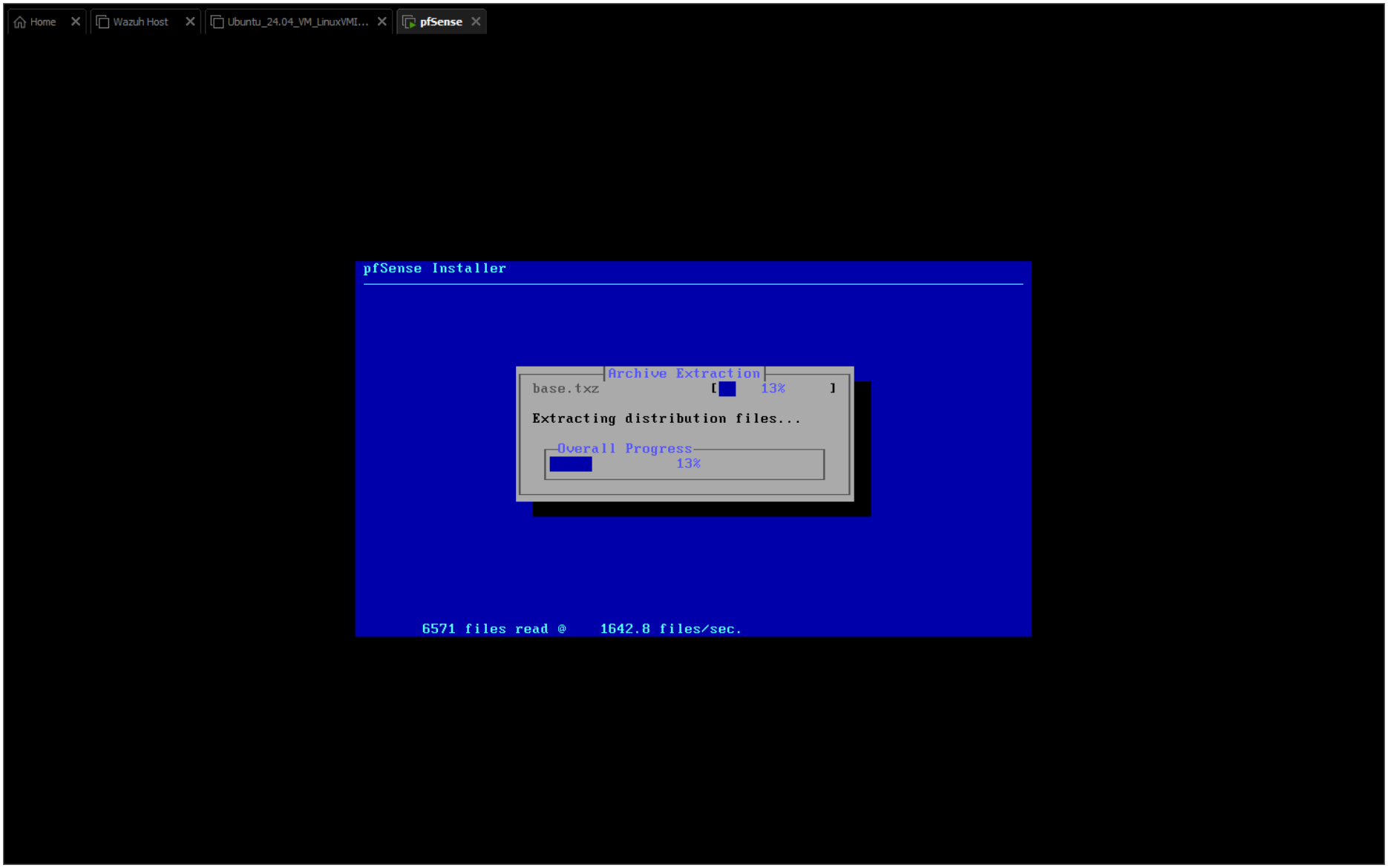
pfSense Installation

Talal Ahmed | Team Lambda

Downloading pfSense ISO

Download pfSense CE 2.7.2 from a netgate mirror: https://atxfiles.netgate.com/mirror/downloads/

Extract and install like a normal OS


Home
Wazuh Host
Ubuntu_24.04_VM_LinuxVMI...
pfSense
pfSense Installer
Archive Extraction
base.txz [13%]
Extracting distribution files...
Overall Progress
13%
6571 files read @ 1642.8 files/sec.

This is initial config.

I set up the VMWare virtual network like this:

VM	*OS*	*Role*	*Network*
VM1	Ubuntu 24.04	Wazuh Manager	Host-only (LAN) 192.168.164.2
VM2	Ubuntu 24.04	Wazuh Agent	Host-only (LAN) DHCP
VM3	pfSense 2.7	Firewall	WAN DHCP, LAN static 192.168.164.1

