

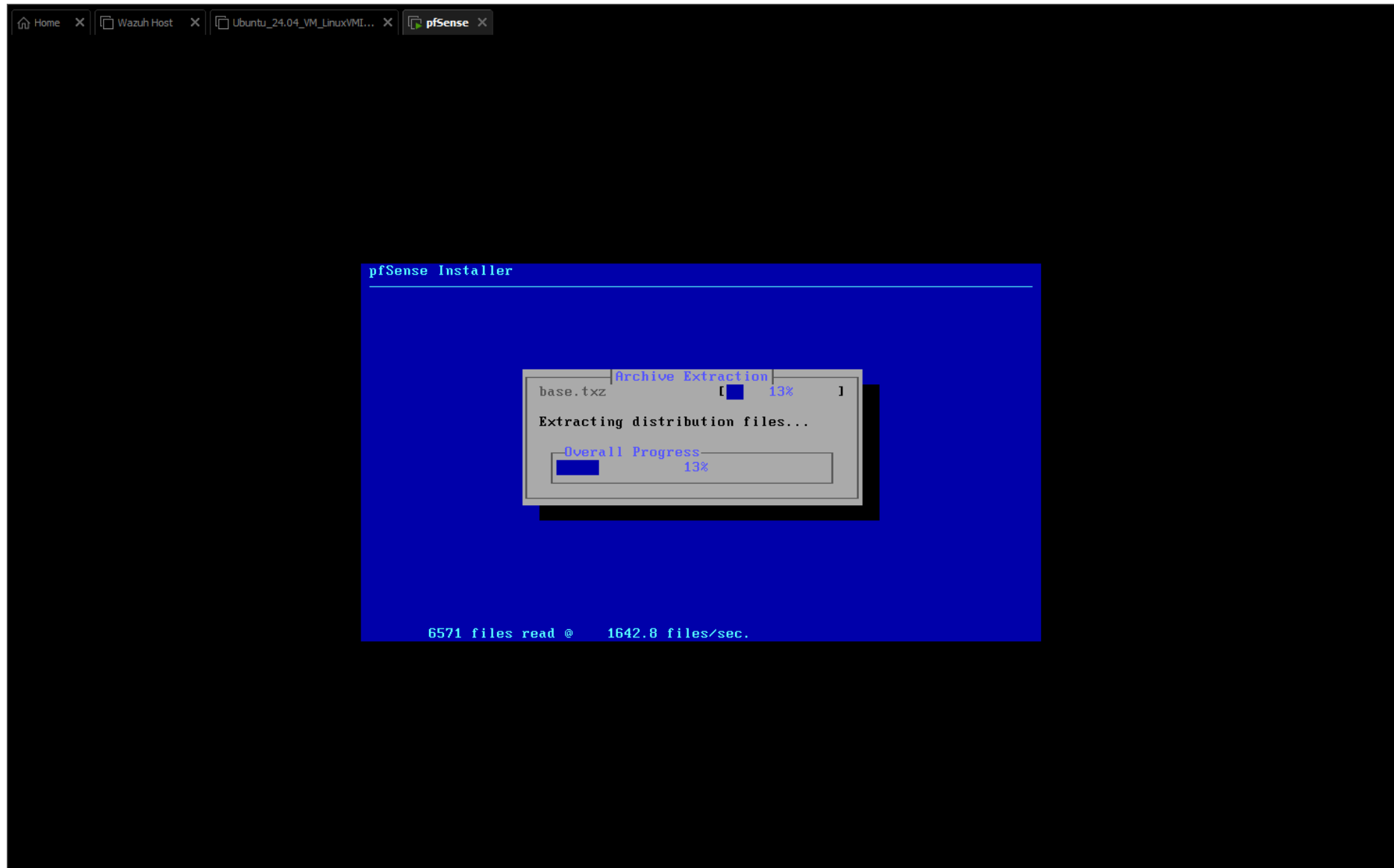
pfSense Installation

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



```

LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 1

Valid interfaces are:

em0      00:0c:29:18:0c:79   (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:18:0c:83   (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? █

```

This is initial config.

I set up the VMWare virtual network like this:

<i>VM</i>	<i>OS</i>	<i>Role</i>	<i>Network</i>
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

The IPv4 LAN address has been set to dhcp

The IPv6 LAN address has been set to dhcp6

Press <ENTER> to continue.

VMware Virtual Machine - Netgate Device ID: 17fe1f5afb2170108060

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)	-> em0	-> v4/DHCP4: 192.168.170.132/24
LAN (lan)	-> em1	-> v4/DHCP4: 192.168.164.130/24

- | | |
|-----------------------------------|----------------------------------|
| 0) Logout (SSH only) | 9) pfTop |
| 1) Assign Interfaces | 10) Filter Logs |
| 2) Set interface(s) IP address | 11) Restart webConfigurator |
| 3) Reset webConfigurator password | 12) PHP shell + pfSense tools |
| 4) Reset to factory defaults | 13) Update from console |
| 5) Reboot system | 14) Enable Secure Shell (sshd) |
| 6) Halt system | 15) Restore recent configuration |
| 7) Ping host | 16) Restart PHP-FPM |
| 8) Shell | |

