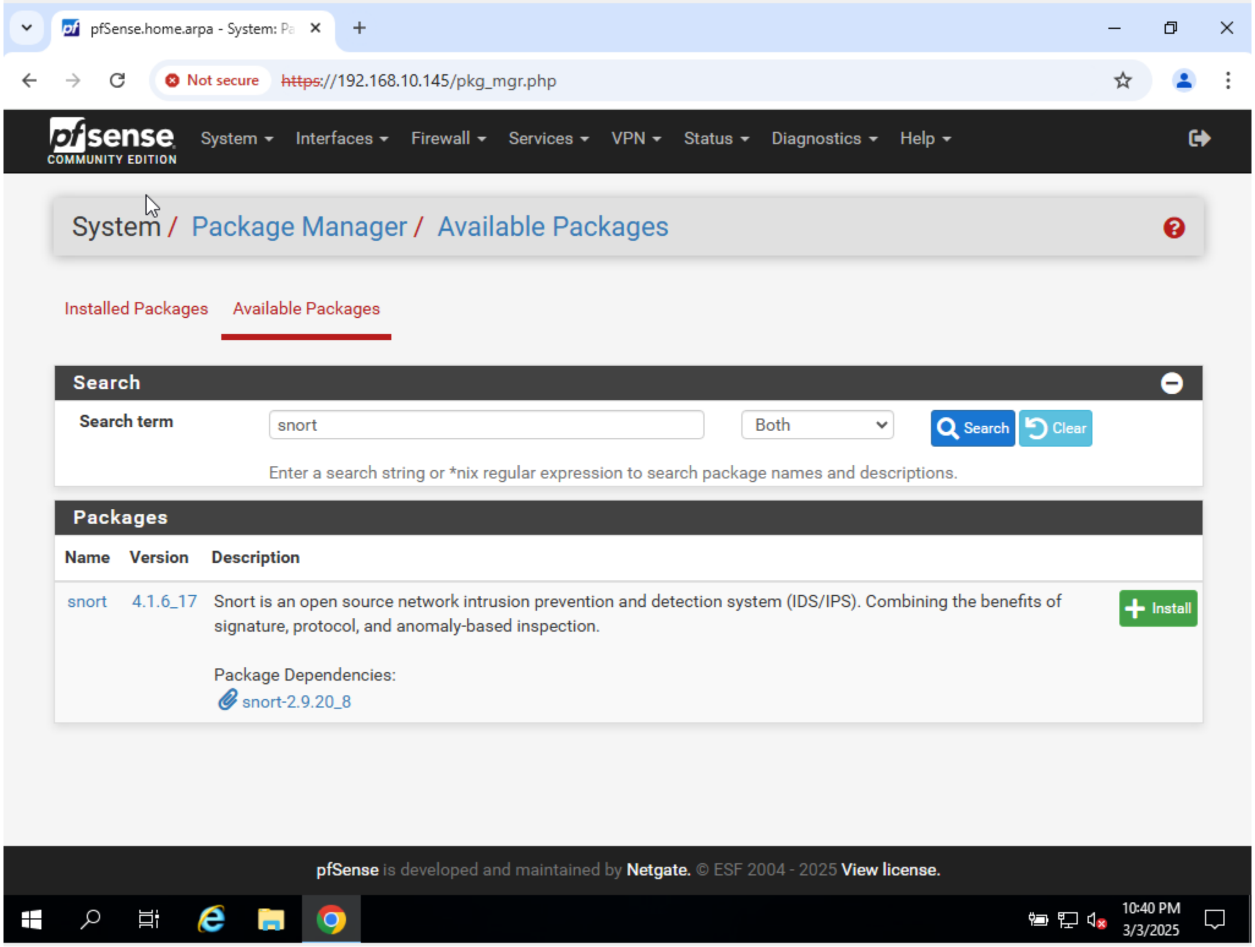
Lab 4: Adding a Snort IDS to pfSense

Objective 1: Installation and Initial Setup

- I accessed the **pfSense Web Portal** by opening my browser and logging into the interface.

- I navigated to **System** > **Package Manager** to install the necessary package.
- In the **Available Packages** tab, I searched for **Snort**, clicked **Install**, and confirmed the installation.



System / Package Manager / Available Packages

Search

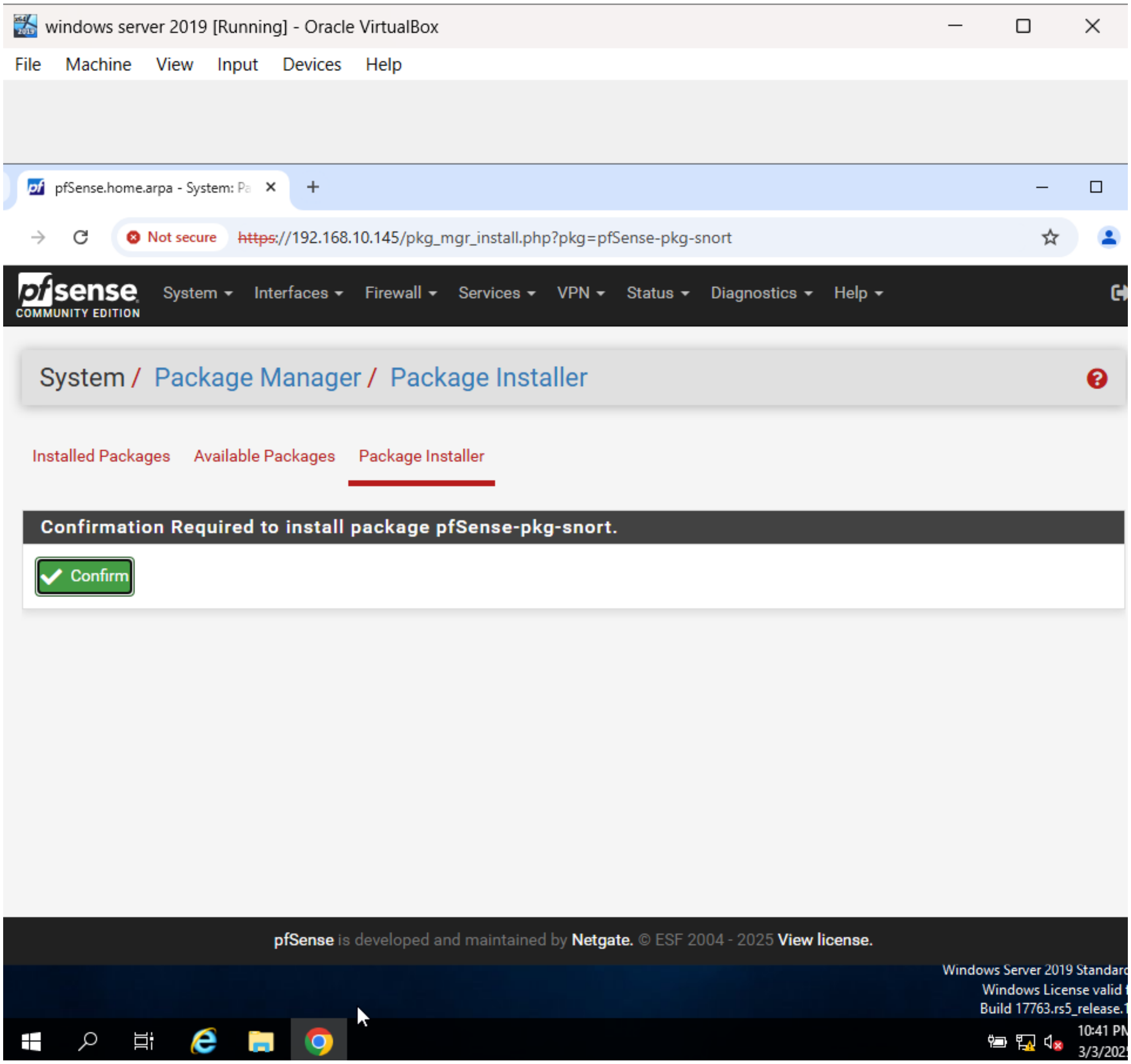
Search term: snort — Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
snort	4.1.6_17	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: snort-2.9.20_8

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.



windows server 2019 [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
pfSense.home.arpa - System: Pa
Not secure
https://192.168.10.145/pkg_mgr_install.php?pkg=pfSense-pkg-snort
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

System / Package Manager / Package Installer

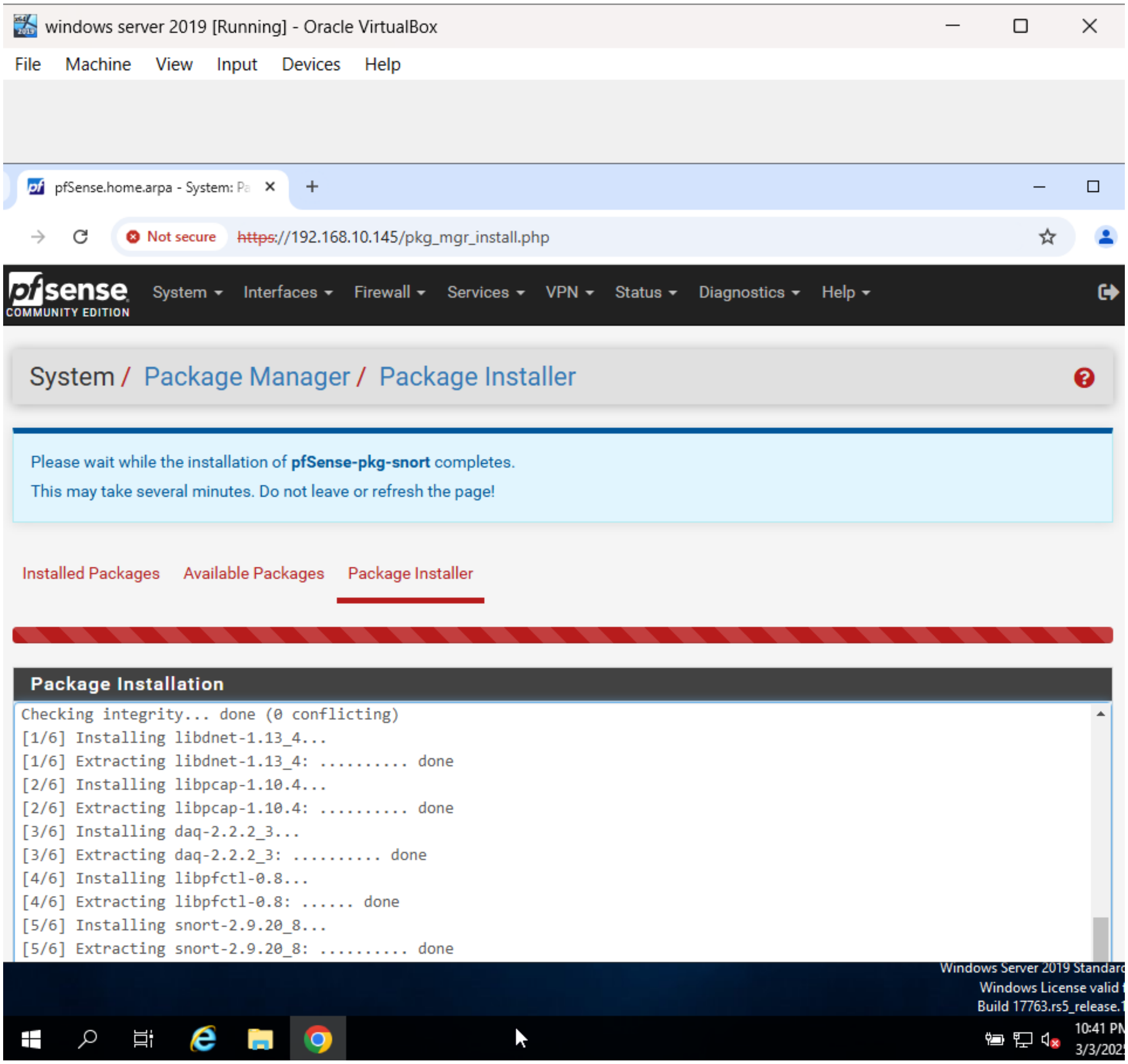
Installed Packages | Available Packages | Package Installer

Confirmation Required to install package pfSense-pkg-snort.

