time<1ms TTL=127
Reply from 192.168.199.128: bytes=32 time<1ms TTL=127
Reply from 192.168.199.128: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.199.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Anonymous>_
```

Step 3: Installed Wazuh Agent on Windows 10 VM



Wazuh Agent

Wazuh v4.12.0

Agent: Auth key not imported. (0) - 0

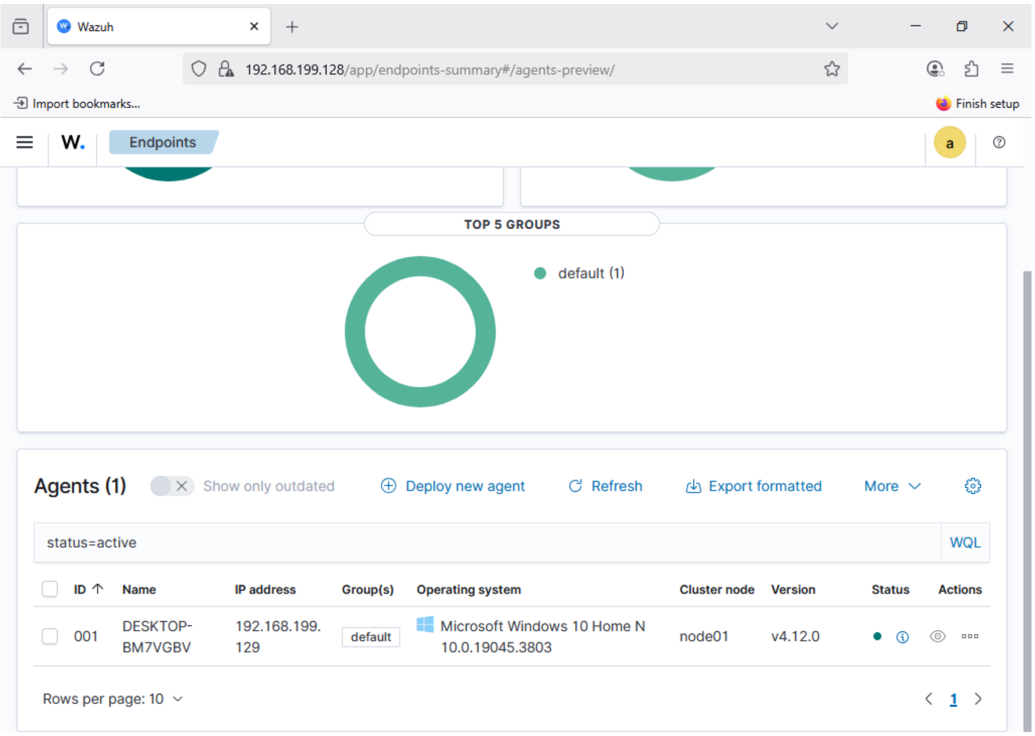
Status: Require import of authentication key.
- Not Running

Manager IP: 192.168.199.128

Authentication key: <insert_auth_key_here>

https://wazuh.com | Revision rc1

Step 4: Enabled Agent in Wazuh Dashboard

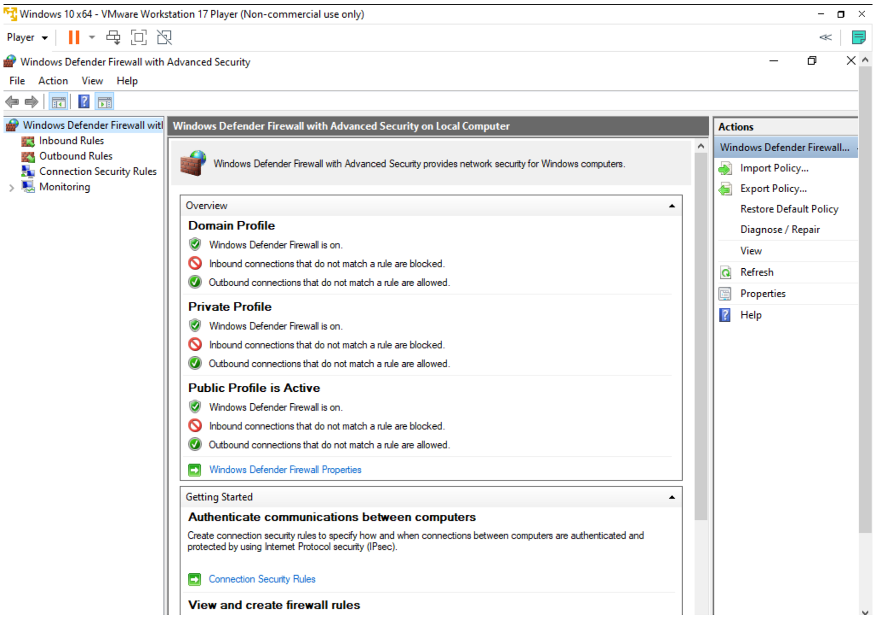


status=active

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	DESKTOP-BM7VGBV	192.168.199.129	default	Microsoft Windows 10 Home N 10.0.19045.3803	node01	v4.12.0	●	

Step 5: Configuring the Task Rules

A. Enabled Windows Firewall Logging


Windows 10 x64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Overview
Getting Started
Actions
Windows Defender Firewall...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

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

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

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

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

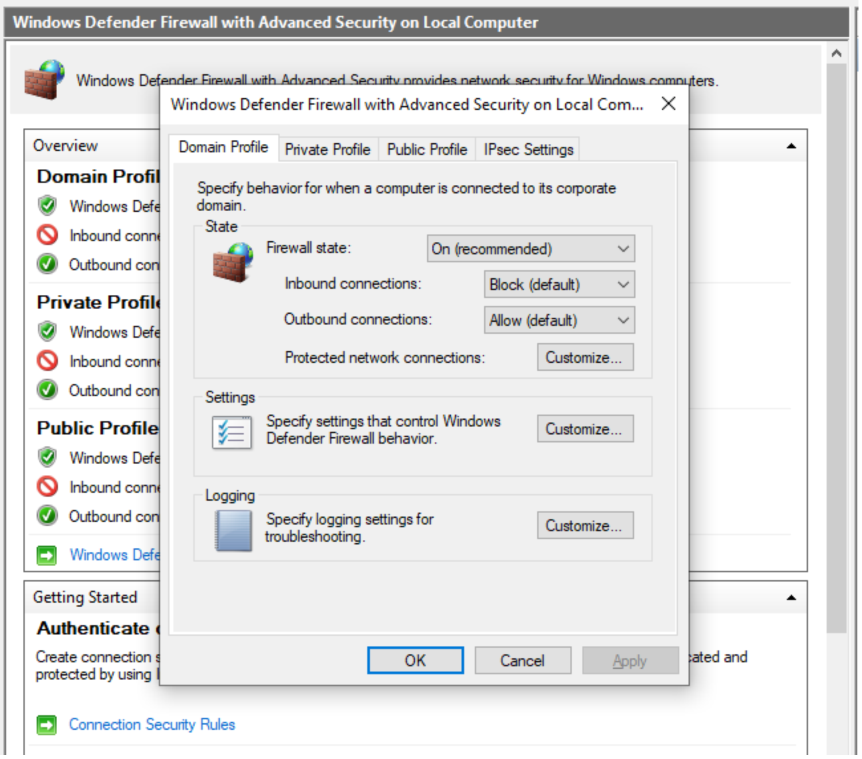
Windows Defender Firewall Properties

Authenticate communications between computers

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

Connection Security Rules

View and create firewall rules



