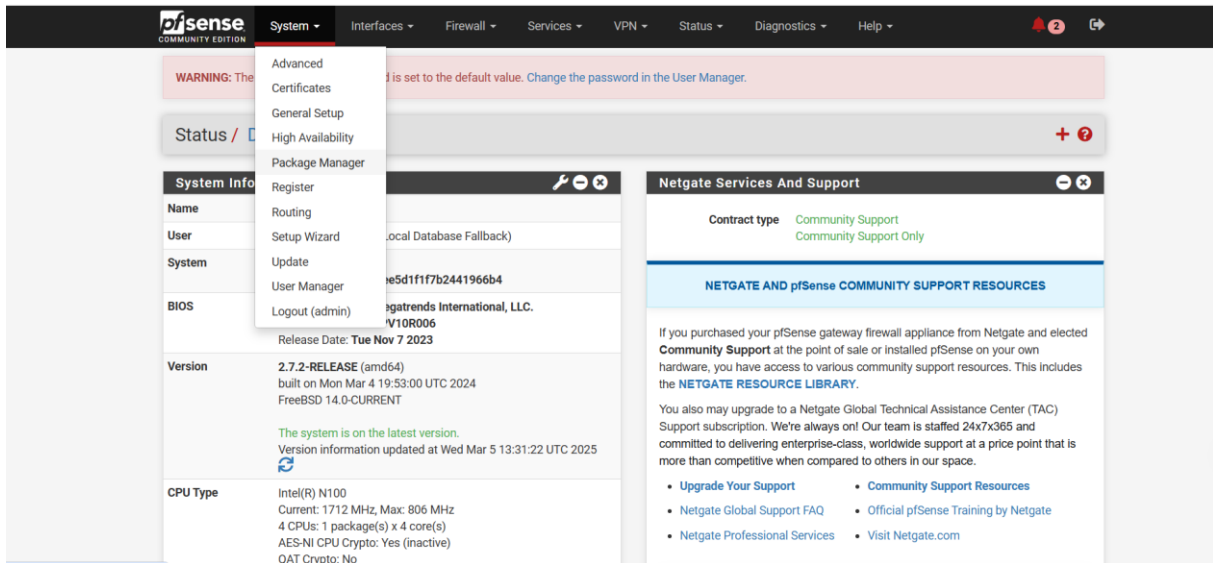
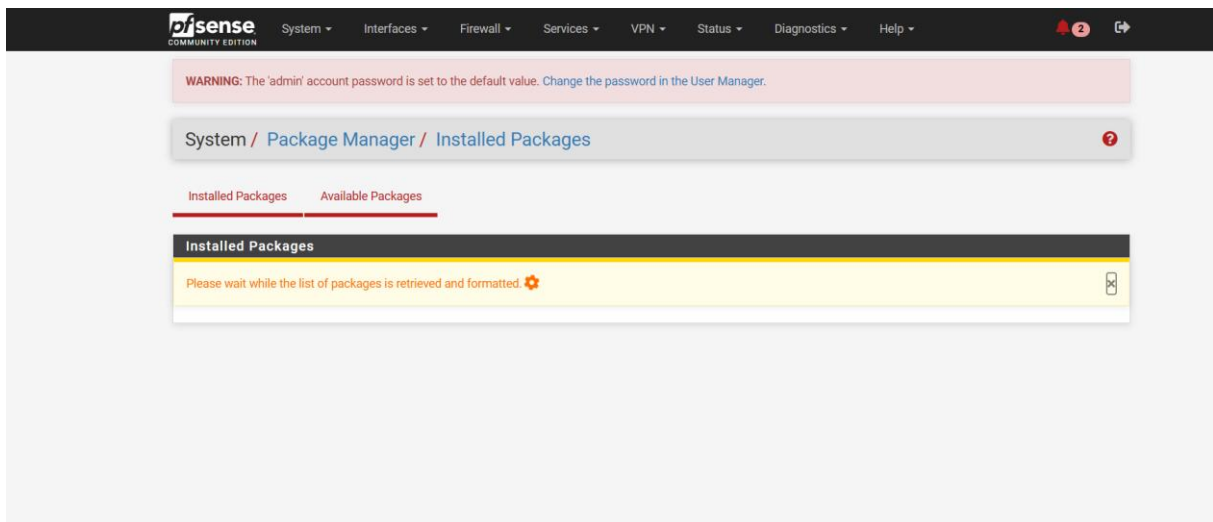


