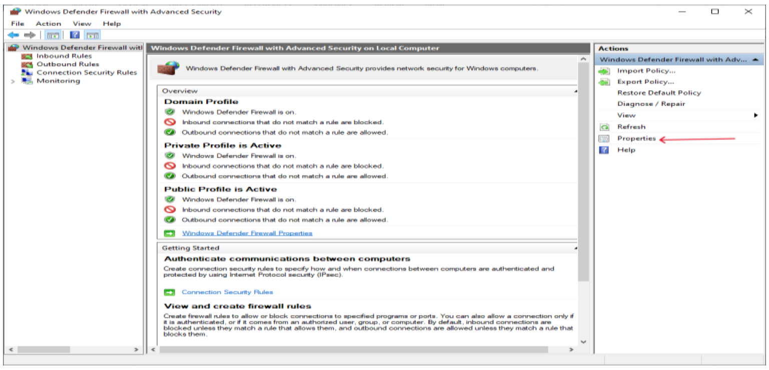
WINDOWS DEFENDER FIREWALL LOGS

Importance of firewall logs

- For analysis and investigation against malicious activities
- To verify if firewall rules work properly

Start by creating the firewall log file

1. Go to windows defender, under windows defender firewall click on advanced settings. Then select properties to create log entries for log dropped packets and log successful connections.


Windows Defender Firewall with Advanced Security
File Action View Help
Windows Defender Firewall wit
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Actions
Windows Defender Firewall with Adv...
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.

Overview

Domain Profile

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

Private Profile 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.

Public Profile is Active

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

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

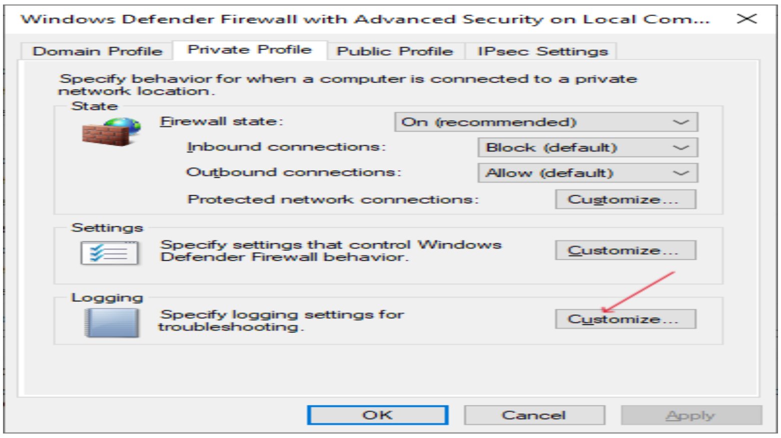
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

2.Under private profile Click on customize to under specific logging settings for troubleshoot ing



Specify behavior for when a computer is connected to a private network location.

Firewall state: On (recommended)

Inbound connections: Block (default)

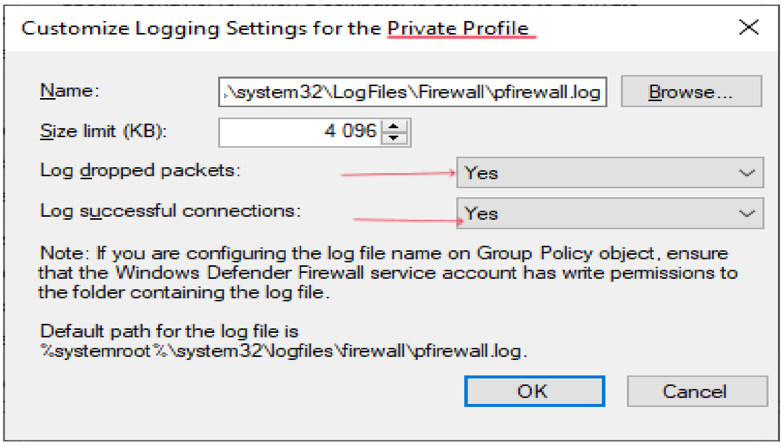
Outbound connections: Allow (default)

Protected network connections:

Specify settings that control Windows Defender Firewall behavior.

Specify logging settings for troubleshooting.