Windows Defender Firewall with Advanced Security on Local Computer

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

Windows Defender Firewall with Advanced Security on Local Com...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

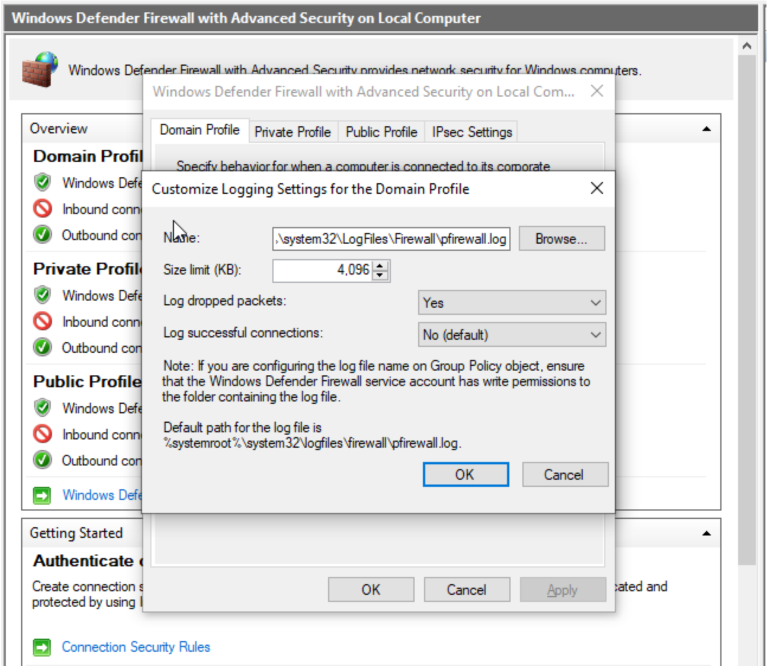
Protected network connections: Customize...

Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...



Windows Defender Firewall with Advanced Security on Local Computer

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

Windows Defender Firewall with Advanced Security on Local Com...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate

Customize Logging Settings for the Domain Profile

Name: .\system32\LogFiles\Firewall\pfirewall.log Browse...

Size limit (KB): 4,096

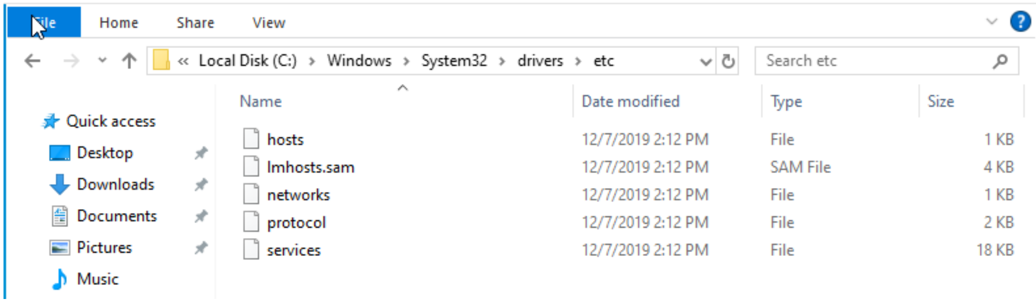
Log dropped packets: Yes

Log successful connections: No (default)

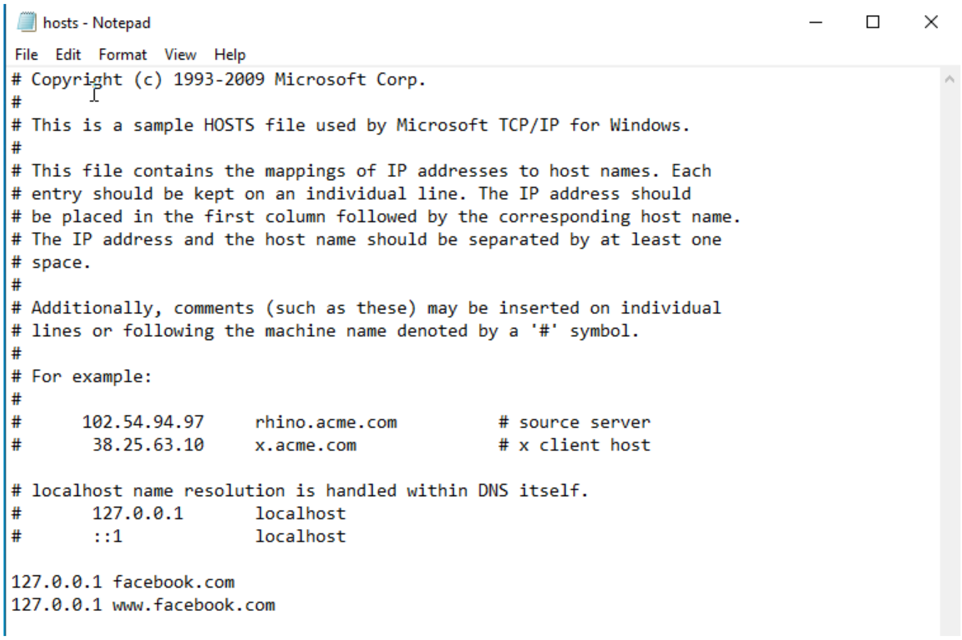
Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Defender Firewall service account has write permissions to the folder containing the log file.

Default path for the log file is %systemroot%\system32\logfiles\firewall\pfirewall.log.

B. Blocked Websites



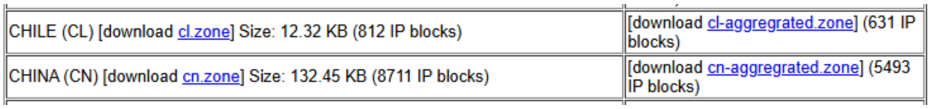
Name	Date modified	Type	Size
hosts	12/7/2019 2:12 PM	File	1 KB
lmhosts.sam	12/7/2019 2:12 PM	SAM File	4 KB
networks	12/7/2019 2:12 PM	File	1 KB
protocol	12/7/2019 2:12 PM	File	2 KB
services	12/7/2019 2:12 PM	File	18 KB



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

127.0.0.1 facebook.com
127.0.0.1 www.facebook.com
```