✓ Confirm

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

Windows Server 2019 Standard
Windows License valid
Build 17763.rs5_release.
10:41 PM
3/3/202


windows server 2019 [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
pfSense.home.arpa - System: Pa
Not secure
https://192.168.10.145/pkg_mgr_install.php
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

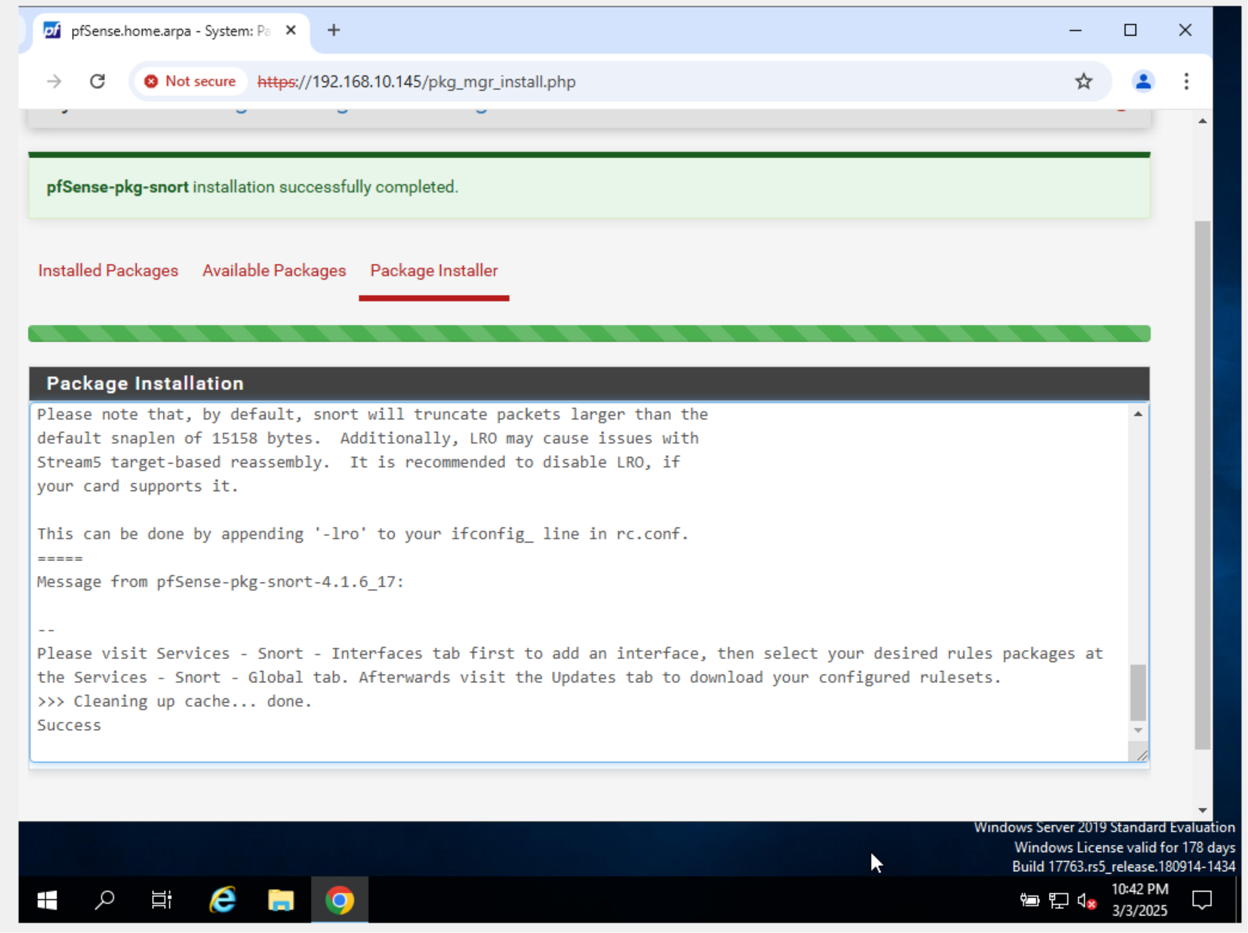
System / Package Manager / Package Installer

Please wait while the installation of **pfSense-pkg-snort** completes.

This may take several minutes. Do not leave or refresh the page!

Package Installation

```
Checking integrity... done (0 conflicting)
[1/6] Installing libdnet-1.13_4...
[1/6] Extracting libdnet-1.13_4: .......... done
[2/6] Installing libpcap-1.10.4...
[2/6] Extracting libpcap-1.10.4: .......... done
[3/6] Installing daq-2.2.2_3...
[3/6] Extracting daq-2.2.2_3: .......... done
[4/6] Installing libpfctl-0.8...
[4/6] Extracting libpfctl-0.8: ...... done
[5/6] Installing snort-2.9.20_8...
[5/6] Extracting snort-2.9.20_8: .......... done
```


pfSense.home.arpa - System: Pa
Not secure
https://192.168.10.145/pkg_mgr_install.php

pfSense-pkg-snort installation successfully completed.

Installed Packages
Available Packages
Package Installer

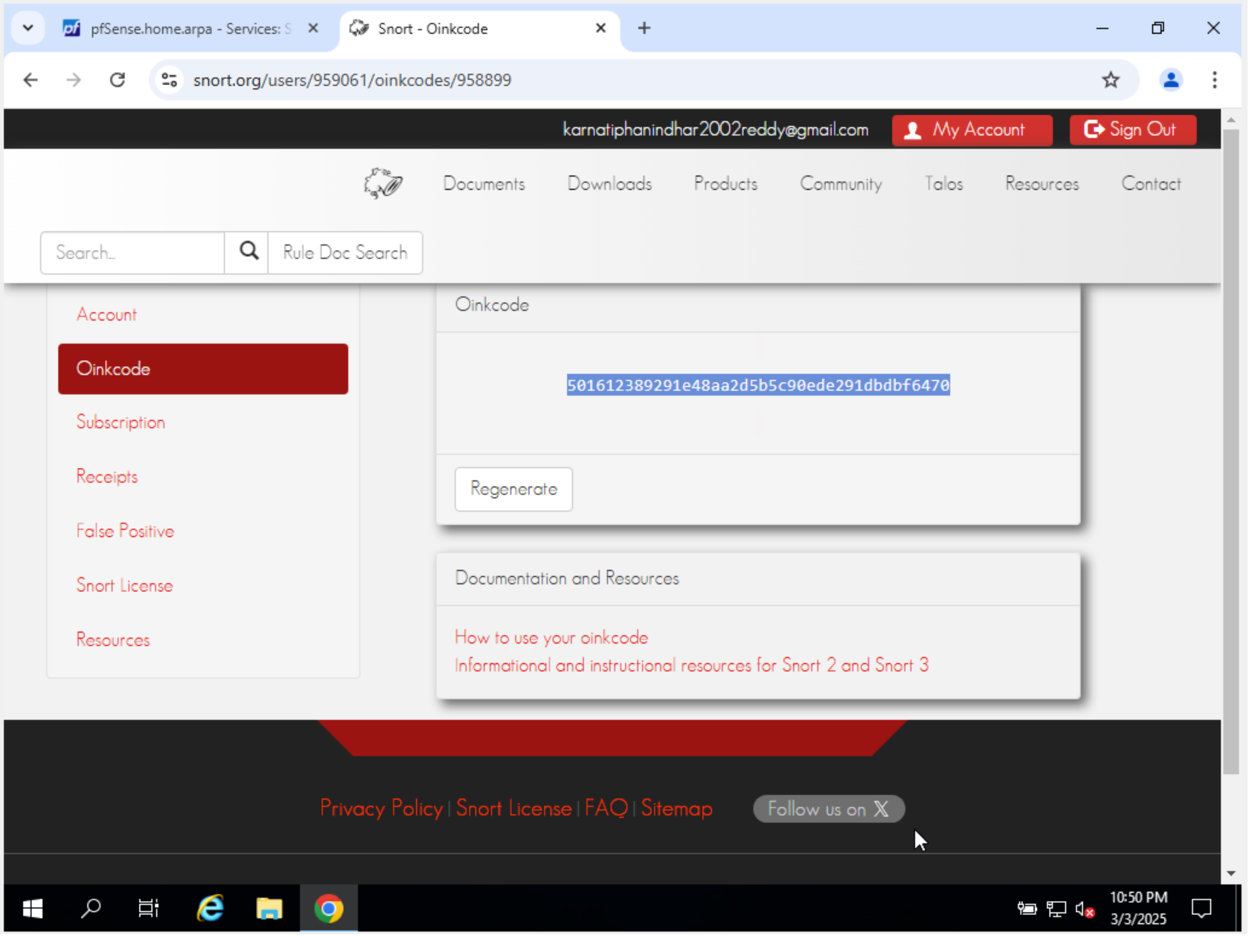
Package Installation

```
Please note that, by default, snort will truncate packets larger than the
default snaplen of 15158 bytes.  Additionally, LRO may cause issues with
Stream5 target-based reassembly.  It is recommended to disable LRO, if
your card supports it.

This can be done by appending '-lro' to your ifconfig_ line in rc.conf.
=====
Message from pfSense-pkg-snort-4.1.6_17:

--
Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at
the Services - Snort - Global tab. Afterwards visit the Updates tab to download your configured rulesets.
>>> Cleaning up cache... done.
Success
```

Windows Server 2019 Standard Evaluation
Windows License valid for 178 days
Build 17763.rs5_release.180914-1434
10:42 PM
3/3/2025



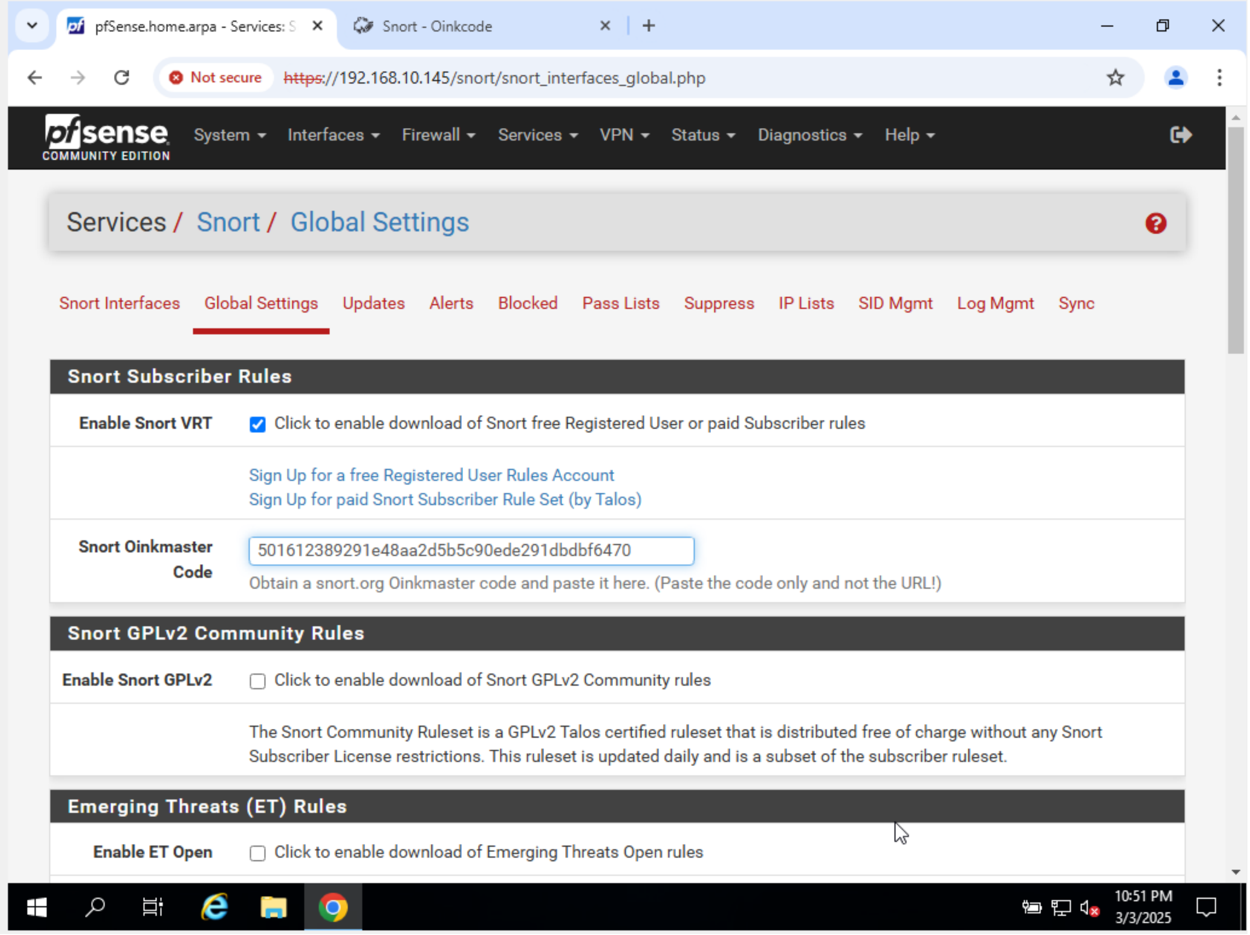
Oinkcode

501612389291e48aa2d5b5c90ede291dbdbf6470

Documentation and Resources

How to use your oinkcode
Informational and instructional resources for Snort 2 and Snort 3

- I have logedin to Oinkmaster code and Generated code.



