PFSENSE & SNORT

Installation Guide

PICO PC®

MNHO-043

MNHO-048

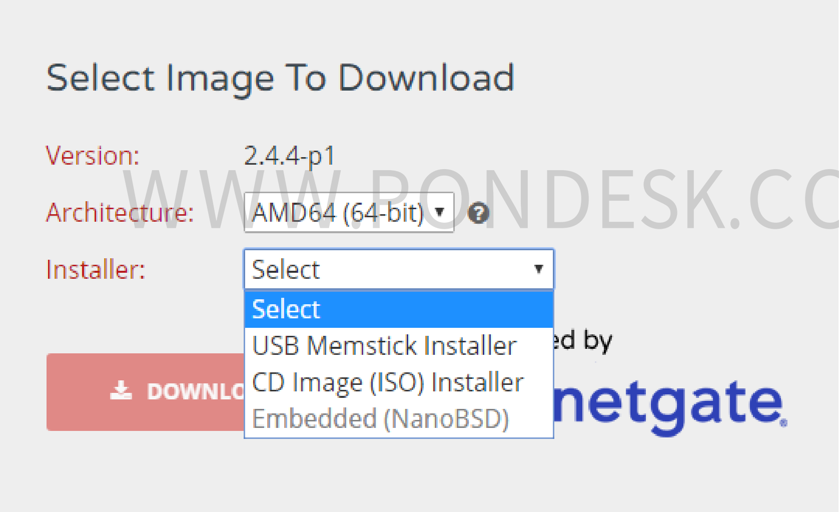
MNHO-073

Installing pfSense

1. Pre-requisites

Before proceeding to the installation, the intended user should know that in order to install pfSense on mini PC the following steps should be followed:

- pfSense stable release version only
- USB flash drive 2.0 or 3.0
- Size 8 GB (minimum)
- pfSense memory stick image as shown below



Select Image To Download

Version: 2.4.4-p1

Architecture: AMD64 (64-bit)

Installer: Select

- Utility that helps create boot-able USBs for example, PowerISO or Rufus etc.
- Architecture selected should be AMD64 (64-bit) as PICO PC® has a 64-bit architecture.
- The image file for USB flash drive installer should have a name like **“pfSense-CE-memstick-2.4.4-RELEASE-p1-amd64.img”.**
- Once you have downloaded the pfSense image make sure to verify the integrity of the downloaded file. Refer to the website https://pfsense.org

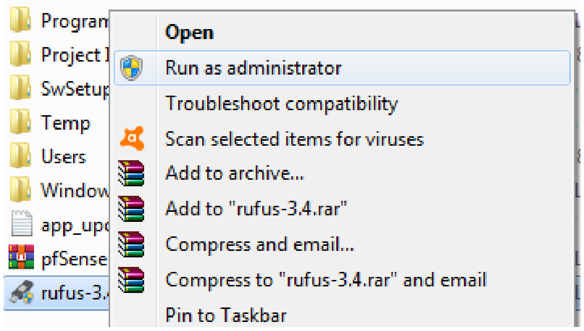
2. Preparing for installation

- The installation image file downloaded previously must be transferred to the USB flash drive. The usual copying of image directly to the drive is not the answer.
- Appropriate utility is required to make the flash drive bootable.
- We'll be using Rufus which is a free utility to make bootable USB flash drives. You can also use other utilities as well.

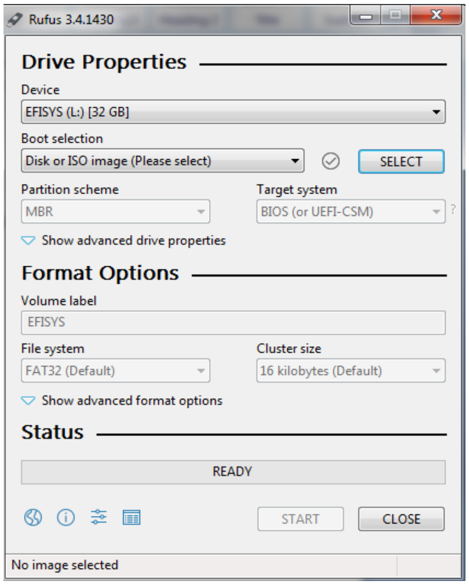
Warning: Please be very careful when writing disk images. Make sure to select the appropriate disk drive if you have more than one drive(s) in the client PC as it is possible to select the wrong drive. This will overwrite the portion of that drive with the installer disk hence rendering the disk completely unreadable except to certain disk recovery programs.

3. Writing the Image

- If you haven't downloaded Rufus utility to make the USB flash drive bootable then you can download from https://rufus.ie
- Make sure the USB flash drive is blank and formatted as once the image is written all previous contents will be deleted.
- Run the program as administrator.



- Once you plug in the USB flash drive you will find that it has been detected by Rufus straightaway as shown:



Drive Properties

Device: EFISYS (L:) [32 GB]

Boot selection: Disk or ISO image (Please select)

Partition scheme: MBR

Target system: BIOS (or UEFI-CSM)

Show advanced drive properties

Format Options

Volume label: EFISYS

File system: FAT32 (Default)

Cluster size: 16 kilobytes (Default)

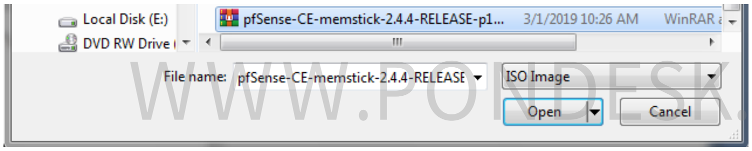
Show advanced format options

Status

READY

No image selected

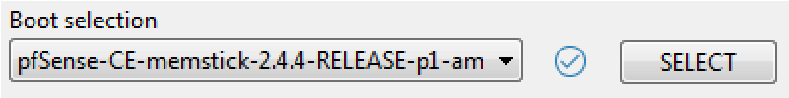
- Now click on the “select” button and specify the pfSense image file on the client PC.



pfSense-CE-memstick-2.4.4-RELEASE-p1... 3/1/2019 10:26 AM WinRAR a

File name: pfSense-CE-memstick-2.4.4-RELEASE ISO Image

- Once done you will find the pfSense image file name in the “boot selection” section.

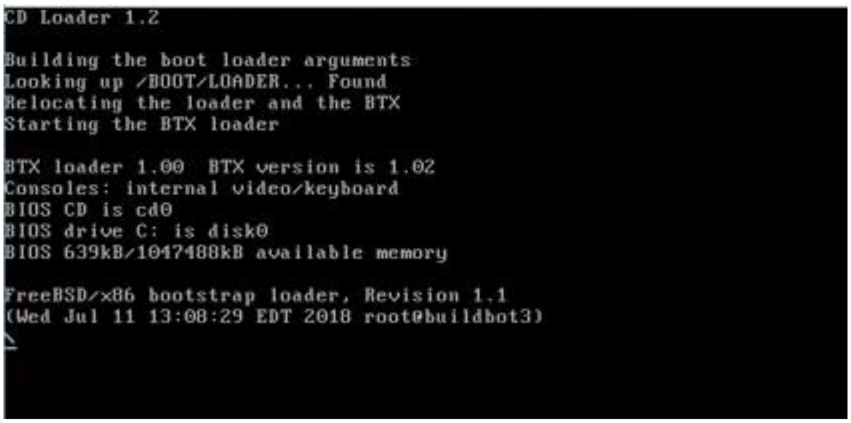


Boot selection: pfSense-CE-memstick-2.4.4-RELEASE-p1-am

- Now simply go ahead and click on “start”.
- Once underway it will show the status of the process in the form of progress bar with percentage. It will only take a minute or two to complete the process.
- Once the process is completed you are now ready to go.

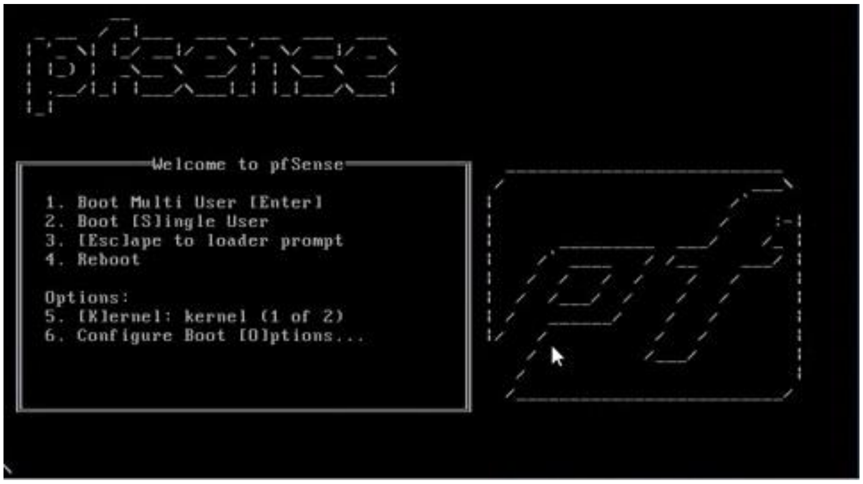
4. Installation

- Once you have plugged in the USB flash drive in one of the two ports in the back of the mini PC then simply power it up.
- Once you see the “Winston Marriot logo” then simply press **CTRL+S** and it will start the booting process.