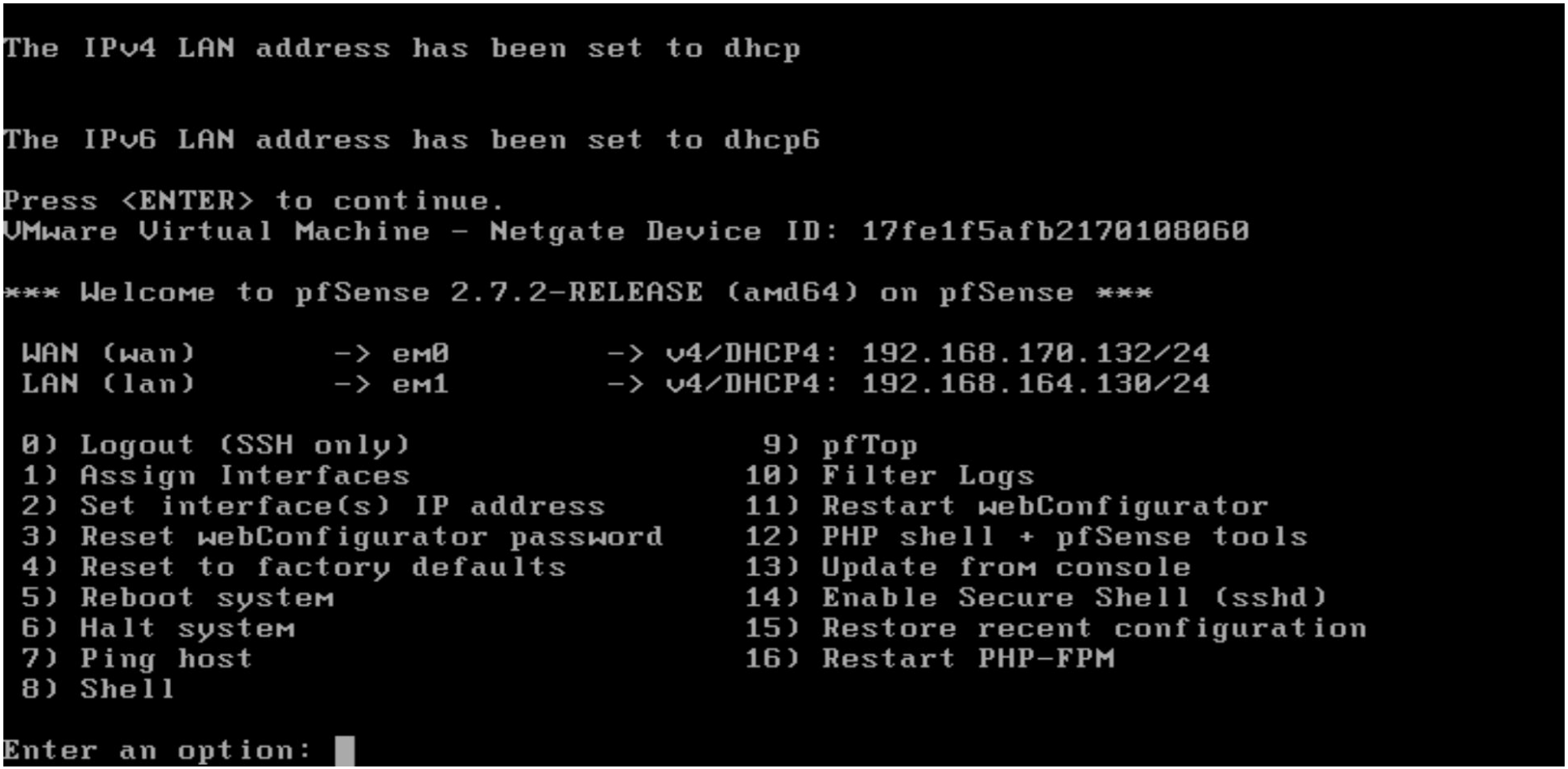
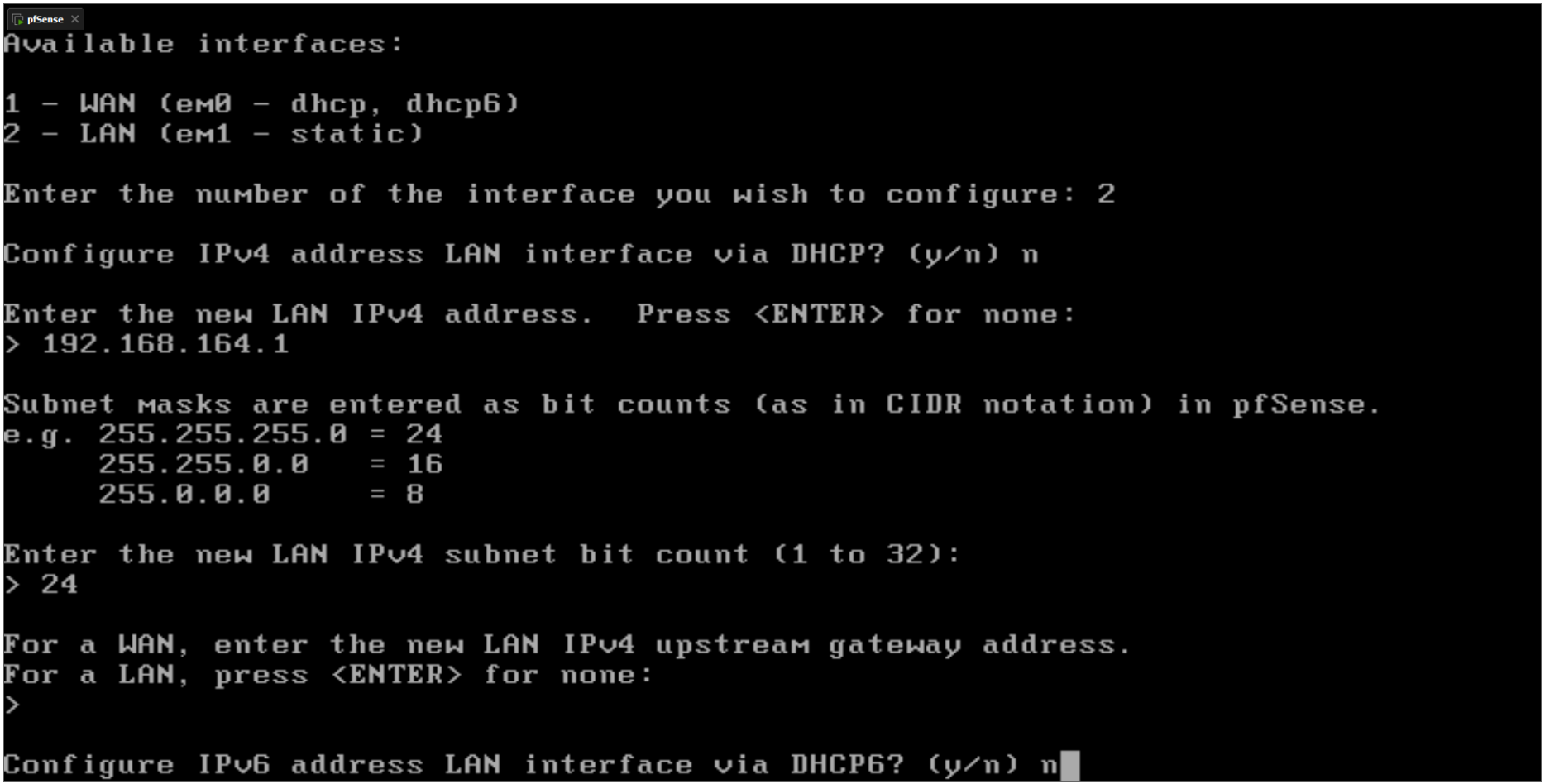