Services / Snort / Global Settings

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 501612389291e48aa2d5b5c90ede291dbdbf6470
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

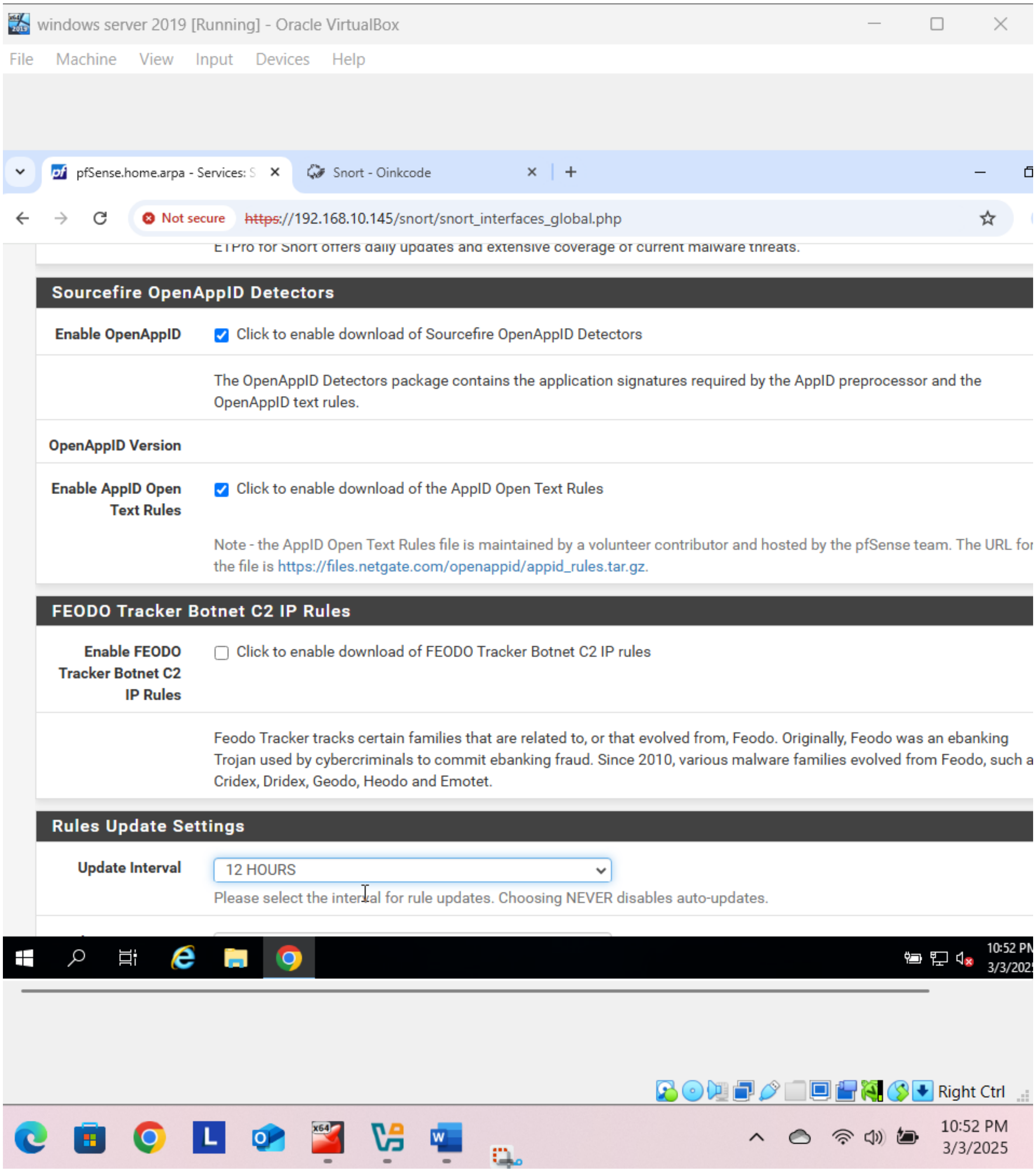
Enable Snort GPLv2 □ Click to enable download of Snort GPLv2 Community rules

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

- Once the installation was complete, I went to **Services** > **Snort** to begin configuration.
- In the **Global Settings** tab, I enabled the following options:
  - **Snort VRT** (entered my Oinkmaster code)
  - **Snort GPLv2**
  - **ET Open**
  - **OpenAppID**
  - **AppID Open Text Rules**


windows server 2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pfSense.home.arpa - Services: S
Snort - Oinkcode
Not secure
https://192.168.10.145/snort/snort_interfaces_global.php
Right Ctrl
10:52 PM
3/3/2025

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

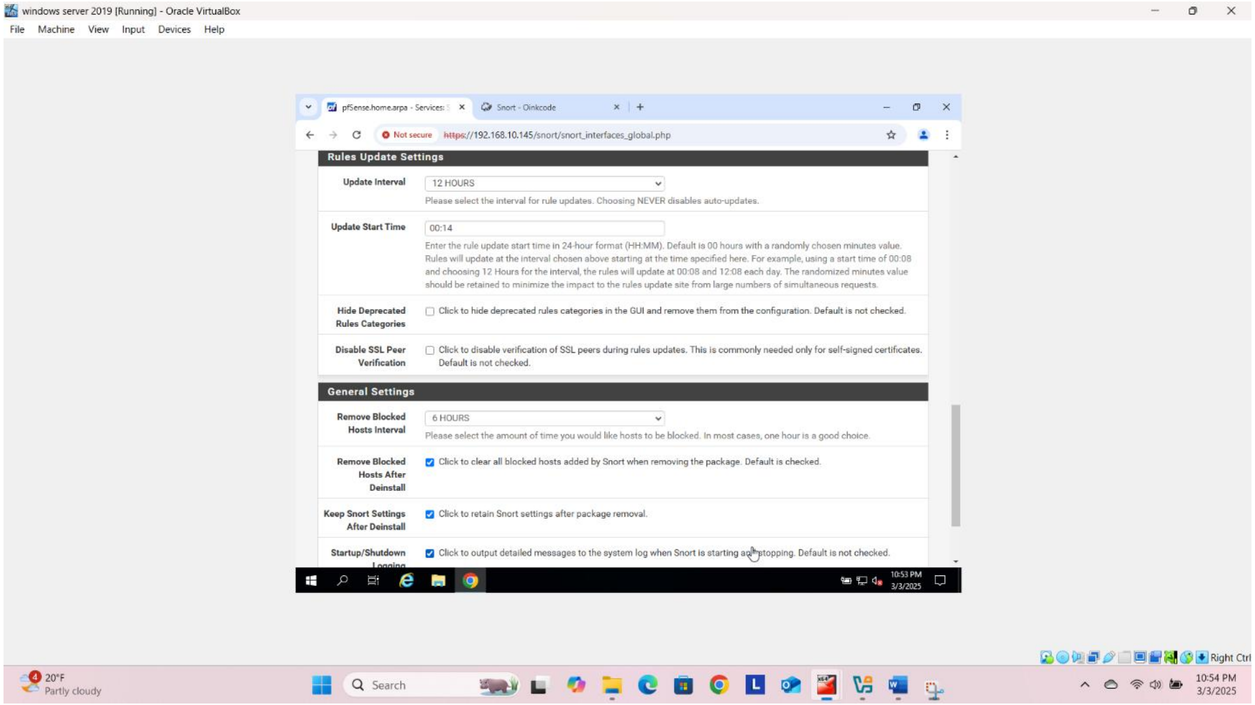
Feodo Tracker tracks certain families that are related to, or that evolved from, Feodo. Originally, Feodo was an ebanking Trojan used by cybercriminals to commit ebanking fraud. Since 2010, various malware families evolved from Feodo, such a Cridex, Dridex, Geodo, Heodo and Emotet.

Rules Update Settings

Update Interval: 12 HOURS

Please select the interval for rule updates. Choosing NEVER disables auto-updates.

- I set the update interval to **12 hours**, the removal of blocked hosts to **6 hours**, and configured a random start time.


windows server 2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pfSense.home.arpa - Services: S
Snort - Oinkcode
Not secure
https://192.168.10.145/snort/snort_interfaces_global.php
10:53 PM
3/3/2025
Right Ctrl
20°F
Partly cloudy
Search
10:54 PM
3/3/2025

Rules Update Settings

Update Interval 12 HOURS
Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Update Start Time 00:14
Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.

Hide Deprecated Rules Categories ☐ Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.

Disable SSL Peer Verification ☐ Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

General Settings

Remove Blocked Hosts Interval 6 HOURS
Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.

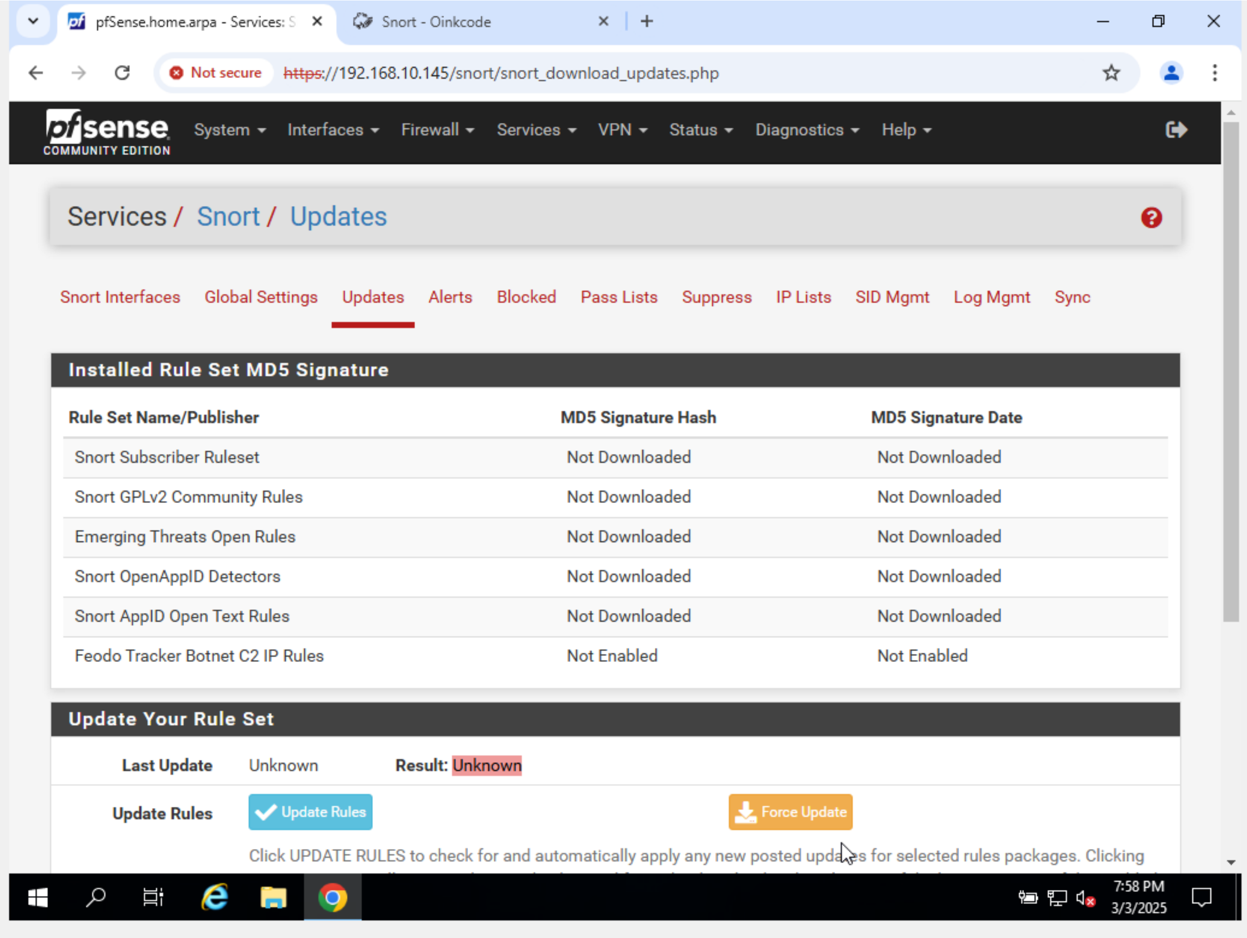
Remove Blocked Hosts After Deinstall ☑ Click to clear all blocked hosts added by Snort when removing the package. Default is checked.

Keep Snort Settings After Deinstall ☑ Click to retain Snort settings after package removal.

Startup/Shutdown Logging ☑ Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

- I clicked **Save** to apply the settings.

- Next, I navigated to the **Updates** tab and clicked **Force Update** to fetch the latest Snort rules.
- I verified the update by checking for the **MD5 signature** with the current time and date.


pfSense.home.arpa - Services: S
Snort - Oinkcode
Not secure
https://192.168.10.145/snort/snort_download_updates.php
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