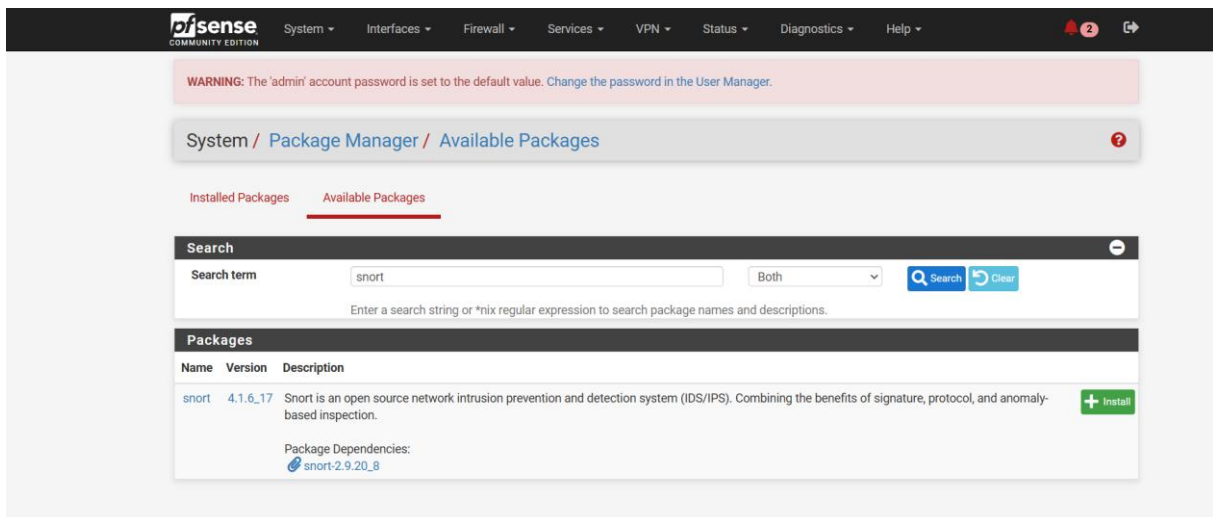
Installation service Snort



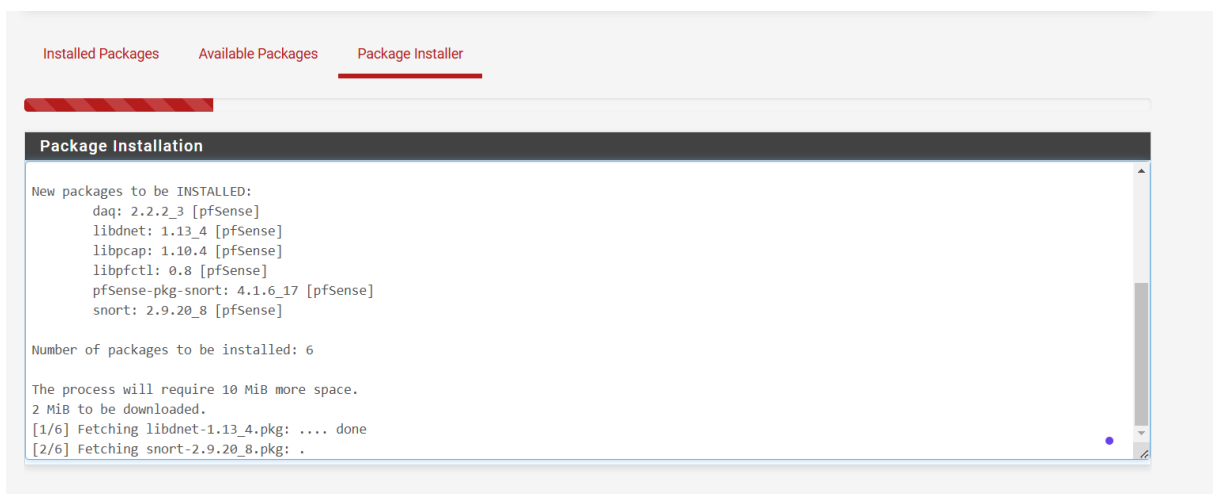
Connecter vous au PfSense, cliquez sur système puis Package Manager.



