Lab 4: Adding a Snort IDS to pfSense

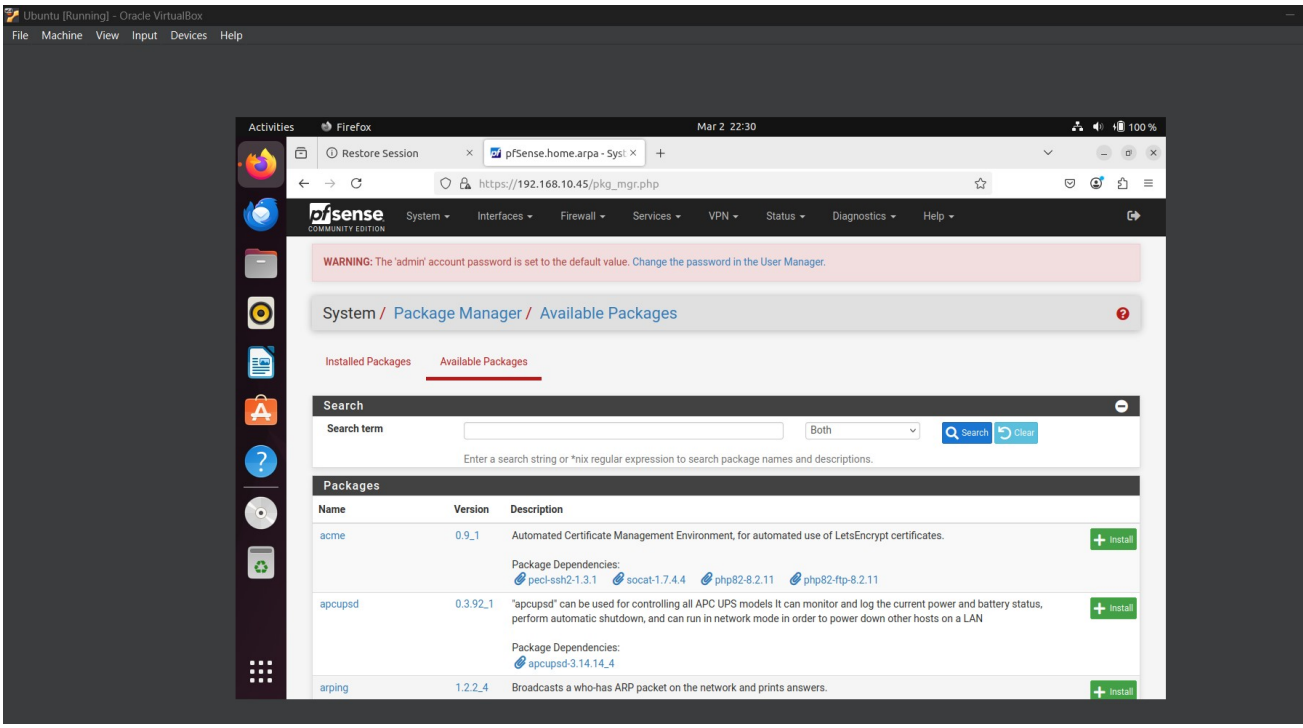
Objective 1: Installation and Initial Setup

Accessed the pfSense Web Portal

Opened a web browser and logged in to the pfSense web portal.

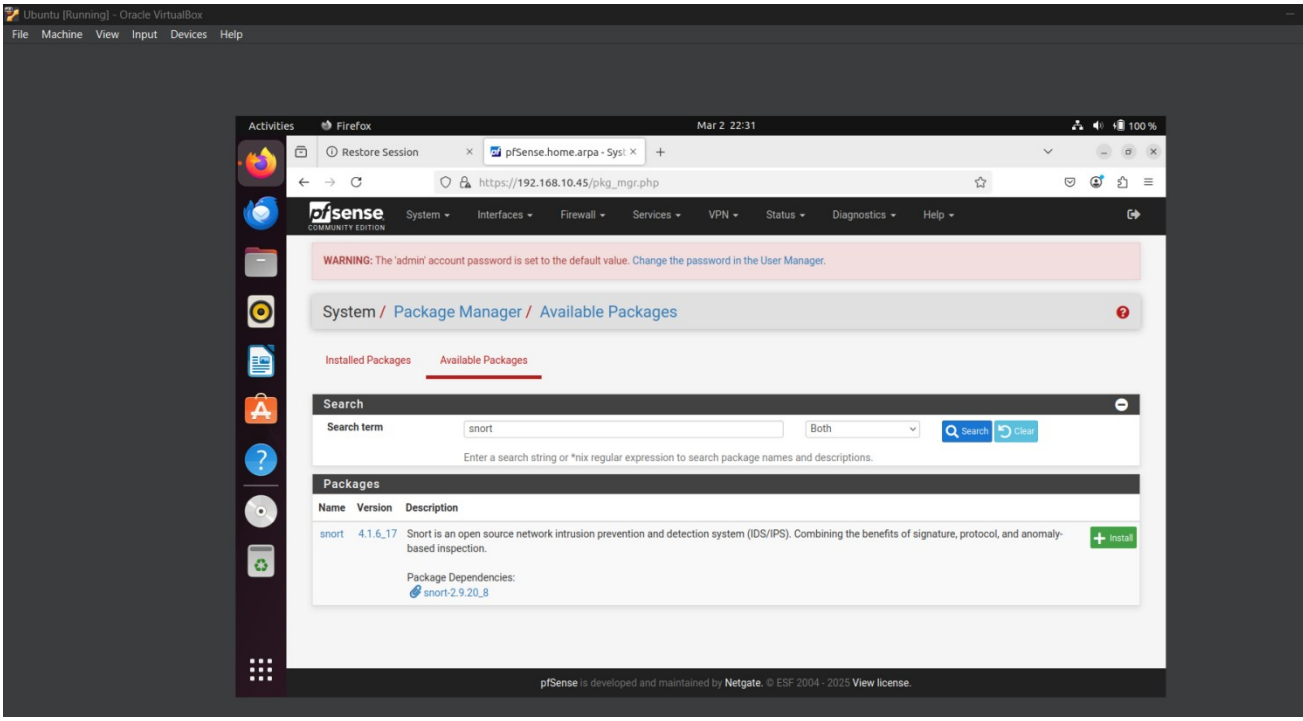
Navigated to the Package Manager

Went to *System* > *Package Manager*.