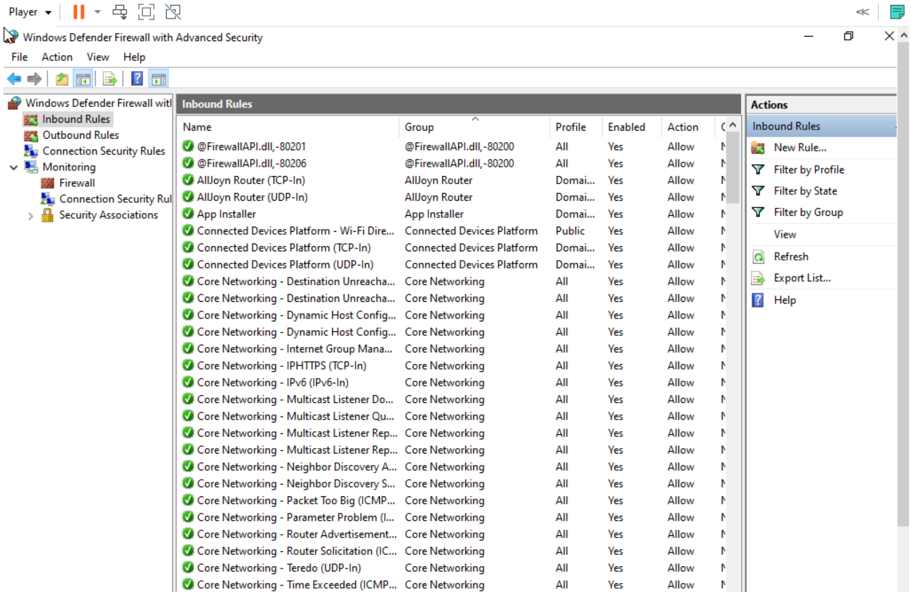
C. Blocked Country IPs

Downloaded country IP list from: https://www.ipdeny.com/ipblocks/



CHILE (CL) [download cl.zone] Size: 12.32 KB (812 IP blocks)	[download cl-aggregrated.zone] (631 IP blocks)
CHINA (CN) [download cn.zone] Size: 132.45 KB (8711 IP blocks)	[download cn-aggregrated.zone] (5493 IP blocks)