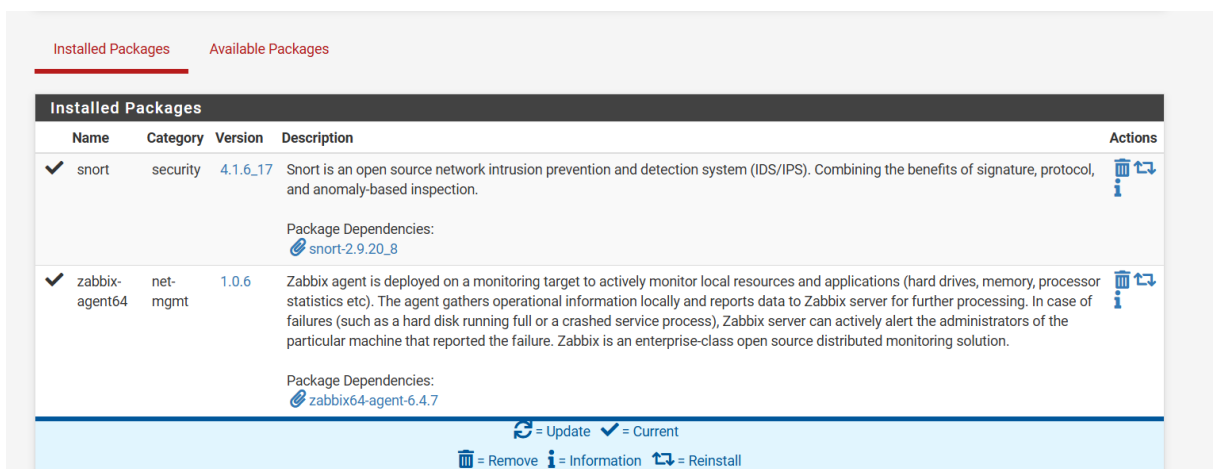
Cliquez sur Available Packages.



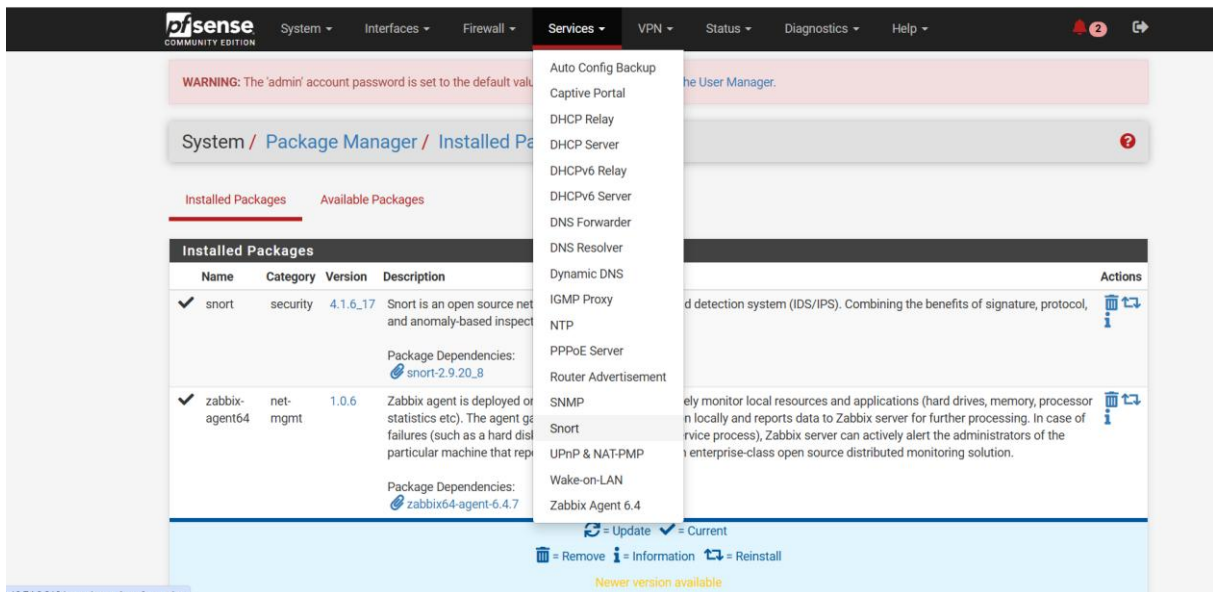
Dans la barre de recherche tapez « snort » puis sur recherché et enfin cliquez sur installer.