Enter an option: █

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

```

pfSense x
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

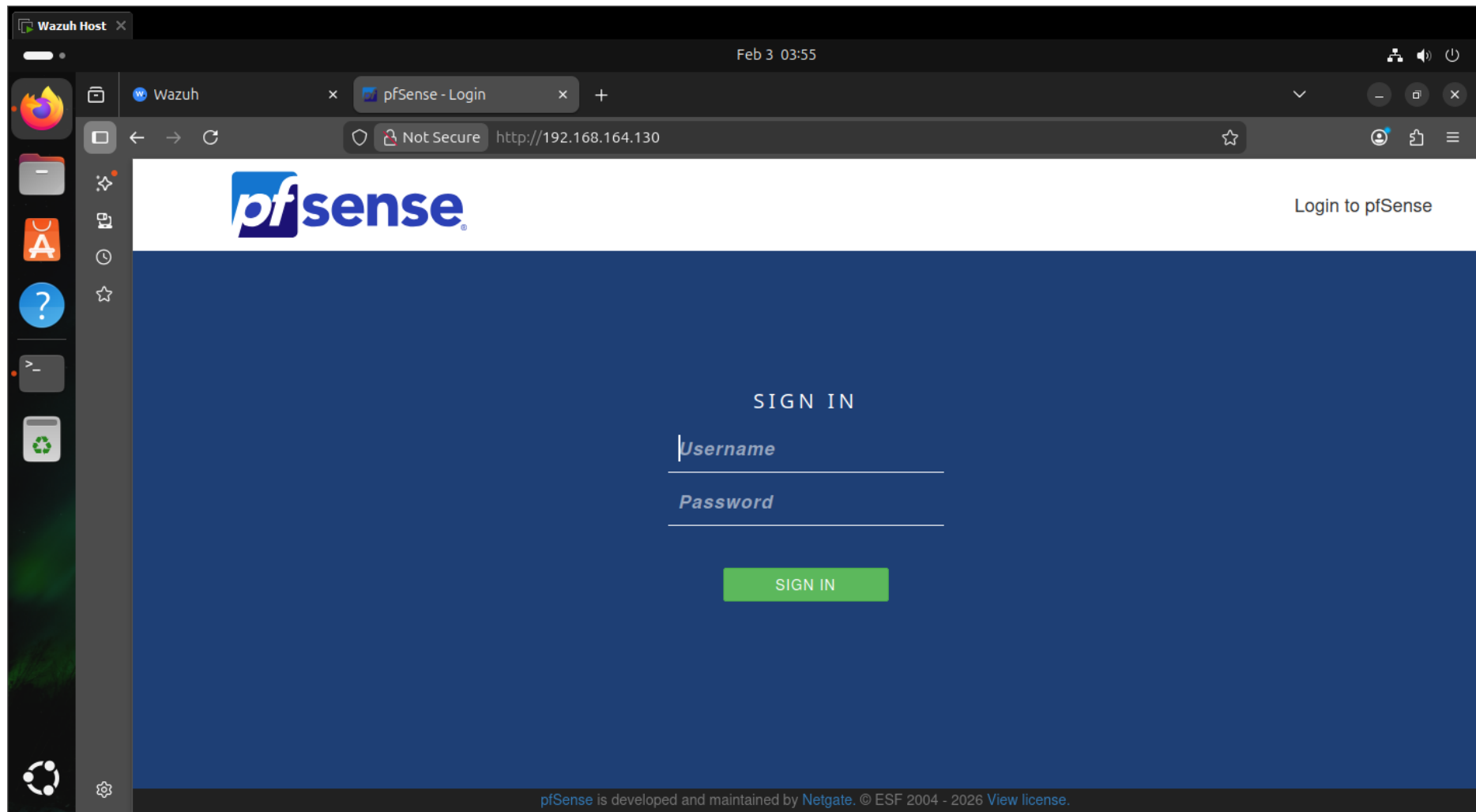
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

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: x

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 05:51

pfSense-fw.home.arpa - F

Not Secure

http://192.168.164.1/firewall_rules_edit.php?id=0

Action

Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☒ Invert match

Address or Alias

192.168.164.2

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

Address or Alias

192.168.164.1

Wazuh Host

Feb 3 05:52

pfSense-fw.home.arpa - S x

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.

Wazuh Host

Feb 3 05:57

pfSense-fw.home.arpa - 5 x

+

Not Secure http://192.168.164.1/services_unbound.php

If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in "tun" mode. The domain in [System: General Setup](#) should also be set to the proper value.

Display Custom Options

Hide Custom Options

Custom options