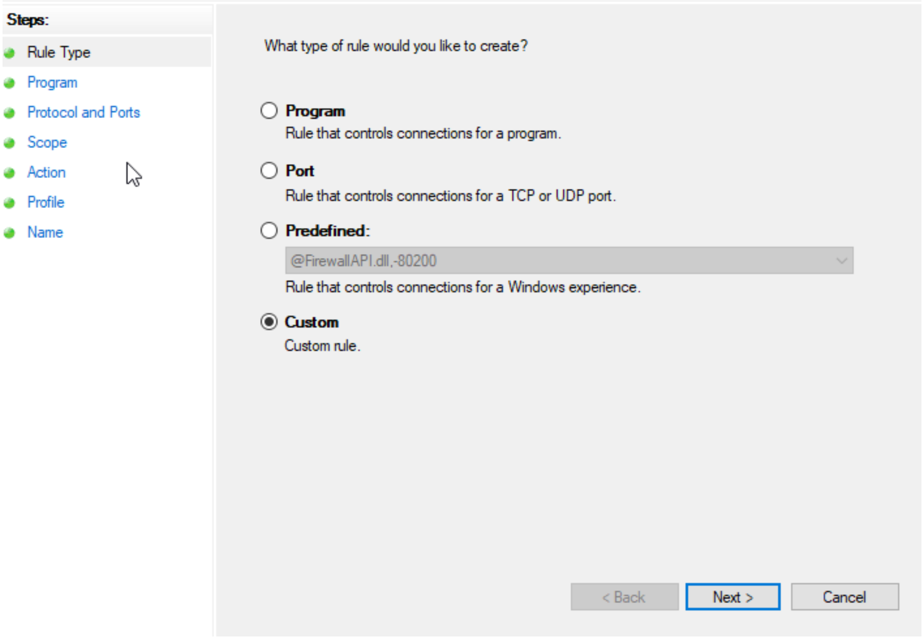
Creating new inbound and outbound rules in Windows Firewall:



Inbound Rules

Name	Group	Profile	Enabled	Action	C
✓ @FirewallAPI.dll,-80201	@FirewallAPI.dll,-80200	All	Yes	Allow	N
✓ @FirewallAPI.dll,-80206	@FirewallAPI.dll,-80200	All	Yes	Allow	N
✓ AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow	N
✓ AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow	N
✓ App Installer	App Installer	Domai...	Yes	Allow	N
✓ Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public	Yes	Allow	N
✓ Connected Devices Platform (TCP-In)	Connected Devices Platform	Domai...	Yes	Allow	N
✓ Connected Devices Platform (UDP-In)	Connected Devices Platform	Domai...	Yes	Allow	N
✓ Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Destination Unreacha...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow	N
✓ Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow	N
✓ Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	N
✓ Core Networking - Multicast Listener Do...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Multicast Listener Qu...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Multicast Listener Rep...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Neighbor Discovery S...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Parameter Problem (I...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Router Advertisement...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	Allow	N
✓ Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow	N
✓ Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow	N

Select the type of firewall rule to create.



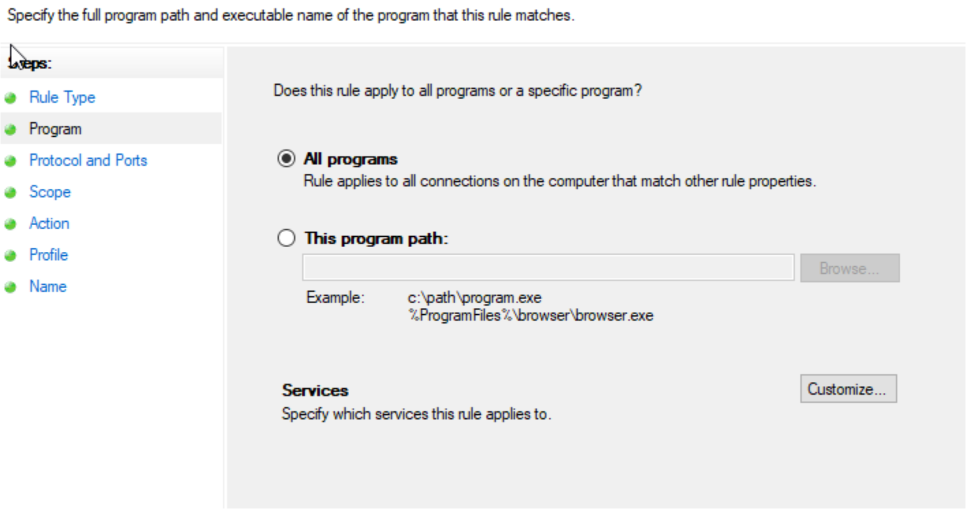
What type of rule would you like to create?

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

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

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

● **Custom**
Custom rule.



Specify the full program path and executable name of the program that this rule matches.

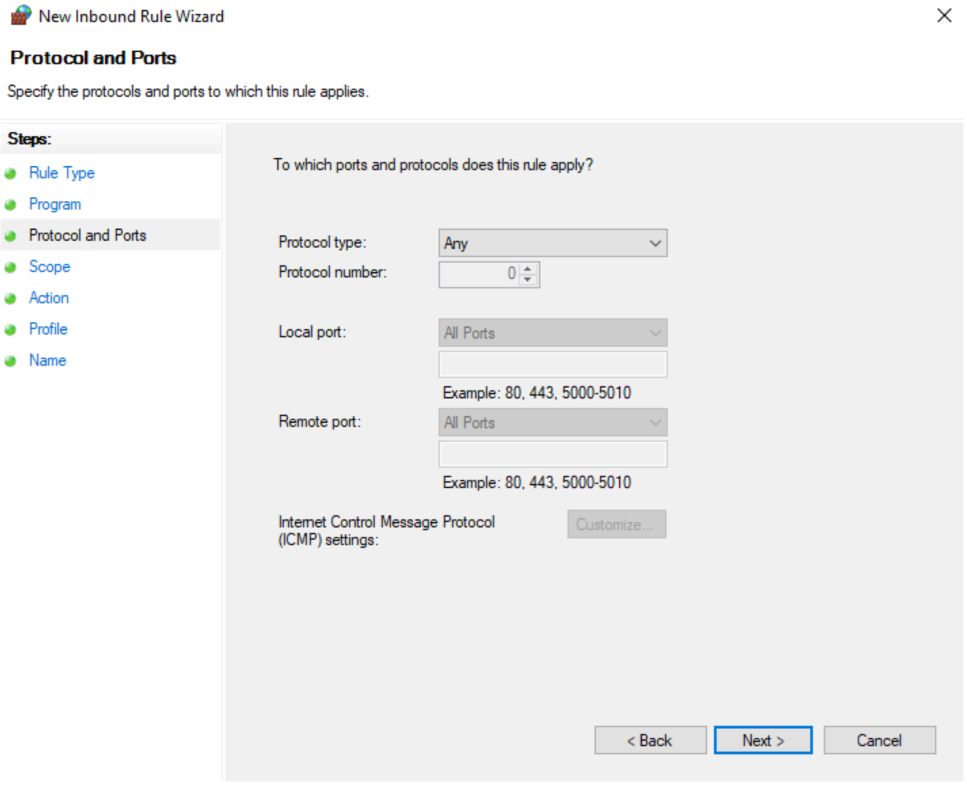
Does this rule apply to all programs or a specific program?