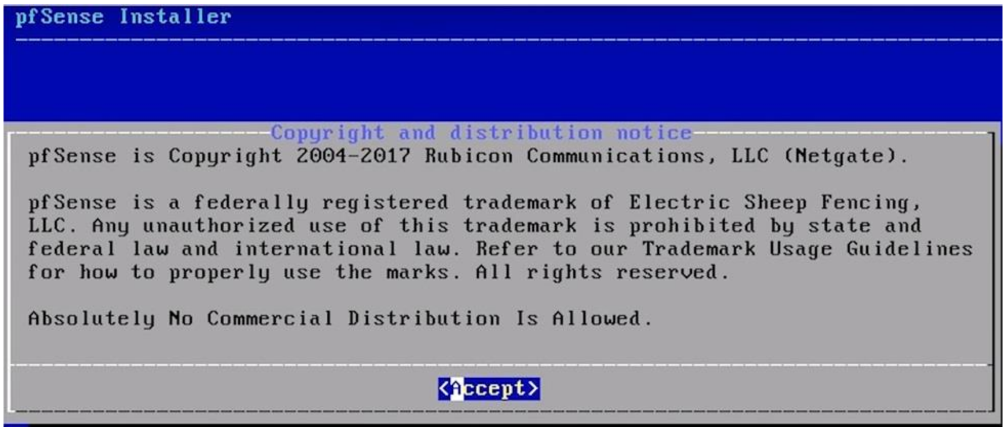
```
CD Loader 1.2

Building the boot loader arguments
Looking up /BOOT/LOADER... Found
Relocating the loader and the BTX
Starting the BTX loader

BTX loader 1.00  BTX version is 1.02
Consoles: internal video/keyboard
BIOS CD is cd0
BIOS drive C: is disk0
BIOS 639kB/1047488kB available memory

FreeBSD/x86 bootstrap loader, Revision 1.1
(Wed Jul 11 13:08:29 EDT 2018 root@buildbot3)
\
```

- You will be prompted to enter a choice on the pfSense boot screen. Let it run its course as this will start the installer.



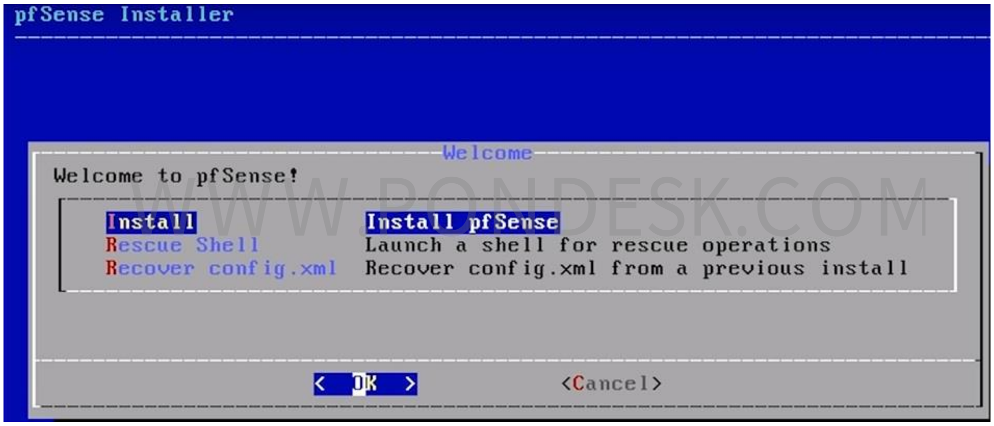
```
Welcome to pfSense

 1. Boot Multi User [Enter]
 2. Boot [S]ingle User
 3. [Esc]ape to loader prompt
 4. Reboot

 Options:
 5. [K]ernel: kernel (1 of 2)
 6. Configure Boot [O]ptions...
```

- Once the installer starts you will be presented with the copyright and distribution notice. Press “enter” to accept and proceed.



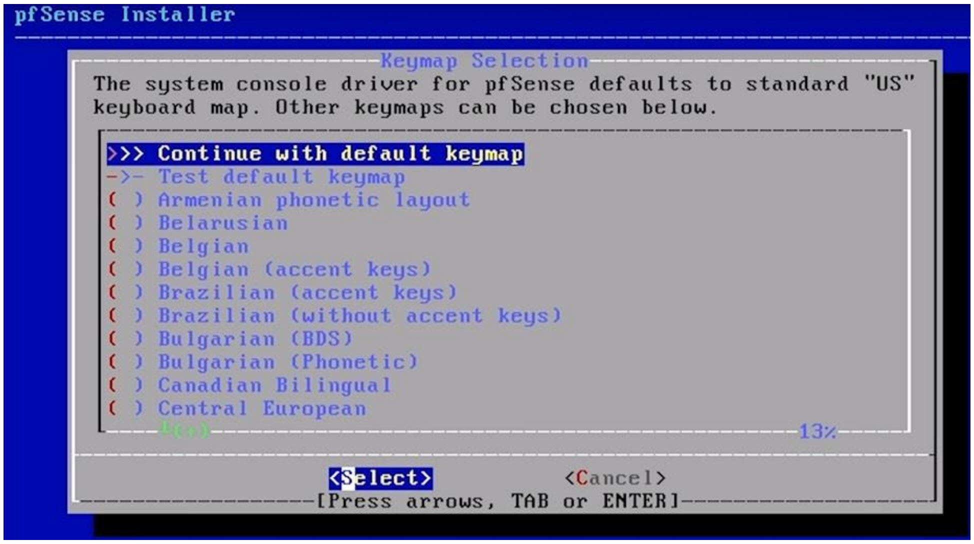
```
pfSense Installer

Copyright and distribution notice
pfSense is Copyright 2004-2017 Rubicon Communications, LLC (Netgate).

pfSense is a federally registered trademark of Electric Sheep Fencing,
LLC. Any unauthorized use of this trademark is prohibited by state and
federal law and international law. Refer to our Trademark Usage Guidelines
for how to properly use the marks. All rights reserved.

Absolutely No Commercial Distribution Is Allowed.

<Accept>
```

- On the next screen you will be prompted to install or rescue shell or recover the configuration file. Since we are installing pfSense proceed with install by pressing enter for OK.



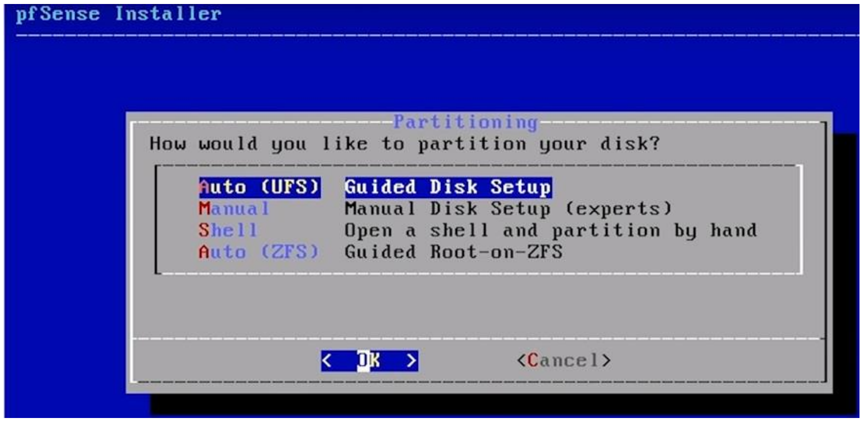
```
pfSense Installer

Welcome
Welcome to pfSense!

   Install             Install pfSense
   Rescue Shell        Launch a shell for rescue operations
   Recover config.xml  Recover config.xml from a previous install

< OK >          <Cancel>
```

- Next up is to select the keyboard layout. Default is “US Keyboard” layout. Select “Continue with default key map”.