Services / Snort / Updates

Installed Rule Set MD5 Signature

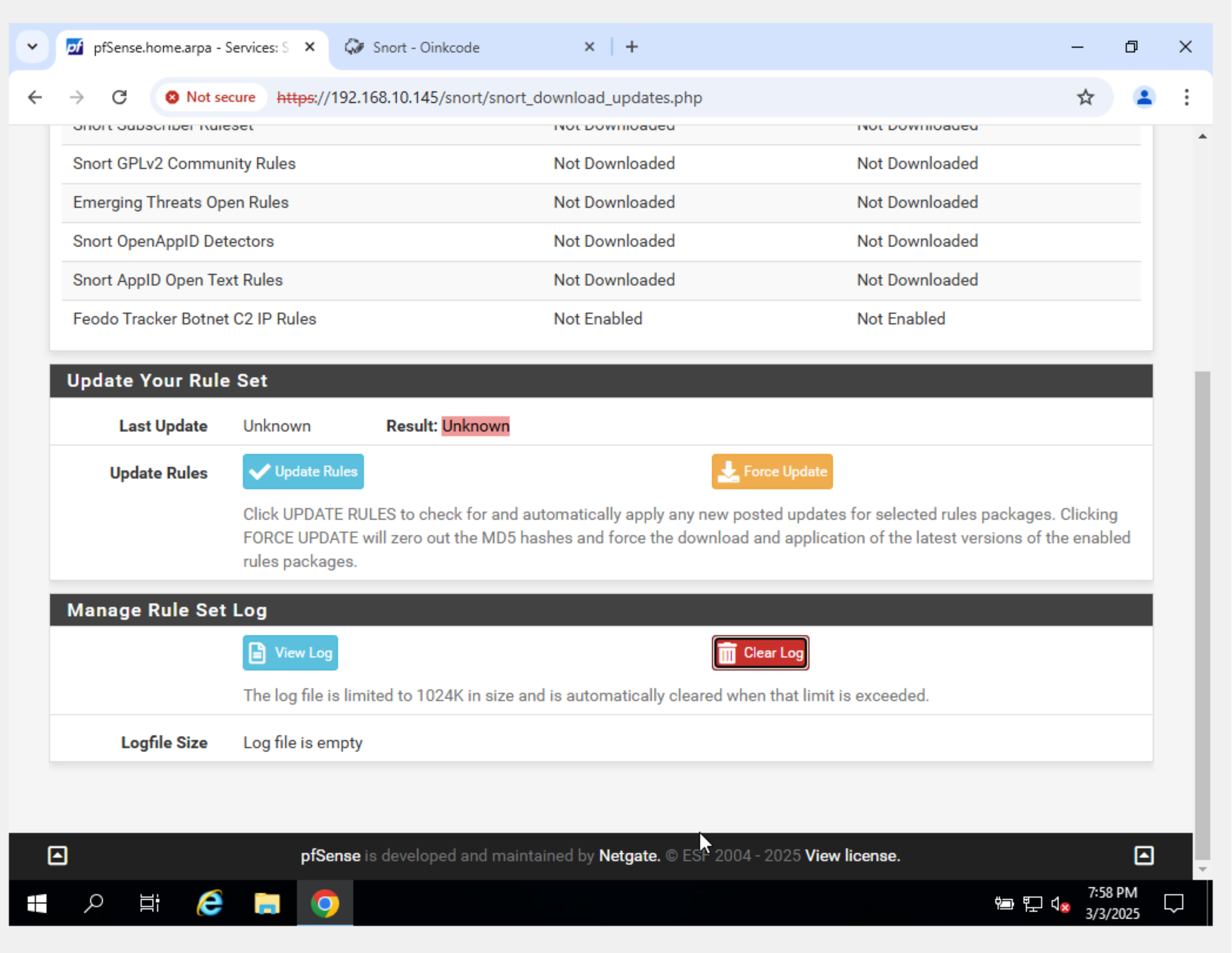
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Downloaded	Not Downloaded
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort OpenAppID Detectors	Not Downloaded	Not Downloaded
Snort AppID 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

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking


pfSense.home.arpa - Services: S
Snort - Oinkcode
Not secure
https://192.168.10.145/snort/snort_download_updates.php

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

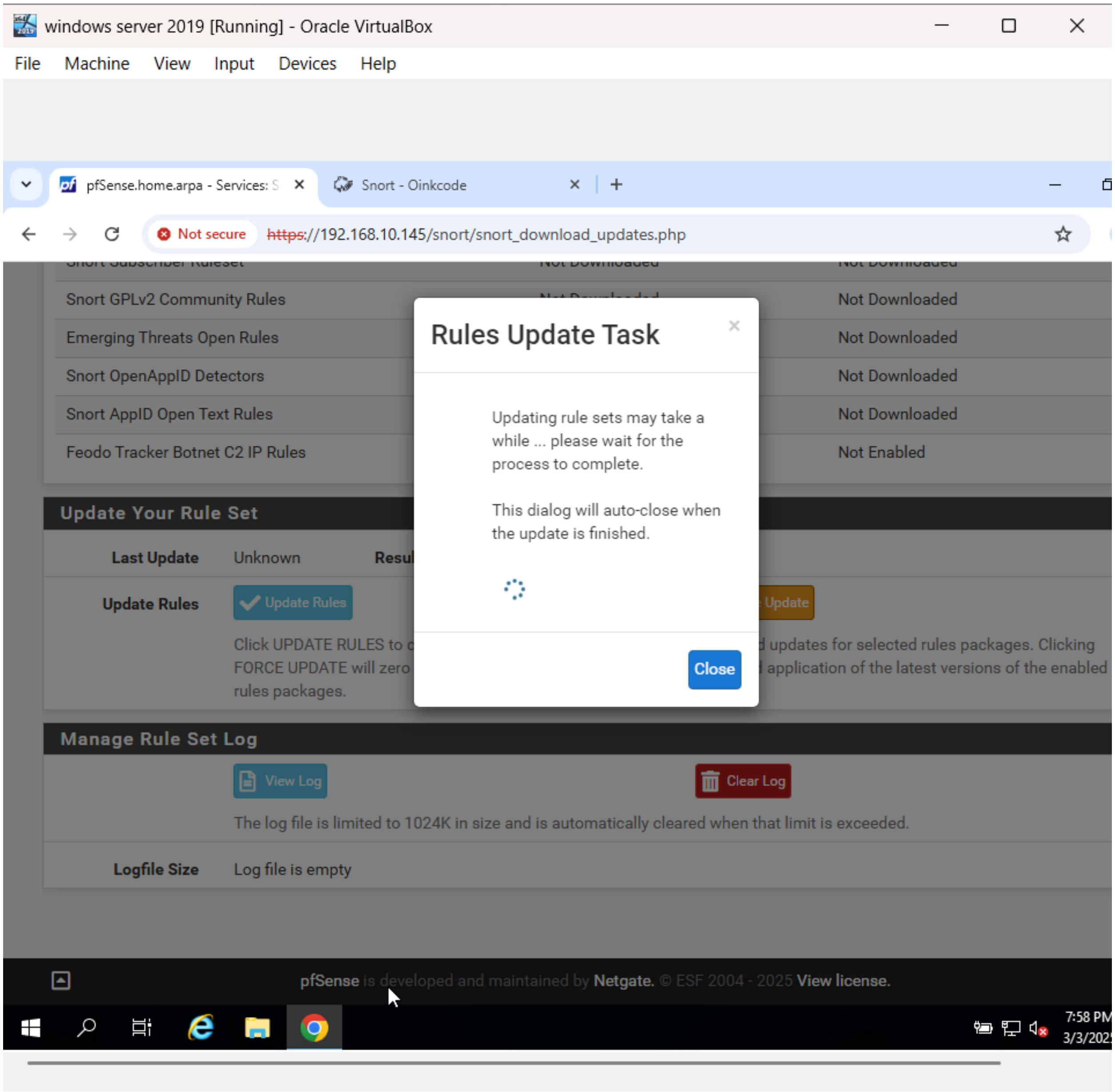
Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Manage Rule Set Log

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size Log file is empty

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.



windows server 2019 [Running] - Oracle VirtualBox

https://192.168.10.145/snort/snort_download_updates.php

Snort Subscriber Ruleset	Not Downloaded	Not Downloaded
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Emerging Threats Open Rules		Not Downloaded
Snort OpenAppID Detectors		Not Downloaded
Snort AppID Open Text Rules		Not Downloaded
Feodo Tracker Botnet C2 IP Rules		Not Enabled

Update Your Rule Set

Last Update Unknown **Resul**

Update Rules

Click UPDATE RULES to c ... d updates for selected rules packages. Clicking FORCE UPDATE will zero ... d application of the latest versions of the enabled rules packages.

Rules Update Task

Updating rule sets may take a while ... please wait for the process to complete.

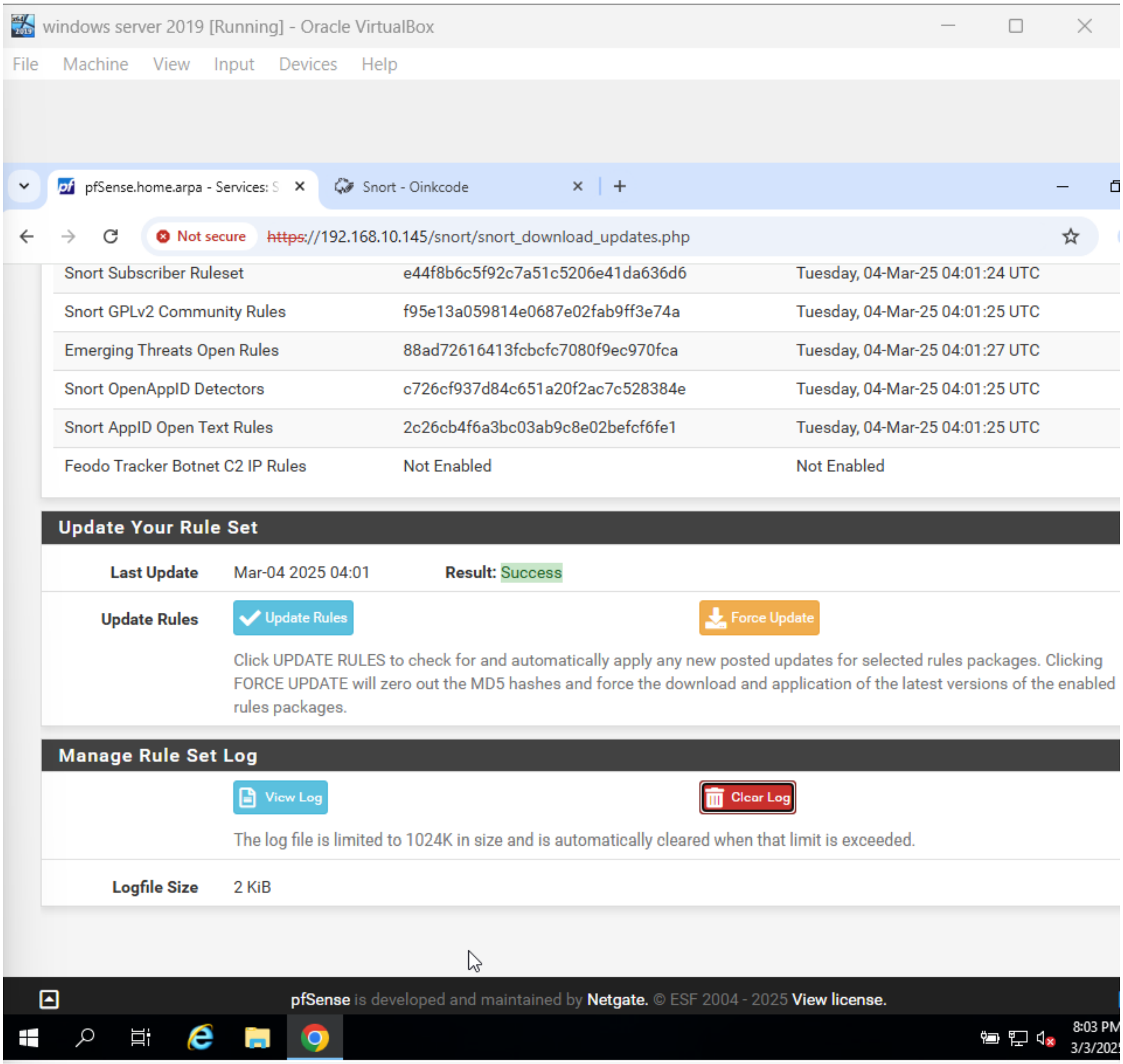
This dialog will auto-close when the update is finished.

Manage Rule Set Log

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size Log file is empty

pfSense is developed and maintained by **Netgate.** © ESF 2004 - 2025 **View license.**


windows server 2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pfSense.home.arpa - Services: S
Snort - Oinkcode
Not secure
https://192.168.10.145/snort/snort_download_updates.php

Snort Subscriber Ruleset	e44f8b6c5f92c7a51c5206e41da636d6	Tuesday, 04-Mar-25 04:01:24 UTC
Snort GPLv2 Community Rules	f95e13a059814e0687e02fab9ff3e74a	Tuesday, 04-Mar-25 04:01:25 UTC
Emerging Threats Open Rules	88ad72616413fcbcfc7080f9ec970fca	Tuesday, 04-Mar-25 04:01:27 UTC
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Tuesday, 04-Mar-25 04:01:25 UTC
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Tuesday, 04-Mar-25 04:01:25 UTC
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update Mar-04 2025 04:01 **Result:** Success