● **All programs**
Rule applies to all connections on the computer that match other rule properties.

○ **This program path:**

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

To which ports and protocols does this rule apply?

Protocol type: Any

Protocol number: 0

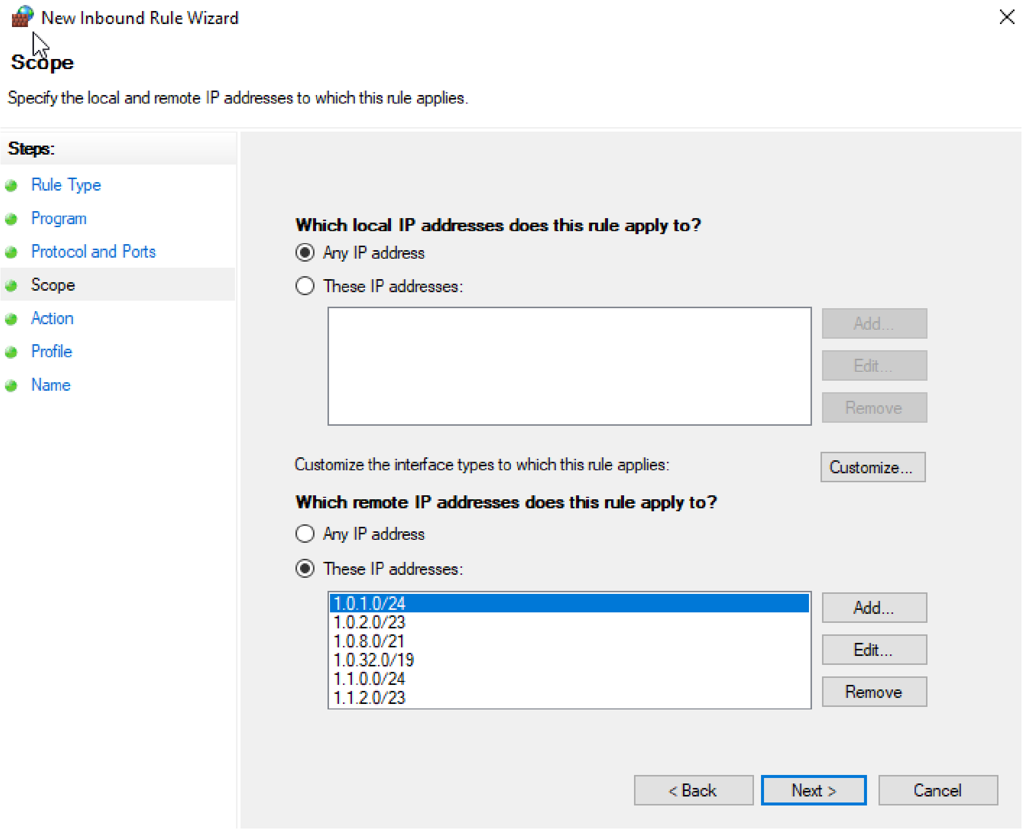
Local port: All Ports

Example: 80, 443, 5000-5010

Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:



New Inbound Rule Wizard

Scope

Specify the local and remote IP addresses to which this rule applies.

Which local IP addresses does this rule apply to?

● Any IP address

○ These IP addresses:

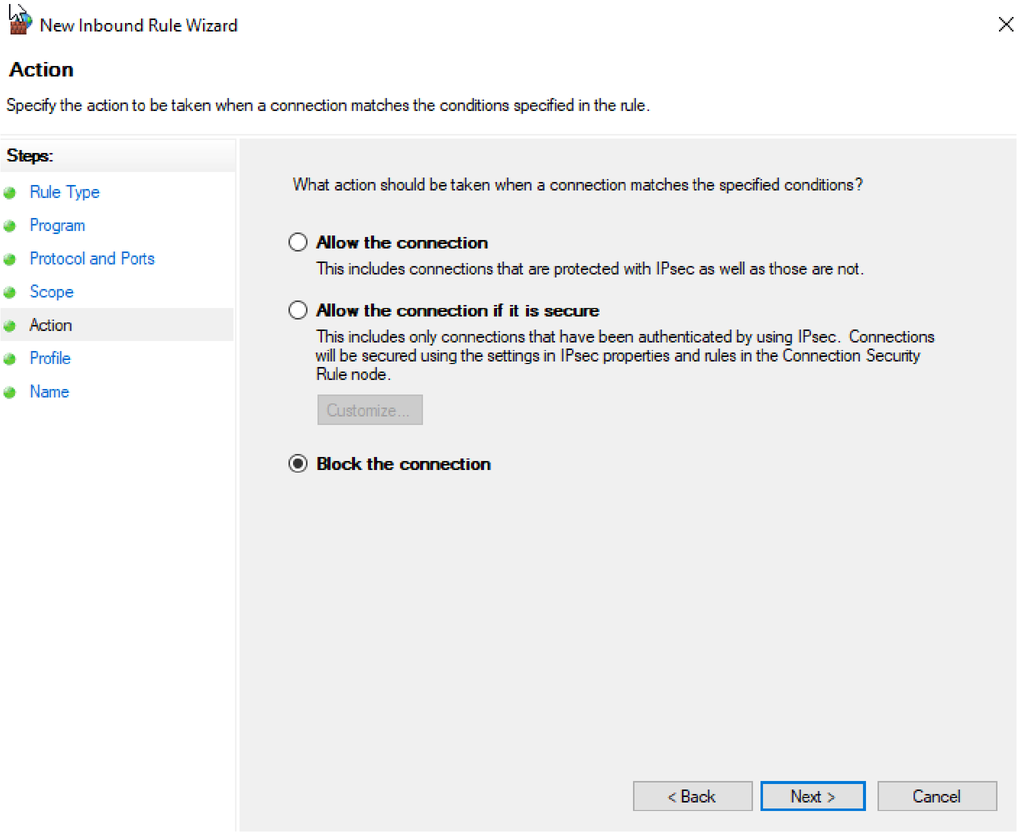
Customize the interface types to which this rule applies:

Which remote IP addresses does this rule apply to?

○ Any IP address

● These IP addresses:

```
1.0.1.0/24
1.0.2.0/23
1.0.8.0/21
1.0.32.0/19
1.1.0.0/24
1.1.2.0/23
```



New Inbound Rule Wizard

Action

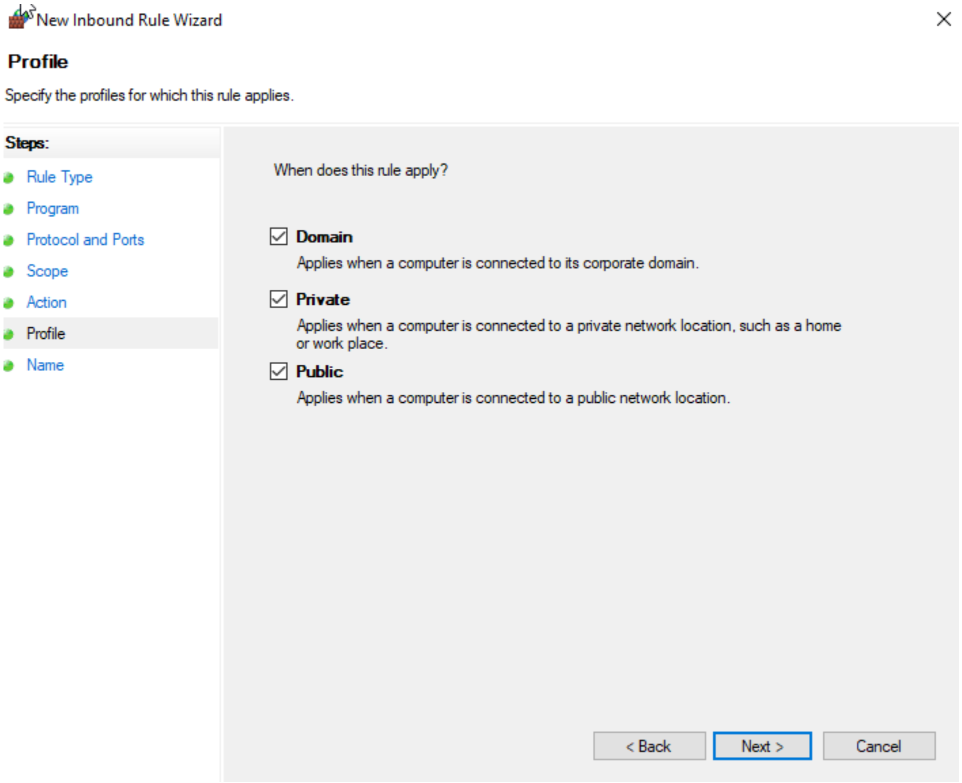
Specify the action to be taken when a connection matches the conditions specified in the rule.