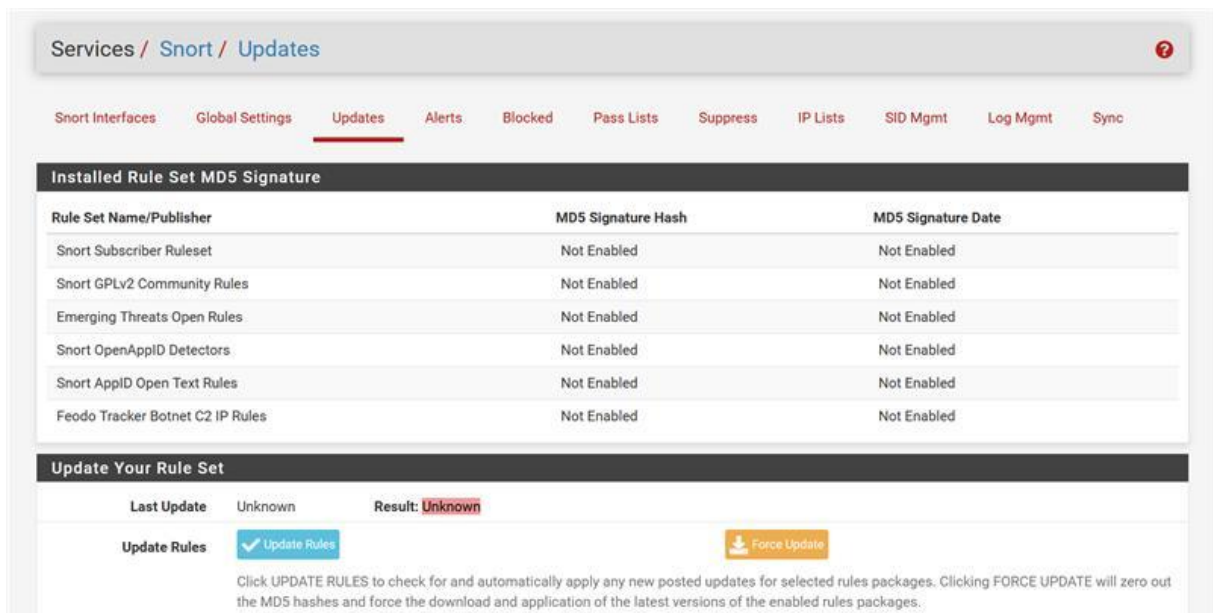
Le téléchargement va débuter et installer tous les packages nécessaire



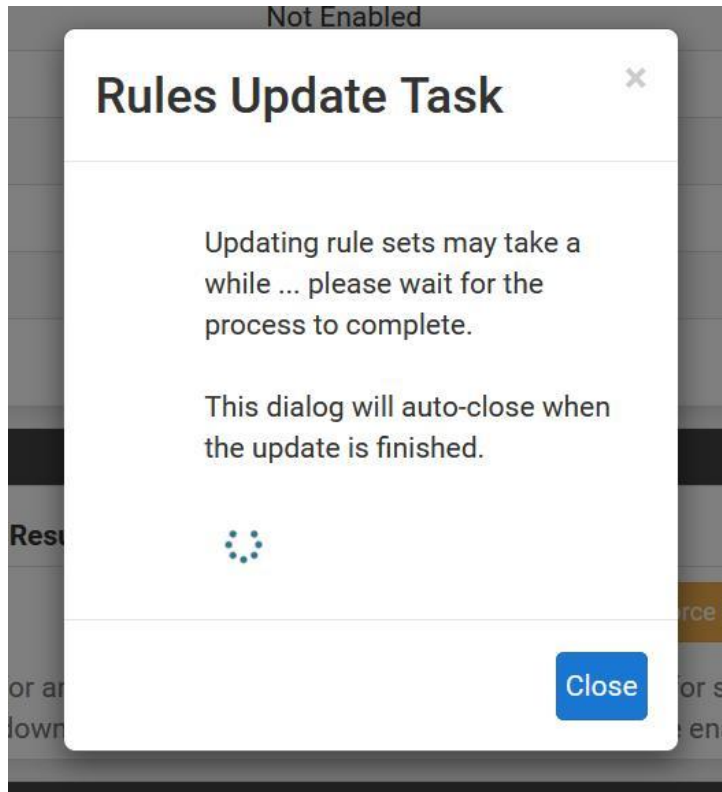
Dans l'onglet Installed Packages, l'add-on « Snort » est bien installé.