```
server:  
local-zone: "facebook.com" redirect  
local-data: "facebook.com A 127.0.0.1"
```

Enter any additional configuration parameters to add to the DNS Resolver configuration here, separated by a newline.

Save

Host Overrides

Host	Parent domain of host	IP to return for host	Description	Actions
------	-----------------------	-----------------------	-------------	---------

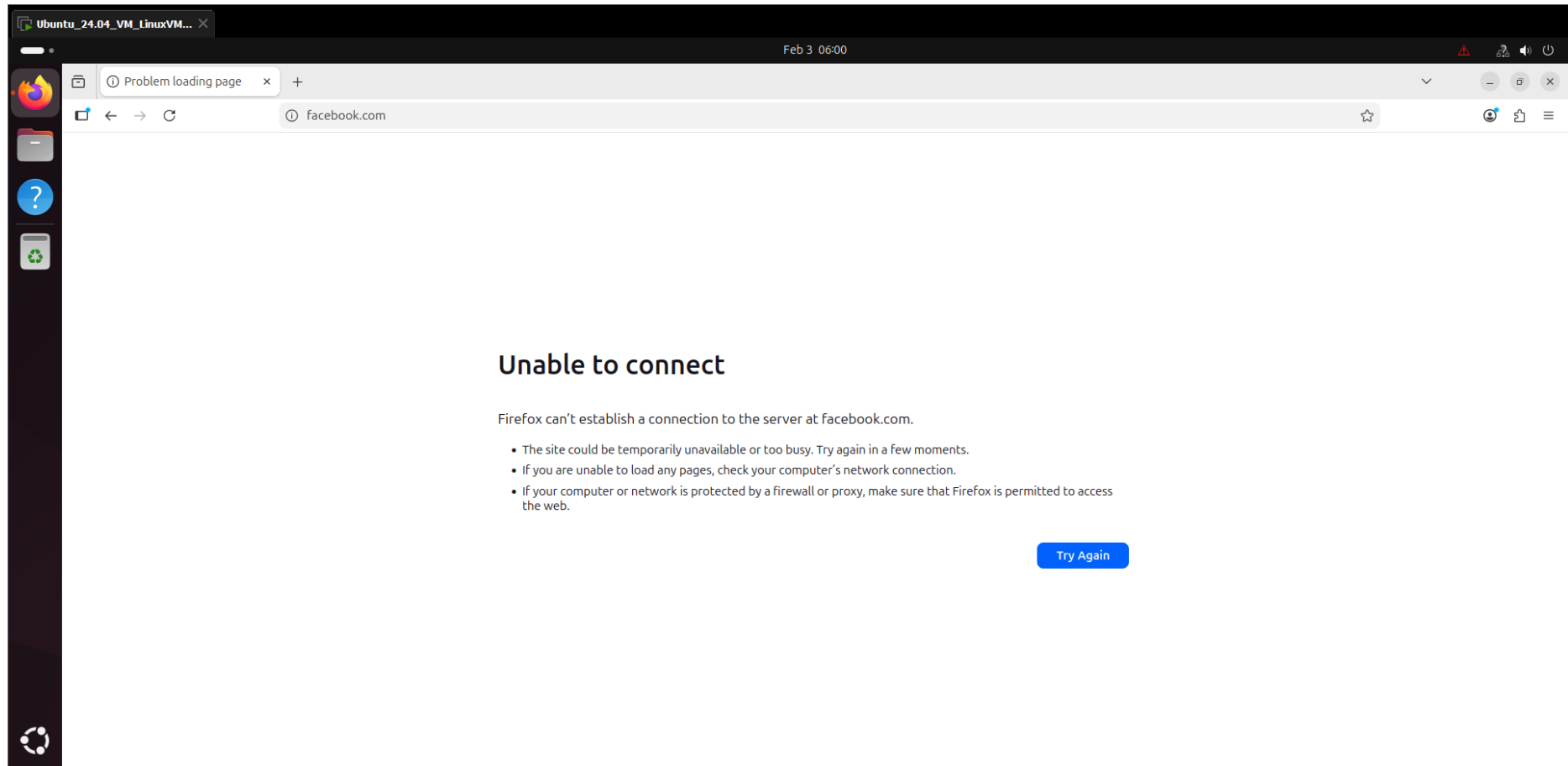
Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.

Add

Domain Overrides

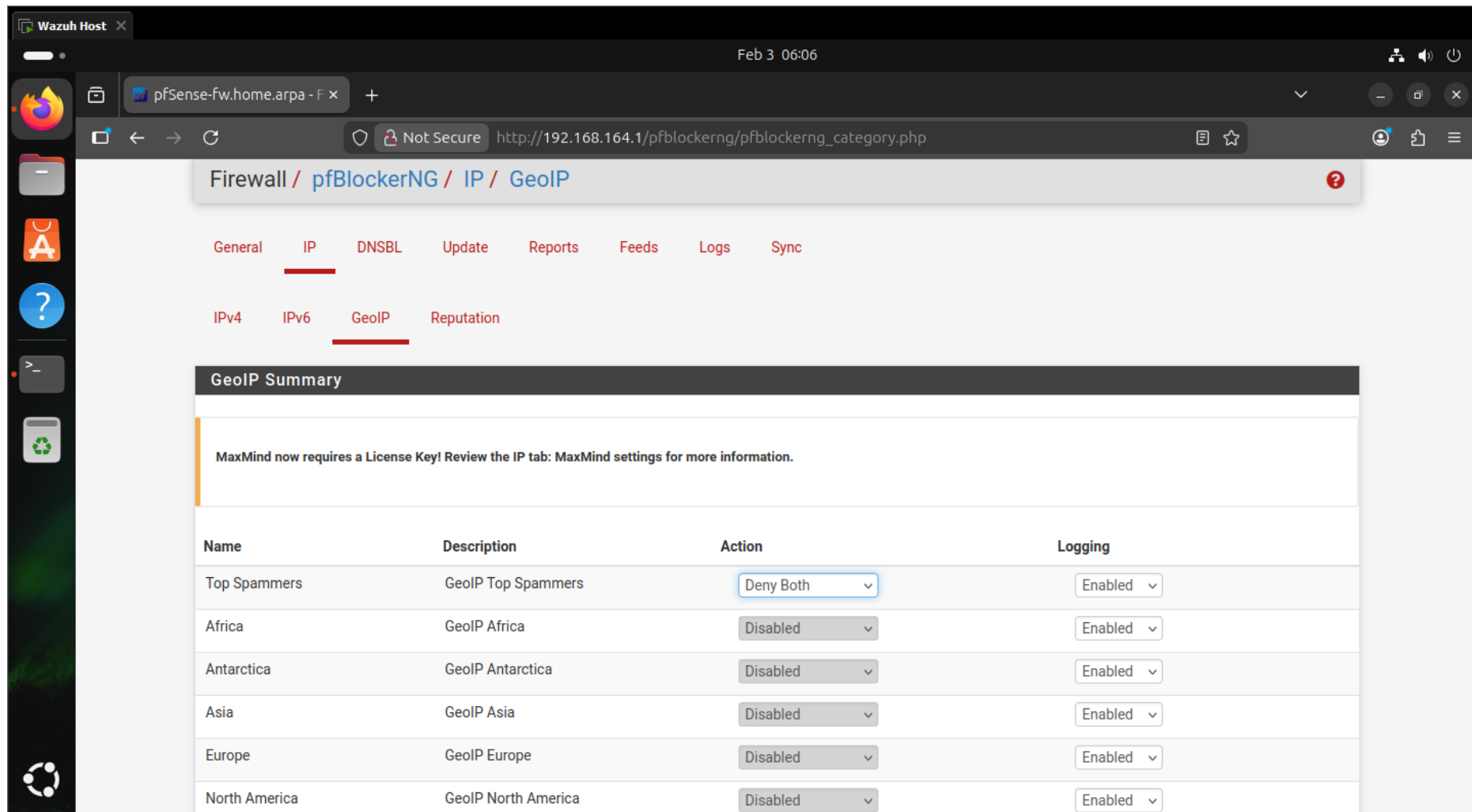
Domain	Lookup Server IP Address	Description	Actions
--------	--------------------------	-------------	---------

Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is



Block Specific Countries

I used pfBlockerNG plugin to geo block IPs.

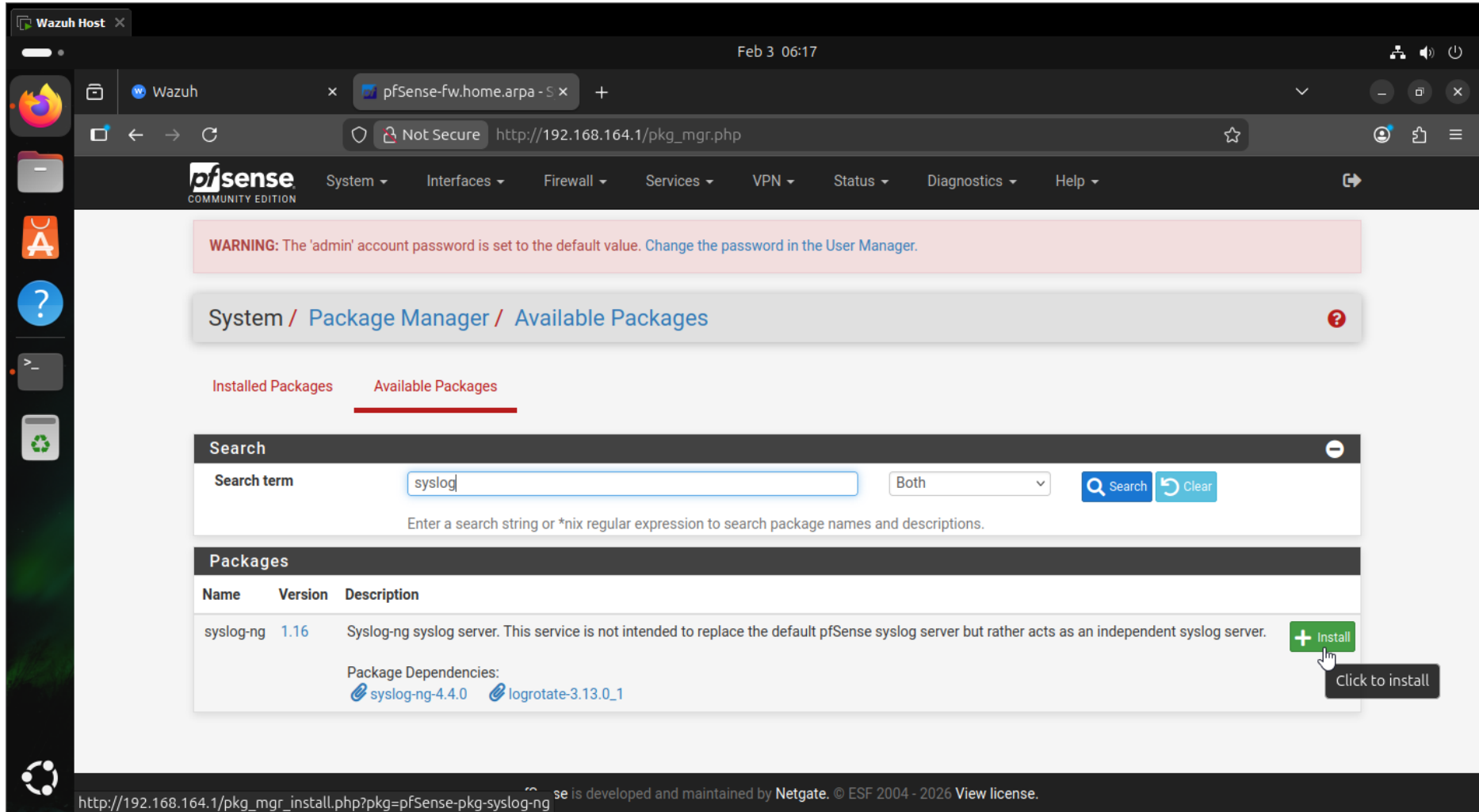


The screenshot shows the pfSense web interface for the pfBlockerNG plugin. The browser address bar indicates the URL `http://192.168.164.1/pfblockerng/pfblockerng_category.php`. The breadcrumb trail is `Firewall / pfBlockerNG / IP / GeoIP`. The `IP` tab is selected, and within it, the `GeoIP` sub-tab is active. A message states: "MaxMind now requires a License Key! Review the IP tab: MaxMind settings for more information."

Name	Description	Action	Logging
