



Procédure PFSense - Snort Installation

➤ Ouvrez un logiciel de navigateur, entrez l'adresse IP de votre pare-feu Pfsense et accédez à l'interface Web.

➤ Dans le contexte HSP, l'URL suivante a été saisie dans le navigateur :

<https://172.16.0.101>

L'interface web Pfsense doit être présentée.

SIGN IN

Username

Password

SIGN IN

➤ Sur l'écran rapide, entrez les informations de connexion Pfsense Default Password.

- Username : pfsense

- Mot de passe : *****

Après une connexion réussie, vous serez envoyé au tableau de bord Pfsense.

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / Dashboard

System Information

Name: firewall.techexpert.tips

User: admin@192.168.15.9 (Local Database)

System: VirtualBox Virtual Machine
Netgate Device ID: 98b7aa49047384d25c9d

BIOS: Vendor: innotek GmbH
Version: VirtualBox
Release Date: Fri Dec 1 2006

Version: 2.4.4-RELEASE-p3 (amd64)
built on Wed May 15 18:53:44 EDT 2019
FreeBSD 11.2-RELEASE-p10

The system is on the latest version.
Version information updated at Wed Sep 25 23:57:25 -03 2019

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Accéder au menu Pfsense System et sélectionner l'option De gestionnaire de paquets.

System ▾

- Advanced
- Cert. Manager
- General Setup
- High Avail. Sync
- Logout (admin)
- Package Manager**
- Routing
- Setup Wizard
- Update
- User Manager

- Sur l'écran du gestionnaire de paquets, accéder à l'onglet Paquets disponibles.
- Sur l'onglet Paquets disponibles, recherchez SNORT et installer le paquet SNORT.

Packages

Name	Version	Description
<u>snort</u>	<u>3.2.9.10</u>	Snort is an open source network intrusion prevention and detection system (IDS/IPS) based inspection.

Package Dependencies:
[snort-2.9.15](#) [barnyard2-1.13_1](#)

[+ Install](#)

- Dans notre exemple, nous avons installé la version 3.2.9.10 du paquet SNORT.
- Attendre la fin de l'installation SNORT.
- Accéder au menu Pfsense Services et sélectionnez l'option SNORT.



- Sur l'onglet Paramètres Global, localisez les règles d'abonné SNORT et effectuez la configuration suivante :
- Activer Snort VRT - Oui
 - > accédez au site Web Snort, créez un compte et obtenez un Oinkcode gratuit.

Snort Subscriber Rules	
Enable Snort VRT	<input checked="" type="checkbox"/> 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	<input type="text" value="AAAAAAAAAAAAA"/>

- > Localiser la zone Paramètres de mise à jour des règles et effectuer la configuration suivante :
- Intervalle de mise à jour - Sélectionnez l'intervalle de mise à jour souhaité
- Heure de démarrage de mise à jour - Définir l'heure désirée pour mettre à jour les règles Snort

Rules Update Settings	
Update Interval	<div>1 DAY</div> <div>Please select the interval for rule updates. Choosing NEVER disables</div>
Update Start Time	<div>00:05</div> <div>Enter the rule update start time in 24-hour format (HH:MM). Default specified here. For example, using the default start time of 00:05 and choos</div>
Hide Deprecated Rules Categories	<input type="checkbox"/> Click to hide deprecated rules categories in the GUI and remove them
Disable SSL Peer Verification	<input type="checkbox"/> Click to disable verification of SSL peers during rules updates. This is

- Localiser la zone Paramètres généraux et effectuer la configuration suivante :
- Supprimer l'intervalle des hôtes bloqués - 1 heure
- Supprimer les hôtes bloqués après la désinstallation – Non
- Conserver les paramètres snort après la désinstallation – Oui
- Intervalle de mise à jour de démarrage/shutdown - non

General Settings	
Remove Blocked Hosts Interval	<div>1 HOUR</div> <div>Please select the amount of time you would like hosts to be blocked.</div>
Remove Blocked Hosts After Deinstall	<input type="checkbox"/> Click to clear all blocked hosts added by Snort when removing the
Keep Snort Settings After Deinstall	<input checked="" type="checkbox"/> Click to retain Snort settings after package removal.
Startup/Shutdown Logging	<input type="checkbox"/> Click to output detailed messages to the system log when Snort is

- Sur l'onglet Mises à jour, cliquez sur le bouton Règles de mise à jour pour télécharger les règles Snort.

Update Your Rule Set		
Last Update	Unknown	Result: Unknown
Update Rules	Update Rules	Force Update

- Sur l'onglet Interfaces Snort, cliquez sur le bouton Ajouter et effectuez la configuration suivante.
- Activer – Oui
- Interface - Sélectionnez l'interface désirée pour surveiller

General Settings	
Enable	<input checked="" type="checkbox"/> Enable interface
Interface	<div>WAN (em0) ▼</div> <p>Choose the interface where this Snort instance will inspect traffic.</p>
Description	<div>WAN</div> <p>Enter a meaningful description here for your reference.</p>
Snap Length	1518

➤ Localiser la zone Paramètres d'alerte et effectuer la configuration suivante :

Envoyer des alertes au journal du système - Oui

- Bloquer les contrevenants - Activer si vous voulez bloquer les délinquants

États de tuer - Oui

Quel IP bloquer - BOTH

Alert Settings	
Send Alerts to System Log	<input checked="" type="checkbox"/> Snort will send Alerts to the firewall's system log.
System Log Facility	<div>LOG_AUTH ▼</div> <p>Select system log Facility to use for reporting.</p>
System Log Priority	<div>LOG_ALERT ▼</div> <p>Select system log Priority (Level) to use for reporting.</p>
Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate
Kill States	<input checked="" type="checkbox"/> Checking this option will kill firewall states for the blocked IP.
Which IP to Block	BOTH ▼

➤ Après avoir terminé la configuration, cliquez sur le bouton Enregistrer.

➤ Sur l'écran des interfaces Snort, modifiez la configuration de l'interface.

Interface Settings Overview						
Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
WAN (em0)		AC-BNFA	ENABLED	DISABLED	WAN	

➤ Accédez à l'onglet Catégories Wan et effectuez la configuration suivante :

Résoudre les débits - Oui

- Utiliser la politique IPS - Oui

Sélection des politiques IPS - Connectivité

Automatic Flowbit Resolution

Resolve Flowbits

☒ If checked, Snort will auto-enable rules required for checked flowbits.
 Snort will examine the enabled rules in your chosen rule categories for automatically enabled and added to the list of files in the interface rules

Snort Subscriber IPS Policy Selection

Use IPS Policy

☒ If checked, Snort will use rules from one of three pre-defined IPS policies

 Selecting this option disables manual selection of Snort Subscriber selected if enabled on the Global Settings tab. These will be added to

IPS Policy Selection

Connectivity

- Dans notre exemple, nous avons activé la fonctionnalité IPS et sélectionné la stratégie nommée **Connectivité**.
- Après avoir terminé la configuration, cliquez sur le bouton Enregistrer et démarrez le service Snort sur l'interface.

Interface Settings Overview						
Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
 WAN (em0)		AC-BNFA	ENABLED	DISABLED	WAN	  

SNORT est désormais installé sur PFSense