3. Click yes on log dropped packets and yes on log successful connections and then click ok.



Customize Logging Settings for the Private Profile

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

Size limit (KB): 4 096

Log dropped packets: Yes

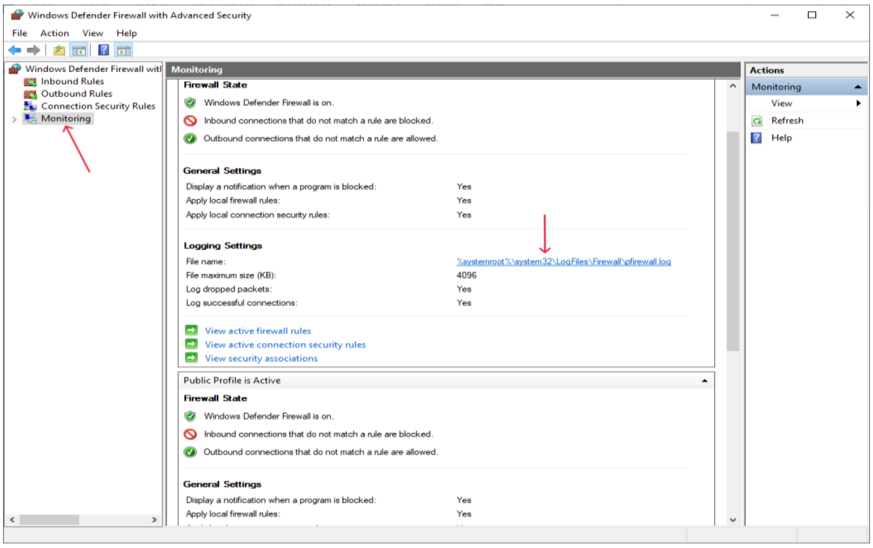
Log successful connections: Yes

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.

4.Repeat the steps for the public profile

5.Click under monitoring to check the log file



Windows Defender Firewall with Advanced Security

Monitoring

Firewall State

- 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.

General Settings

Display a notification when a program is blocked: Yes
Apply local firewall rules: Yes
Apply local connection security rules: Yes

Logging Settings

File name: %systemroot%\system32\LogFiles\Firewall\pfirewall.log
File maximum size (KB): 4096
Log dropped packets: Yes
Log successful connections: Yes

View active firewall rules
View active connection security rules
View security associations

Public Profile is Active

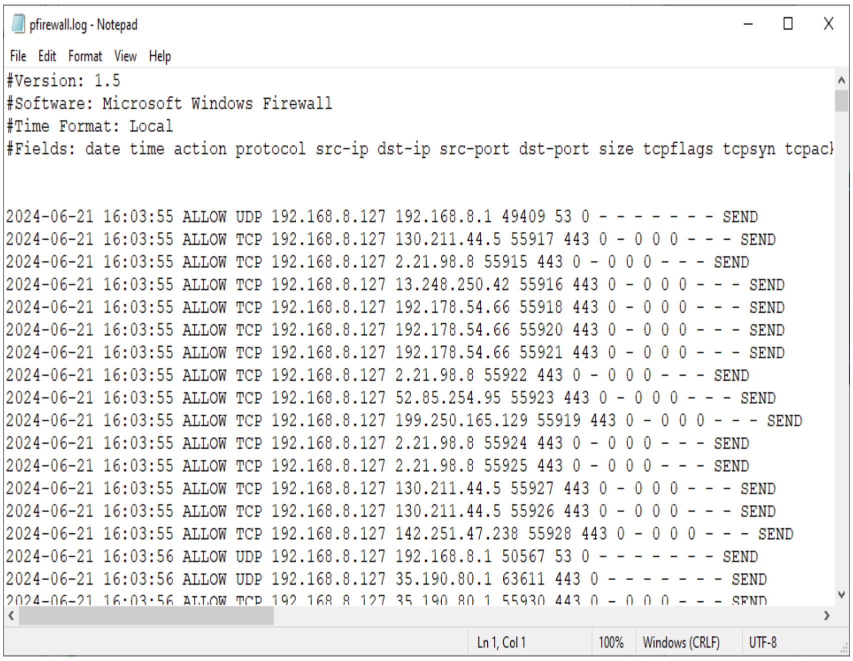
Firewall State

- 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.

General Settings

Display a notification when a program is blocked: Yes
Apply local firewall rules: Yes

6.Click on the file path next to file name to open the log file (%systemroot%\system32\logfiles\firewall\pfirewall.log)



```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpac


2024-06-21 16:03:55 ALLOW UDP 192.168.8.127 192.168.8.1 49409 53 0 - - - - - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 130.211.44.5 55917 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 2.21.98.8 55915 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 13.248.250.42 55916 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 192.178.54.66 55918 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 192.178.54.66 55920 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 192.178.54.66 55921 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 2.21.98.8 55922 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 52.85.254.95 55923 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 199.250.165.129 55919 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 2.21.98.8 55924 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 2.21.98.8 55925 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 130.211.44.5 55927 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 130.211.44.5 55926 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 142.251.47.238 55928 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:56 ALLOW UDP 192.168.8.127 192.168.8.1 50567 53 0 - - - - - - - SEND
2024-06-21 16:03:56 ALLOW UDP 192.168.8.127 35.190.80.1 63611 443 0 - - - - - - - SEND
2024-06-21 16:03:56 ALLOW TCP 192.168.8.127 35.190.80.1 55930 443 0 - 0 0 0 - - - SEND
```

Details of the above log fields

Date = Date(YYYY-MM-DD)

time = Time

src-ip = Source IP Address

dst-ip = Destination IP Address

srcport = Source Port

dstport = Destination Port

size = Packet size in bytes.

Tcpflags = TCP control flags in TCP headers.

tcpsyn = TCP sequence number in the packet.

tcpack = TCP acknowledgement number in the packet.

Tcpwin= TCP window size, in bytes, in the packet.