Update Rules

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

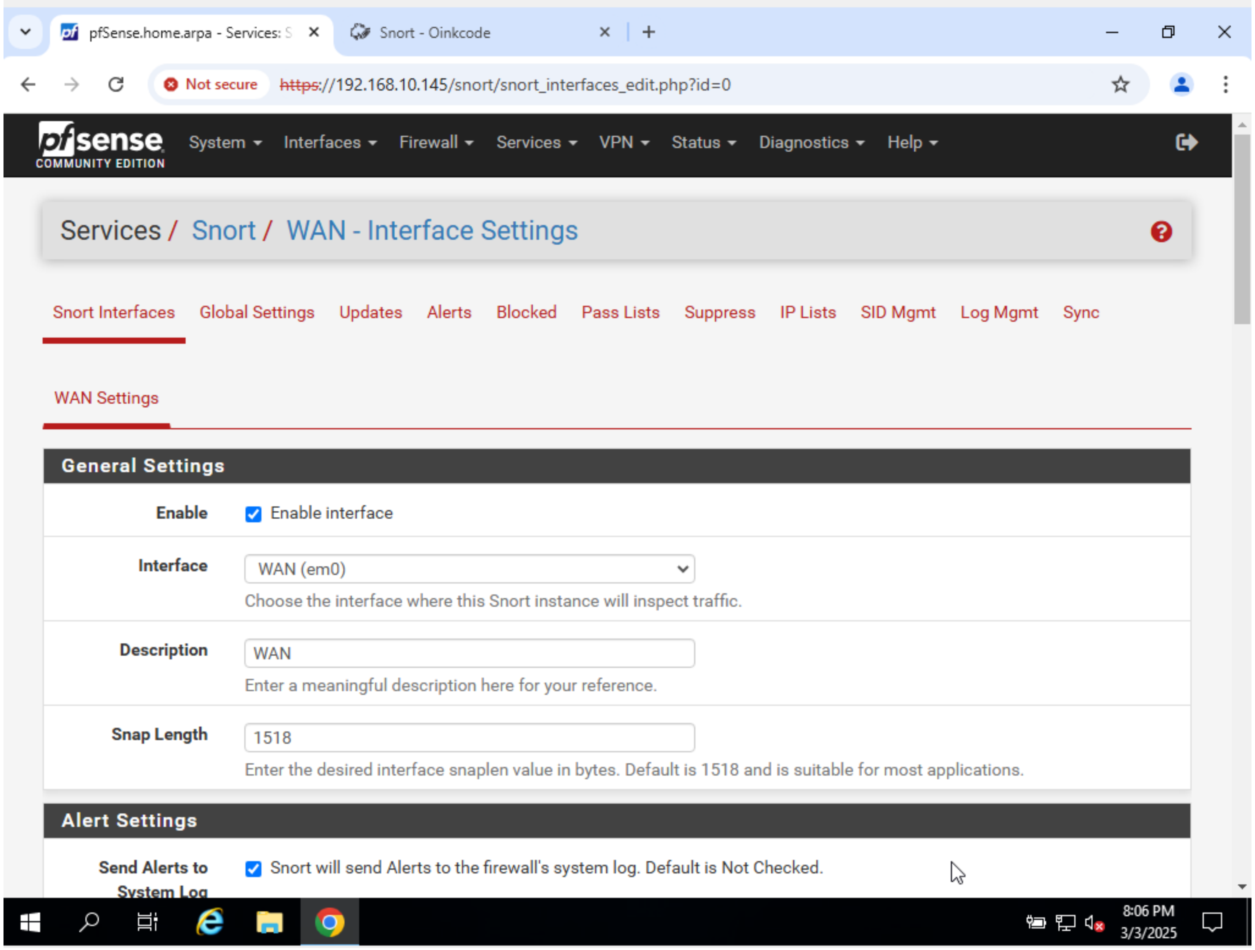
The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size 2 KiB

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

Objective 2: Configuring Snort Interfaces

- I navigated to the **Snort Interfaces** tab and clicked **Add** to create a new Snort interface.
- In the interface configuration, I set:
  - ➢ **Interface:** WAN
  - ➢ **Send Alerts to System Log:** Enabled
  - ➢ **System Log Priority:** LOG_NOTICE
  - ➢ **Block Offenders:** Enabled (Legacy Mode, blocking both source and destination IPs)


pfSense.home.arpa - Services: S
Snort - Oinkcode
Not secure
~~https~~://192.168.10.145/snort/snort_interfaces_edit.php?id=0
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
8:06 PM
3/3/2025

Services / Snort / WAN - Interface Settings

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

WAN Settings

General Settings

Enable: ☑ Enable interface

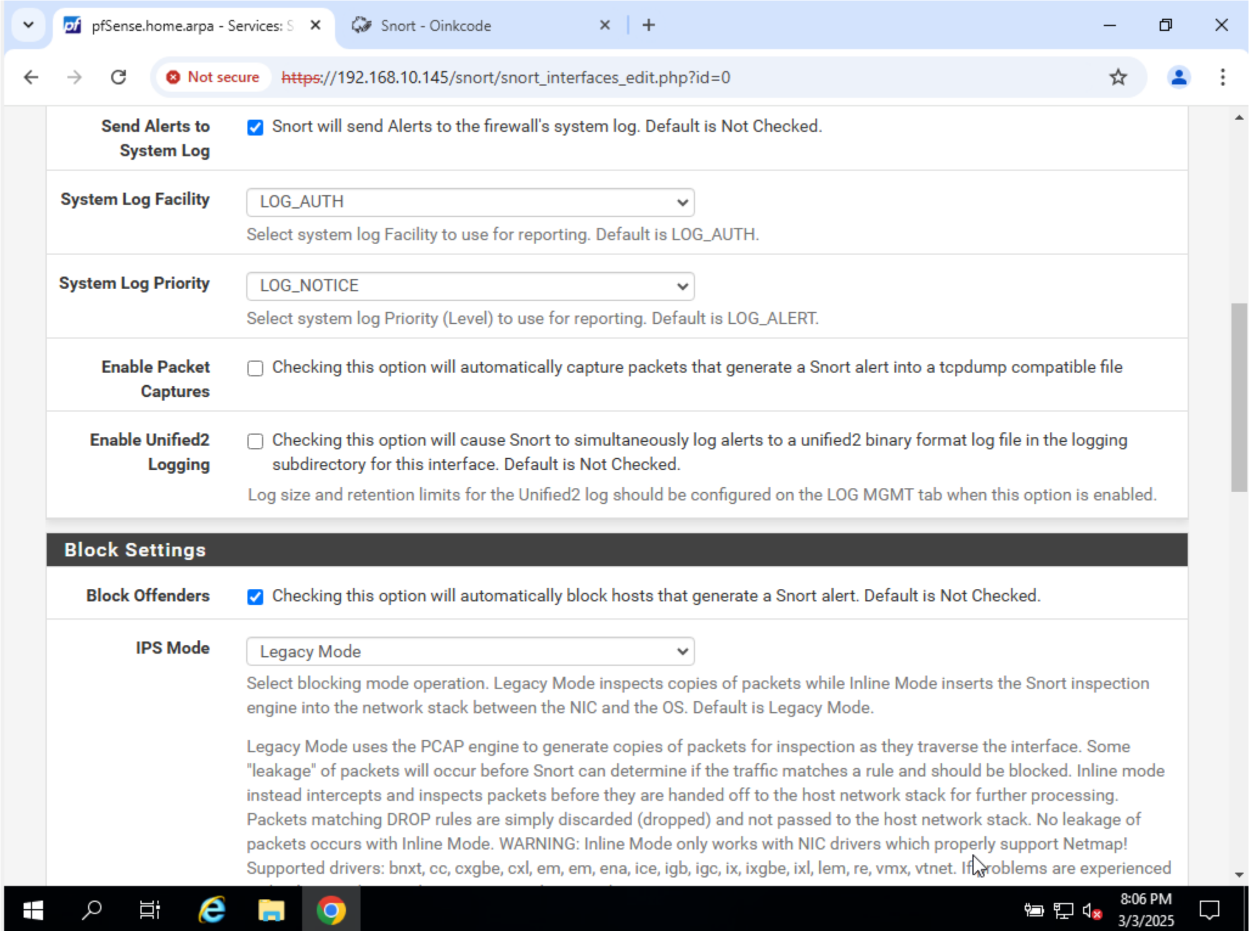
Interface: WAN (em0)
Choose the interface where this Snort instance will inspect traffic.

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.



pfSense.home.arpa - Services: S
Snort - Oinkcode
Not secure
~~https~~://192.168.10.145/snort/snort_interfaces_edit.php?id=0

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 Unified2 Logging □ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.

Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

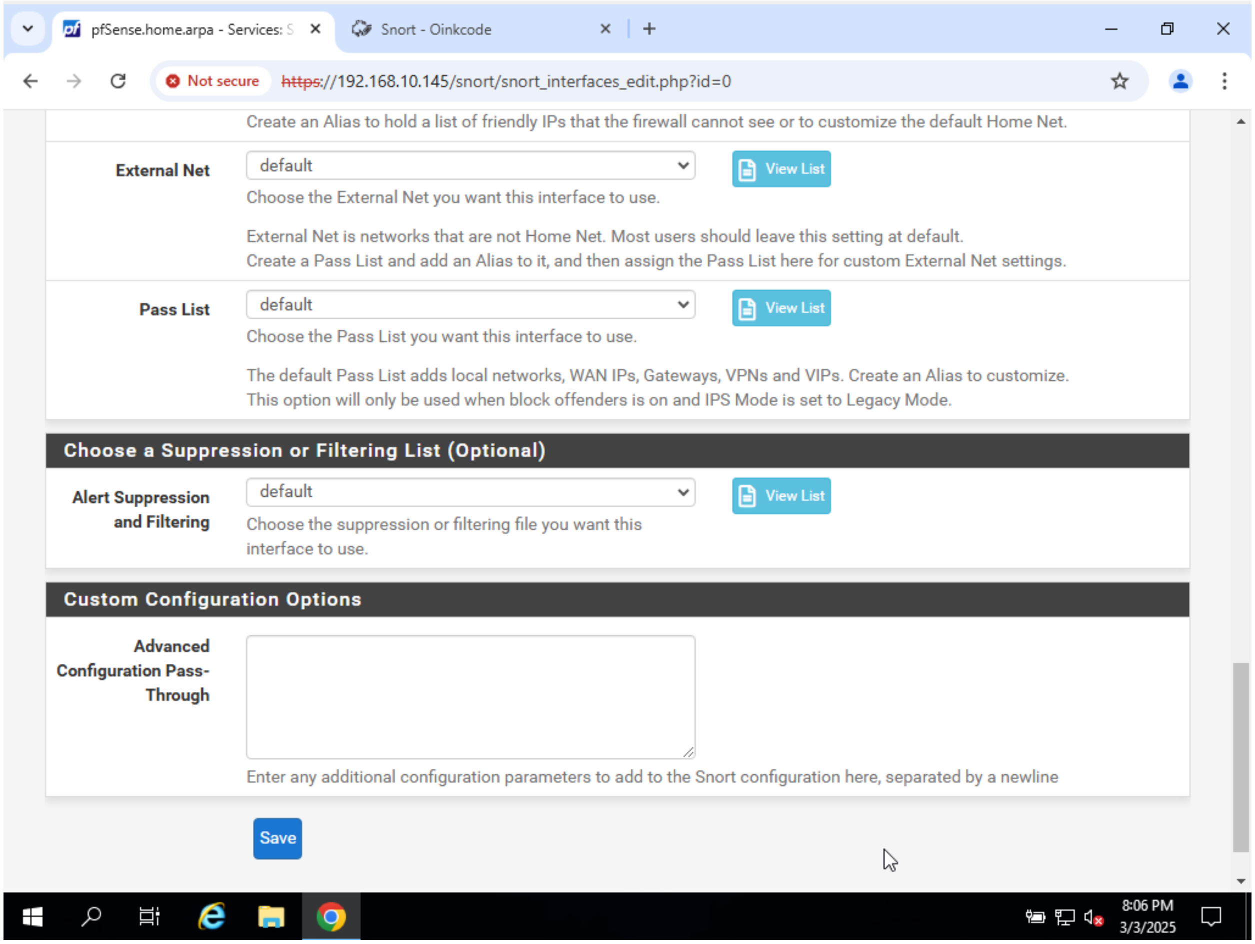
Block Settings

Block Offenders ☑ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced


pfSense.home.arpa - Services: S
Snort - Oinkcode
Not secure
https://192.168.10.145/snort/snort_interfaces_edit.php?id=0

Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.

External Net default

Choose the External Net you want this interface to use.

External Net is networks that are not Home Net. Most users should leave this setting at default.
Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.

Pass List default

Choose the Pass List you want this interface to use.

The default Pass List adds local networks, WAN IPs, Gateways, VPNs and VIPs. Create an Alias to customize.
This option will only be used when block offenders is on and IPS Mode is set to Legacy Mode.

Choose a Suppression or Filtering List (Optional)

Alert Suppression and Filtering default

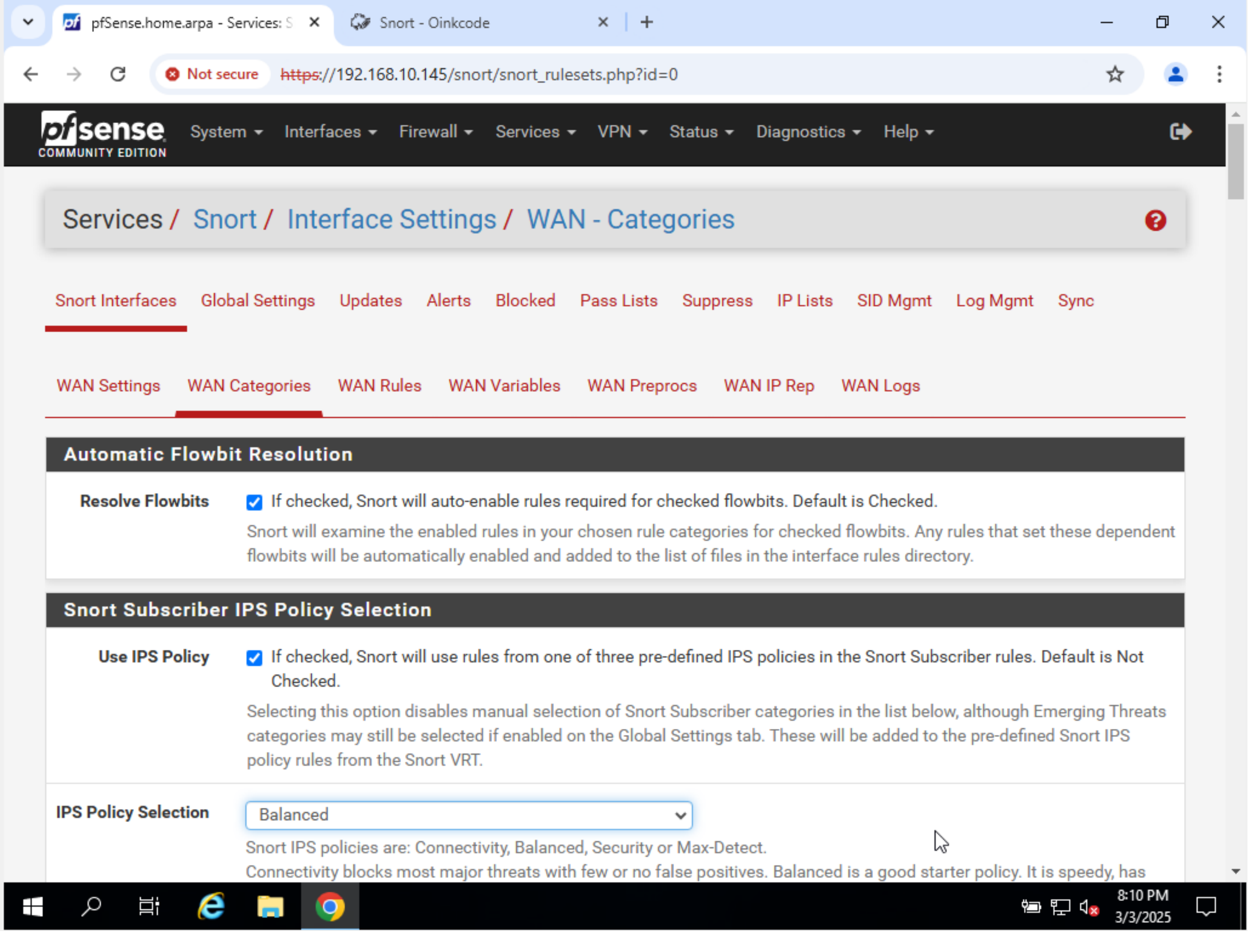
Choose the suppression or filtering file you want this interface to use.