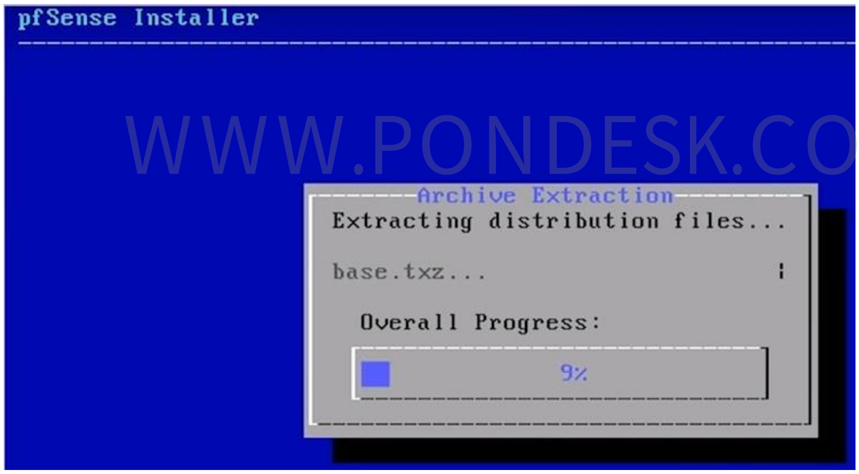
```
pfSense Installer

Keymap Selection
The system console driver for pfSense defaults to standard "US"
keyboard map. Other keymaps can be chosen below.

>>> Continue with default keymap
->- Test default keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
( ) Central European
                                                    13%

<Select>        <Cancel>
[Press arrows, TAB or ENTER]
```

- Select “Auto UFS” on the next screen to proceed with the partition as this is the classic disk setup



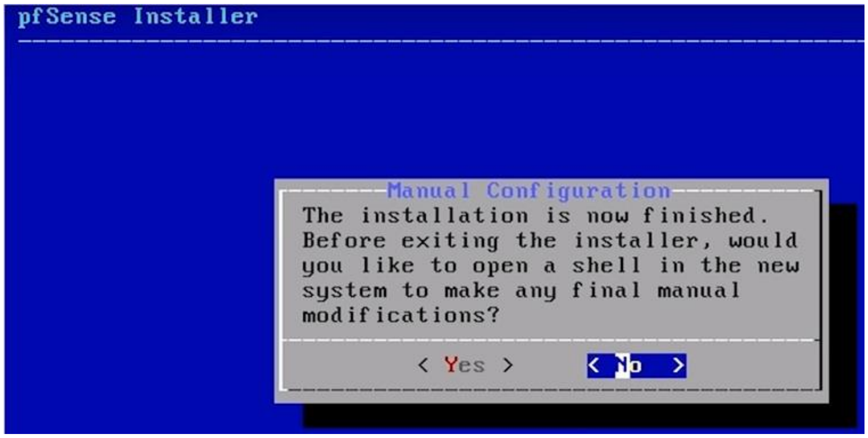
```
pfSense Installer

Partitioning
How would you like to partition your disk?

  Auto (UFS)   Guided Disk Setup
  Manual       Manual Disk Setup (experts)
  Shell        Open a shell and partition by hand
  Auto (ZFS)   Guided Root-on-ZFS

        < OK >            <Cancel>
```

- Once this is completed then the actual installation will be done.



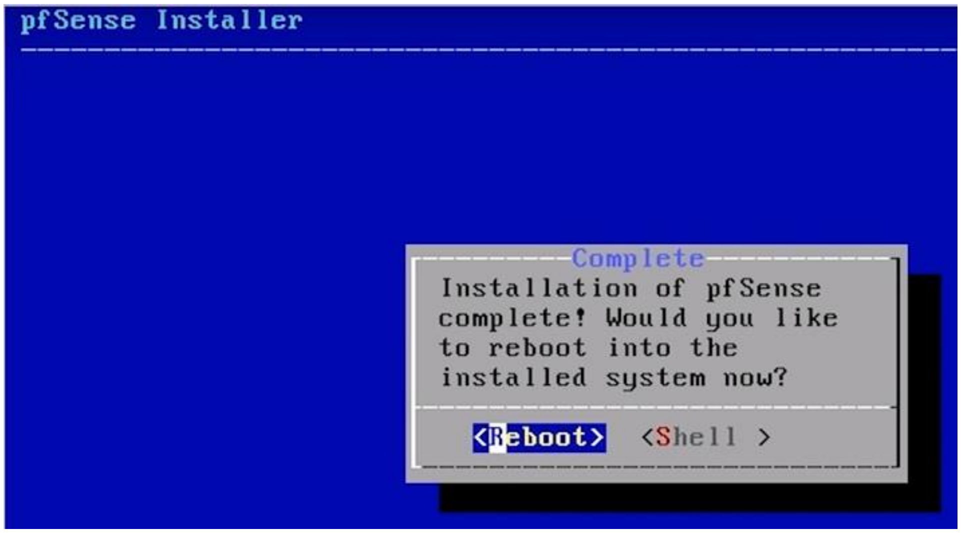
```
pfSense Installer

Archive Extraction
Extracting distribution files...

base.txz...                          |

  Overall Progress:

              9%
```

- At the end of the installation you will be prompted to make any final manual modifications via shell before proceeding. Select “No” and proceed.



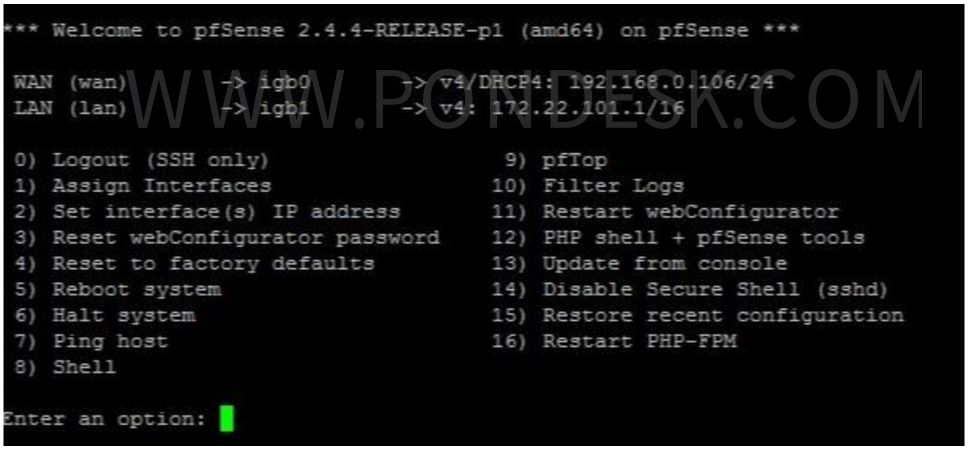
```
pfSense Installer

Manual Configuration
The installation is now finished.
Before exiting the installer, would
you like to open a shell in the new
system to make any final manual
modifications?

     < Yes >      < No >
```

- Finally, you will be prompted to “Reboot” or “Shell”. Select “Reboot”.



```
pfSense Installer

Complete
Installation of pfSense
complete! Would you like
to reboot into the
installed system now?
```

- Once rebooted you will land on the following page:

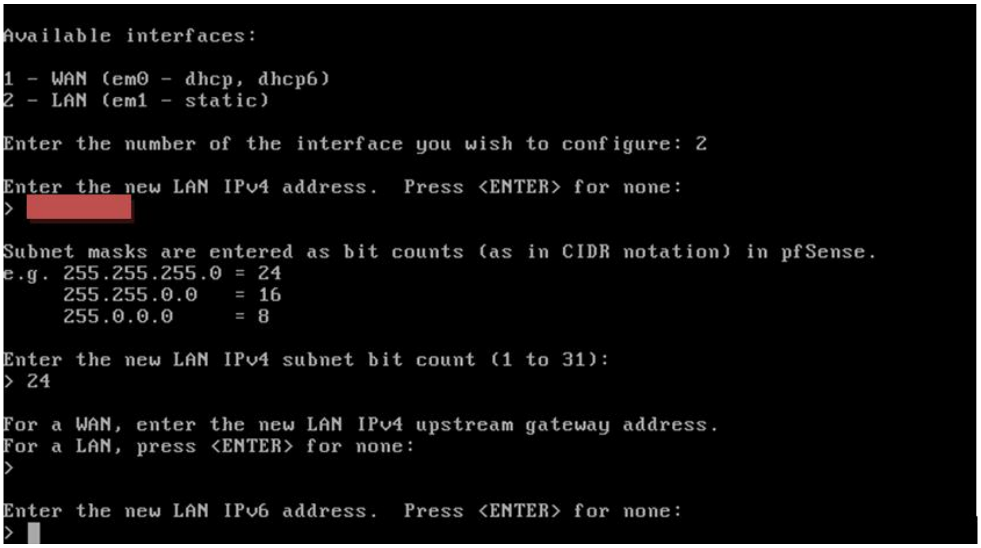


```
*** Welcome to pfSense 2.4.4-RELEASE-p1 (amd64) on pfSense ***

 WAN (wan)       -> igb0       -> v4/DHCP4: 192.168.0.106/24
 LAN (lan)       -> igb1       -> v4: 172.22.101.1/16

 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) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

By default, the LAN interface is configured with IP 192.168.1.1 but this can cause an issue when working with VPNs as they also utilize a similar subnet so to avoid confusion change it to a different one (recommended).

- In order to configure IP address on an interface select the option 2 from the screen and proceed.

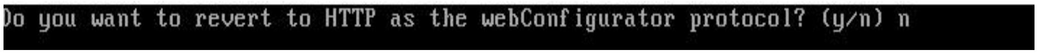
- In order to configure IP address on an interface select the option 2 from the screen and proceed.