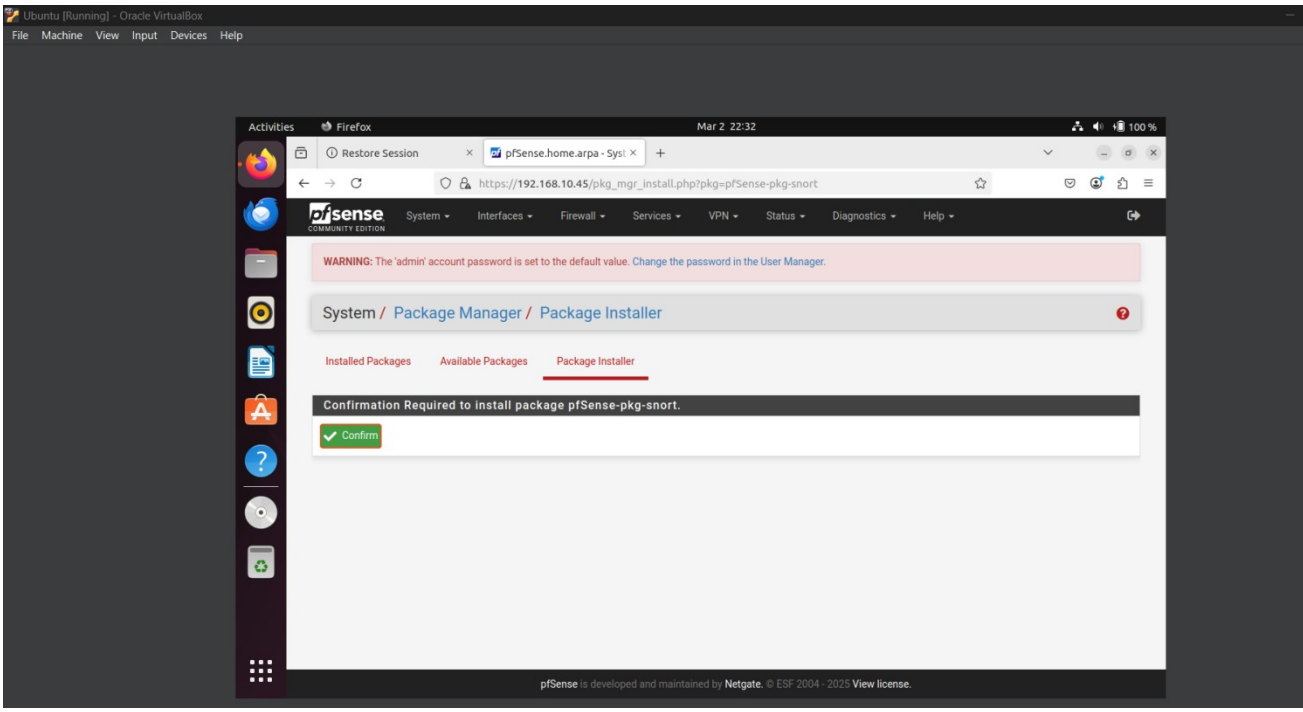


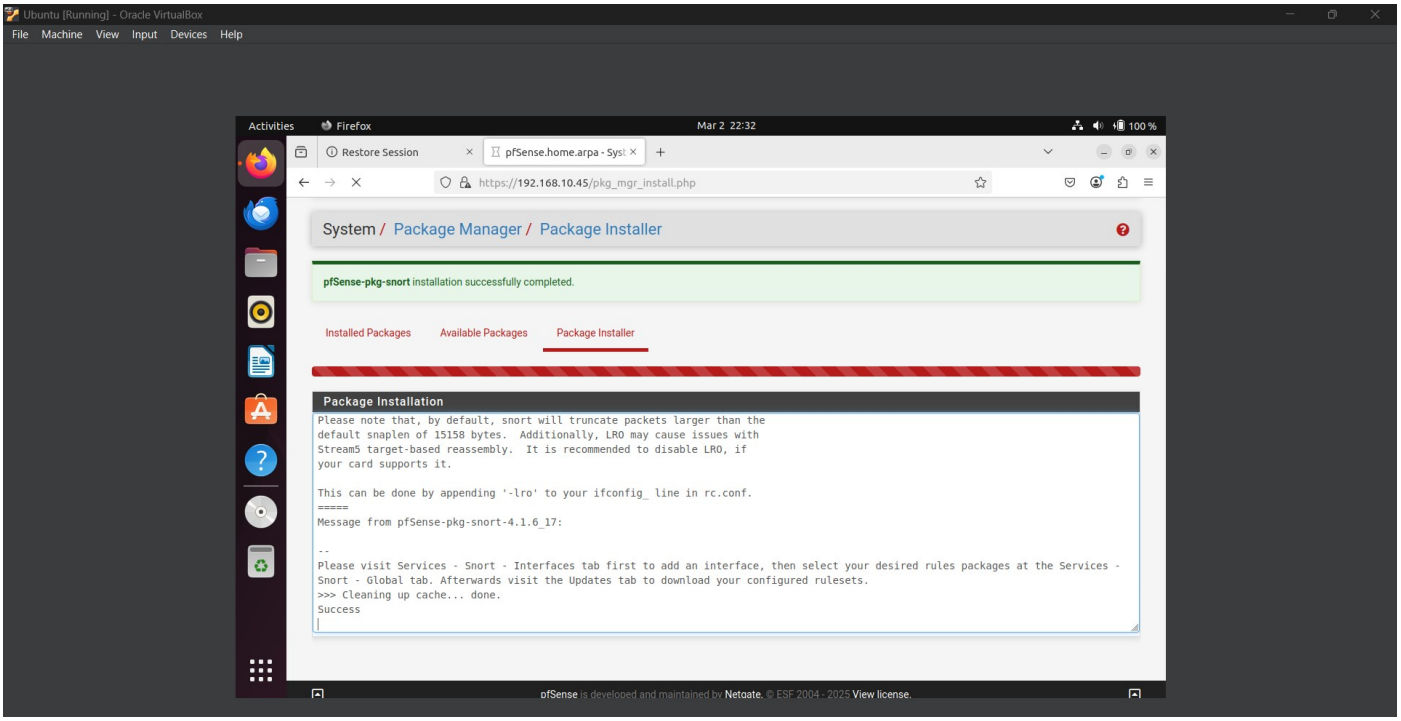
Installed the Snort Package

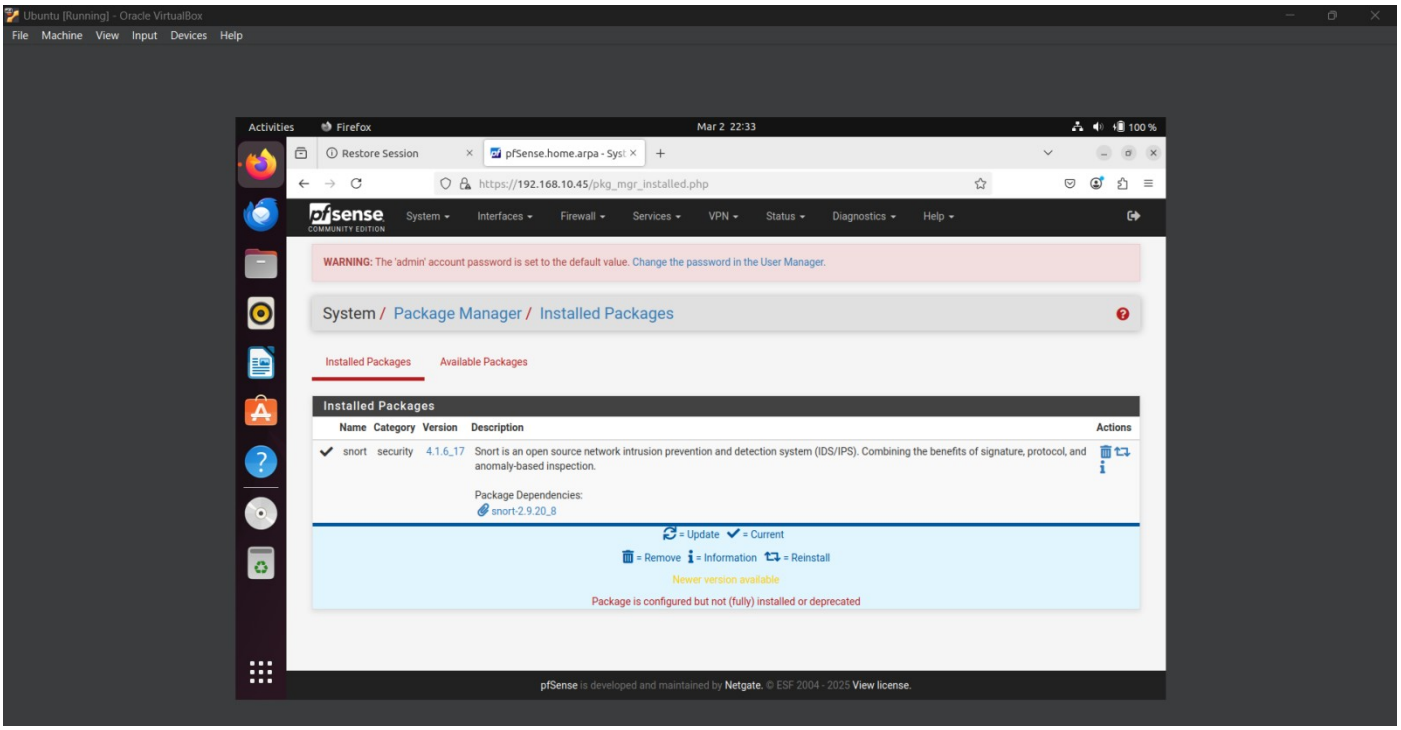
Clicked on the *Available Packages* tab and searched for Snort.



Clicked *Install* and confirmed to begin the installation process.

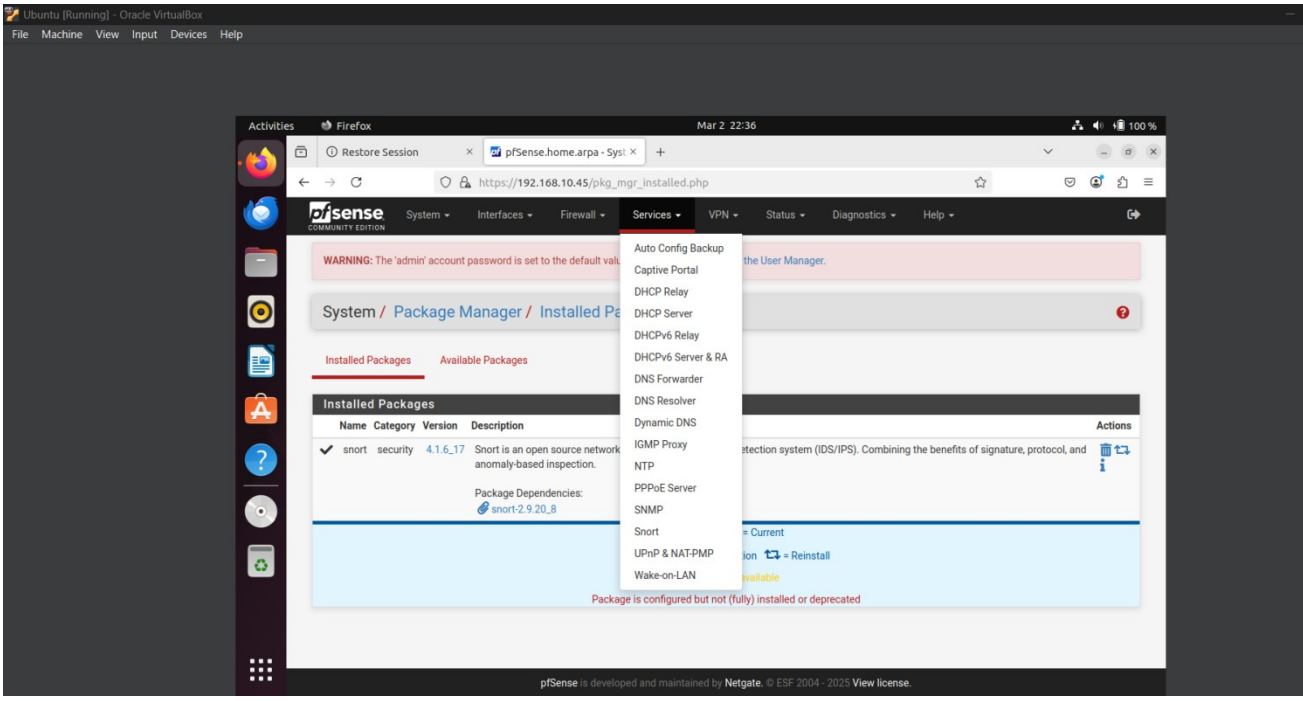






Configured Global Settings

Navigated to *Services* > *Snort* to access the *Snort Interfaces Configuration* page.



Switched to the *Global Settings* tab and configured the following:

Enabled Snort VRT by entering the Oinkmaster code from Security Onion.

Enabled Snort GPLv2.

Enabled ET Open.

Enabled OpenAppID.

Enabled AppID Open Text Rules.