Top Spammers	GeoIP Top Spammers	Deny Both	Enabled
Africa	GeoIP Africa	Disabled	Enabled
Antarctica	GeoIP Antarctica	Disabled	Enabled
Asia	GeoIP Asia	Disabled	Enabled
Europe	GeoIP Europe	Disabled	Enabled
North America	GeoIP North America	Disabled	Enabled

Connecting with Wazuh

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



The screenshot shows the pfSense Community Edition web interface. The browser address bar displays `http://192.168.164.1/pkg_mgr.php`. The page title is "System / Package Manager / Available Packages". A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below the breadcrumb, there are tabs for "Installed Packages" and "Available Packages". The "Available Packages" tab is selected. A search bar contains the text "syslog". Below the search bar, a table lists available packages:

Name	Version	Description	Action
syslog-ng	1.16	Syslog-ng syslog server. This service is not intended to replace the default pfSense syslog server but rather acts as an independent syslog server. Package Dependencies: syslog-ng-4.4.0 logrotate-3.13.0_1	+ Install

A tooltip "Click to install" appears over the "+ Install" button. The footer of the page shows the URL `http://192.168.164.1/pkg_mgr_install.php?pkg=pfSense-pkg-syslog-ng` and a copyright notice: "se is developed and maintained by Netgate. © ESF 2004 - 2026 View license."