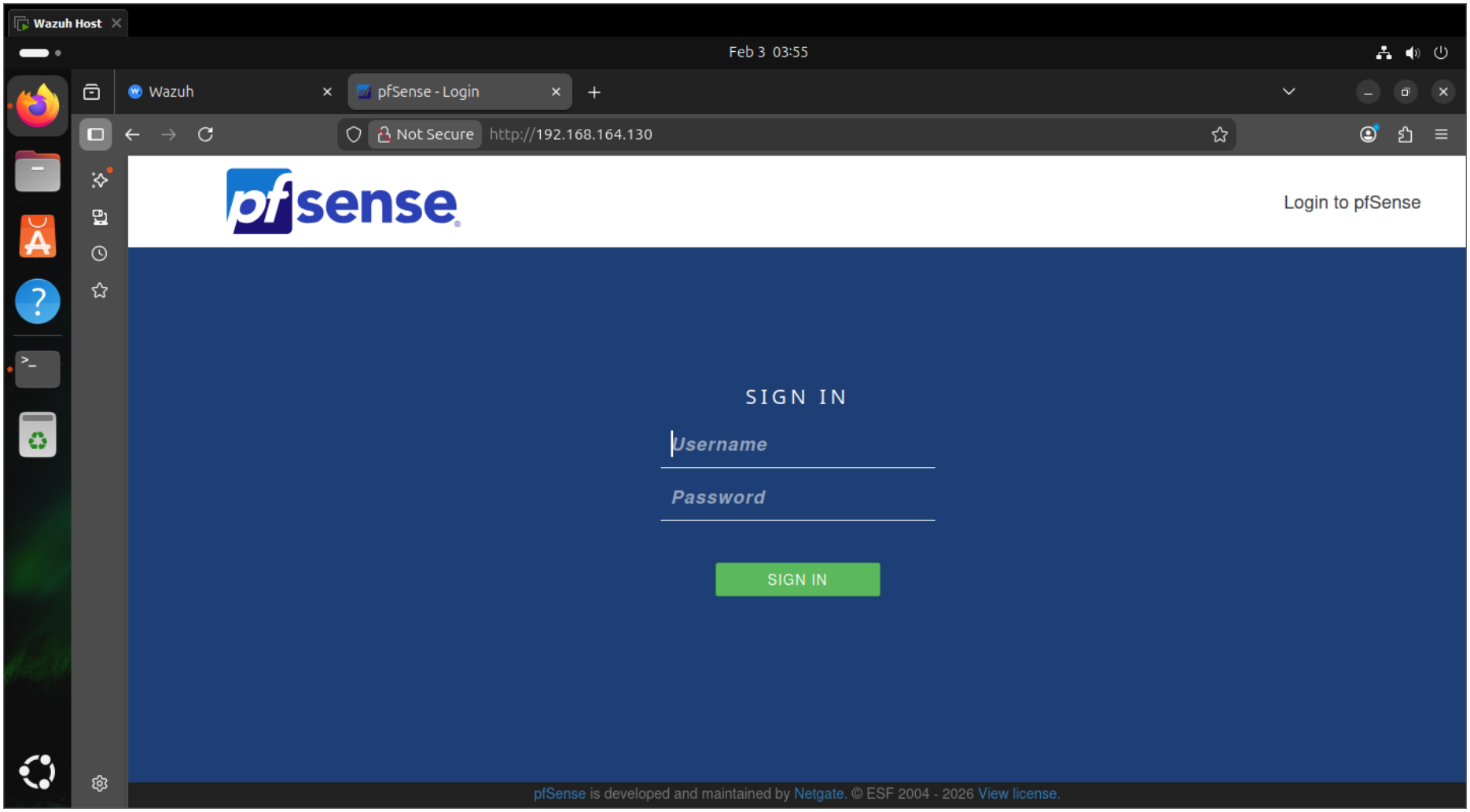
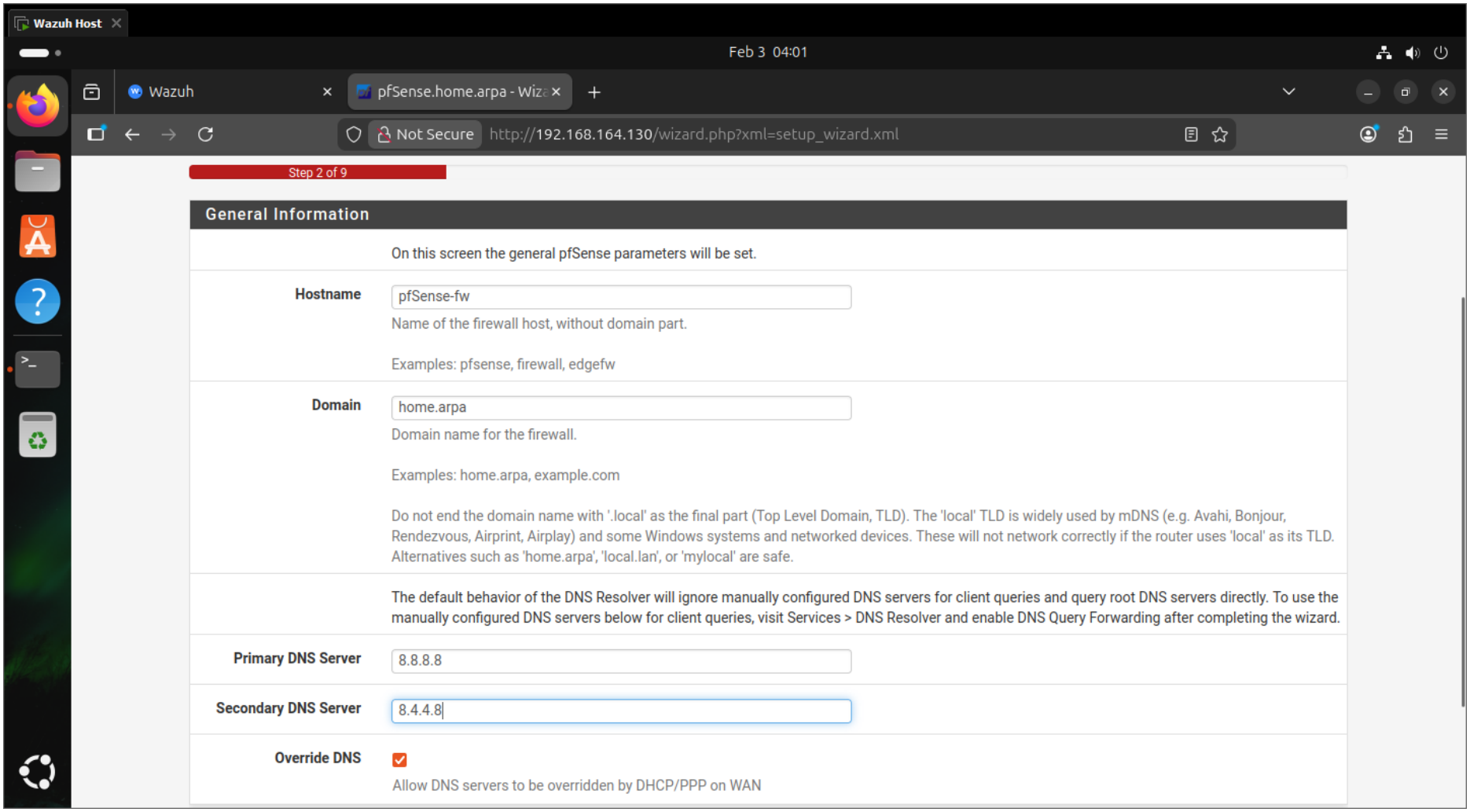