Set the following:

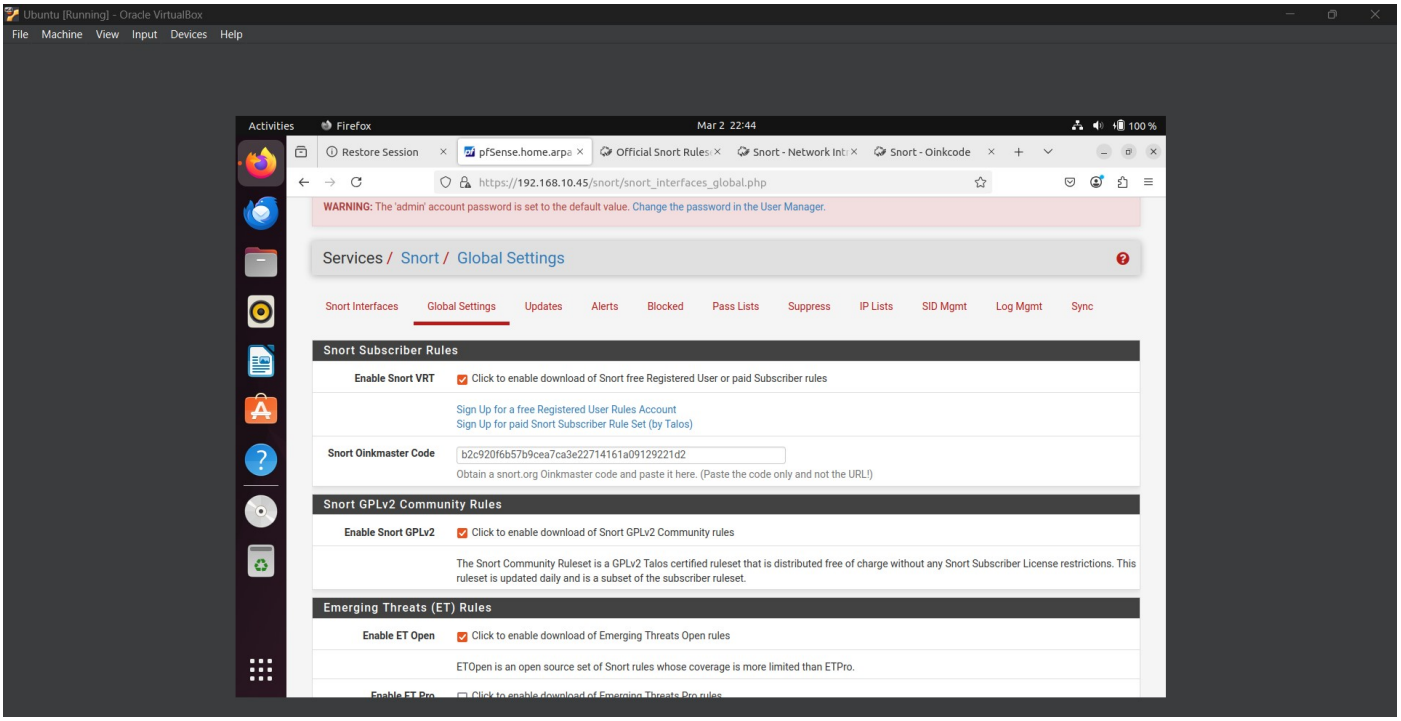
Update Interval: 12 HOURS.

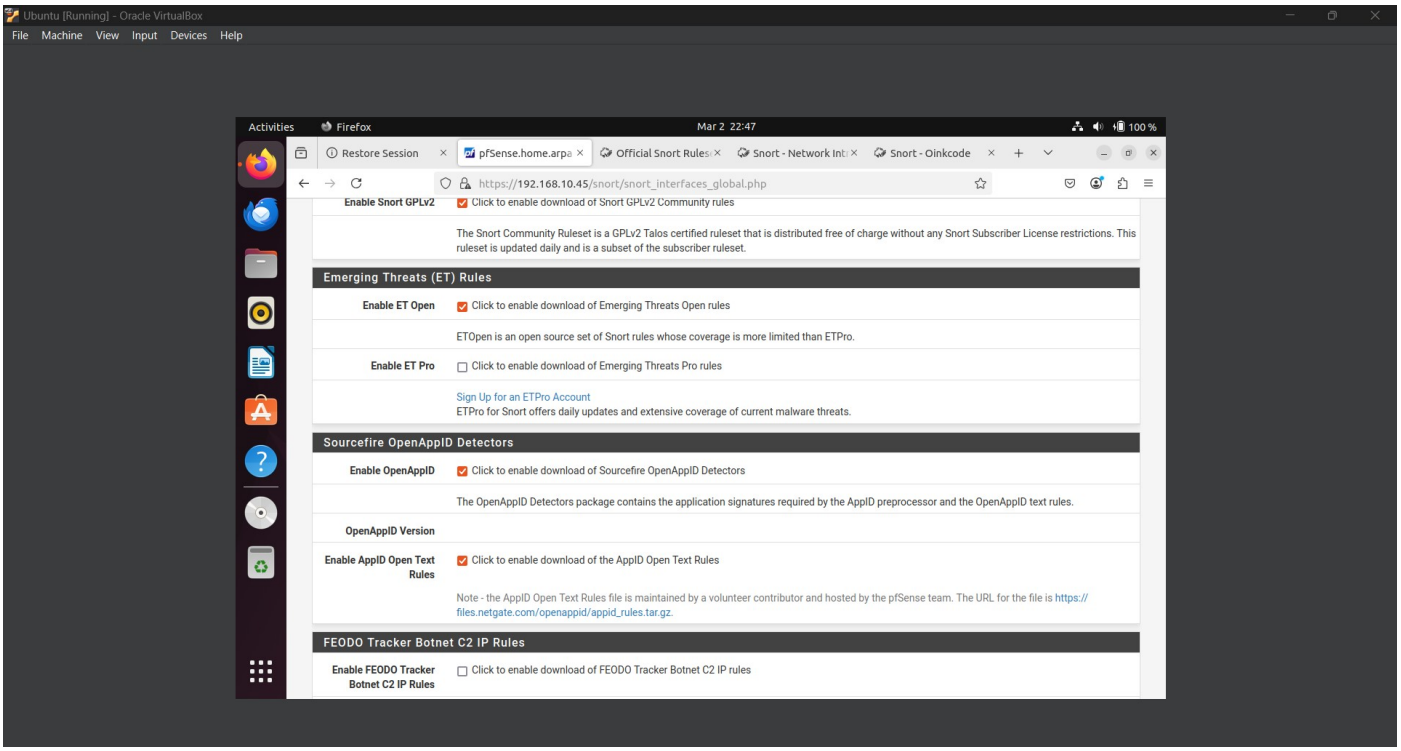
Update Start Time: 00:51.

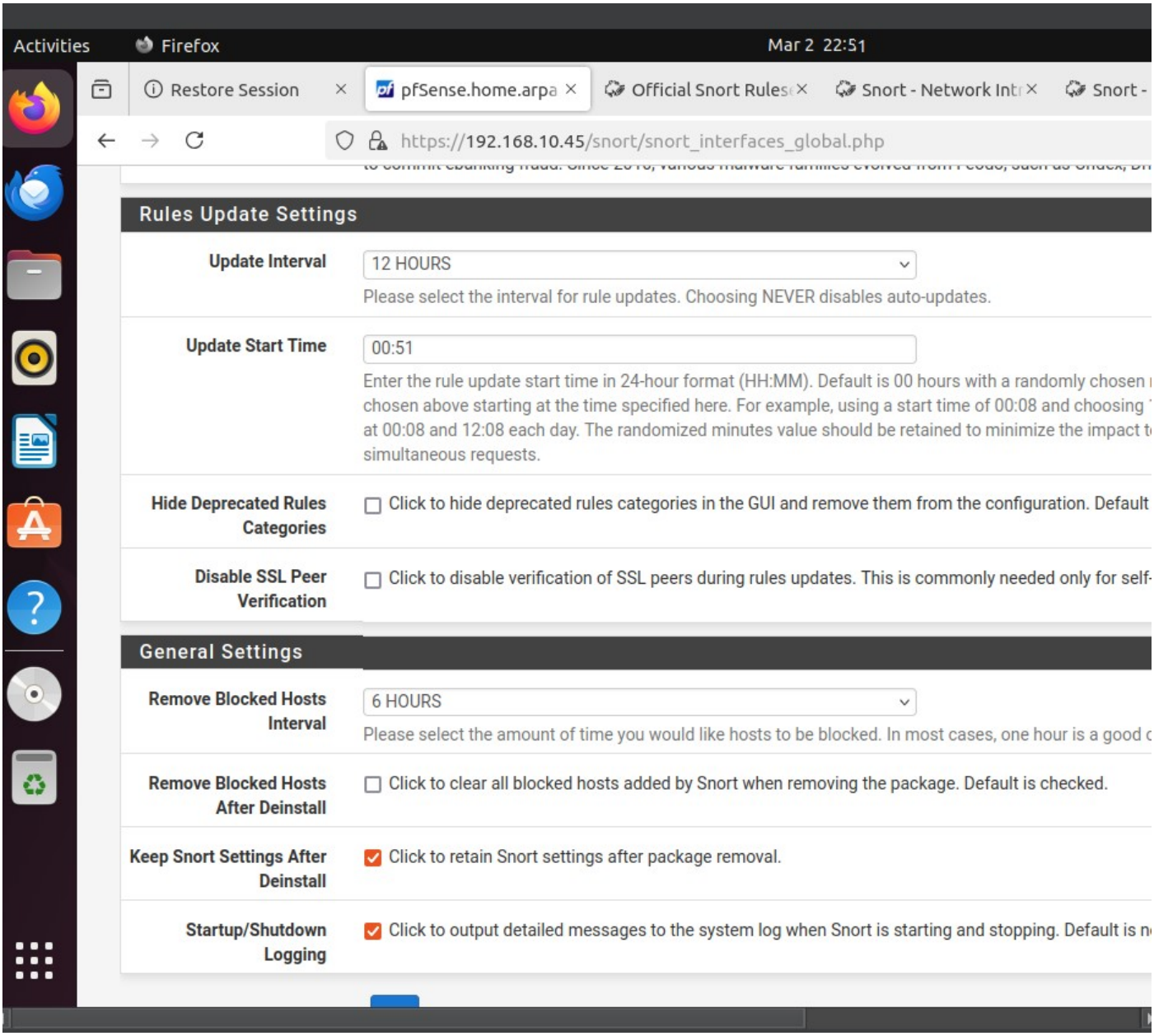
Remove Blocked Hosts Interval: 6 HOURS.

Enabled Startup/Shutdown Logging.

Clicked *Save* to apply these configurations.