```
Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> [redacted]

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 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
> 
```

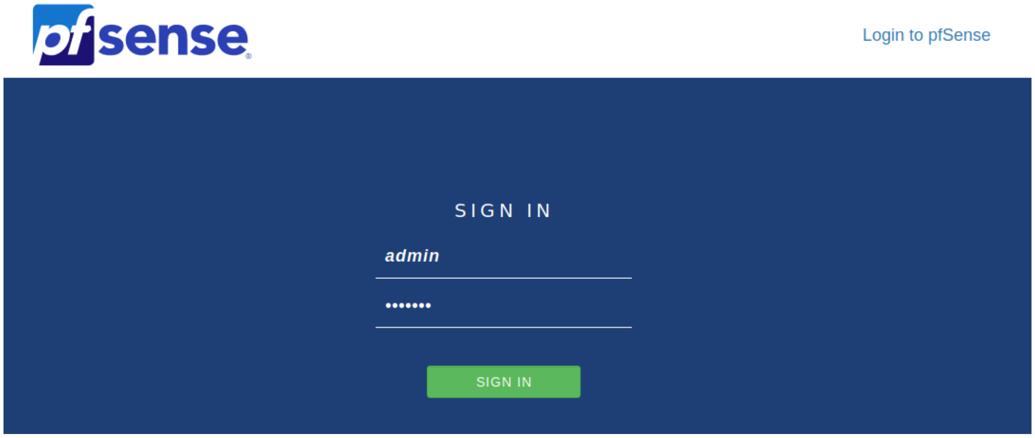
When configuring LAN interface make sure that it is set to static. Depending upon the internet connection type WAN interface can either be DHCP or static.

- Next you will be prompted to either set HTTP or HTTPS as the web configurator. It is highly recommended that you select "n" in this scenario as HTTPS is secure.



```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

- Now you are ready to access the web interface of pfSense. All you need to is to open a web browser and type https://172.22.101.16
- You will be prompted with a security warning for the HTTPS certificate, you simply need to mark it as an exception and proceed to the login screen.

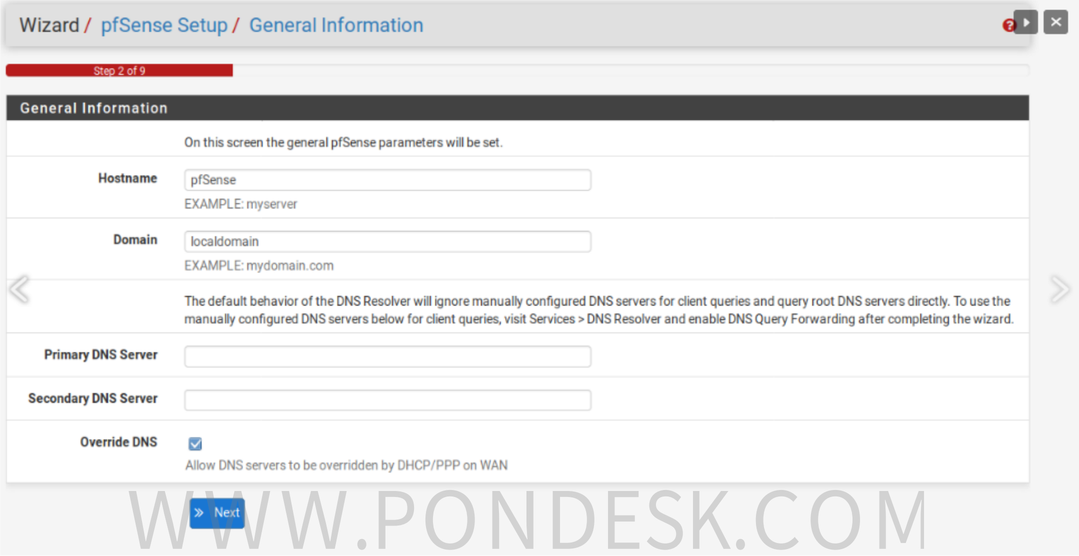


admin

•••••••

- The default username and password are “admin” and “pfSense”. It is highly recommended you change it afterwards from the “user manager” section or change it when going through the initial setup wizard.

- Once you are logged in go through the initial configuration setup wizard. It’s a nine-step process.



Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSense
EXAMPLE: myserver

Domain: localdomain
EXAMPLE: mydomain.com

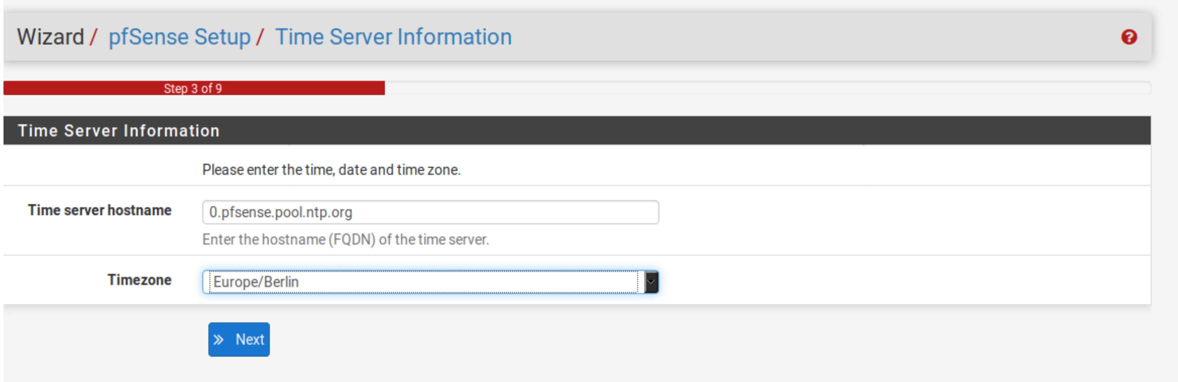
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server:

Secondary DNS Server:

Override DNS: ☑
Allow DNS servers to be overridden by DHCP/PPP on WAN

- Set your time zone.



Wizard / pfSense Setup / Time Server Information

Step 3 of 9

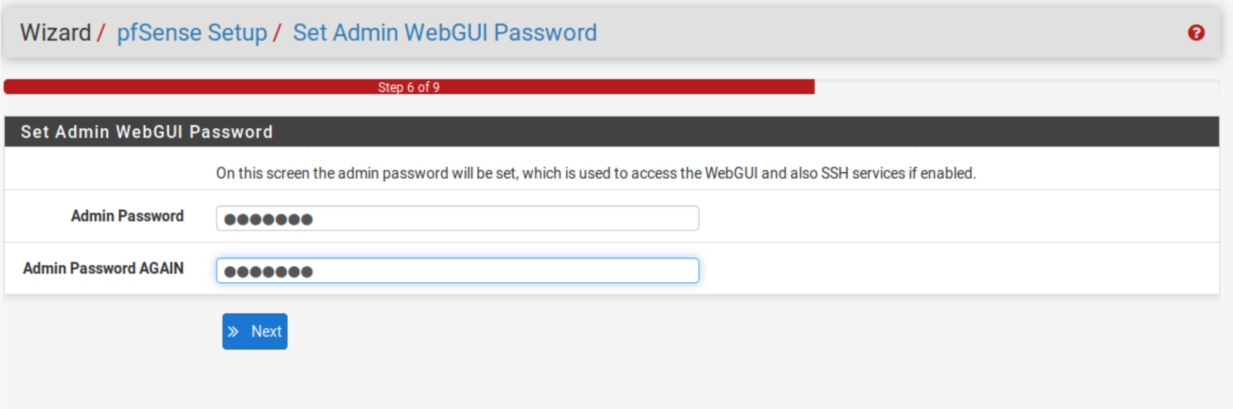
Time Server Information

Please enter the time, date and time zone.

Time server hostname: 0.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone: Europe/Berlin

- Changing your admin password



Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

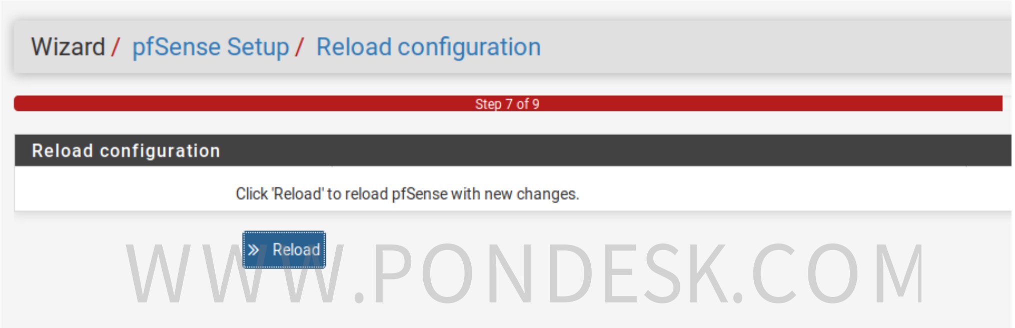
Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password ●●●●●●●

Admin Password AGAIN ●●●●●●●

- Reload pfSense with new changes.