Figure 1 I updated the ip from ...130 to .1 afterwards


pfSense
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.164.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
255.255.0.0 = 16
255.0.0.0 = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Configure IPv6 address LAN interface via DHCP6? (y/n) n

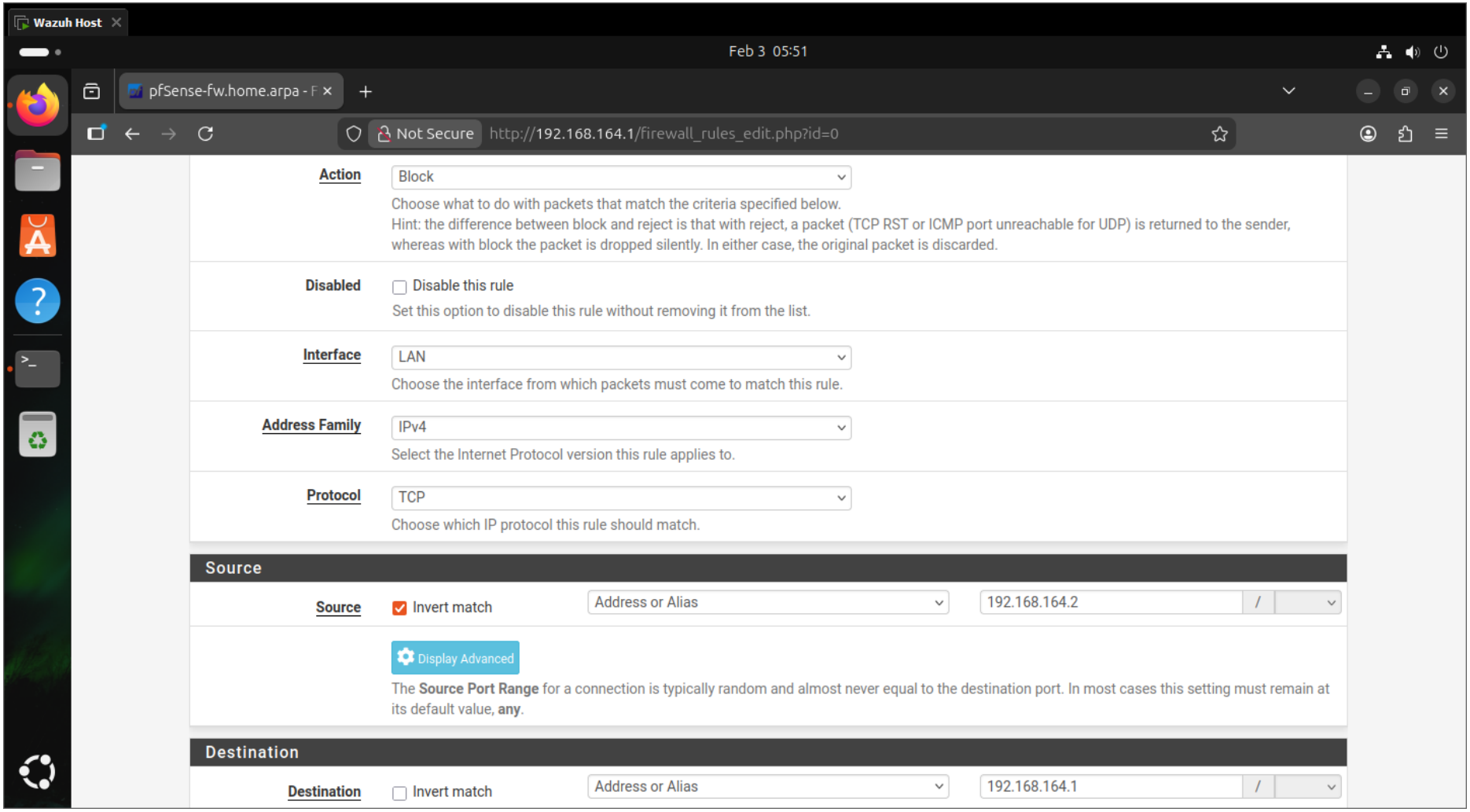


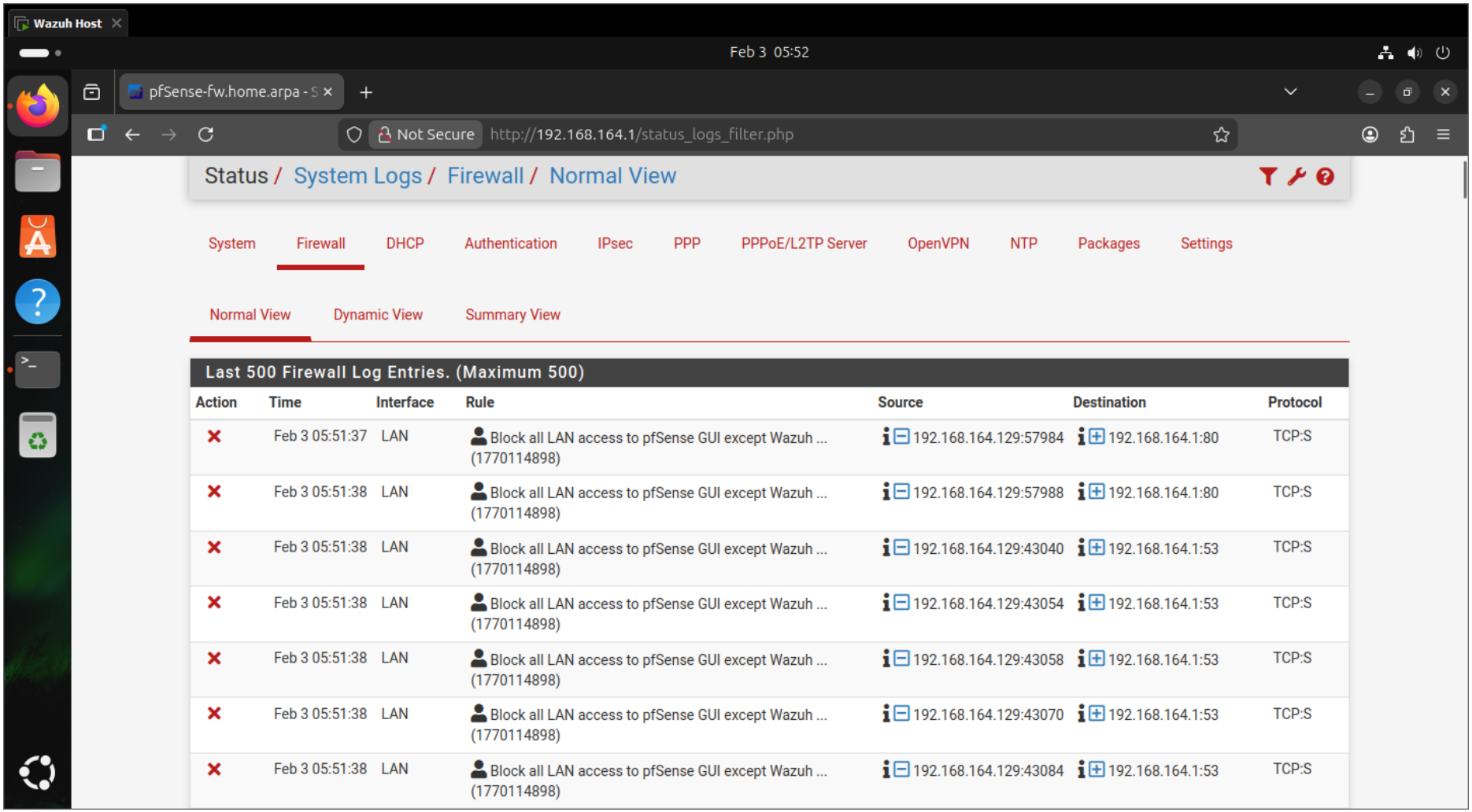
Login with default credentials of admin and pfSense as password.


Wazuh Host
Feb 3 04:01
Wazuh
pfSense.home.arpa - Wiz
Not Secure
http://192.168.164.130/wizard.php?xml=setup_wizard.xml
Step 2 of 9
General Information
On this screen the general pfSense parameters will be set.
Hostname
pfSense-fw
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw
Domain
home.arpa
Domain name for the firewall.
Examples: home.arpa, example.com
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.
Primary DNS Server
8.8.8.8
Secondary DNS Server
8.4.4.8
Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN

Administrator privileges rule

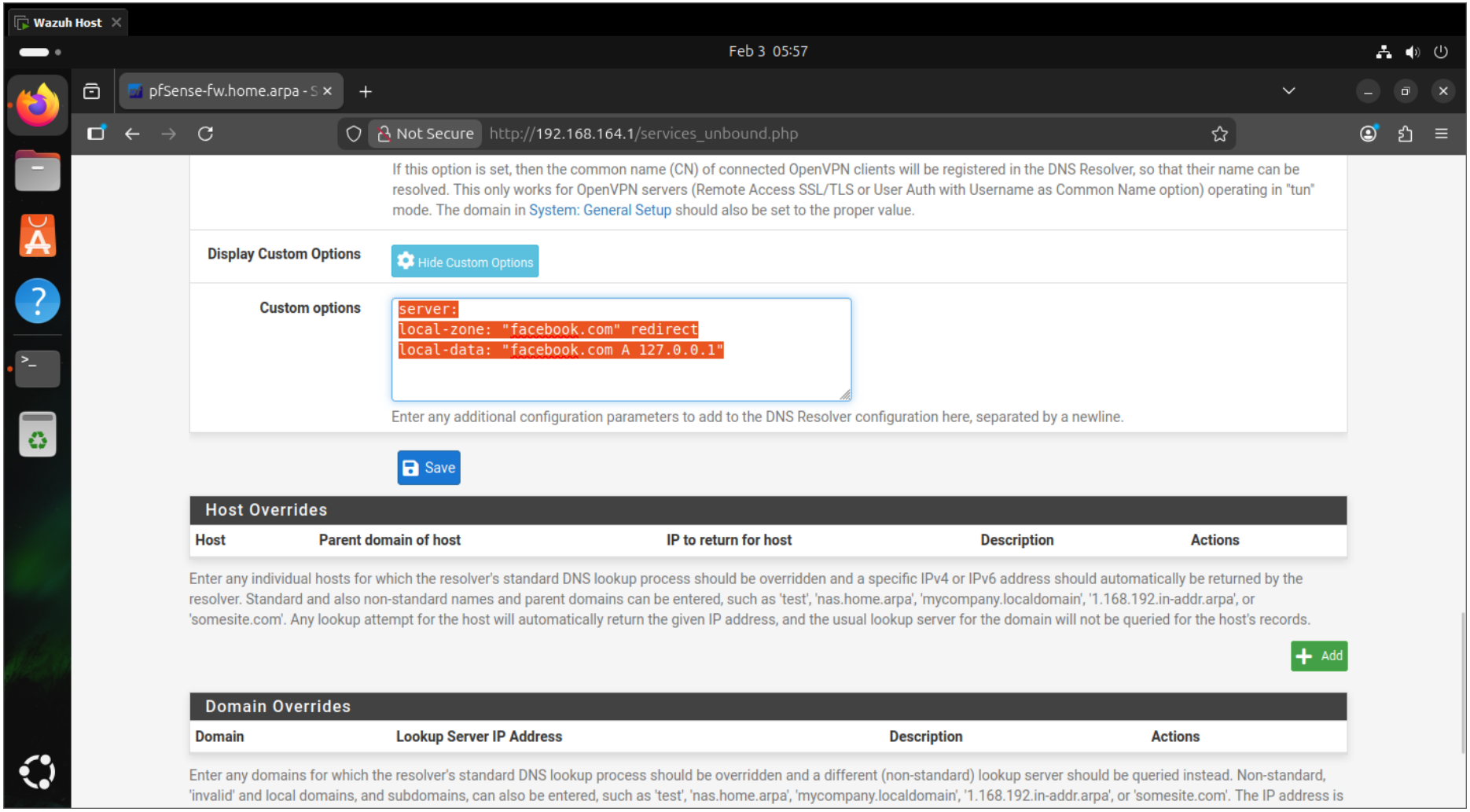
I blocked TCP (HTTP) requests from any IP other than the Wazuh-manager to the gateway to block access to the pfSense dashboard.