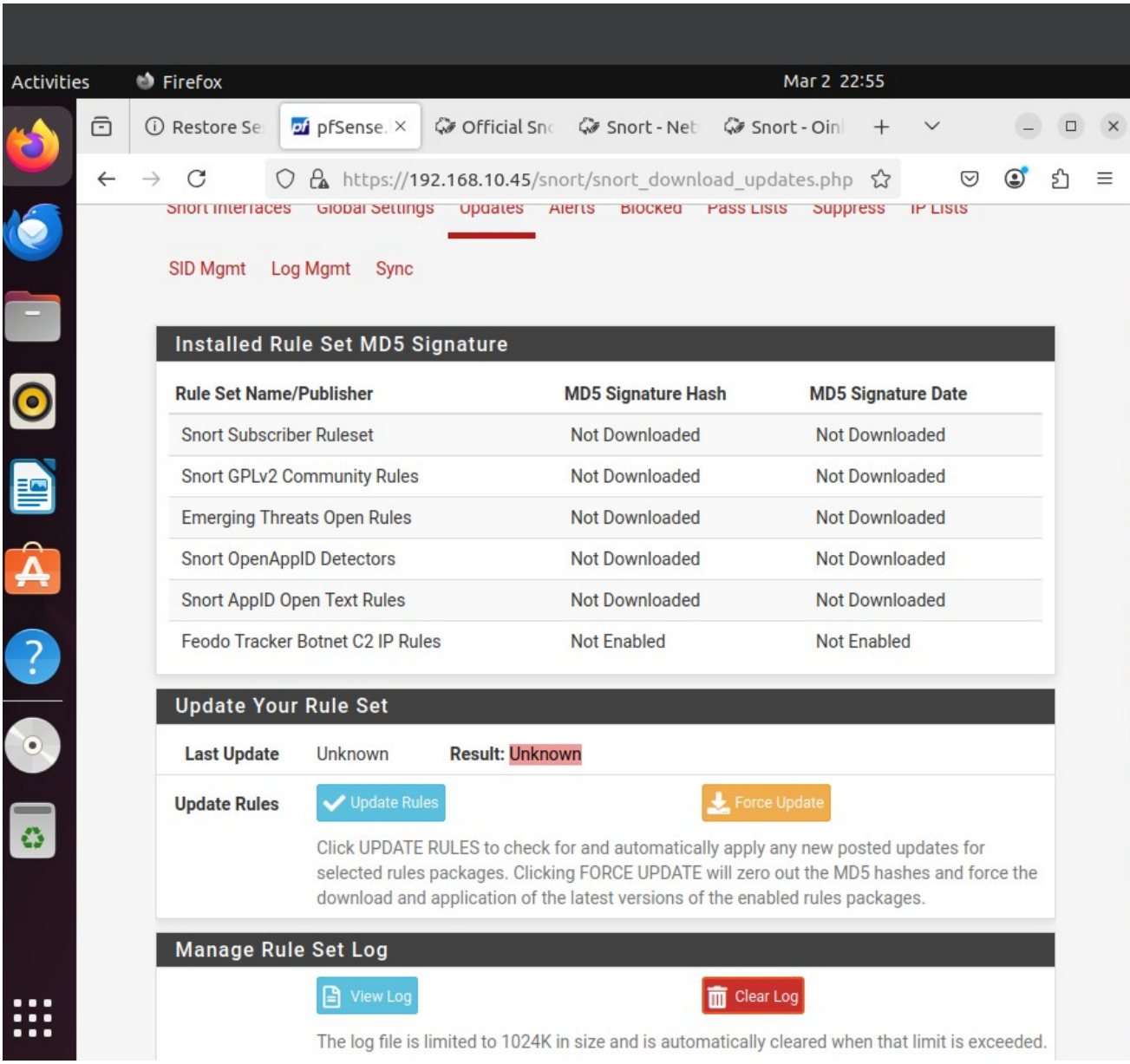

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox
Mar 2 22:44
100 %
Restore Session
pfSense.home.arpa
Official Snort Rules
Snort - Network Int
Snort - Oinkcode
https://192.168.10.45/snort/snort_interfaces_global.php
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Services / Snort / Global Settings
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Snort Subscriber Rules
Enable Snort VRT
Click to enable download of Snort free Registered User or paid Subscriber rules
Sign Up for a free Registered User Rules Account
Sign Up for paid Snort Subscriber Rule Set (by Talos)
Snort Oinkmaster Code
b2c920f6b57b9cea7ca3e22714161a09129221d2
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)
Snort GPLv2 Community Rules
Enable Snort GPLv2
Click to enable download of Snort GPLv2 Community rules
The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.
Emerging Threats (ET) Rules
Enable ET Open
Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

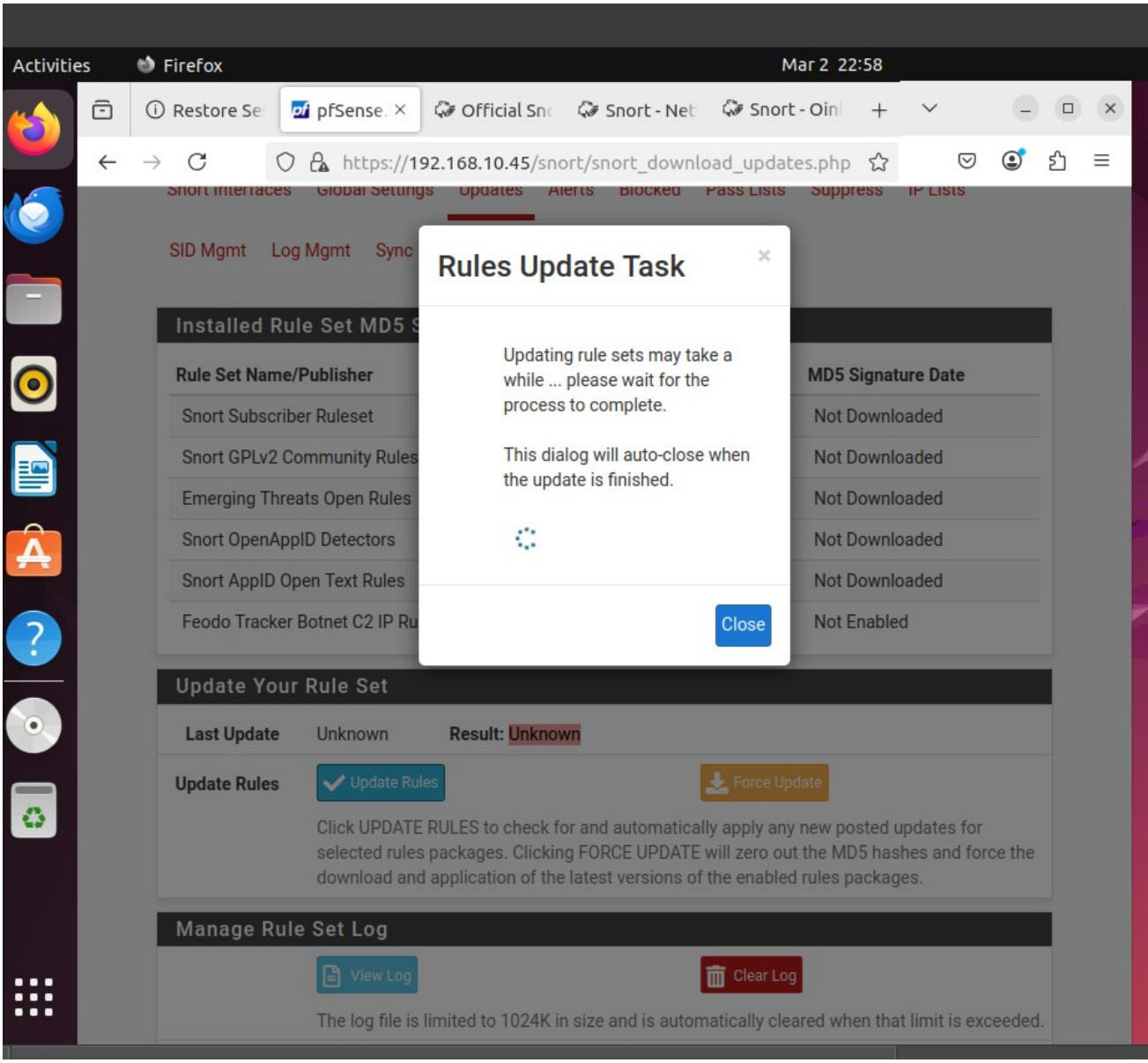

Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Firefox
Mar 2 22:47
100 %
Restore Session
pfSense.home.arpa
Official Snort Rules
Snort - Network Int
Snort - Oinkcode
https://192.168.10.45/snort/snort_interfaces_global.php
Enable Snort GPLv2
Click to enable download of Snort GPLv2 Community rules
The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.
Emerging Threats (ET) Rules
Enable ET Open
Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.
Enable ET Pro
Click to enable download of Emerging Threats Pro rules
Sign Up for an ETPro Account
ETPro for Snort offers daily updates and extensive coverage of current malware threats.
Sourcefire OpenAppID Detectors
Enable OpenAppID
Click to enable download of Sourcefire OpenAppID Detectors
The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.
OpenAppID Version
Enable AppID Open Text Rules
Click to enable download of the AppID Open Text Rules
Note - the AppID Open Text Rules file is maintained by a volunteer contributor and hosted by the pfSense team. The URL for the file is https://files.netgate.com/openappid/appid_rules.tar.gz.
FEODO Tracker Botnet C2 IP Rules
Enable FEODO Tracker Botnet C2 IP Rules
Click to enable download of FEODO Tracker Botnet C2 IP rules