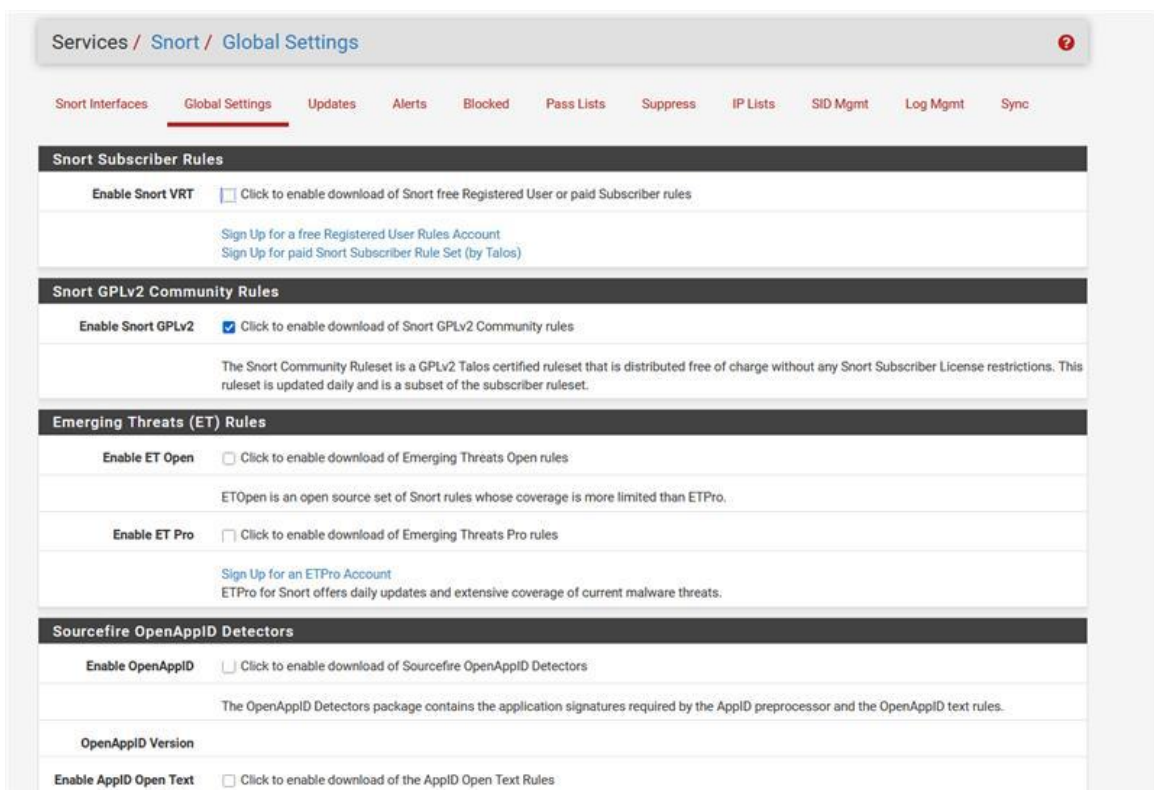
Dans la catégorie services, un onglet snort est disponible, cliqué dessus



Dans l'onglet Updates, cliquez sur Update Rules.



Dans l'onglet Global Settings, créer un compte gratuit snort, enfin prenez le code Oinkmaster. Enfin ajoutez les différentes options cochées ci-dessous.



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 as Crìdex, Dridex, Geodo, Heodo and Emotet.