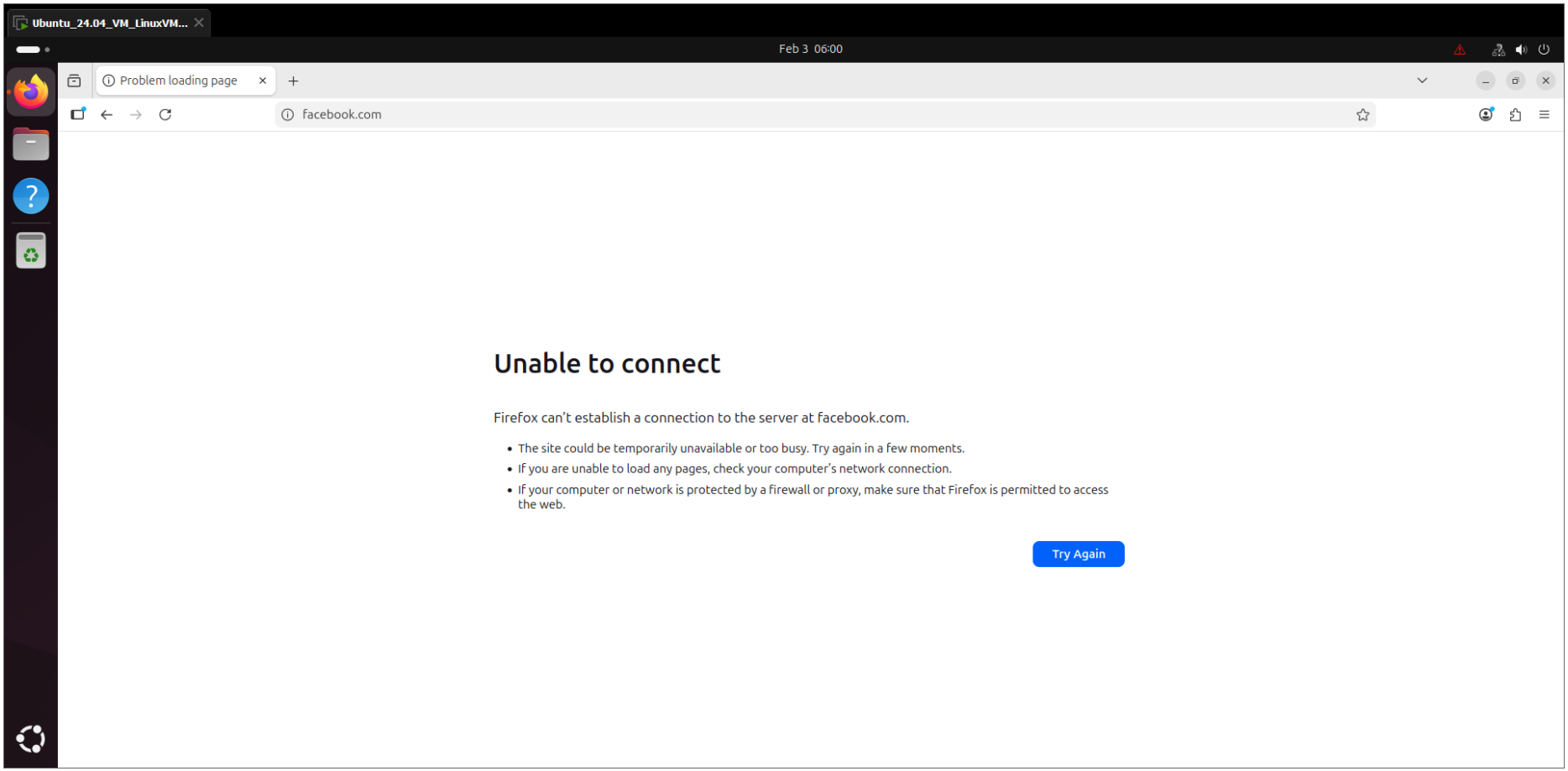



Wazuh Host
Feb 3 05:52
pfSense-fw.home.arpa - S
Not Secure
http://192.168.164.1/status_logs_filter.php
Status / System Logs / Firewall / Normal View
System
Firewall
DHCP
Authentication
IPsec
PPP
PPPoE/L2TP Server
OpenVPN
NTP
Packages
Settings
Normal View
Dynamic View
Summary View
Last 500 Firewall Log Entries. (Maximum 500)
Action
Time
Interface
Rule
Source
Destination
Protocol
Feb 3 05:51:37 LAN Block all LAN access to pfSense GUI except Wazuh ... (1770114898) 192.168.164.129:57984 192.168.164.1:80 TCP:S
Feb 3 05:51:38 LAN Block all LAN access to pfSense GUI except Wazuh ... (1770114898) 192.168.164.129:57988 192.168.164.1:80 TCP:S
Feb 3 05:51:38 LAN Block all LAN access to pfSense GUI except Wazuh ... (1770114898) 192.168.164.129:43040 192.168.164.1:53 TCP:S
Feb 3 05:51:38 LAN Block all LAN access to pfSense GUI except Wazuh ... (1770114898) 192.168.164.129:43054 192.168.164.1:53 TCP:S
Feb 3 05:51:38 LAN Block all LAN access to pfSense GUI except Wazuh ... (1770114898) 192.168.164.129:43058 192.168.164.1:53 TCP:S
Feb 3 05:51:38 LAN Block all LAN access to pfSense GUI except Wazuh ... (1770114898) 192.168.164.129:43070 192.168.164.1:53 TCP:S
Feb 3 05:51:38 LAN Block all LAN access to pfSense GUI except Wazuh ... (1770114898) 192.168.164.129:43084 192.168.164.1:53 TCP:S

Block Facebook

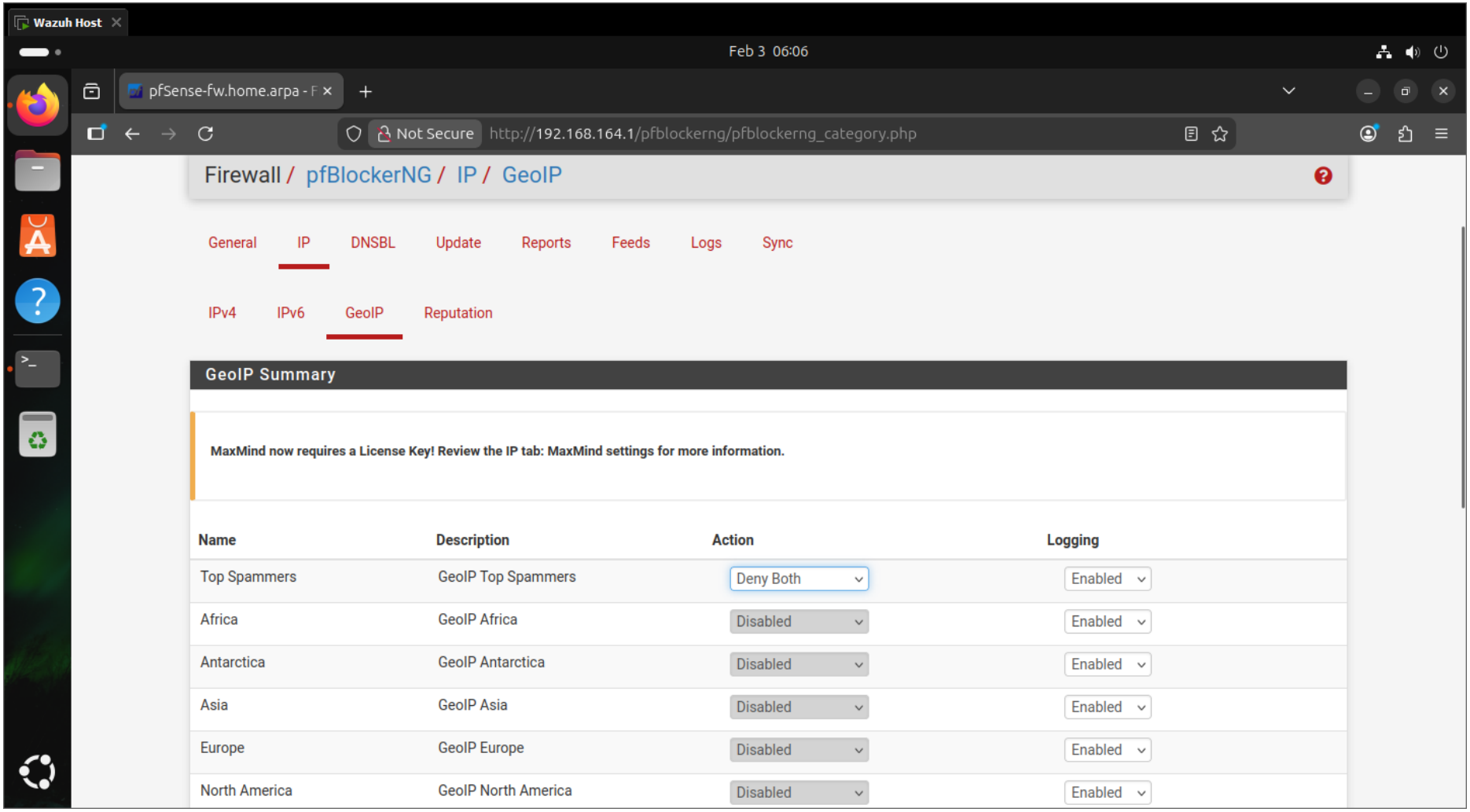
To block Facebook, I added a DNS rule like this.