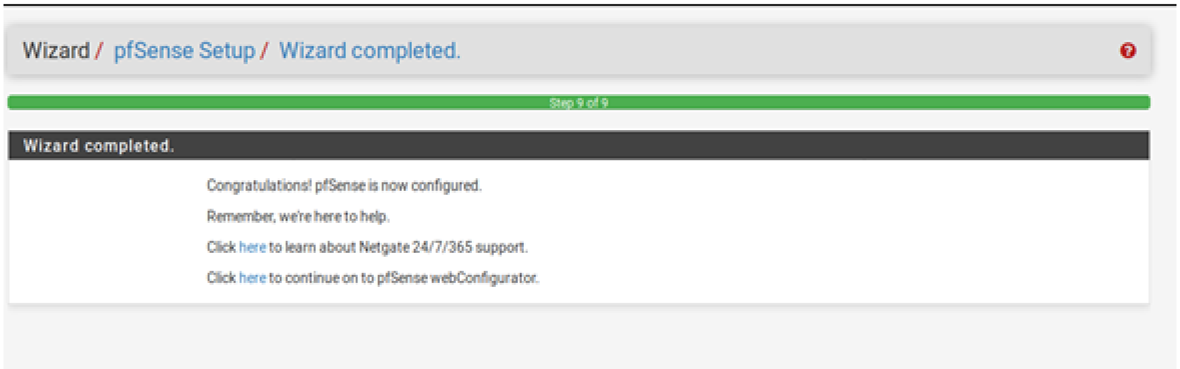
Wizard / pfSense Setup / Reload configuration

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

- Wizard completion.



Wizard / pfSense Setup / Wizard completed.

Step 9 of 9

Wizard completed.

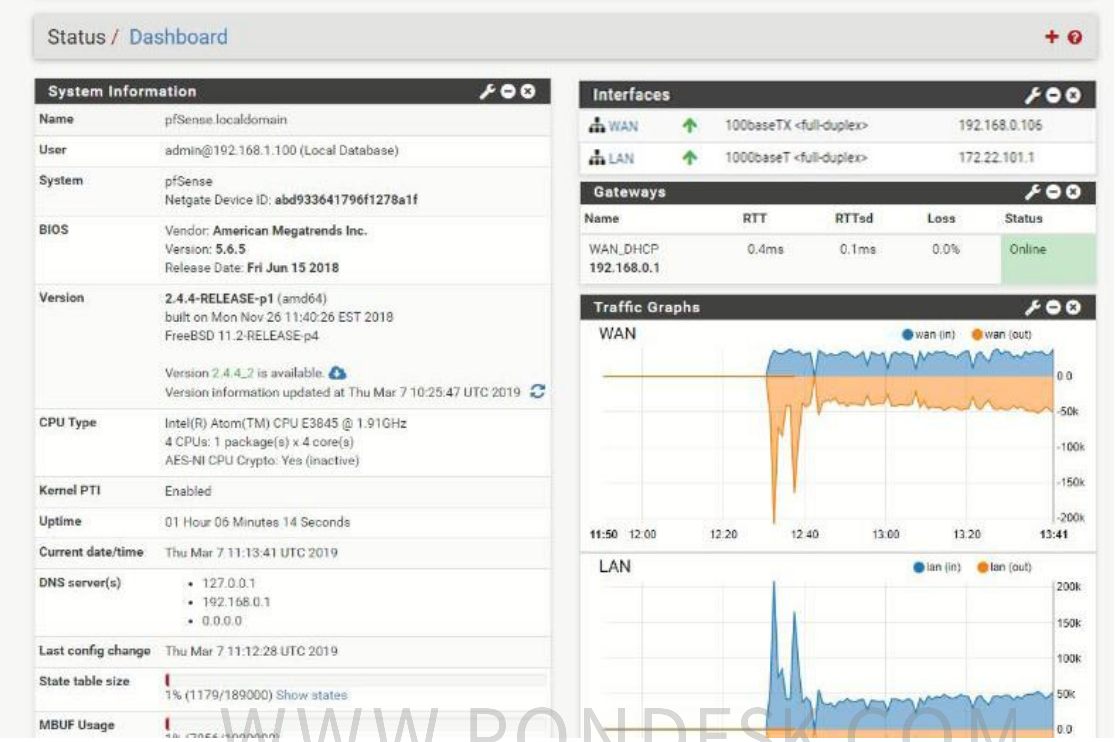
Congratulations! pfSense is now configured.

Remember, we're here to help.

Click here to learn about Netgate 24/7/365 support.

Click here to continue on to pfSense webConfigurator.

Dashboard



Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@192.168.1.100 (Local Database)
System	pfSense Netgate Device ID: **abd933641796f1278a1f**
BIOS	Vendor: **American Megatrends Inc.** Version: **5.6.5** Release Date: **Fri Jun 15 2018**
Version	**2.4.4-RELEASE-p1** (amd64) built on Mon Nov 26 11:40:26 EST 2018 FreeBSD 11.2-RELEASE-p4 Version 2.4.4_2 is available. Version information updated at Thu Mar 7 10:25:47 UTC 2019
CPU Type	Intel(R) Atom(TM) CPU E3845 @ 1.91GHz 4 CPUs: 1 package(s) x 4 core(s) AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Enabled
Uptime	01 Hour 06 Minutes 14 Seconds
Current date/time	Thu Mar 7 11:13:41 UTC 2019
DNS server(s)	• 127.0.0.1 • 192.168.0.1 • 0.0.0.0
Last config change	Thu Mar 7 11:12:28 UTC 2019
State table size	1% (1179/189000) Show states
MBUF Usage	1% (7056/1000000)

Interfaces

WAN	↑	100baseTX <full-duplex>	192.168.0.106
LAN	↑	1000baseT <full-duplex>	172.22.101.1

Gateways

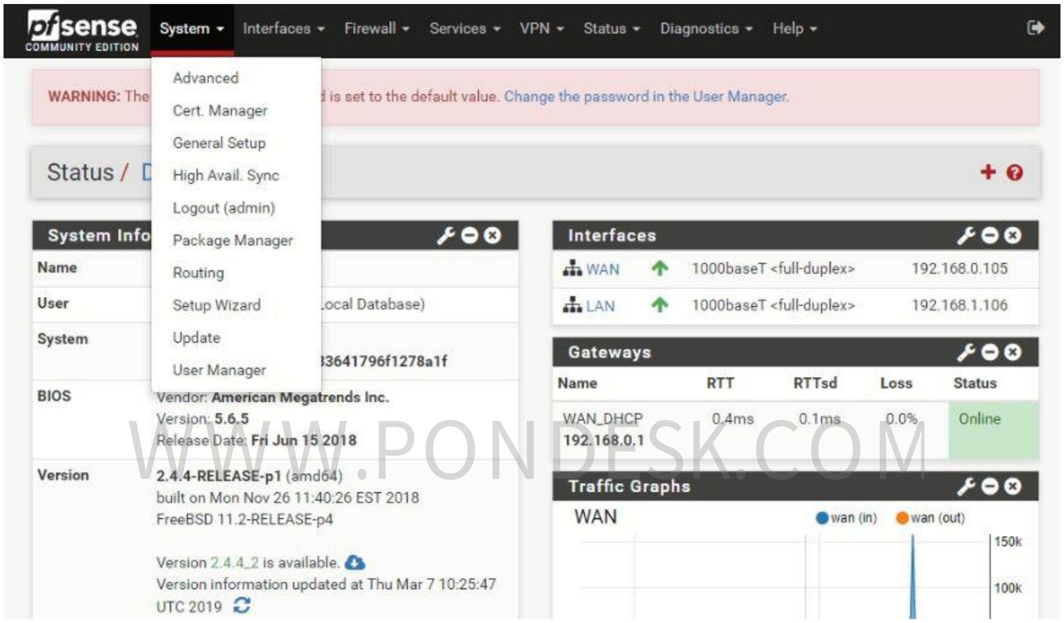
Name	RTT	RTTsd	Loss	Status
WAN_DHCP **192.168.0.1**	0.4ms	0.1ms	0.0%	Online

Traffic Graphs

Note: By default, internet is accessible from LAN which is due to the “Default allow LAN to any rule”. You can make modifications to the rule set according to your requirement in which you can set which traffic to pass on to the internet and vice versa.

Snort Package

- Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.
- Installing packages in pfSense is very to do. All you need to do is to go from “Systems” then select “Packages”.



WARNING: The ... is set to the default value. Change the password in the User Manager.