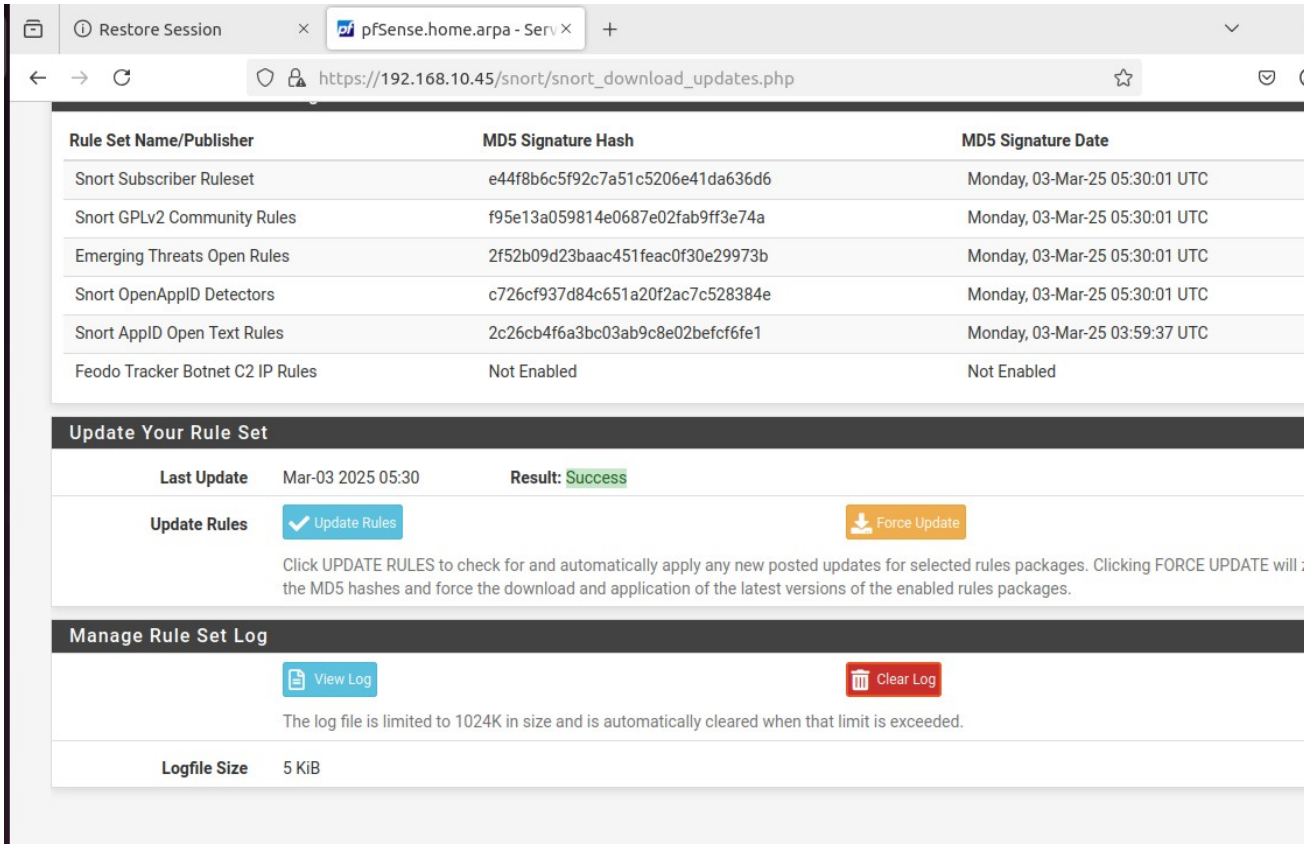
Forced Initial Rule Update

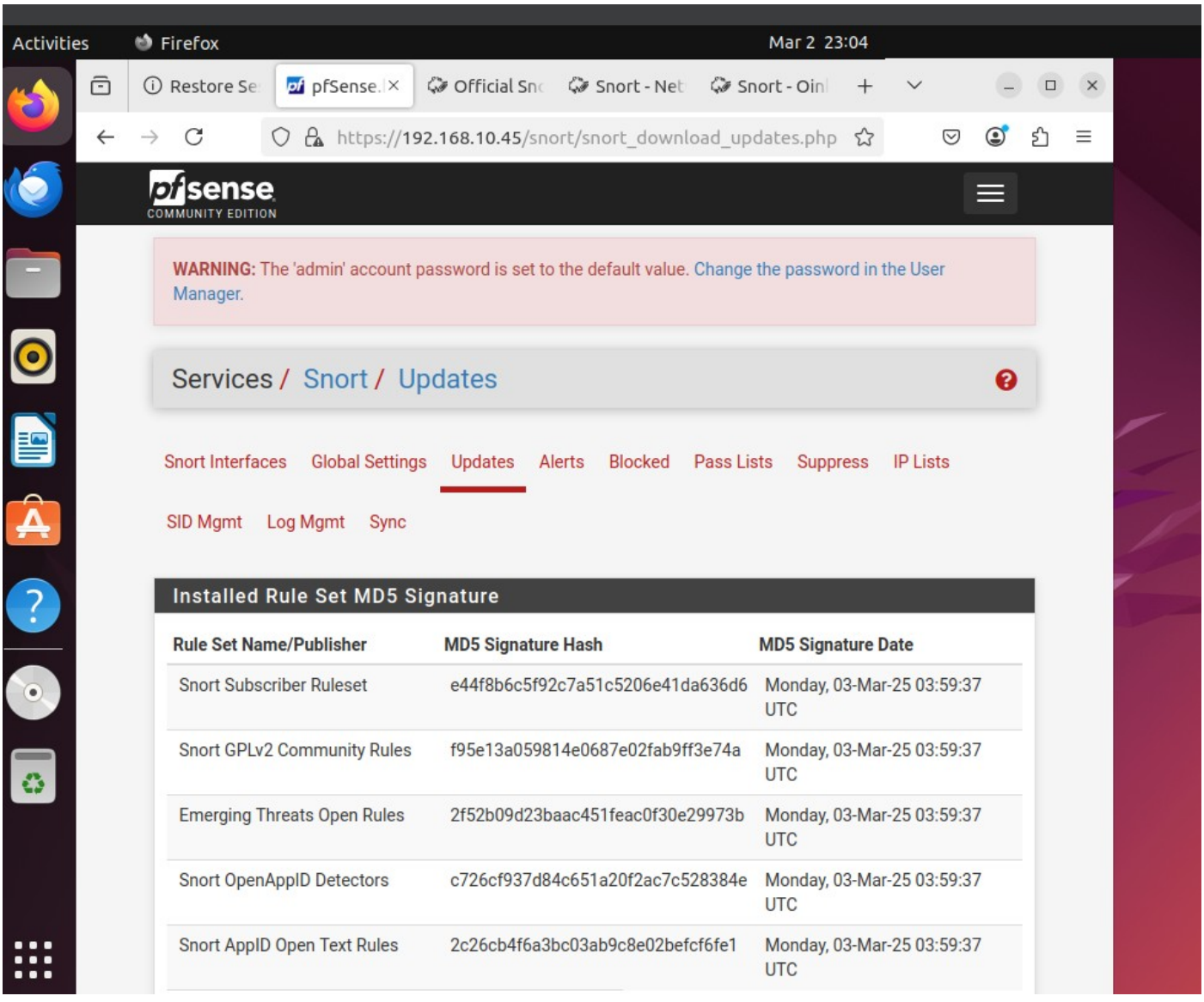
Switched to the *Updates* tab and clicked *Force Update* to start the initial rule update.


Activities
Firefox
Mar 2 22:55
Restore Se
pfSense.
Official Sn
Snort - Net
Snort - Oin
https://192.168.10.45/snort/snort_download_updates.php
Updates
SID Mgmt
Log Mgmt
Sync
Installed Rule Set MD5 Signature
Rule Set Name/Publisher
MD5 Signature Hash
MD5 Signature Date
Snort Subscriber Ruleset
Not Downloaded
Not Downloaded
Snort GPLv2 Community Rules
Not Downloaded
Not Downloaded
Emerging Threats Open Rules
Not Downloaded
Not Downloaded
Snort OpenAppID Detectors
Not Downloaded
Not Downloaded
Snort AppID Open Text Rules
Not Downloaded
Not Downloaded
Feodo Tracker Botnet C2 IP Rules
Not Enabled
Not Enabled
Update Your Rule Set
Last Update
Unknown
Result: Unknown
Update Rules
Update Rules
Force Update
Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.
Manage Rule Set Log
View Log
Clear Log
The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.



Verified the update by checking for an MD5 signature with the current time and date.