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

○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

● **Block the connection**



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

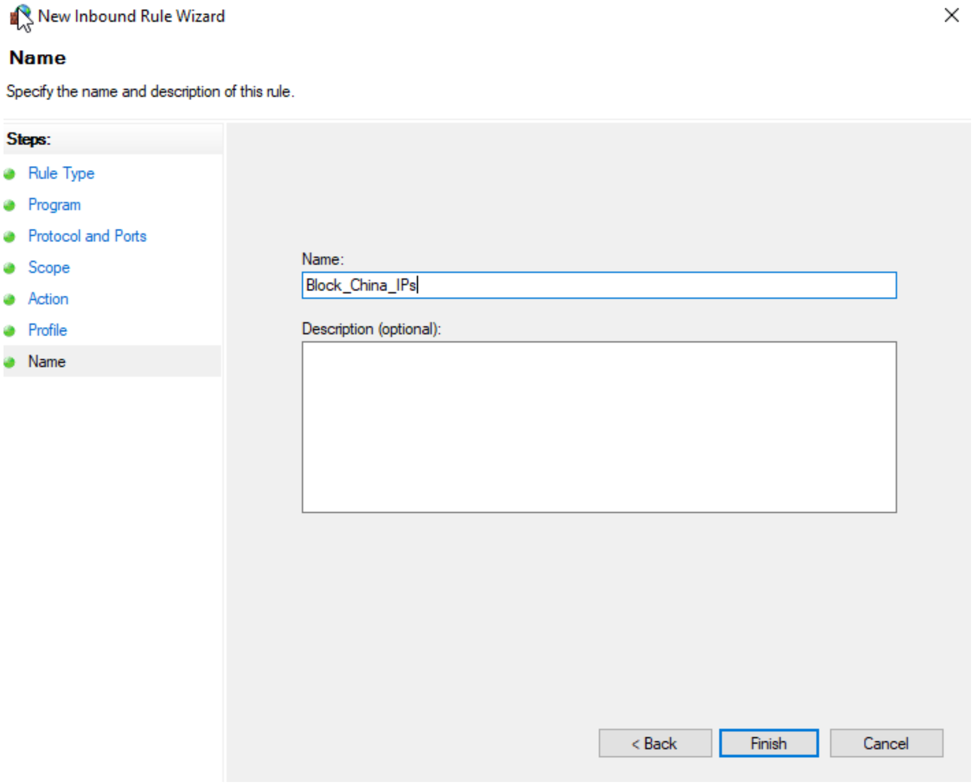
Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

When does this rule apply?

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

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

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



New Inbound Rule Wizard

Name

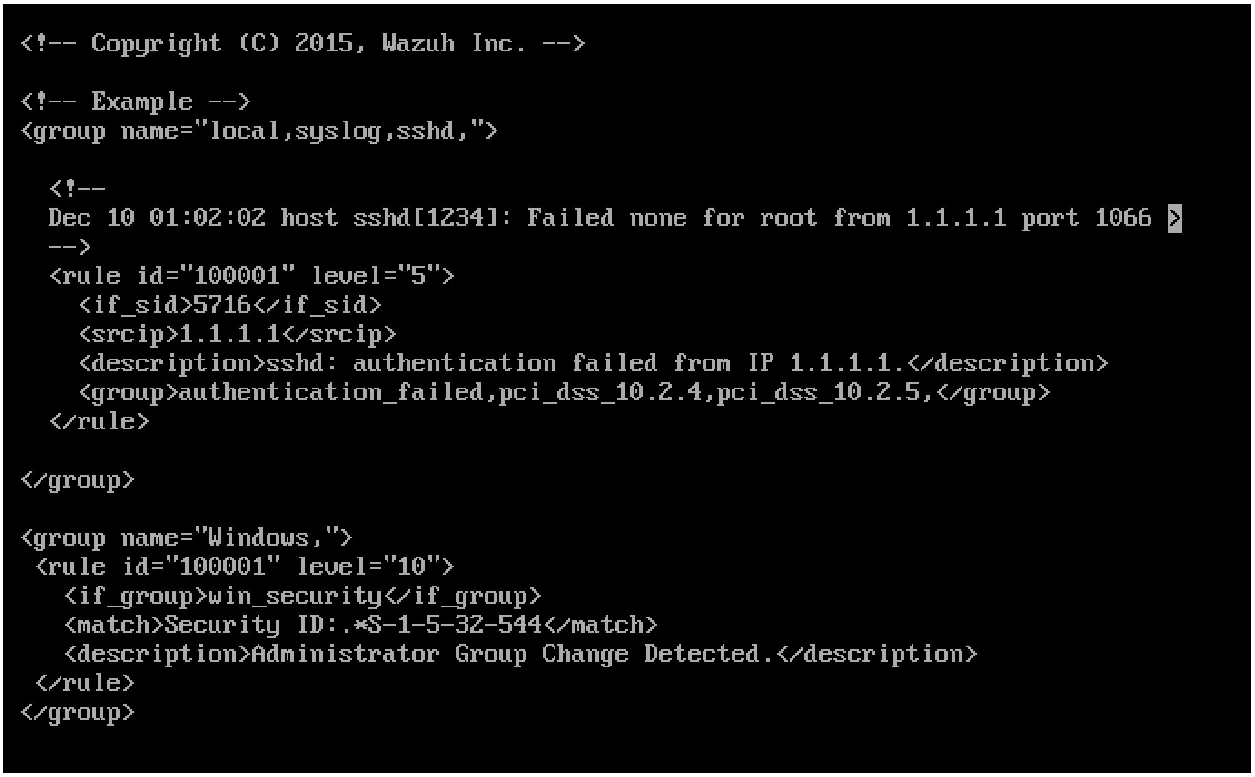
Specify the name and description of this rule.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Name:
Block_China_IPs

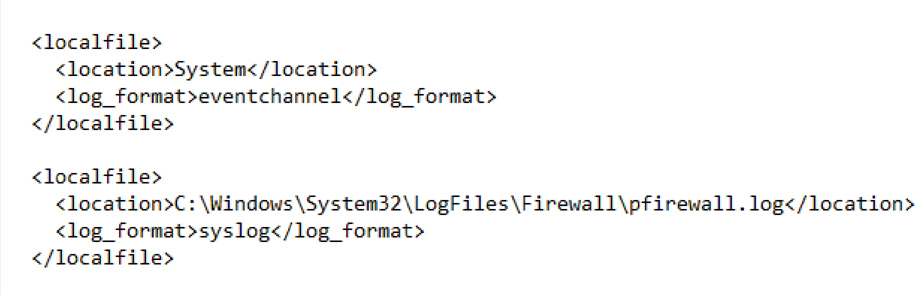
Description (optional):