Custom Configuration Options

Advanced Configuration Pass-Through

Enter any additional configuration parameters to add to the Snort configuration here, separated by a newline

- I left the other settings as default and clicked **Save**.


pfSense.home.arpa - Services: S
Snort - Oinkcode
Not secure
https://192.168.10.145/snort/snort_rulesets.php?id=0
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help

Services / Snort / Interface Settings / WAN - Categories

Automatic Flowbit Resolution

Resolve Flowbits ☑ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.

Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Snort Subscriber IPS Policy Selection

Use IPS Policy ☑ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.

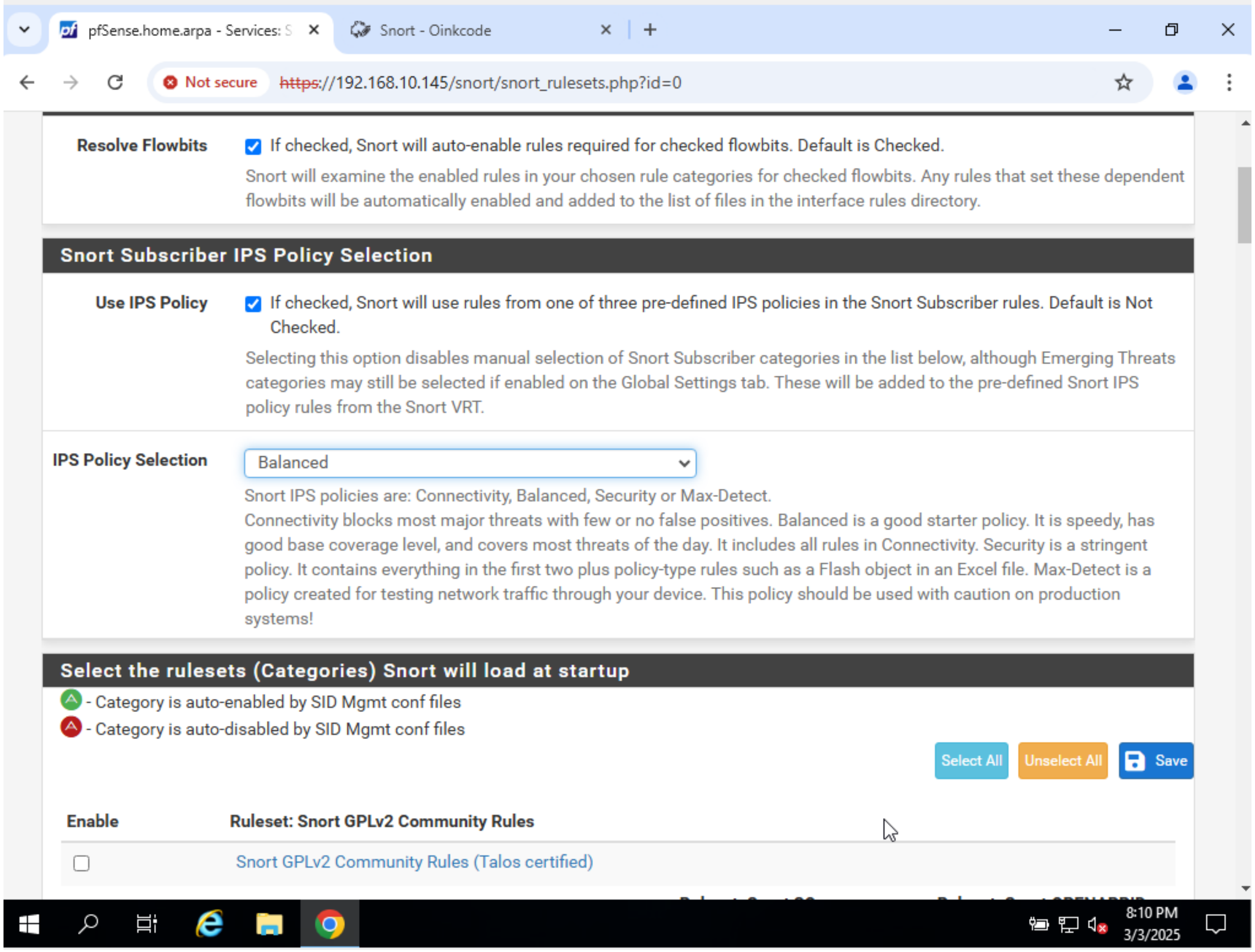
Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection Balanced

Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.

Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has

- In the **WAN Categories** tab, I enabled **Use IPS Policy** and set the **IPS Policy Mode** to **Balanced**.



pfSense.home.arpa - Services: S
Snort - Oinkcode
Not secure
https://192.168.10.145/snort/snort_rulesets.php?id=0

Resolve Flowbits ☑ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.

Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Snort Subscriber IPS Policy Selection

Use IPS Policy ☑ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.

Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection: Balanced

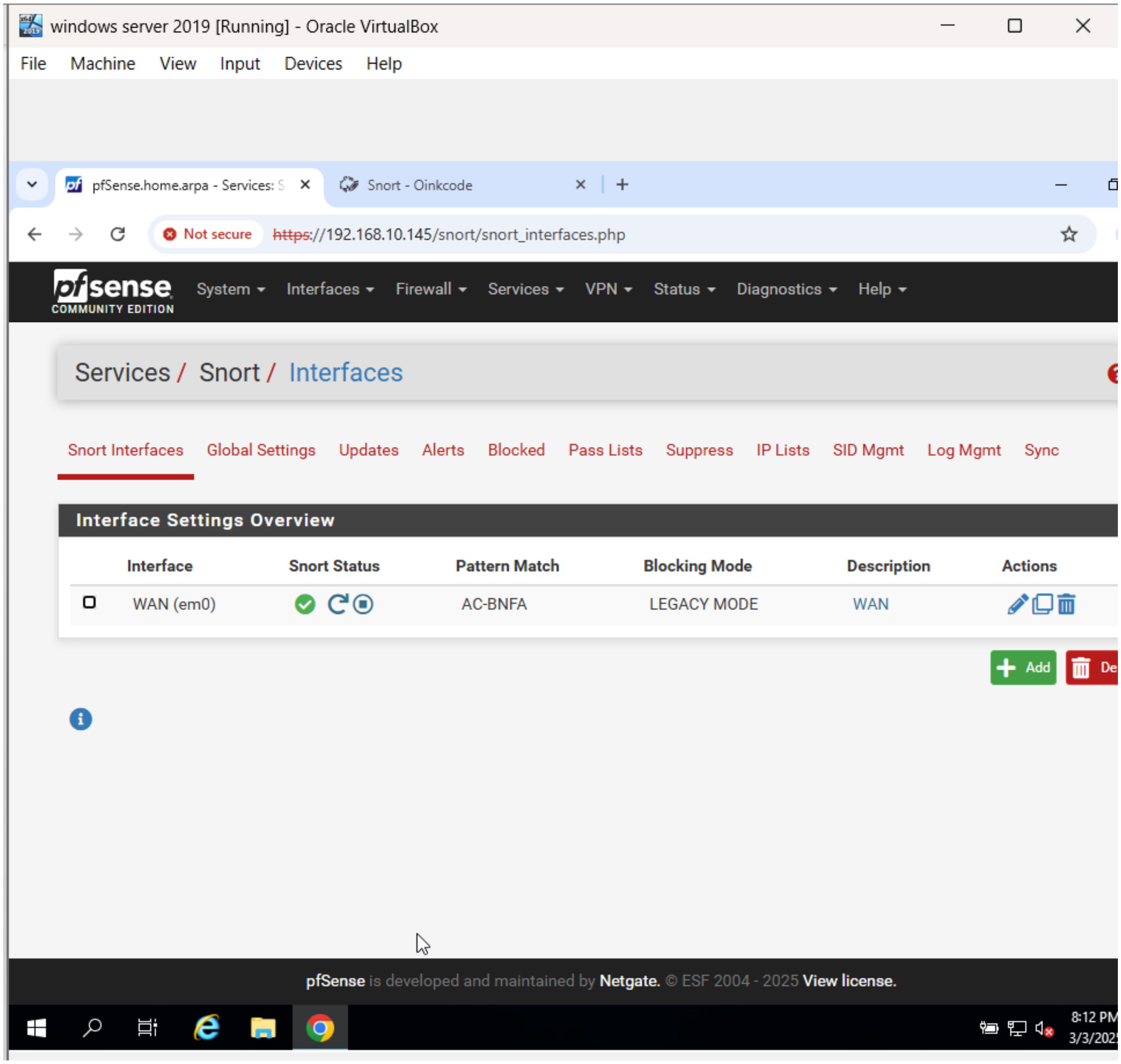
Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.
Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

Select the rulesets (Categories) Snort will load at startup

🟩 - Category is auto-enabled by SID Mgmt conf files
🟥 - Category is auto-disabled by SID Mgmt conf files

Enable	Ruleset: Snort GPLv2 Community Rules
☐	Snort GPLv2 Community Rules (Talos certified)

- I clicked **Save** to finalize the configuration.

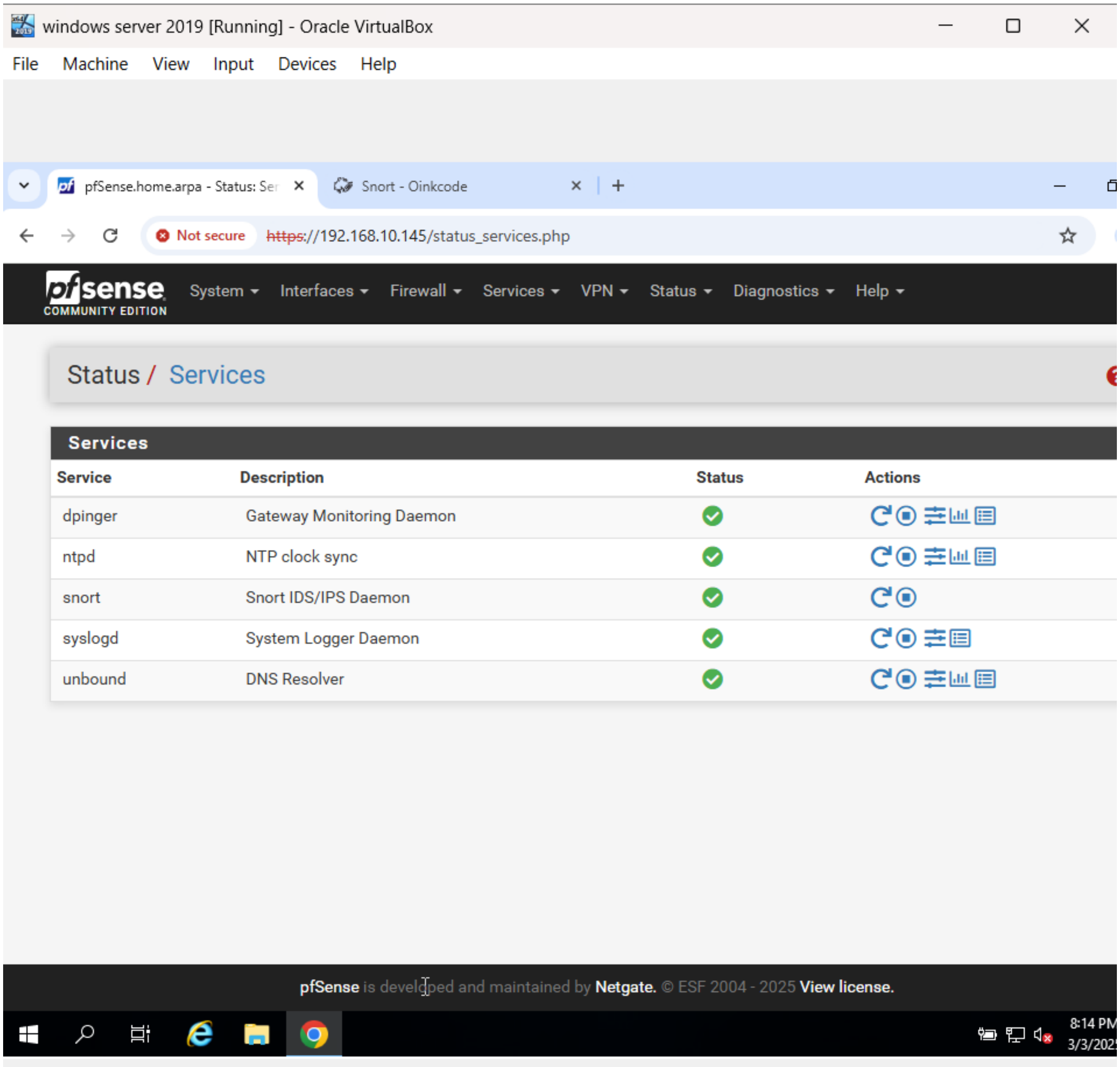


windows server 2019 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pfSense.home.arpa - Services: S
Snort - Oinkcode
Not secure
https://192.168.10.145/snort/snort_interfaces.php
pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
Services / Snort / Interfaces
Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync
Add
De
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.
8:12 PM
3/3/202

Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
□	WAN (em0)	✓	AC-BNFA	LEGACY MODE	WAN	

- I navigated to **Services > Snort > Interfaces** and clicked **Start Snort** to activate monitoring on the WAN interface.


windows server 2019 [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
pfSense.home.arpa - Status: Ser
Snort - Oinkcode
Not secure
https://192.168.10.145/status_services.php
pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
8:14 PM
3/3/202

Status / Services

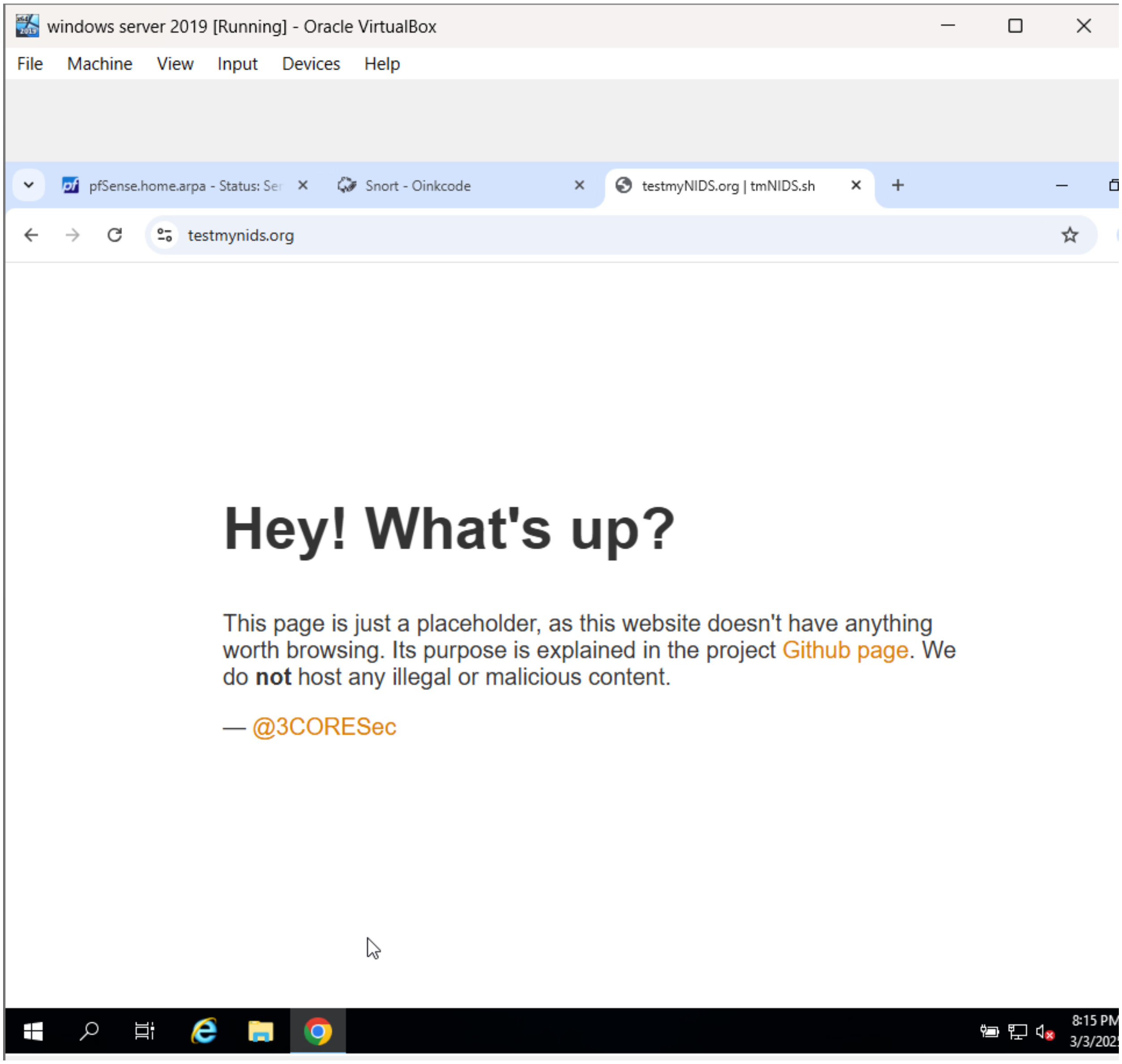
Services

Service	Description	Status	Actions
dpinger	Gateway Monitoring Daemon	✓	↻ ◉ ☰ 📊 ▤
ntpd	NTP clock sync	✓	↻ ◉ ☰ 📊 ▤
snort	Snort IDS/IPS Daemon	✓	↻ ◉
syslogd	System Logger Daemon	✓	↻ ◉ ☰ ▤
unbound	DNS Resolver	✓	↻ ◉ ☰ 📊 ▤

pfSense is developed and maintained by **Netgate.** © ESF 2004 - 2025 **View license.**

- I confirmed that Snort was running by checking the **Service Status** widget on the main pfSense dashboard.

Objective 3: Testing Snort Configuration

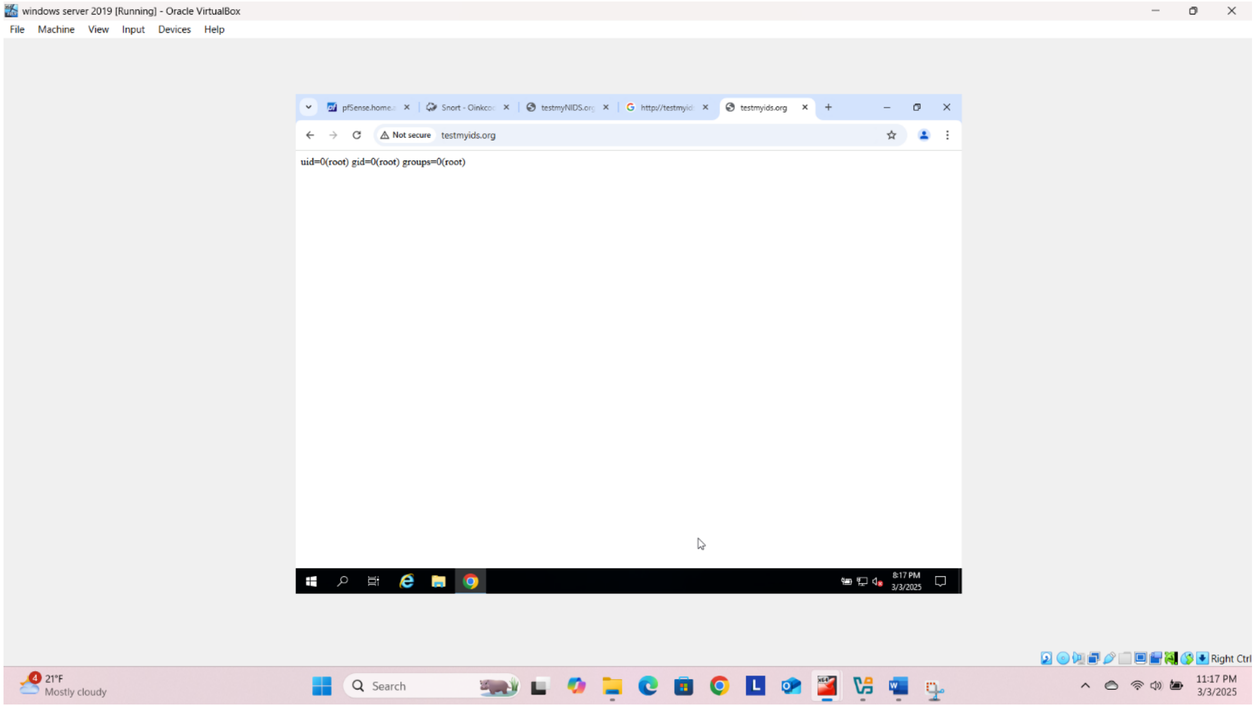

windows server 2019 [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
pfSense.home.arpa - Status: Ser
Snort - Oinkcode
testmyNIDS.org | tmNIDS.sh
testmynids.org
8:15 PM
3/3/202

Hey! What's up?

This page is just a placeholder, as this website doesn't have anything worth browsing. Its purpose is explained in the project Github page. We do **not** host any illegal or malicious content.

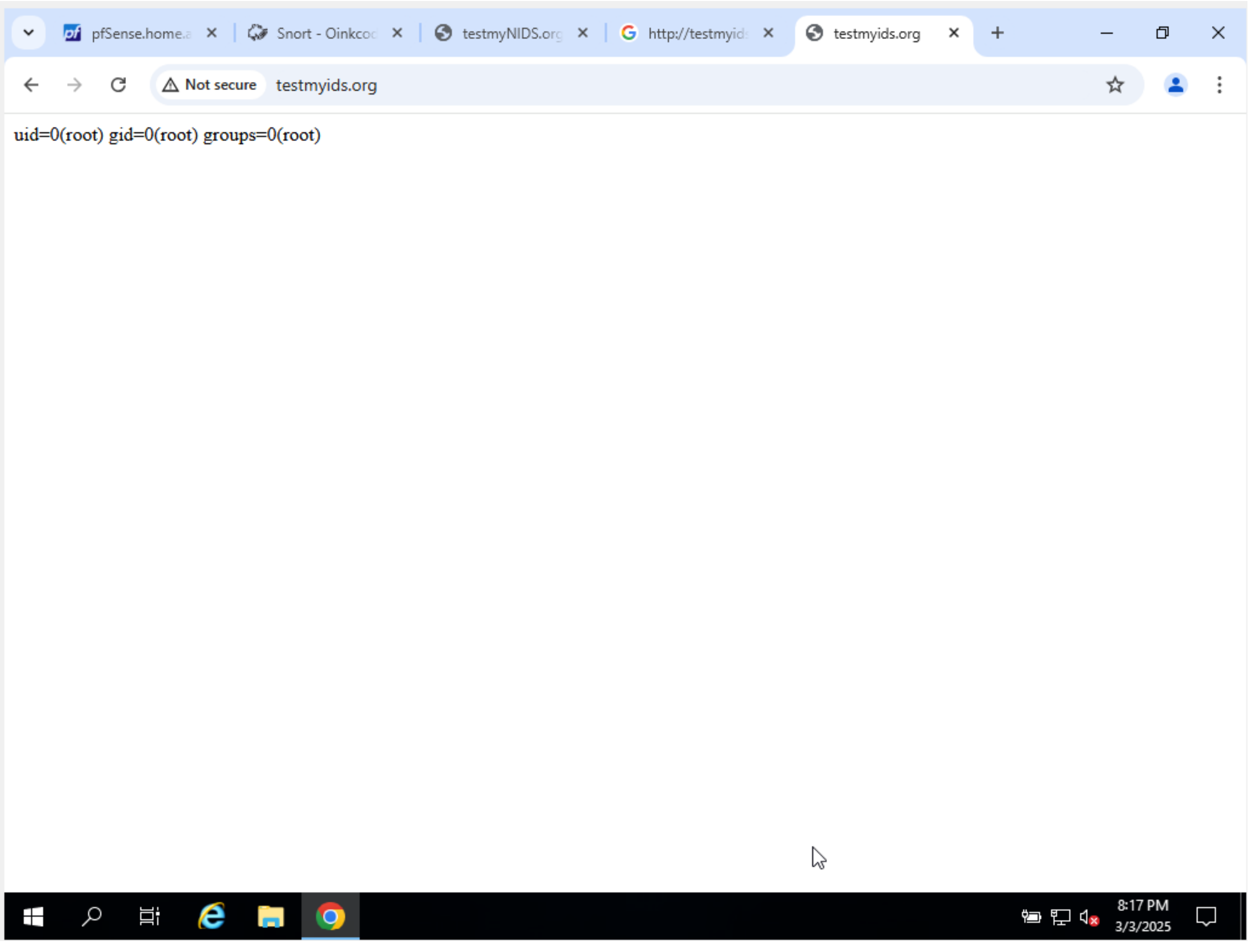
— @3CORESec

- To test Snort, I opened a browser on a machine protected by pfSense and visited https://testmynids.org.