System Info

Name	
User	...ocal Database)
System	...3641796f1278a1f
BIOS	Vendor: American Megatrends Inc. Version: 5.6.5 Release Date: Fri Jun 15 2018
Version	2.4.4-RELEASE-p1 (amd64) built on Mon Nov 26 11:40:26 EST 2018 FreeBSD 11.2-RELEASE-p4 Version 2.4.4_2 is available. Version information updated at Thu Mar 7 10:25:47 UTC 2019

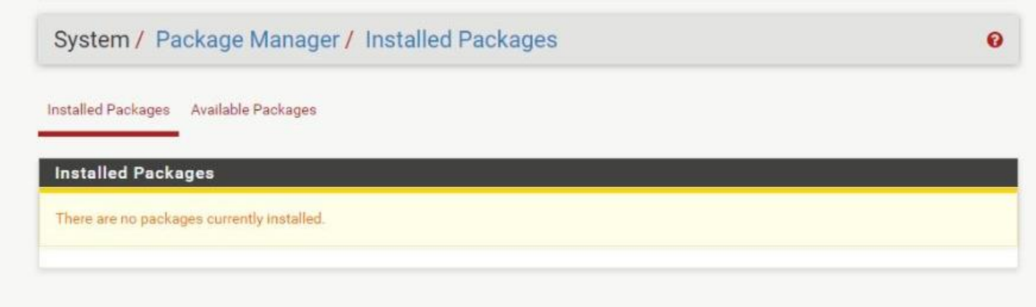
Interfaces

WAN	↑	1000baseT <full-duplex>	192.168.0.105
LAN	↑	1000baseT <full-duplex>	192.168.1.106

Gateways

Name	RTT	RTTsd	Loss	Status
WAN_DHCP 192.168.0.1	0.4ms	0.1ms	0.0%	Online

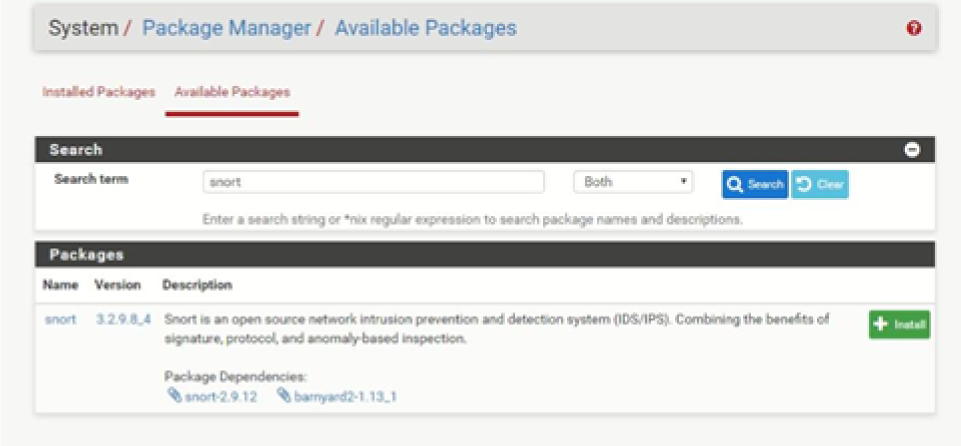
- You will be given two options “Installed Packages” and “Available Packages”. Select “Available Packages”.



Installed Packages

There are no packages currently installed.

- Now you will be a given a list of available packages which can be installed. Type in search and look for “Snort” and select “Install”.



System / Package Manager / Available Packages

Search

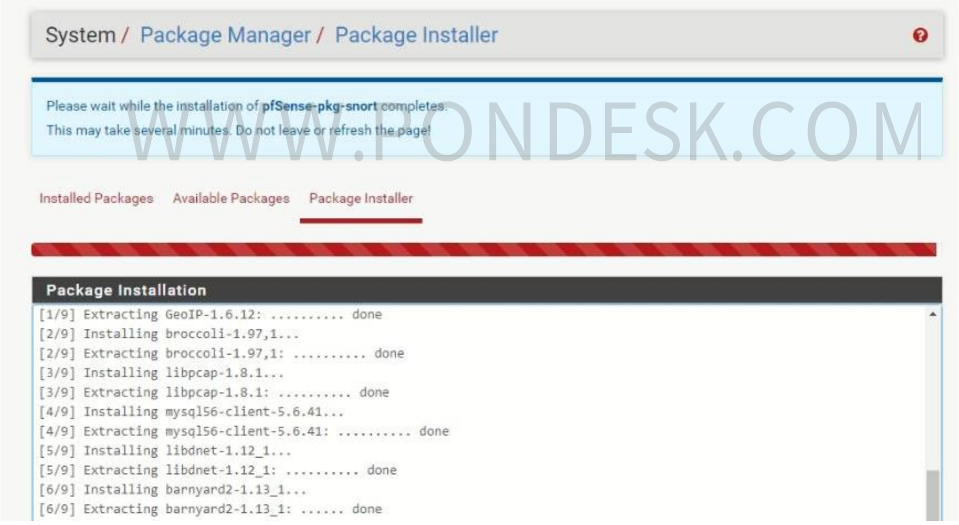
Search term: snort — Both

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

Packages

Name	Version	Description	
snort	3.2.9.8_4	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-2.9.12 barnyard2-1.13_1	Install

- Select "confirm" to proceed with the installation process.
- This will trigger the "package installer" and the installation will only take less than a minute.



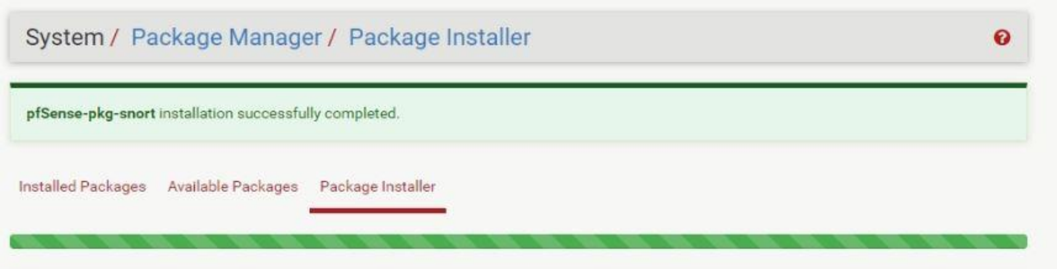
System / Package Manager / Package Installer

Please wait while the installation of **pfSense-pkg-snort** completes.
This may take several minutes. Do not leave or refresh the page!

Package Installation

```
[1/9] Extracting GeoIP-1.6.12: .......... done
[2/9] Installing broccoli-1.97,1...
[2/9] Extracting broccoli-1.97,1: .......... done
[3/9] Installing libpcap-1.8.1...
[3/9] Extracting libpcap-1.8.1: .......... done
[4/9] Installing mysql56-client-5.6.41...
[4/9] Extracting mysql56-client-5.6.41: .......... done
[5/9] Installing libdnet-1.12_1...
[5/9] Extracting libdnet-1.12_1: .......... done
[6/9] Installing barnyard2-1.13_1...
[6/9] Extracting barnyard2-1.13_1: ...... done
```

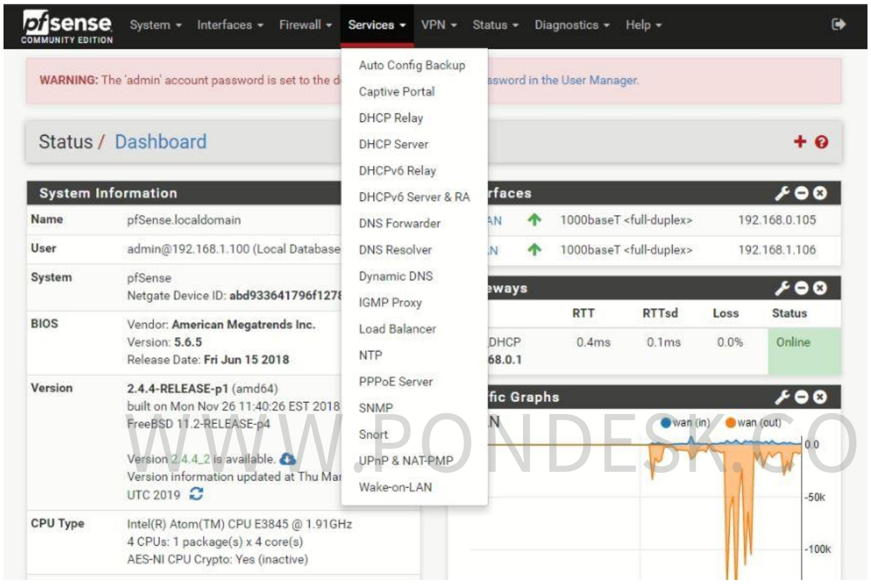
- You will be prompted once the installation is done.



System / Package Manager / Package Installer

pfSense-pkg-snort installation successfully completed.

- Now the installation is complete. All we need to do is to configure snort as per our requirement.
- There are a lot of videos available which show how to configure snort but at the end of the day it all depends upon your requirements how you wish snort to operate.
- The minimum requirement for snort to run is **1 GB** but **2 GB** or more is recommended.
- Select “Snort” from “Services”.



WARNING: The 'admin' account password is set to the d ... ssword in the User Manager.