Feb 3 09:56

Wazuh x pfSense-fw.home.arpa - f x +

Not Secure http://192.168.164.1/pkg_edit.php?xml=syslog-ng.xml&id=0

pfSense
COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Package / Services: Syslog-ng / General

General Advanced Log Viewer

General Options

Enable ☒ Select this option to enable syslog-ng

Interface Selection

LAN
WAN
loopback

Select interfaces you want to listen on

Default Protocol UDP

Select the default protocol you want to listen on

CA

Select Certificate Authority for TLS protocol.
You can use it in your object definition as ca-dir(/var/etc/syslog-ng/ca.d) option of tls().

Certificate GUI default (6981b4d3ce9f2)

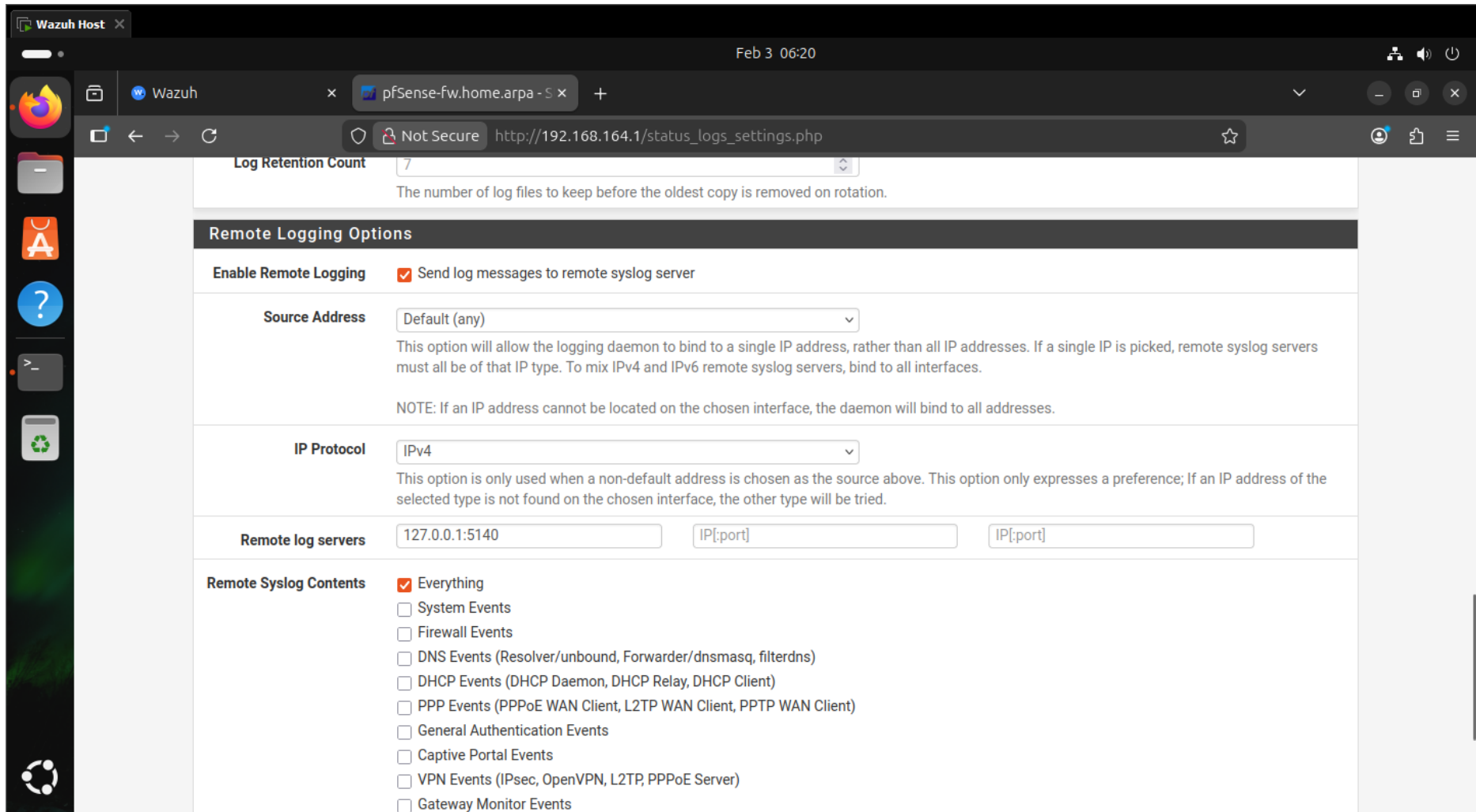
Select server certificate for TLS protocol.
You can use it in your object definition as key-file(/var/etc/syslog-ng/syslog-ng.key) and cert-file(/var/etc/syslog-ng/syslog-ng.cert) options of tls().

Default Port 5140

Enter default port number you want to listen on

Default Log Directory /var/syslog-ng

Enable and select LAN and loopback interfaces.



The screenshot shows a terminal window titled "Wazuh Host" with a browser displaying the pfSense configuration page for log retention and remote logging. The browser address bar shows "http://192.168.164.1/status_logs_settings.php".

Log Retention Count is set to 7. The description states: "The number of log files to keep before the oldest copy is removed on rotation."

Remote Logging Options

- Enable Remote Logging** is checked. The description says: "Send log messages to remote syslog server".
- Source Address** is set to "Default (any)". The description states: "This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces. NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses."
- IP Protocol** is set to "IPv4". The description states: "This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried."
- Remote log servers** are listed as "127.0.0.1:5140", "IP[:port]", and "IP[:port]".
- Remote Syslog Contents** are selected:
 - ☒ Everything
 - ☐ System Events
 - ☐ Firewall Events
 - ☐ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
 - ☐ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
 - ☐ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)
 - ☐ General Authentication Events
 - ☐ Captive Portal Events
 - ☐ VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)
 - ☐ Gateway Monitor Events

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

General

Advanced

Log Viewer

General Options

Object Name

wazuh

Enter the object name

Object Type

Destination

Select the object type

Object Parameters