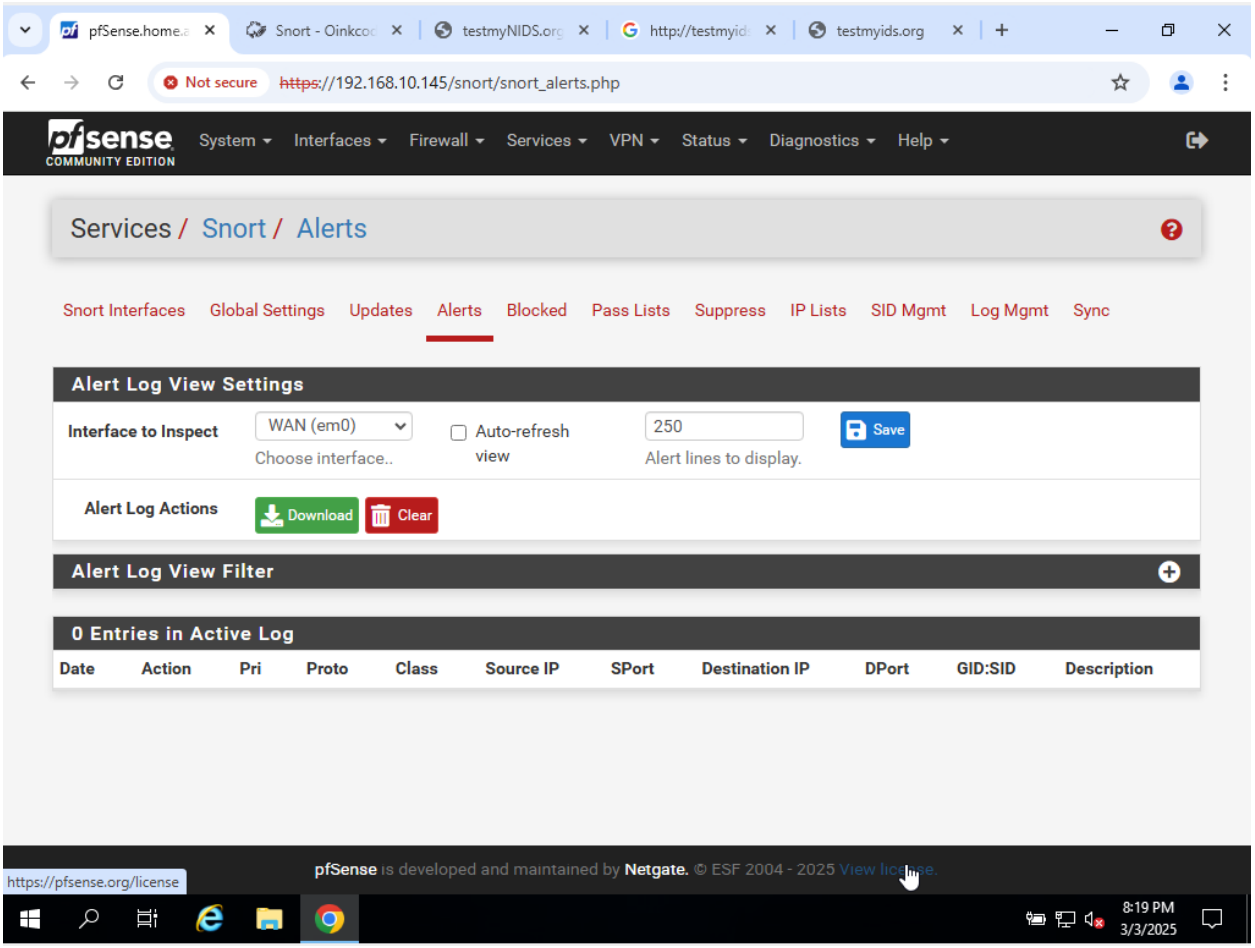
```
uid=0(root) gid=0(root) groups=0(root)
```

- Initially, the page loaded, but after refreshing, the site was blocked by pfSense.
- I confirmed that Snort was detecting and blocking threats in **Legacy Mode**.



```
uid=0(root) gid=0(root) groups=0(root)
```

- After that I have opened the website http://testmyids.org
- After that I viewed the code.



Services / Snort / Alerts

Alert Log View Settings

Interface to Inspect: WAN (em0) — Choose interface..

□ Auto-refresh view

250 — Alert lines to display.

Alert Log Actions

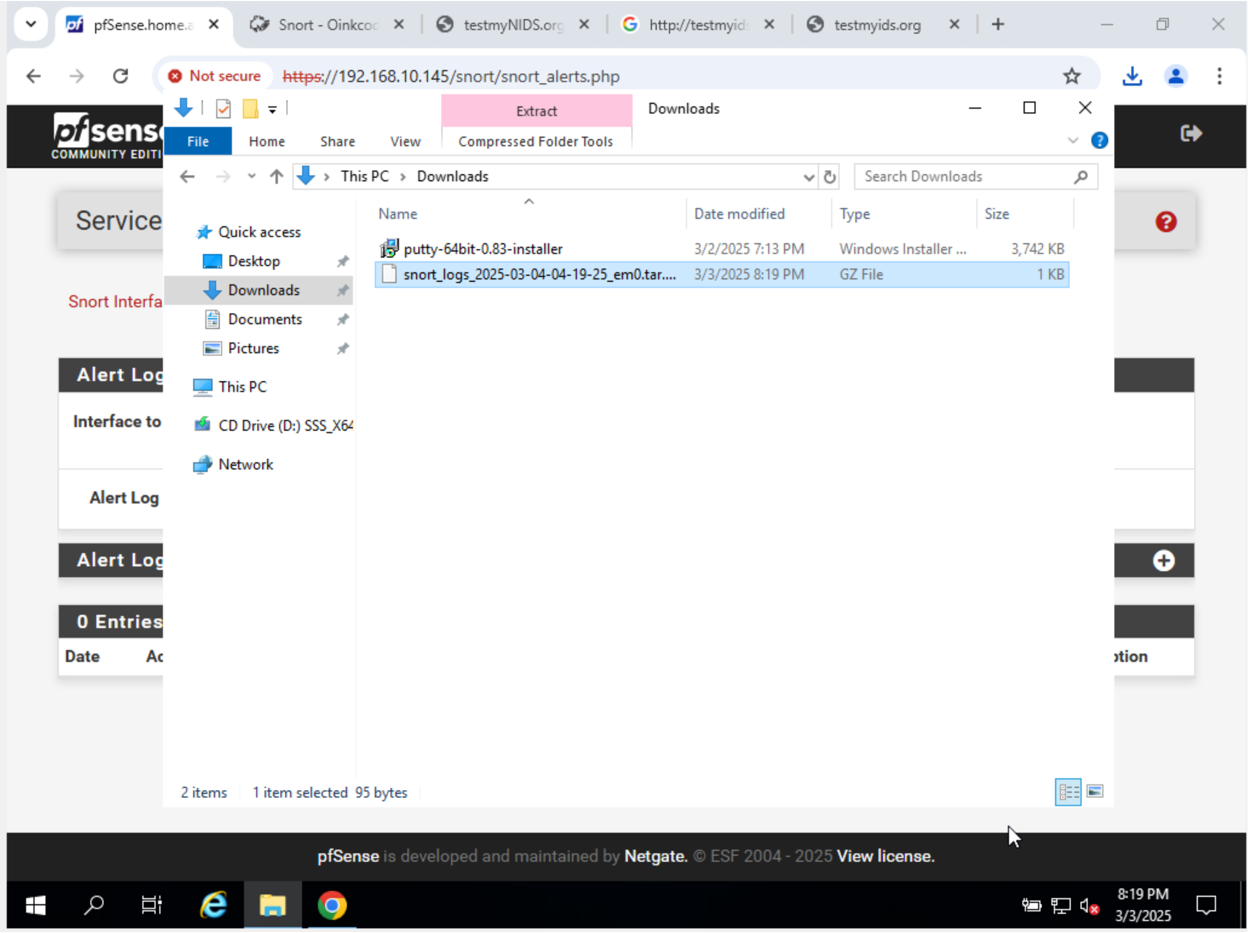
Alert Log View Filter

0 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

- To view alerts, I navigated to **Services** > **Snort** > **Alerts** and verified the logs.
- I can't find alerts and I asked my student assistants so they told it is fine.



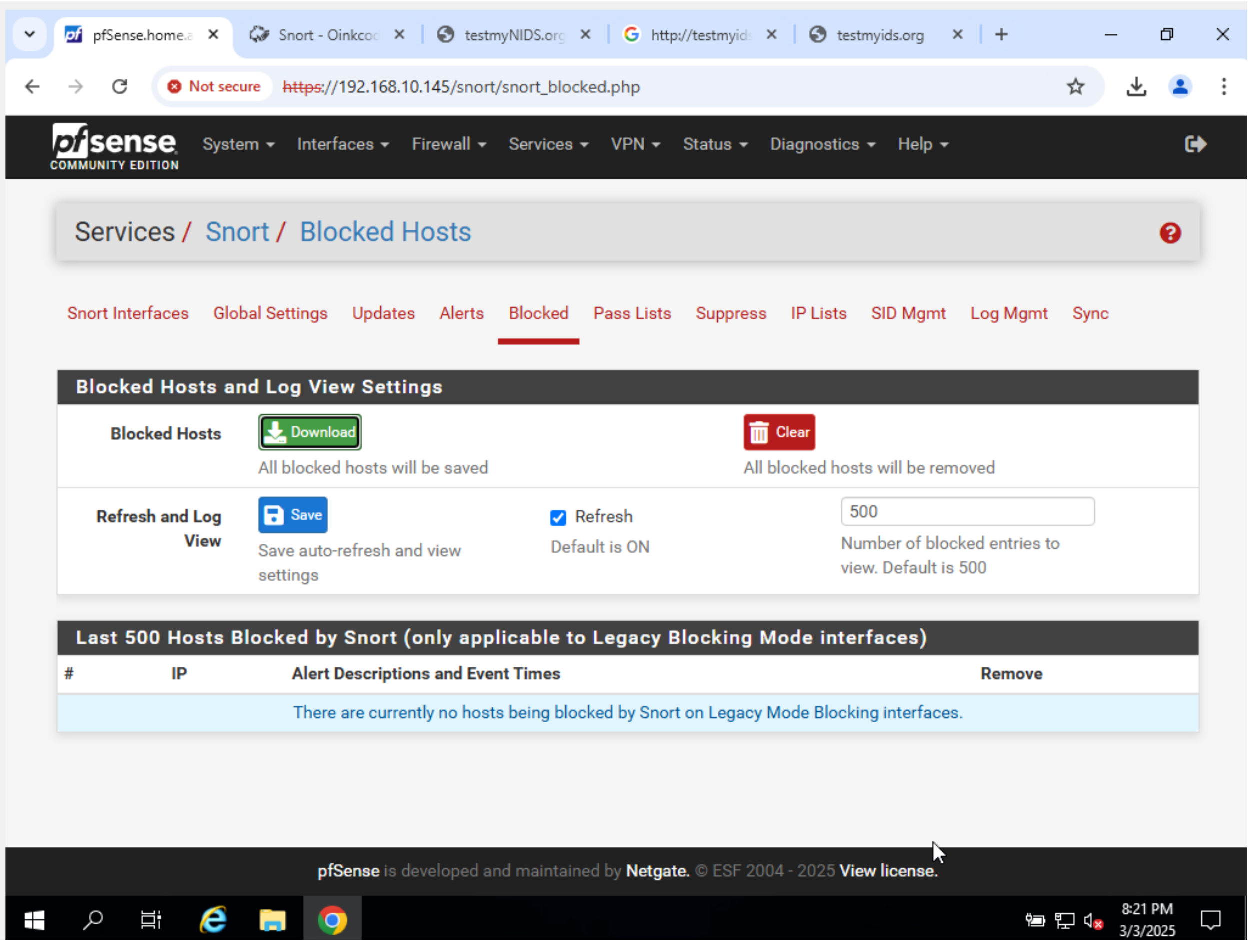
https://192.168.10.145/snort/snort_alerts.php

This PC › Downloads

Name	Date modified	Type	Size
putty-64bit-0.83-installer	3/2/2025 7:13 PM	Windows Installer ...	3,742 KB
snort_logs_2025-03-04-04-19-25_em0.tar....	3/3/2025 8:19 PM	GZ File	1 KB

2 items 1 item selected 95 bytes

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.



Services / Snort / Blocked Hosts

Blocked Hosts and Log View Settings

Blocked Hosts — Download — All blocked hosts will be saved — Clear — All blocked hosts will be removed

Refresh and Log View — Save — Save auto-refresh and view settings — ☑ Refresh — Default is ON — 500 — Number of blocked entries to view. Default is 500

Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove

There are currently no hosts being blocked by Snort on Legacy Mode Blocking interfaces.

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.

- In the **Blocked** tab, I checked the list of blocked IP addresses.

  (To ensure that alerts were being recorded in the **ELK stack**, I searched for a **MALWARE-OTHER** message in **Kibana's Discovery page**.)
  it doesn't worked for us.

Conclusion

Through this lab, I successfully installed and configured **Snort IDS on pfSense**, enabling **Intrusion Prevention System (IPS) functionality**. The setup effectively blocked threats and logged security events, improving the firewall's ability to detect malicious activity. By integrating Snort with pfSense, I added an additional layer of protection to the network.