D. Monitoring Admin Privileges



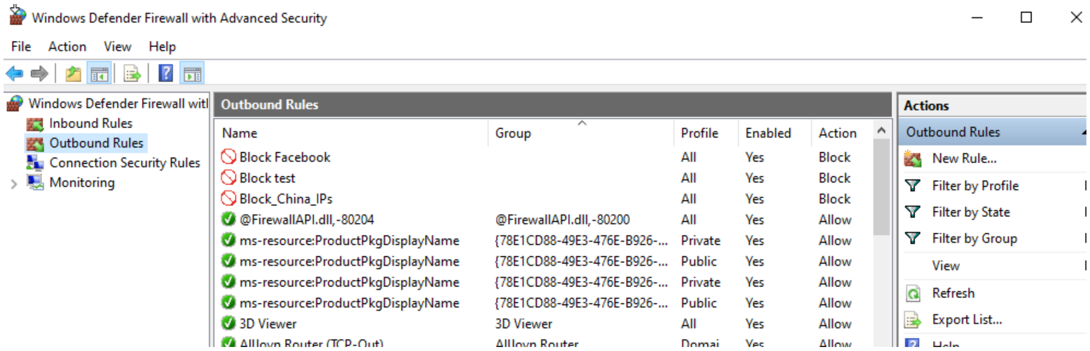
```
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 >
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

</group>

<group name="Windows,">
 <rule id="100001" level="10">
   <if_group>win_security</if_group>
   <match>Security ID:.*S-1-5-32-544</match>
   <description>Administrator Group Change Detected.</description>
 </rule>
</group>
```

Step 6: Sending Logs to Wazuh

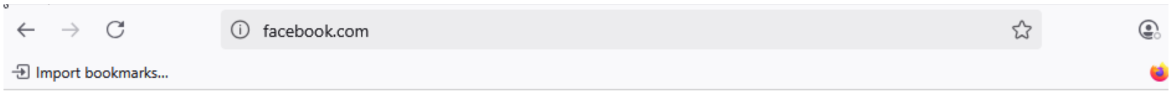


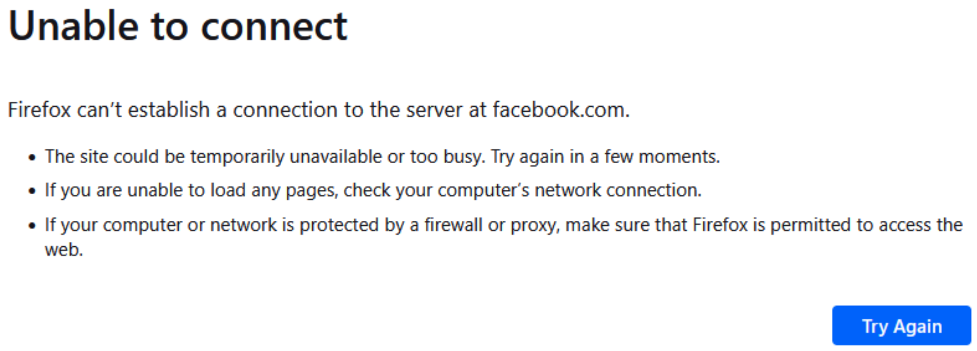
```
<localfile>
  <location>System</location>
  <log_format>eventchannel</log_format>
</localfile>

<localfile>
  <location>C:\Windows\System32\LogFiles\Firewall\pfirewall.log</location>
  <log_format>syslog</log_format>
</localfile>
```

Step 7: Testing



Name	Group	Profile	Enabled	Action
Block Facebook		All	Yes	Block
Block test		All	Yes	Block
Block_China_IPs		All	Yes	Block
@FirewallAPI.dll,-80204	@FirewallAPI.dll,-80200	All	Yes	Allow
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Private	Yes	Allow
ms-resource:ProductPkgDisplayName	{78E1CD88-49E3-476E-B926-...	Public	Yes	Allow
3D Viewer	3D Viewer	All	Yes	Allow
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai	Yes	Allow

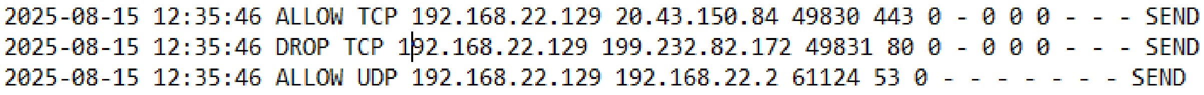




Unable to connect

Firefox can't establish a connection to the server at facebook.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.



```
2025-08-15 12:35:46 ALLOW TCP 192.168.22.129 20.43.150.84 49830 443 0 - 0 0 0 - - - SEND
2025-08-15 12:35:46 DROP TCP 192.168.22.129 199.232.82.172 49831 80 0 - 0 0 0 - - - SEND
2025-08-15 12:35:46 ALLOW UDP 192.168.22.129 192.168.22.2 61124 53 0 - - - - - - - SEND
```

Result:

This lab successfully demonstrated how to:

- Isolate Wazuh Manager and Agent traffic from the internet.
- Configure Windows firewall logging for security event monitoring.
- Forward logs from a Windows endpoint to a Wazuh Manager.
- Detect and alert on both blocked traffic and admin privilege changes.