```
{ network("192.168.164.2" transport(udp) localip(192.168.164.1));
};
```

Enter the object parameters

Description

Connect to Wazuh

Enter the description for this item

 Save

Create a destination config like this.

Then route the default logs to this destination.

General

Advanced

Log Viewer

General Options

Object Name

Enter the object name

Object Type

Select the object type

Object Parameters

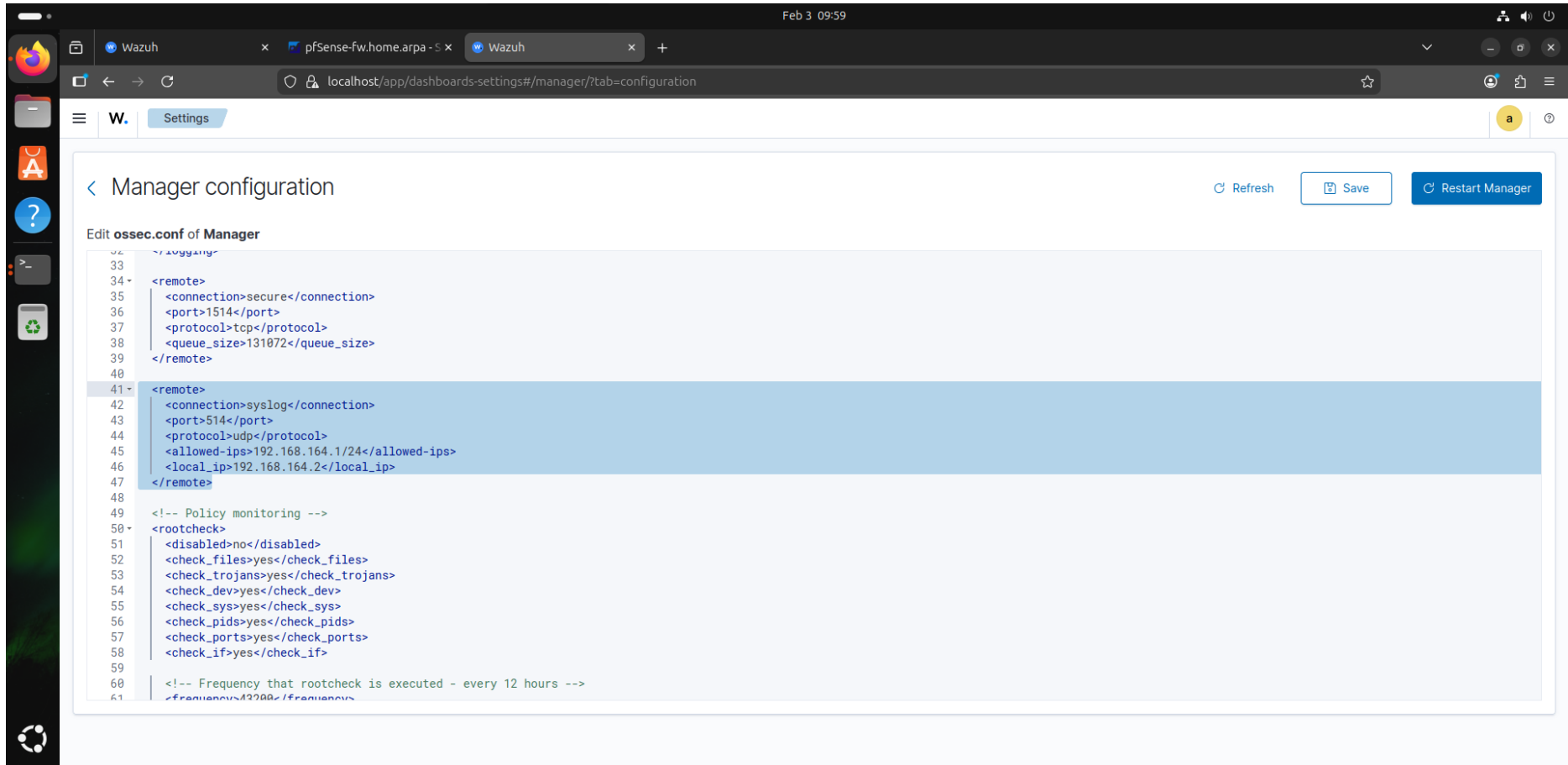
Enter the object parameters

Description

Enter the description for this item

 Save

In Wazuh configuration, add a UDP listener for port 514



The screenshot shows a web browser window with the Wazuh Manager configuration page. The browser's address bar shows the URL `localhost/app/dashboards-settings#/manager/?tab=configuration`. The page title is "Manager configuration". In the top right corner, there are three buttons: "Refresh", "Save", and "Restart Manager". The main content area is titled "Edit ossec.conf of Manager" and displays a configuration file with the following XML content:

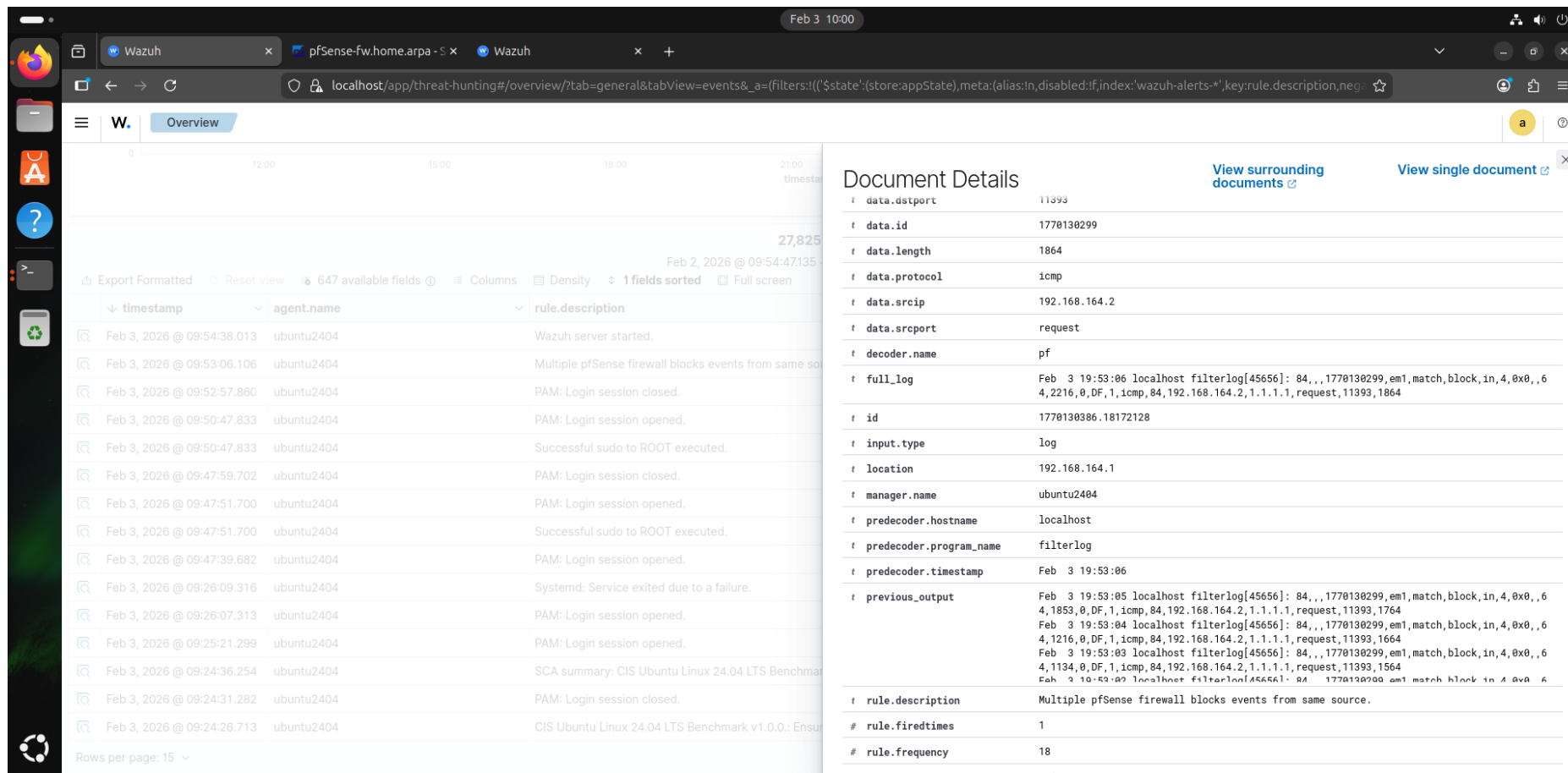
```