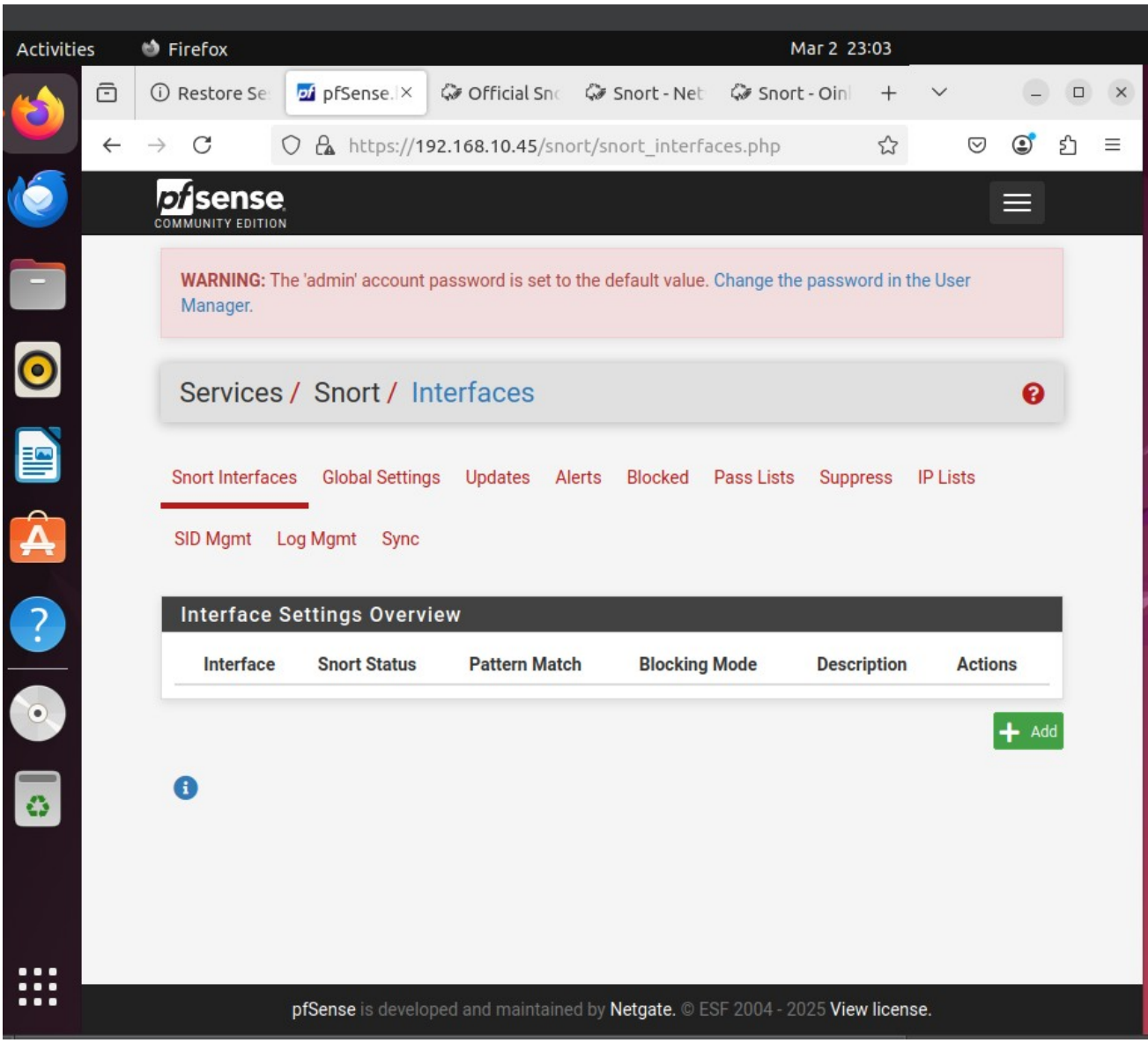

Restore Session
pfSense.home.arpa - Serv
https://192.168.10.45/snort/snort_download_updates.php
Rule Set Name/Publisher
MD5 Signature Hash
MD5 Signature Date
Snort Subscriber Ruleset
e44f8b6c5f92c7a51c5206e41da636d6
Monday, 03-Mar-25 05:30:01 UTC
Snort GPLv2 Community Rules
f95e13a059814e0687e02fab9ff3e74a
Monday, 03-Mar-25 05:30:01 UTC
Emerging Threats Open Rules
2f52b09d23baac451feac0f30e29973b
Monday, 03-Mar-25 05:30:01 UTC
Snort OpenAppID Detectors
c726cf937d84c651a20f2ac7c528384e
Monday, 03-Mar-25 05:30:01 UTC
Snort AppID Open Text Rules
2c26cb4f6a3bc03ab9c8e02befcf6fe1
Monday, 03-Mar-25 03:59:37 UTC
Feodo Tracker Botnet C2 IP Rules
Not Enabled
Not Enabled
Update Your Rule Set
Last Update
Mar-03 2025 05:30
Result: Success
Update Rules
Update Rules
Force Update
Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will
the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.
Manage Rule Set Log
View Log
Clear Log
The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.
Logfile Size
5 KiB


Activities
Firefox
Mar 2 23:04
Restore Se
pfSense.
Official Sn
Snort - Net
Snort - Oin
https://192.168.10.45/snort/snort_download_updates.php
pfsense
COMMUNITY EDITION
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Services / Snort / Updates
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Installed Rule Set MD5 Signature
Rule Set Name/Publisher
MD5 Signature Hash
MD5 Signature Date
Snort Subscriber Ruleset
e44f8b6c5f92c7a51c5206e41da636d6
Monday, 03-Mar-25 03:59:37 UTC
Snort GPLv2 Community Rules
f95e13a059814e0687e02fab9ff3e74a
Monday, 03-Mar-25 03:59:37 UTC
Emerging Threats Open Rules
2f52b09d23baac451feac0f30e29973b
Monday, 03-Mar-25 03:59:37 UTC
Snort OpenAppID Detectors
c726cf937d84c651a20f2ac7c528384e
Monday, 03-Mar-25 03:59:37 UTC
Snort AppID Open Text Rules
2c26cb4f6a3bc03ab9c8e02befcf6fe1
Monday, 03-Mar-25 03:59:37 UTC

Objective 2: Configuring Snort Interfaces

Added a New Snort Interface

Went to the *Snort Interfaces* tab and clicked *Add* to create a new interface.



Configured the interface as follows:

Interface: WAN (to protect the external network interface).

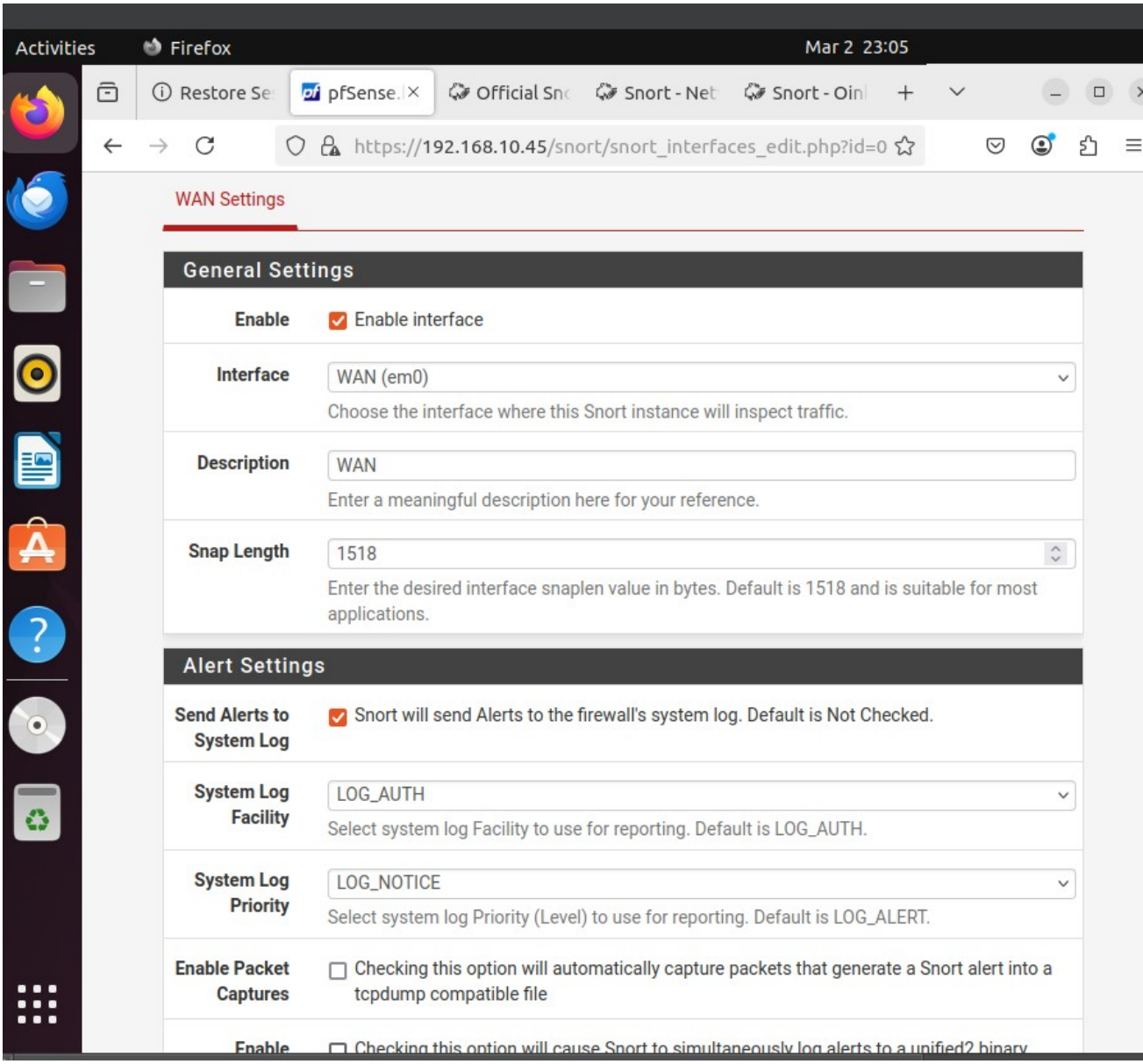
Enabled *Send Alerts to System Log* to forward alerts to the pfSense system log.

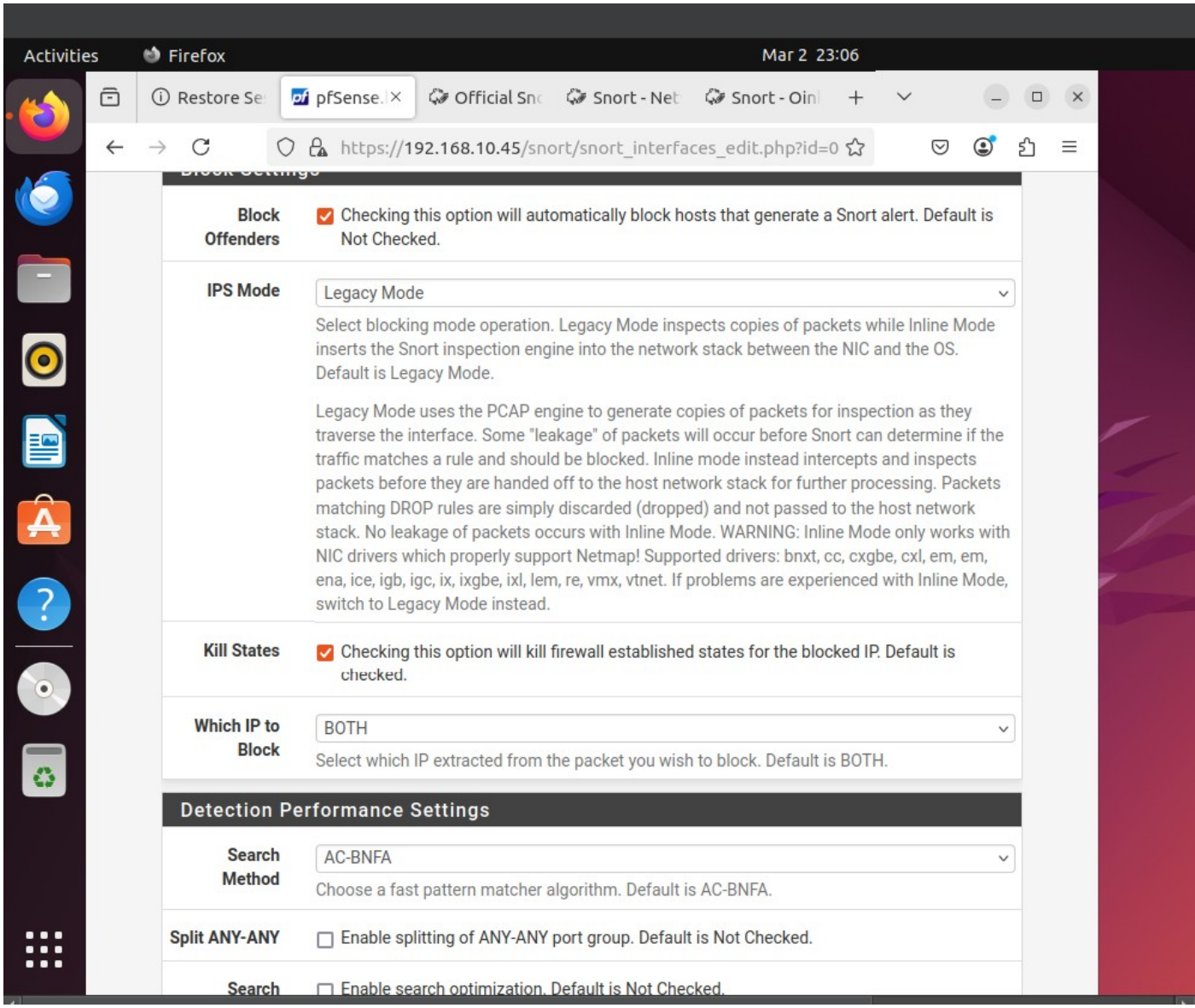
Set *System Log Priority* to LOG_NOTICE for more verbose alerting.