Rules Update Settings

Update Interval 1 DAY

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

Update Start Time 00:46

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 30 MINS

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.

Puis cliquez sur Save

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
<input type="checkbox"/> WAN (igc0)	✘ ▶	AC-BNFA	LEGACY MODE	WAN	✎ 📄 🗑️

Sur l'onglet Snort Interfaces, cliquez sur Add et ajouté l'option Wan.

Cochez les différentes options dans l'onglet Wan Settings.

Services / Snort / WAN - Interface Settings ?

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

WAN Settings WAN Categories WAN Rules WAN Variables WAN Preprocs WAN IP Rep WAN Logs

General Settings

Enable	<input checked="" type="checkbox"/> Enable interface
Interface	<input type="text" value="WAN (igc0)"/> Choose the interface where this Snort instance will inspect traffic.
Description	<input type="text" value="WAN"/> Enter a meaningful description here for your reference.
Snap Length	<input type="text" value="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	<input type="checkbox"/> Snort will send Alerts to the firewall's system log. Default is Not Checked.
Enable Packet Captures	<input checked="" type="checkbox"/> Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Packet Capture File Size	<input type="text" value="128"/> Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_igc09545 is rotated and a new file opened.
Enable Unified2 Logging	<input type="checkbox"/> 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	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	<input type="text" value="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 with Inline Mode, switch to Legacy Mode instead.
Kill States	<input checked="" type="checkbox"/> Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	<input type="text" value="BOTH"/> Select which IP extracted from the packet you wish to block. Default is BOTH.

Detection Performance Settings

Search Method	<input type="text" value="AC-BNFA"/> Choose a fast pattern matcher algorithm. Default is AC-BNFA.
Split ANY-ANY	<input type="checkbox"/> Enable splitting of ANY-ANY port group. Default is Not Checked.
Search Optimize	<input type="checkbox"/> Enable search optimization. Default is Not Checked.
Stream Inserts	<input type="checkbox"/> Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.
Checksum Check Disable	<input type="checkbox"/> Disable checksum checking within Snort to improve performance. Default is Not Checked.

Choose the Networks Snort Should Inspect and Whitelist

Home Net	<input type="text" value="pfSenseInterfaces"/>	View List
Choose the Home Net you want this interface to use.		
Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs. Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.		
External Net	<input type="text" value="default"/>	View List
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	<input type="text" value="pfSenseInterfaces"/>	View List
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	<input type="text" value="wansuppress_67da85675d3cb"/>	View List
Choose the suppression or filtering file you want this interface to use.		

Custom Configuration Options

Advanced Configuration Pass-Through	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>
Enter any additional configuration parameters to add to the Snort configuration here, separated by a newline	

[Save](#)



Sauvegarder la configuration.

Dans l'onglet Wan Categories, cochez les différentes

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.

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

[Select All](#) [Unselect All](#) [Save](#)

Enable **Ruleset: Snort GPLv2 Community Rules**

[Snort GPLv2 Community Rules \(Talos certified\)](#)

rules are not enabled. **Snort Subscriber rules are not enabled.** **Snort OPENAPPID rules are not enabled.**

[Save](#)

Dans la catégorie WAN Preprocs cochez les options suivantes

Services / Snort / Interface Settings / WAN - Preprocessors and Flow ?

[Snort Interfaces](#) [Global Settings](#) [Updates](#) [Alerts](#) [Blocked](#) [Pass Lists](#) [Suppress](#) [IP Lists](#) [SID Mgmt](#) [Log Mgmt](#) [Sync](#)

[WAN Settings](#) [WAN Categories](#) [WAN Rules](#) [WAN Variables](#) [WAN Preprocs](#) [WAN IP Rep](#) [WAN Logs](#)

Important Preprocessor Information

Rules may be dependent on enabled preprocessors! Disabling preprocessors may result in Snort startup failure unless all of the corresponding preprocessor-dependent rules are also disabled. Do not disable any default-enabled preprocessors on this page unless you are very skilled with using Snort. If you experience Snort start-up errors or failures after making changes to preprocessors, trying resetting all preprocessor configurations to their defaults, and then attempt to start Snort.