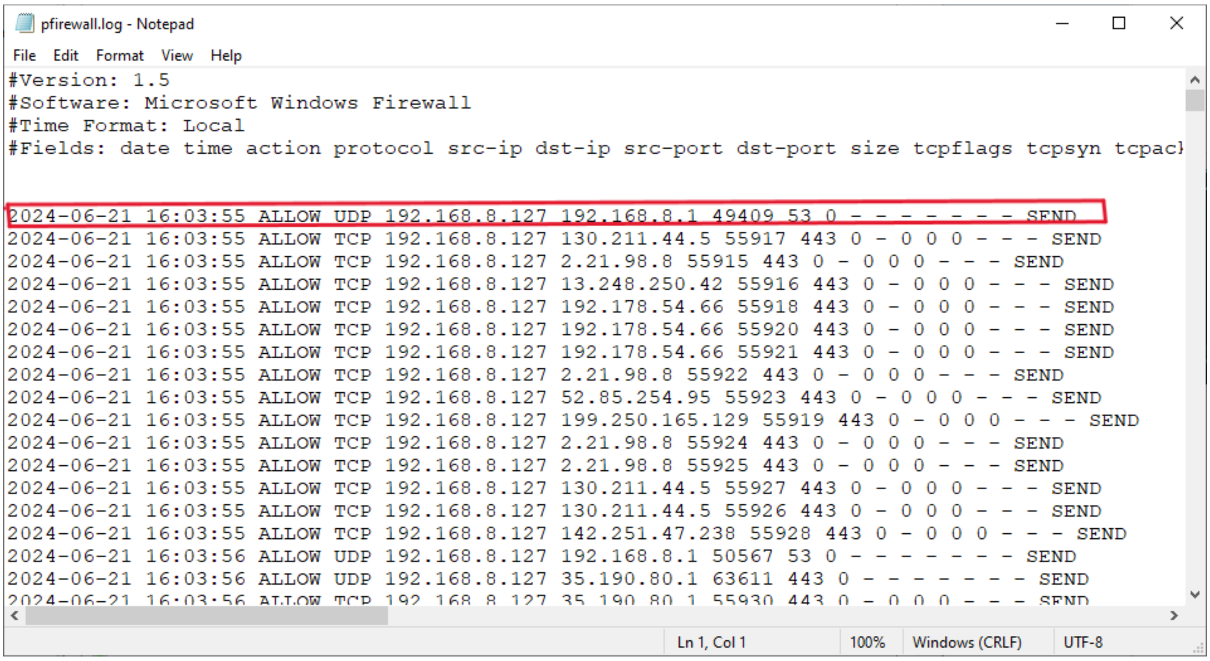
Icmptype= ICMP messages type

icmpcode = messages code

info = info on action taken

path = communication path

Analyzing the 1st packet log



```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack


2024-06-21 16:03:55 ALLOW UDP 192.168.8.127 192.168.8.1 49409 53 0 - - - - - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 130.211.44.5 55917 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 2.21.98.8 55915 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 13.248.250.42 55916 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 192.178.54.66 55918 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 192.178.54.66 55920 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 192.178.54.66 55921 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 2.21.98.8 55922 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 52.85.254.95 55923 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 199.250.165.129 55919 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 2.21.98.8 55924 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 2.21.98.8 55925 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 130.211.44.5 55927 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 130.211.44.5 55926 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:55 ALLOW TCP 192.168.8.127 142.251.47.238 55928 443 0 - 0 0 0 - - - SEND
2024-06-21 16:03:56 ALLOW UDP 192.168.8.127 192.168.8.1 50567 53 0 - - - - - - - SEND
2024-06-21 16:03:56 ALLOW UDP 192.168.8.127 35.190.80.1 63611 443 0 - - - - - - - SEND
2024-06-21 16:03:56 ALLOW TCP 192.168.8.127 35.190.80.1 55930 443 0 - 0 0 0 - - - SEND
```

- **Date:** 2024-06-21
- **Time:** 16:03:55
- **Action:** ALLOW - This signifies that the firewall permitted the traffic to pass through.
- **Protocol:** UDP - This refers to the User Datagram Protocol, a connectionless protocol commonly used for brief exchanges like DNS lookups.
- **Source IP:** 192.168.8.127 - This is the IP address of the device that initiated the communication. It appears to be an internal device on the local network (likely within the 192.168.8.0/24 subnet).
- **Destination IP:** 192.168.8.1 - This is the IP address of the device that received the communication. It seems to be another device on the local network, possibly a router or DNS server.
- **Source Port:** 49409 - This is the port number used by the application on the source device. Since the exact port number isn't typically registered for well-known services, it's difficult to pinpoint the specific application without further investigation.

- **Destination Port:** 53 - This is a well-known port number associated with the DNS (Domain Name System) service. Devices use DNS to translate website names (like [invalid URL removed]) into IP addresses.

This log entry indicates that a device on the local network (192.168.8.127) sent a UDP message to port 53 on another device (likely a DNS server at 192.168.8.1) on the network. This is most likely a DNS request from the first device trying to resolve a website name.