Enabled *Block Offenders* to convert Snort from an IDS to an IPS.

Used *Legacy Mode* and blocked both source and destination IPs.

Clicked *Save*.


Activities
Firefox
Mar 2 23:05
Restore Se
pfSense.
Official Sn
Snort - Net
Snort - Oin
https://192.168.10.45/snort/snort_interfaces_edit.php?id=0
WAN Settings
General Settings
Enable
Enable interface
Interface
WAN (em0)
Choose the interface where this Snort instance will inspect traffic.
Description
WAN
Enter a meaningful description here for your reference.
Snap Length
1518
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.
Alert Settings
Send Alerts to System Log
Snort will send Alerts to the firewall's system log. Default is Not Checked.
System Log Facility
LOG_AUTH
Select system log Facility to use for reporting. Default is LOG_AUTH.
System Log Priority
LOG_NOTICE
Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.
Enable Packet Captures
Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Enable
Checking this option will cause Snort to simultaneously log alerts to a unified2 binary

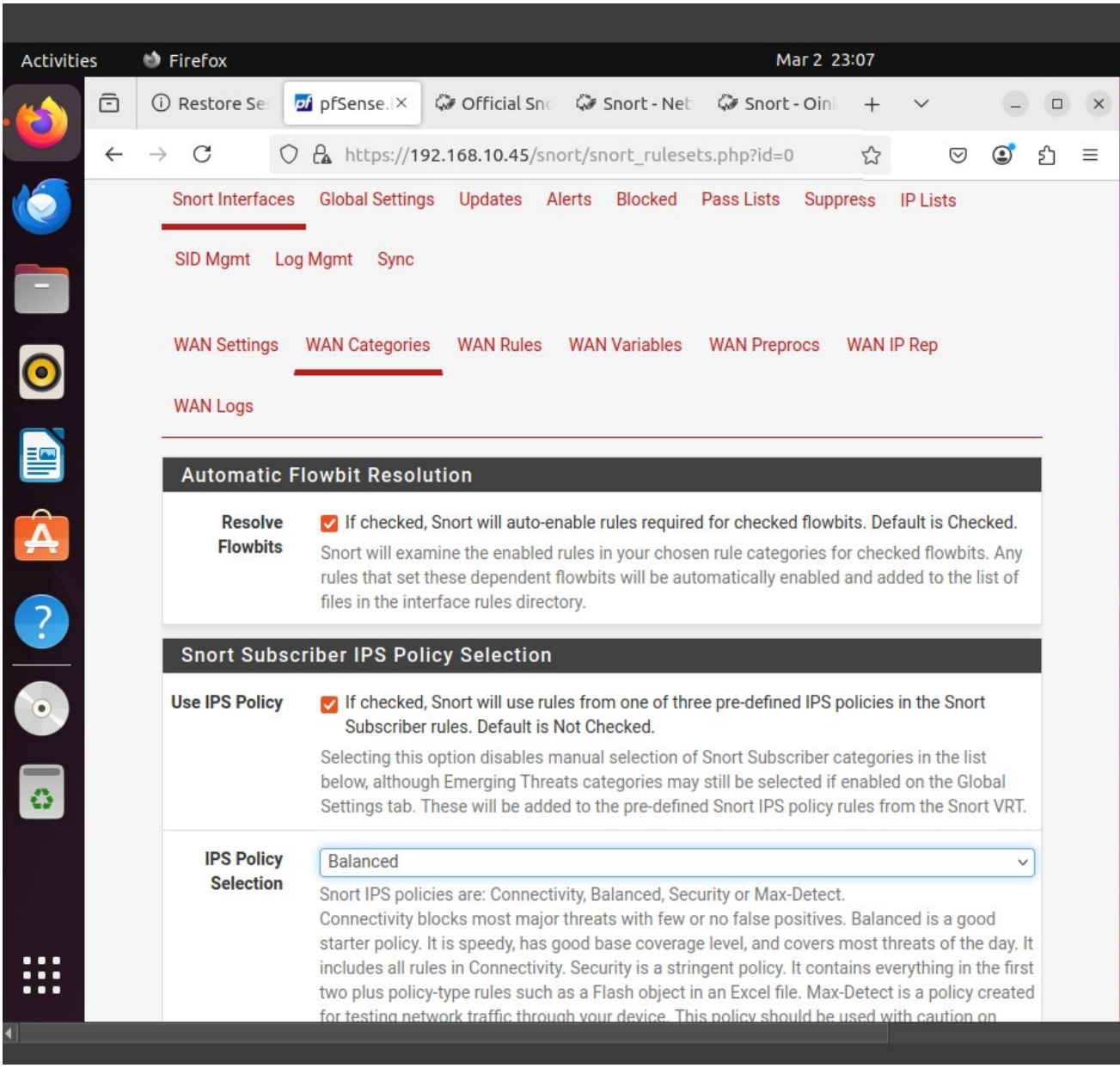


Set IPS Policy

Switched to the *WAN Categories* tab and checked the *Use IPS Policy* option.

Chose *Balanced* for the IPS Policy Mode.

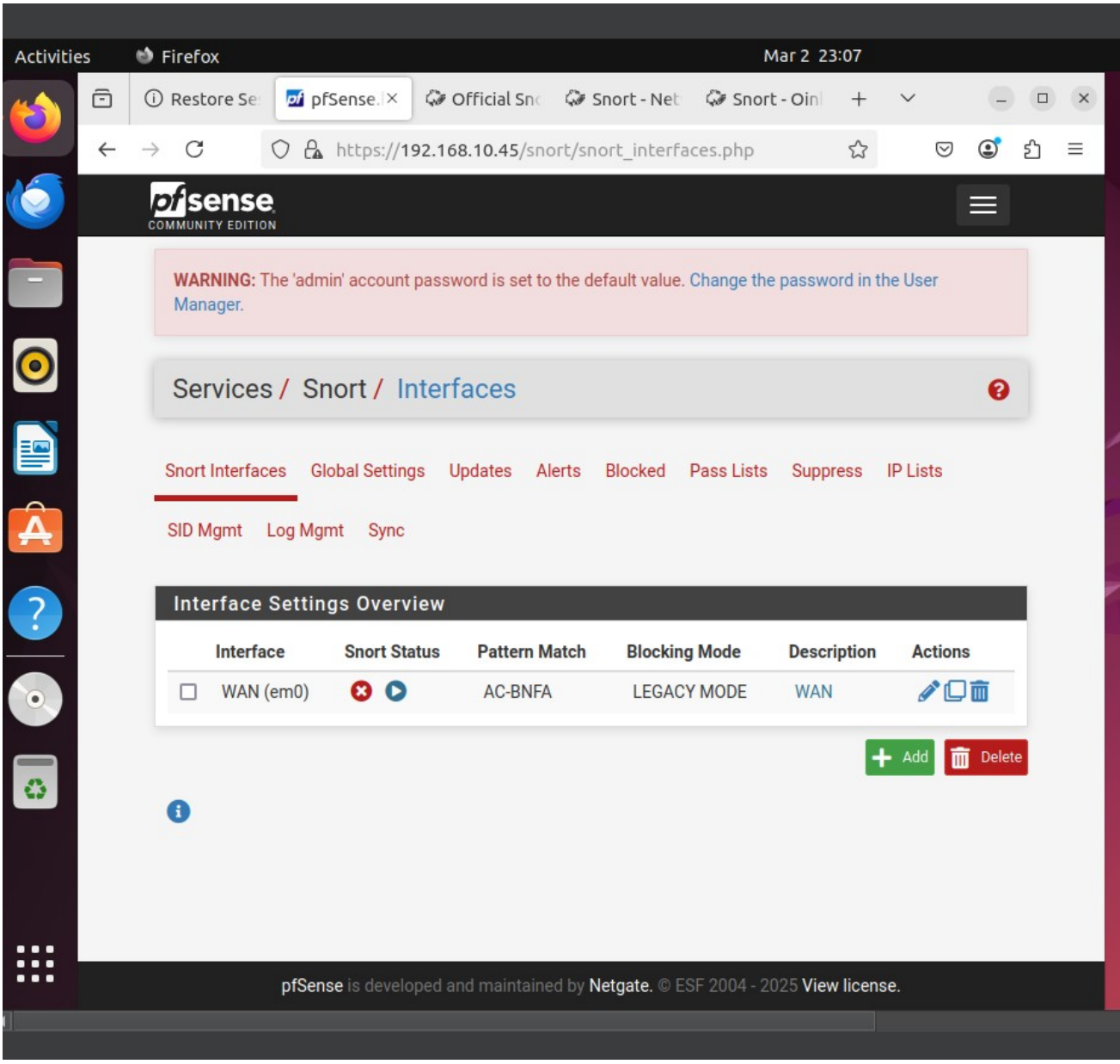
Clicked *Save* to finalize the configuration.