Preprocessors Basic Configuration Settings

Enable Performance Stats Collect Performance Statistics for this interface. Default is Not Checked.
Snort will automatically generate performance statistics for this interface. Enabling this option may have a slight negative performance impact. Statistics may be viewed on the LOGS tab for this interface. Performance Statistics are disabled by default.

Protect Customized Preprocessor Rules Enable this only if you maintain customized preprocessor text rules files for this interface. Default is Not Checked.
Enable this only if you use customized preprocessor text rules files and you do not want them overwritten by automatic Snort Subscriber Rules updates. This option is disabled when Snort Subscriber Rules download is not enabled on the Global Settings tab. Most users should leave this option unchecked.

Auto Rule Disable Auto-disable text rules dependent on disabled preprocessors for this interface. Default is Not Checked.
Enabling this option allows Snort to automatically disable any text rules containing rule options or content modifiers that are dependent upon the preprocessors you have not enabled. This may facilitate starting Snort without errors related to disabled preprocessors, but can substantially compromise the level of protection by automatically disabling detection rules. Enabling this feature will result in decreased protection from Snort.

Enable RPC Decode and Back Orifice Detector Normalize/Decode RPC traffic and detects Back Orifice traffic on the network. Default is Checked.

Enable DCE/RPC2 Detection The DCE/RPC preprocessor detects and decodes SMB and DCE/RPC traffic. Default is Checked.

Enable SIP Detection The SIP preprocessor decodes SIP traffic and detects vulnerabilities. Default is Checked.

Enable GTP Detection The GTP preprocessor decodes GPRS Tunneling Protocol traffic and detects intrusion attempts. Default is Not Checked.

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	Not Enabled	Not Enabled
Snort GPLV2 Community Rules	b0c300c5610bb3793c46cdd7655916b5	Tuesday, 18-Mar-25 10:02:16 UTC
Emerging Threats Open Rules	Not Enabled	Not Enabled
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update: Mar-18 2025 10:08 Result: Success

Update Rules ✔ Update Rules ⬇ Force Update

Click UP Check for and install only new updates any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 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: 25 KIB

Créer une Pass list (Revenir sur Wan Setting pour valider)

Services / Snort / Pass Lists ?

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

Configured Pass Lists

List Name	Assigned	Description	Actions
<input type="checkbox"/> pfSenseInterfaces	No		✎ 🗑

+ Add 🗑 Delete

i



General Information

Name

The list name may only consist of the characters 'a-z, A-Z, 0-9 and _'.

Description

You may enter a description here for your reference.

Auto-Generated IP Addresses

Local Networks Add firewall Locally-Attached Networks to the list (excluding WAN). Default is Checked.

WAN Gateways Add WAN Gateways to the list. Default is Checked.

WAN DNS Servers Add WAN DNS servers to the list. Default is Checked.

Virtual IP Addresses Add Virtual IP Addresses to the list. Default is Checked.

VPN Addresses Add VPN Addresses to the list. Default is Checked.

Custom IP Addresses and Configured Firewall Aliases

Hint Enter as many IP addresses or alias names as desired. Enter ONLY an IP address, IP subnet or alias name! Do NOT enter a FQDN (fully qualified domain name) directly! To use a FQDN, first create the necessary firewall alias, and then provide the alias name here. FQDN aliases are periodically re-resolved and updated by the firewall. You can also provide an IP subnet with a proper netmask of the form network/mask such as 1.2.3.0/24.

IP or Alias



General Settings

Enable Enable interface

Interface

Choose the interface where this Snort instance will inspect traffic.

Description

Enter a meaningful description here for your reference.

Snap Length

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.

Enable Packet Captures Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Packet Capture File Size

Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snorl_igc09545 is rotated and a new file opened.

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.

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (igc0)	✔ ↺	AC-BNFA	LEGACY MODE	WAN	✎ 📄 🗑️

Available Rule Categories

Category Selection: ▼
 Select the rule category to view and manage.

Rule Signature ID (SID) Enable/Disable Overrides

SID Actions:
 Apply
Reset All
Reset Current
Disable All
Enable All

When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.