32 <!-- Logging -->
33 <!--
34 <remote>
35   <connection>secure</connection>
36   <port>1514</port>
37   <protocol>tcp</protocol>
38   <queue_size>131072</queue_size>
39 </remote>
40
41 <remote>
42   <connection>syslog</connection>
43   <port>514</port>
44   <protocol>udp</protocol>
45   <allowed_ips>192.168.164.1/24</allowed_ips>
46   <local_ip>192.168.164.2</local_ip>
47 </remote>
48
49 <!-- Policy monitoring -->
50 <rootcheck>
51   <disabled>no</disabled>
52   <check_files>yes</check_files>
53   <check_trojans>yes</check_trojans>
54   <check_dev>yes</check_dev>
55   <check_sys>yes</check_sys>
56   <check_pids>yes</check_pids>
57   <check_ports>yes</check_ports>
58   <check_if>yes</check_if>
59
60 <!-- Frequency that rootcheck is executed - every 12 hours -->
61 <frequency>43200</frequency>

```

And restart manager.

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



The screenshot displays the Wazuh web interface. The left sidebar shows the navigation menu with options like Overview, Alerts, and Settings. The main content area is divided into two panels. The left panel shows a list of alerts with columns for timestamp, agent.name, and rule.description. The right panel shows the 'Document Details' for a selected alert, including fields like data.dstport, data.id, data.length, data.protocol, data.srcip, data.srcport, decoder.name, full_log, id, input.type, location, manager.name, predecoder.hostname, predecoder.program_name, predecoder.timestamp, and previous_output.

timestamp	agent.name	rule.description
Feb 3, 2026 @ 09:54:38.013	ubuntu2404	Wazuh server started.
Feb 3, 2026 @ 09:53:06.106	ubuntu2404	Multiple pfSense firewall blocks events from same source.
Feb 3, 2026 @ 09:52:57.860	ubuntu2404	PAM: Login session closed.
Feb 3, 2026 @ 09:50:47.833	ubuntu2404	PAM: Login session opened.
Feb 3, 2026 @ 09:50:47.833	ubuntu2404	Successful sudo to ROOT executed.
Feb 3, 2026 @ 09:47:59.702	ubuntu2404	PAM: Login session closed.
Feb 3, 2026 @ 09:47:51.700	ubuntu2404	PAM: Login session opened.
Feb 3, 2026 @ 09:47:51.700	ubuntu2404	Successful sudo to ROOT executed.
Feb 3, 2026 @ 09:47:39.682	ubuntu2404	PAM: Login session opened.
Feb 3, 2026 @ 09:26:09.316	ubuntu2404	Systemd: Service exited due to a failure.
Feb 3, 2026 @ 09:26:07.313	ubuntu2404	PAM: Login session opened.
Feb 3, 2026 @ 09:25:21.299	ubuntu2404	PAM: Login session opened.
Feb 3, 2026 @ 09:24:36.254	ubuntu2404	SCA summary: CIS Ubuntu Linux 24.04 LTS Benchmark
Feb 3, 2026 @ 09:24:31.282	ubuntu2404	PAM: Login session closed.
Feb 3, 2026 @ 09:24:26.713	ubuntu2404	CIS Ubuntu Linux 24.04 LTS Benchmark v1.0.0: Ensure

Document Details

data.dstport	11393
data.id	1770130299
data.length	1864
data.protocol	icmp
data.srcip	192.168.164.2
data.srcport	request
decoder.name	pf
full_log	Feb 3 19:53:06 localhost filterlog[45656]: 84,,1770130299,em1,match,block,in,4,0x0,,6 4,2216,0,DF,1,icmp,84,192.168.164.2,1.1.1.1,request,11393,1864
id	1770130386.18172128
input.type	log
location	192.168.164.1
manager.name	ubuntu2404
predecoder.hostname	localhost
predecoder.program_name	filterlog
predecoder.timestamp	Feb 3 19:53:06
previous_output	Feb 3 19:53:05 localhost filterlog[45656]: 84,,1770130299,em1,match,block,in,4,0x0,,6 4,1853,0,DF,1,icmp,84,192.168.164.2,1.1.1.1,request,11393,1764 Feb 3 19:53:04 localhost filterlog[45656]: 84,,1770130299,em1,match,block,in,4,0x0,,6 4,1216,0,DF,1,icmp,84,192.168.164.2,1.1.1.1,request,11393,1664 Feb 3 19:53:03 localhost filterlog[45656]: 84,,1770130299,em1,match,block,in,4,0x0,,6 4,1134,0,DF,1,icmp,84,192.168.164.2,1.1.1.1,request,11393,1564 Feb 3 19:53:02 localhost filterlog[45656]: 84,,1770130299,em1,match,block,in,4,0x0,,6
rule.description	Multiple pfSense firewall blocks events from same source.
rule.firedtimes	1
rule.frequency	18