Status / Dashboard

System Information

Name	pfSense.localdomain
User	admin@192.168.1.100 (Local Database
System	pfSense Netgate Device ID: abd933641796f1278
BIOS	Vendor: American Megatrends Inc. Version: 5.6.5 Release Date: Fri Jun 15 2018
Version	2.4.4-RELEASE-p1 (amd64) built on Mon Nov 26 11:40:26 EST 2018 FreeBSD 11.2-RELEASE-p4 Version 2.4.4_2 is available. Version information updated at Thu Mar UTC 2019
CPU Type	Intel(R) Atom(TM) CPU E3845 @ 1.91GHz 4 CPUs: 1 package(s) x 4 core(s) AES-NI CPU Crypto: Yes (inactive)

rfaces

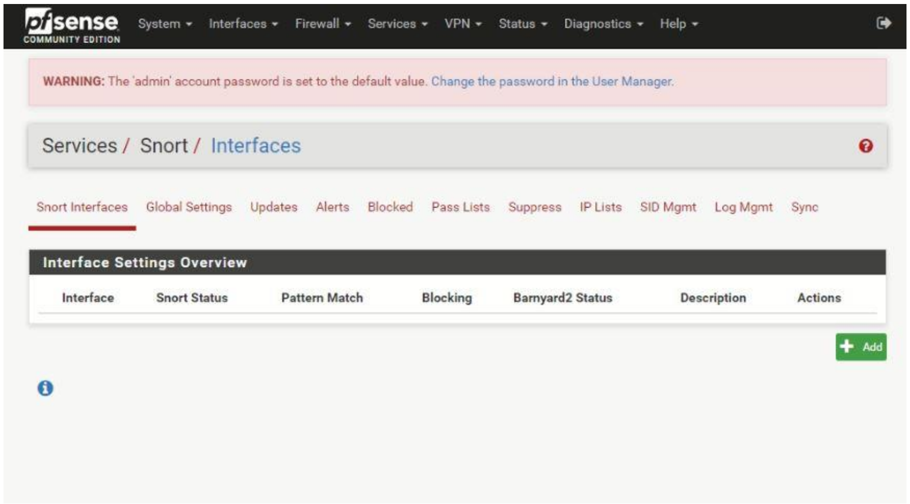
AN	↑	1000baseT <full-duplex>	192.168.0.105
N	↑	1000baseT <full-duplex>	192.168.1.106

eways

	RTT	RTTsd	Loss	Status
DHCP 68.0.1	0.4ms	0.1ms	0.0%	Online

fic Graphs

- You will be taken to the snort dashboard. Select “Global Settings” to get started.



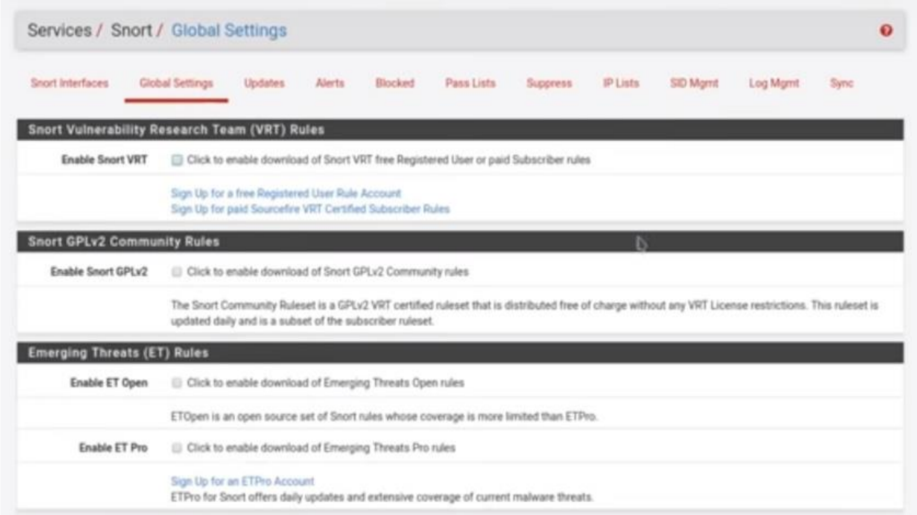
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Services / Snort / Interfaces

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions

- Select global settings to start configuring snort.



Services / Snort / Global Settings

Snort Vulnerability Research Team (VRT) Rules

Enable Snort VRT □ Click to enable download of Snort VRT free Registered User or paid Subscriber rules

Sign Up for a free Registered User Rule Account
Sign Up for paid Sourcefire VRT Certified Subscriber Rules

Snort GPLv2 Community Rules

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

The Snort Community Ruleset is a GPLv2 VRT certified ruleset that is distributed free of charge without any VRT License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

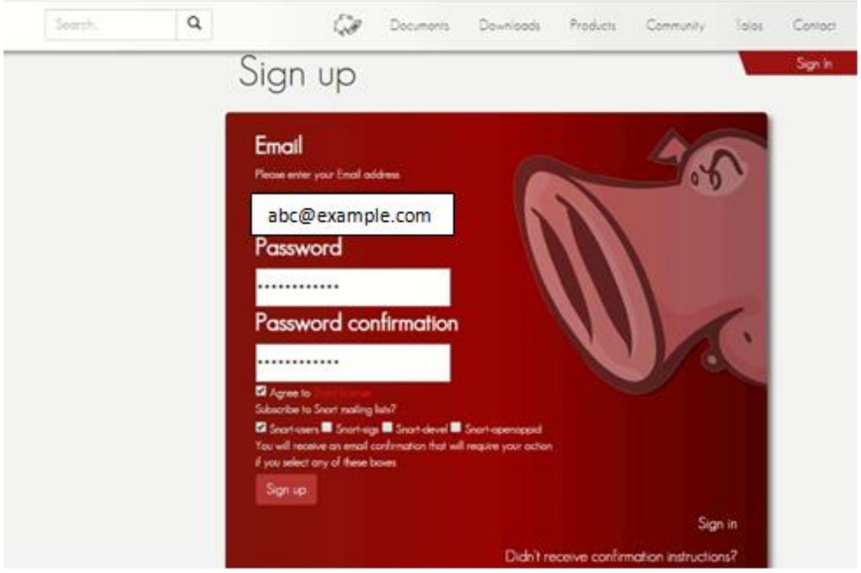
Enable ET Open □ Click to enable download of Emerging Threats Open rules

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.

- Checkmark the “Enable Snort VRT” Rules to enable download of Snort VRT free Registered User or paid Subscriber rules.
- Snort VRT rules are free of charge but require one-time registration for you to actually be able to download the rules. Registered User free accounts only get rules as they age past 30 days.
- There is also a paid version of the Sourcefire VRT Certified Subscriber Rules. Prices start from $29.99 for personal and $399 if you wish to use for business use.
- Click on the “Sign up for a free Registered User Rule Account” to proceed.



Sign up

Email
Please enter your Email address
abc@example.com

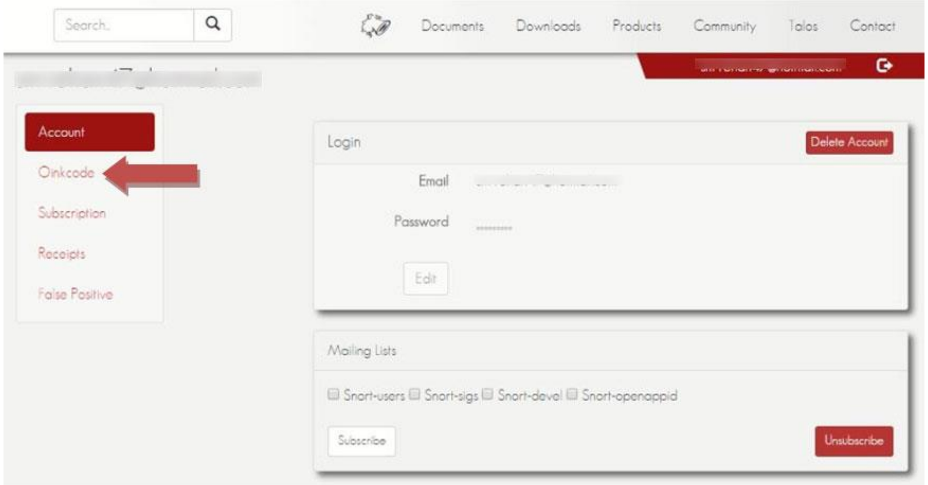
Password
•••••••••••••

Password confirmation
•••••••••••••

☑ Agree to [illegible]
Subscribe to Snort mailing lists?
☑ Snort-users □ Snort-sigs □ Snort-devel □ Snort-openappid
You will receive an email confirmation that will require your action if you select any of these boxes

- Once you are logged in on the website you need to acquire an Oinkmaster code which serves as a pass in allowing you to download the rules.

- Select your email address on the top right-hand corner of the screen and on the left you will find a couple of options and “Oinkmaster code” will be one of them.