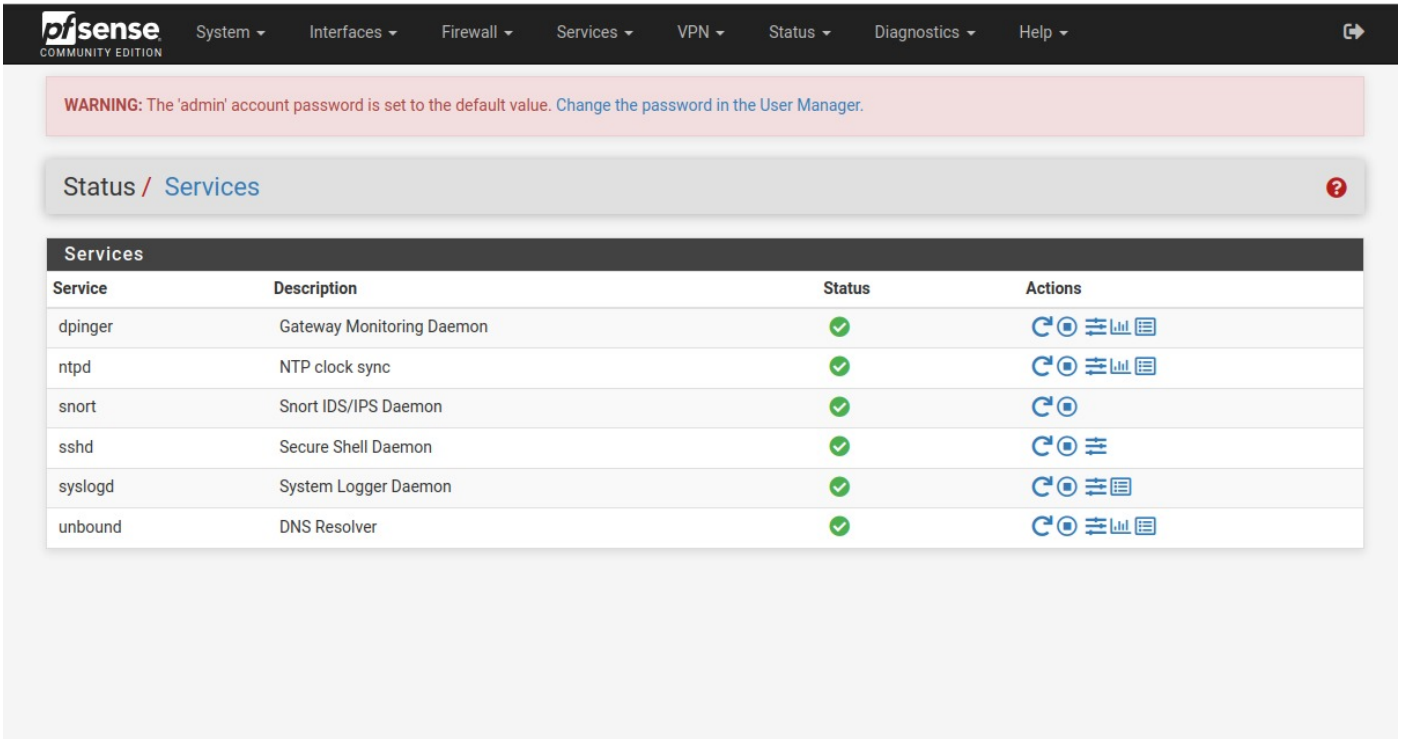


Started Snort

Navigated to *Services* > *Snort* > *Interfaces* and clicked *Start Snort* on the WAN interface.

Verified that Snort was monitoring traffic on the WAN interface using the *Service Status* widget on the main pfSense screen.

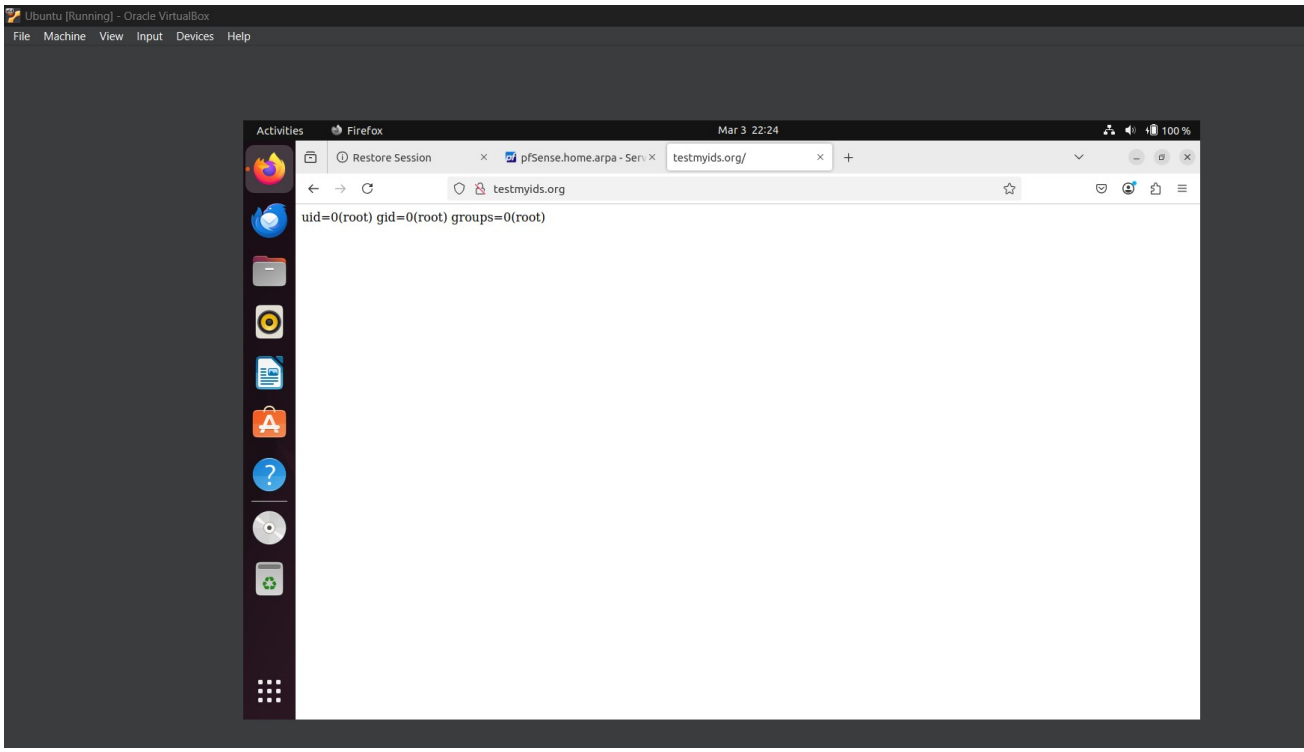

Activities
Firefox
Mar 2 23:07
Restore Se
pfSense
Official Snc
Snort - Net
Snort - Oin
https://192.168.10.45/snort/snort_interfaces.php
pfsense
COMMUNITY EDITION
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Services / Snort / Interfaces
Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync
Interface Settings Overview
Interface
Snort Status
Pattern Match
Blocking Mode
Description
Actions
WAN (em0)
AC-BNFA
LEGACY MODE
WAN
Add
Delete
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

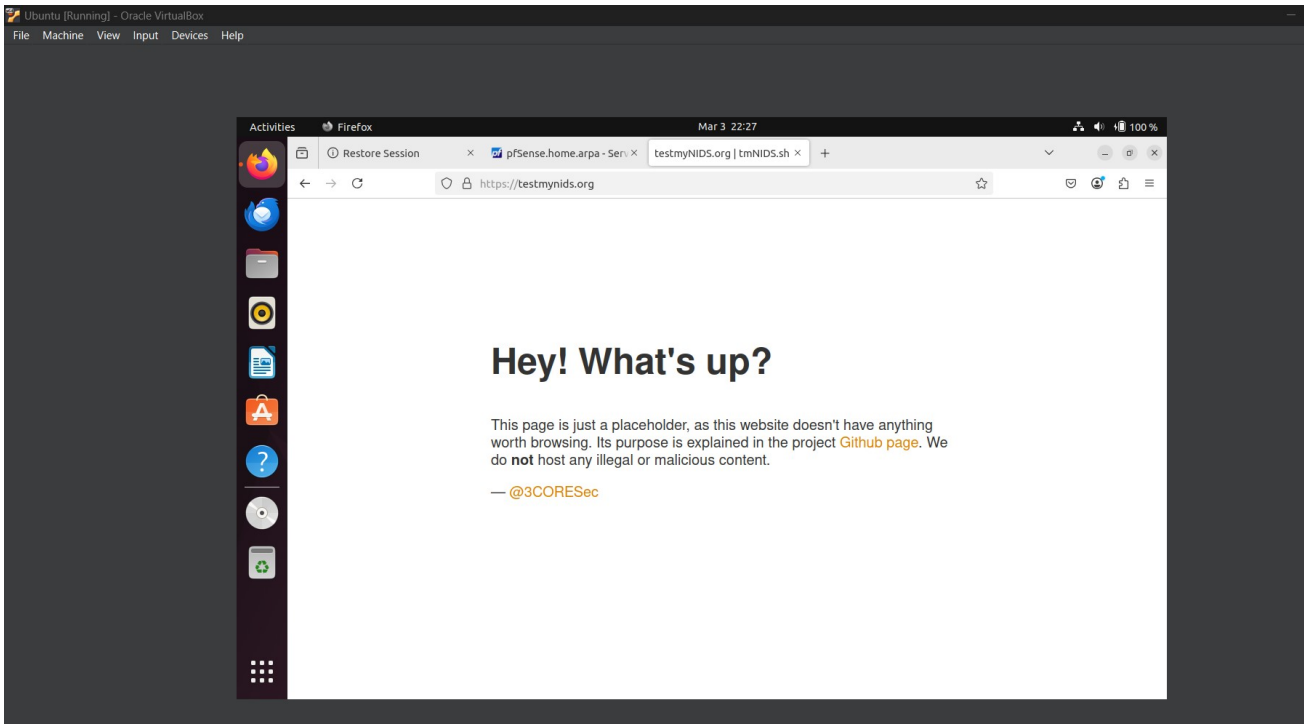

pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Status / Services
Services
Service
Description
Status
Actions
dpinger
Gateway Monitoring Daemon
ntpd
NTP clock sync
snort
Snort IDS/IPS Daemon
sshd
Secure Shell Daemon
syslogd
System Logger Daemon
unbound
DNS Resolver

Objective 3: Testing Snort Configuration

Generated a Snort Alert

On a computer within the network protected by pfSense, I opened a browser and visited `tetsmyids.org and testmynids.org.`





Viewed Snort Alerts

Alerts were viewed on the main dashboard and by navigating to *Services* > *Snort* > *Alerts*. Couln't able to find any alerts generated

The *Blocked* tab was checked to see the IP addresses that had been blocked. No Ip Address has been blocked