Ubuntu_24.04_VM_LinuxVM...
Feb 3 06:00
Problem loading page
facebook.com
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.
Try Again

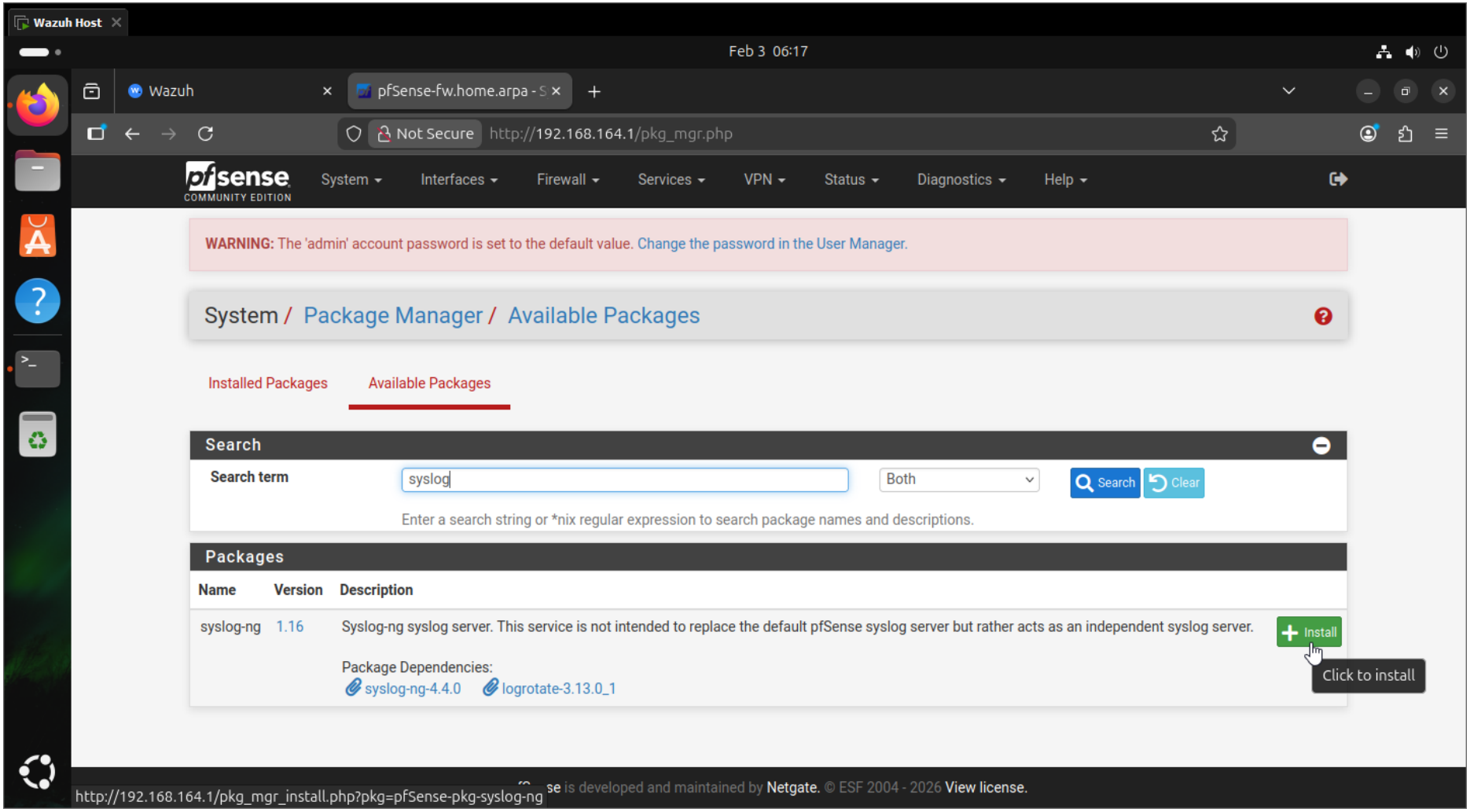
Block Specific Countries

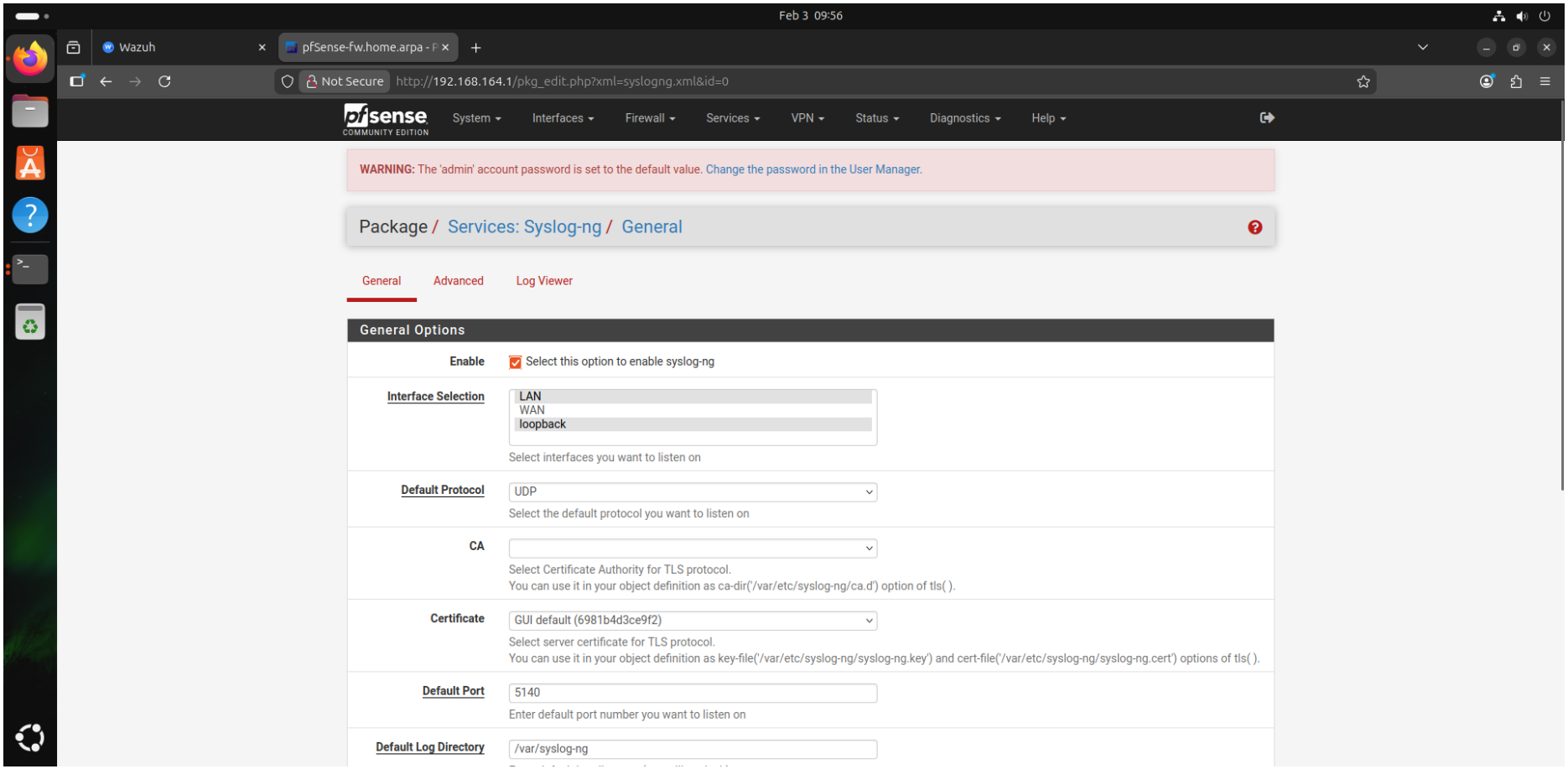
I used pfBlockerNG plugin to geo block IPs.