Rules View Filter +

Selected Category's Rules

Legend:
✔ Default Enabled
✔ Enabled by user
✔ Auto-enabled by SID Mgmt
⚡ Action/content modified by SID Mgmt
⚠ Rule action is alert
✘ Default Disabled
✘ Disabled by user
✘ Auto-disabled by SID Mgmt

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
✘	⚠	1	105	tcp	\$HOME_NET	2589	\$EXTERNAL_NET	any	MALWARE-BACKDOOR - Dagger_1.4.0
✘	⚠	1	108	tcp	\$EXTERNAL_NET	any	\$HOME_NET	7597	MALWARE-BACKDOOR QAZ Worm Client Login access
✘	⚠	1	110	tcp	\$EXTERNAL_NET	any	\$HOME_NET	12345:12346	MALWARE-BACKDOOR netbus getinfo
✘	⚠	1	115	tcp	\$HOME_NET	20034	\$EXTERNAL_NET	any	MALWARE-BACKDOOR NetBus Pro 2.0 connection established
✘	⚠	1	117	tcp	\$HOME_NET	any	\$EXTERNAL_NET	any	MALWARE-BACKDOOR Infector.1.x
✘	⚠	1	118	tcp	\$HOME_NET	666	\$EXTERNAL_NET	any	MALWARE-BACKDOOR

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

WAN Settings WAN Categories **WAN Rules** WAN Variables WAN Preprocs WAN IP Rep WAN Logs

Available Rule Categories

Category Selection: Select the rule category to view and manage.

Rule Signature ID (SID) Enable/Disable Overrides

SID Actions

When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.

Rules View Filter **Enable all rules in the currently selected category**

Selected Category's Rules

Legend: Default Enabled Enabled by user Auto-enabled by SID Mgmt Action/content modified by SID Mgmt Rule action is alert
 Default Disabled Disabled by user Auto-disabled by SID Mgmt

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	105	tcp	\$HOME_NET	2589	\$EXTERNAL_NET	any	MALWARE-BACKDOOR - Dagger_1.4.0
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	108	tcp	\$EXTERNAL_NET	any	\$HOME_NET	7597	MALWARE-BACKDOOR QAZ Worm Client Login access
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	110	tcp	\$EXTERNAL_NET	any	\$HOME_NET	12345:12346	MALWARE-BACKDOOR netbus getinfo
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	115	tcp	\$HOME_NET	20034	\$EXTERNAL_NET	any	MALWARE-BACKDOOR NetBus Pro 2.0 connection established
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	117	tcp	\$HOME_NET	any	\$EXTERNAL_NET	any	MALWARE-BACKDOOR Infector.1.x
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	118	tcp	\$HOME_NET	666	\$EXTERNAL_NET	any	MALWARE-BACKDOOR SatansBackdoor 2.0 Beta

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

WAN Settings WAN Categories **WAN Rules** WAN Variables WAN Preprocs WAN IP Rep WAN Logs

Available Rule Categories

Category Selection: Select the rule category to view and manage.

Rule Signature ID (SID) Enable/Disable Overrides

SID Actions

When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.

Rules View Filter **Enable all rules in the currently selected category**

Selected Category's Rules

Legend: Default Enabled Enabled by user Auto-enabled by SID Mgmt Action/content modified by SID Mgmt Rule action is alert
 Default Disabled Disabled by user Auto-disabled by SID Mgmt

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	105	tcp	\$HOME_NET	2589	\$EXTERNAL_NET	any	MALWARE-BACKDOOR - Dagger_1.4.0
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	108	tcp	\$EXTERNAL_NET	any	\$HOME_NET	7597	MALWARE-BACKDOOR QAZ Worm Client Login access
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	110	tcp	\$EXTERNAL_NET	any	\$HOME_NET	12345:12346	MALWARE-BACKDOOR netbus getinfo
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	115	tcp	\$HOME_NET	20034	\$EXTERNAL_NET	any	MALWARE-BACKDOOR NetBus Pro 2.0 connection established
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	117	tcp	\$HOME_NET	any	\$EXTERNAL_NET	any	MALWARE-BACKDOOR Infector.1.x
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	118	tcp	\$HOME_NET	666	\$EXTERNAL_NET	any	MALWARE-BACKDOOR SatansBackdoor.2.0 Beta
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	119	tcp	\$HOME_NET	6789	\$EXTERNAL_NET	any	MALWARE-BACKDOOR Doly 2.0 access