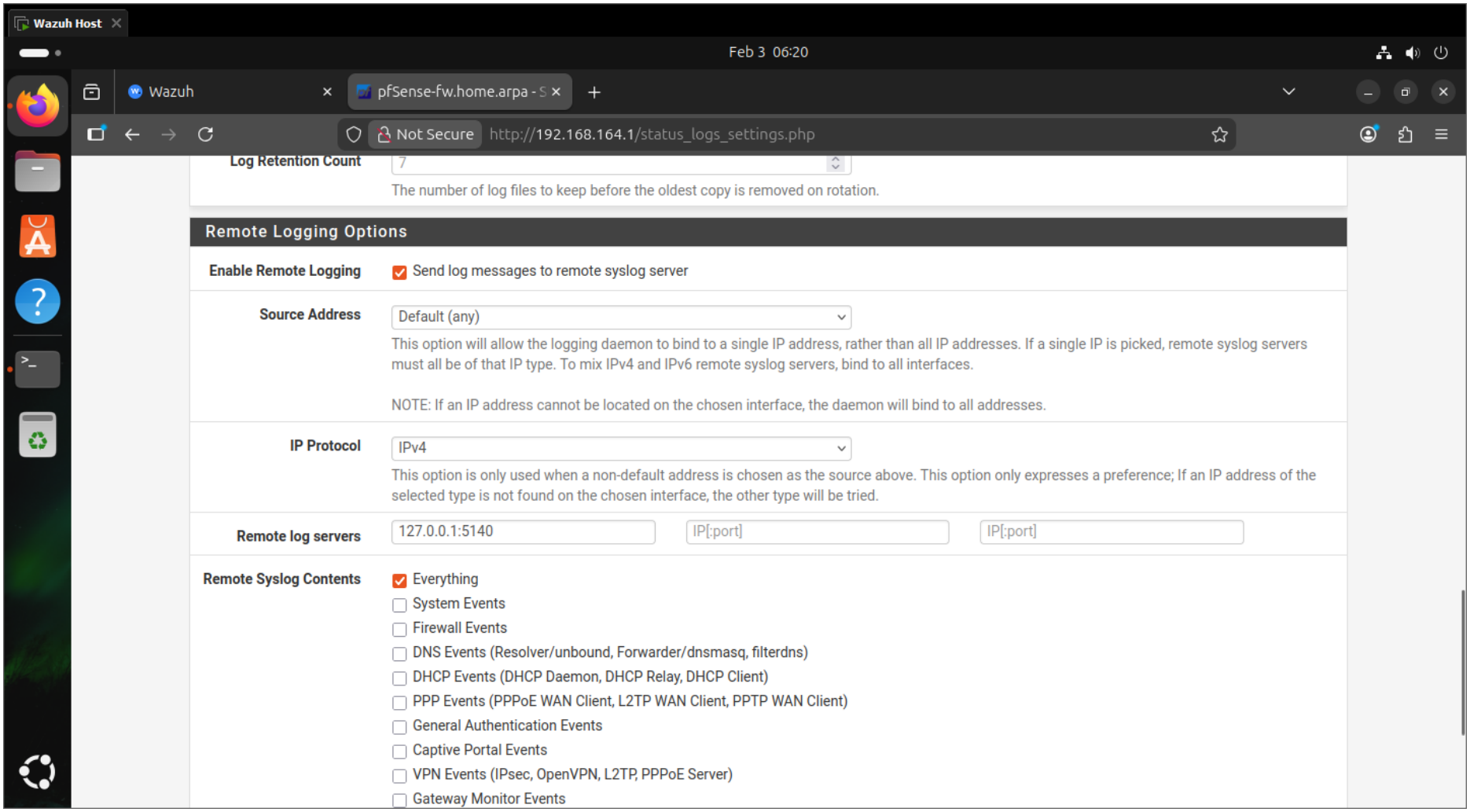
Connecting with Wazuh

To connect with Wazuh, I used Syslog-ng plugin.

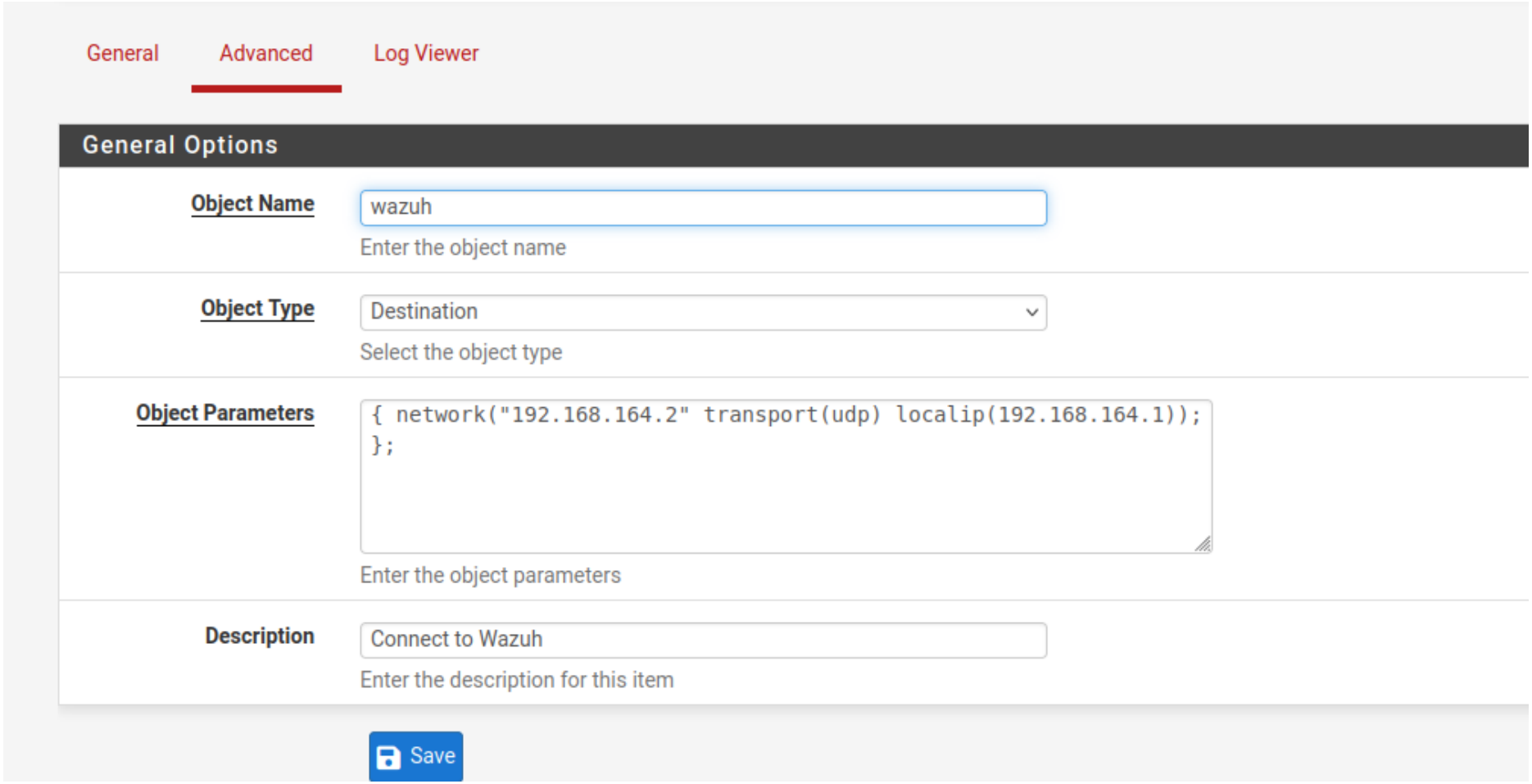




Enable and select LAN and loopback interfaces.

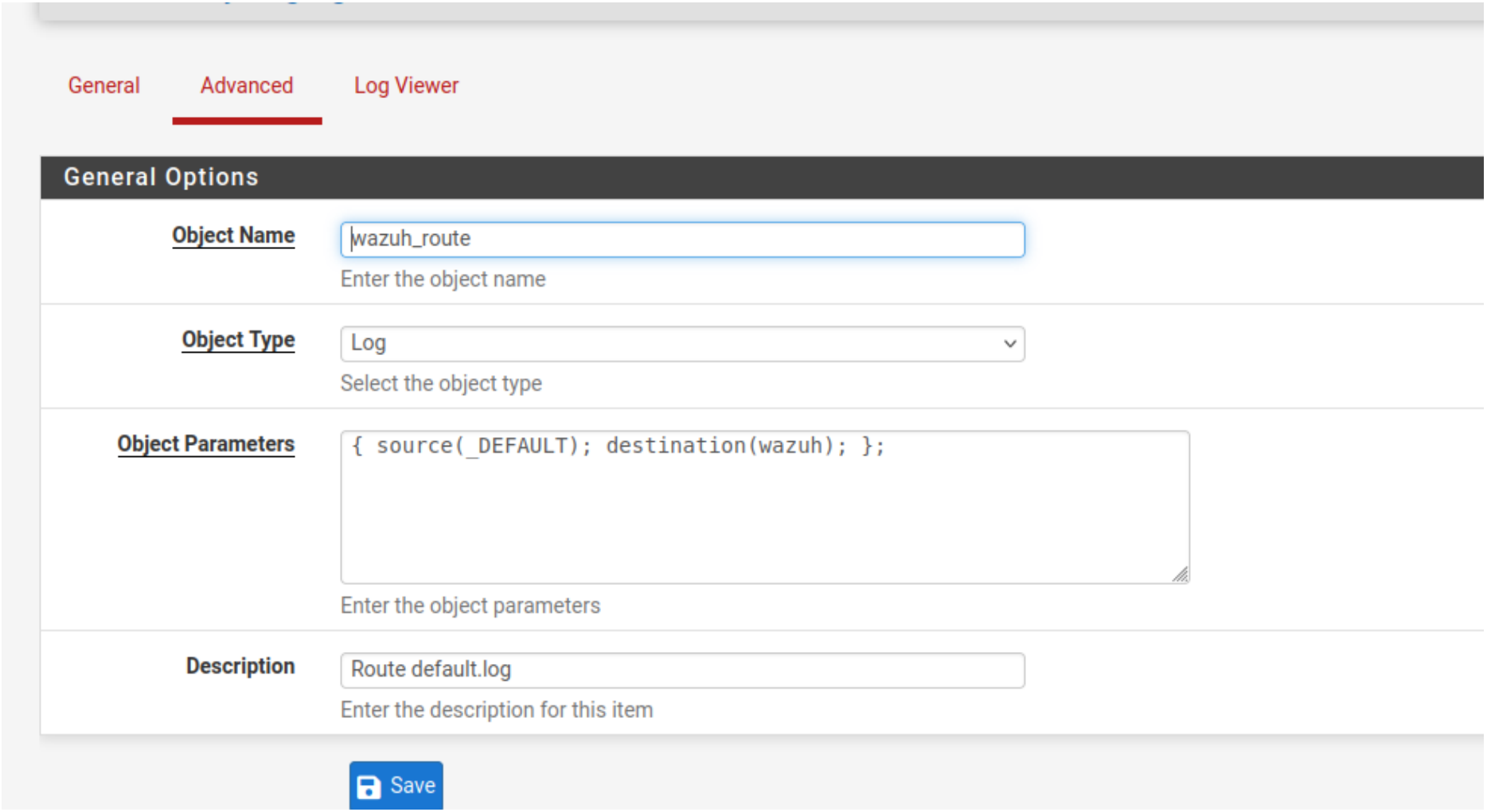


Enable remote logging from log settings and send to loopback address.

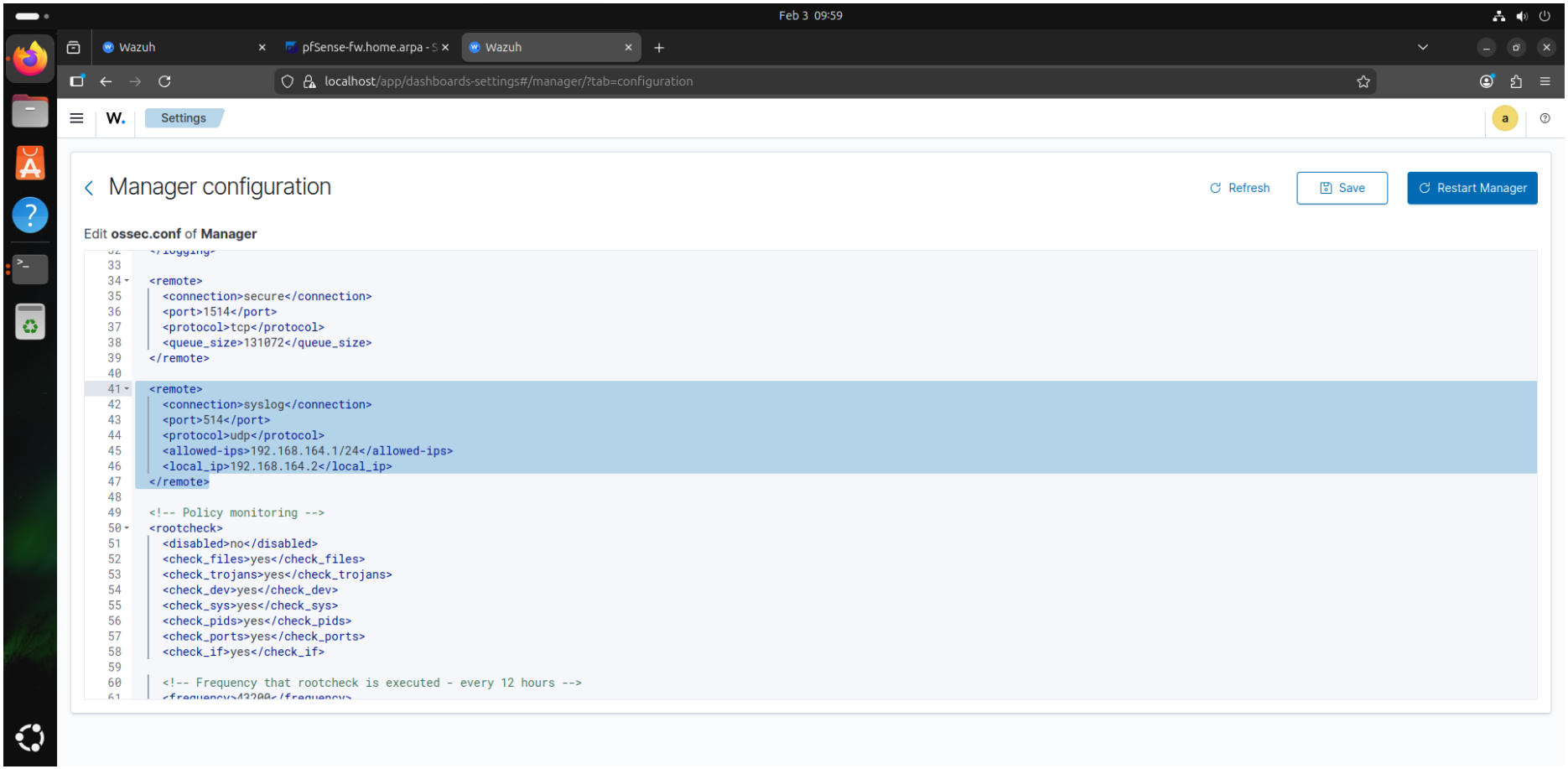


Create a destination config like this.

Then route the default logs to this destination.



In Wazuh configuration, add a UDP listener for port 514



And restart manager.

The logs are automatically decoder by preexisting decoders and rules. The alerts can now be seen in Wazuh.