[redacted]

Login

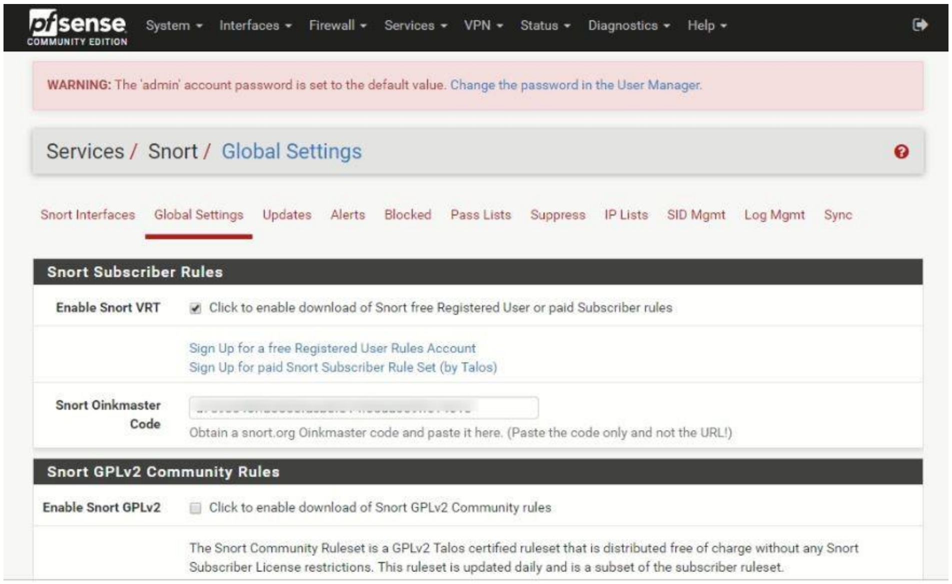
Email [redacted]

Password ....

Mailing Lists

□ Snort-users □ Snort-sigs □ Snort-devel □ Snort-openappid

- Copy the code and paste it in the Oinkmaster code section in the global settings. Remember that Oinkmaster code is unique for everyone.



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

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)

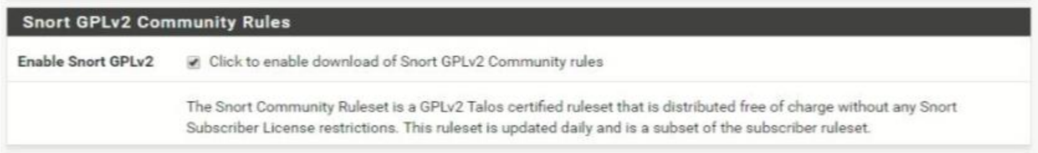
Snort Oinkmaster Code [redacted]
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

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.

- Now put a checkmark in the Enable Snort GPLv2 Community Rules as well. These rules are also free.

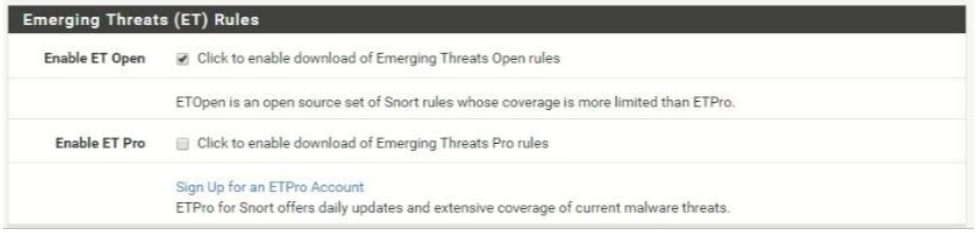


Snort GPLv2 Community Rules

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.

- Next up is the Emerging threats (ET) Rules. Click on "Enable ET Open". These are free rules which will be downloaded.



Emerging Threats (ET) Rules

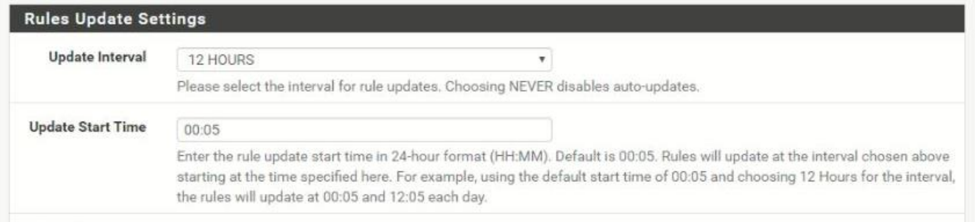
Enable ET Open ☑ Click to enable download of Emerging Threats Open rules

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.

- In "Rule Update Settings" choose the timings when to check for updated rules that will be downloaded next time. If you are in a mission critical environment then set the timer according but it is recommended from experience to have it set either 12 or 24 hrs.

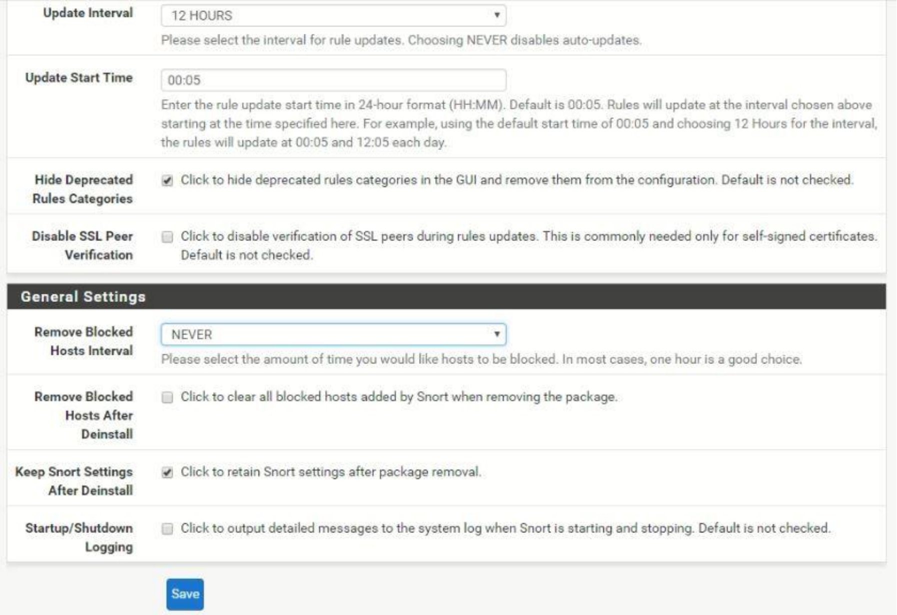


Rules Update Settings

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

Update Start Time: 00:05
Enter the rule update start time in 24-hour format (HH:MM). Default is 00:05. Rules will update at the interval chosen above starting at the time specified here. For example, using the default start time of 00:05 and choosing 12 Hours for the interval, the rules will update at 00:05 and 12:05 each day.

- Put a check mark on "Hide deprecated Rules Categories". If you are a seasoned professional and have worked with "Snort" before then you can fiddle with the "Remove Blocked Hosts Interval" as this will start blocking users in the network which are violating snort rules. Select "Save" to proceed with the configuration.



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

Update Start Time: 00:05
Enter the rule update start time in 24-hour format (HH:MM). Default is 00:05. Rules will update at the interval chosen above starting at the time specified here. For example, using the default start time of 00:05 and choosing 12 Hours for the interval, the rules will update at 00:05 and 12:05 each day.

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

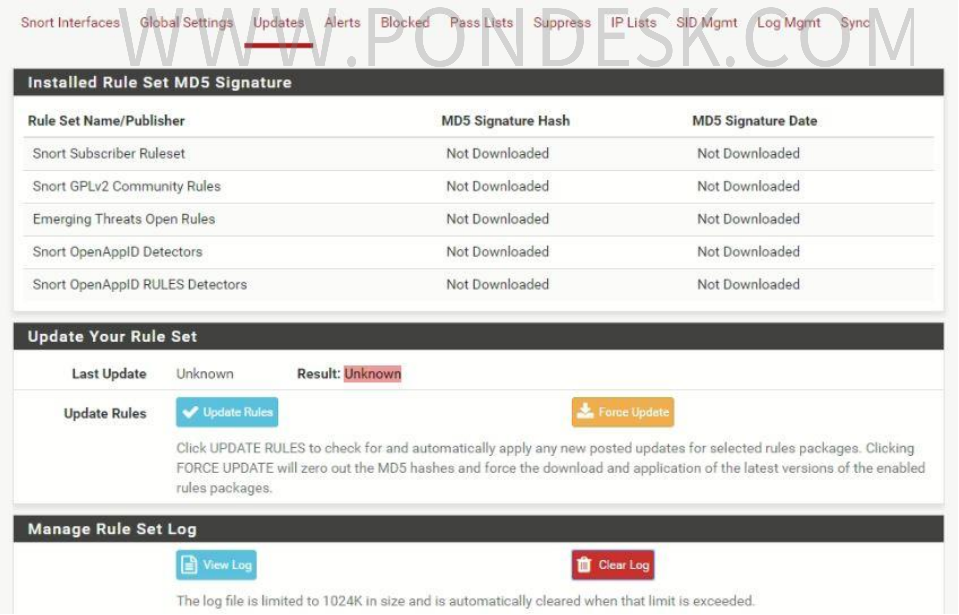
Remove Blocked Hosts Interval: NEVER ▾
Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.

Remove Blocked Hosts After Deinstall: □ Click to clear all blocked hosts added by Snort when removing the package.

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.

- Now we need to download the snort rule set. Select “updates” to get start. Select “Update Rules” to start downloading the rule set.



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 OpenAppID RULES Detectors	Not Downloaded	Not Downloaded

Update Your Rule Set

Last Update: Unknown Result: Unknown

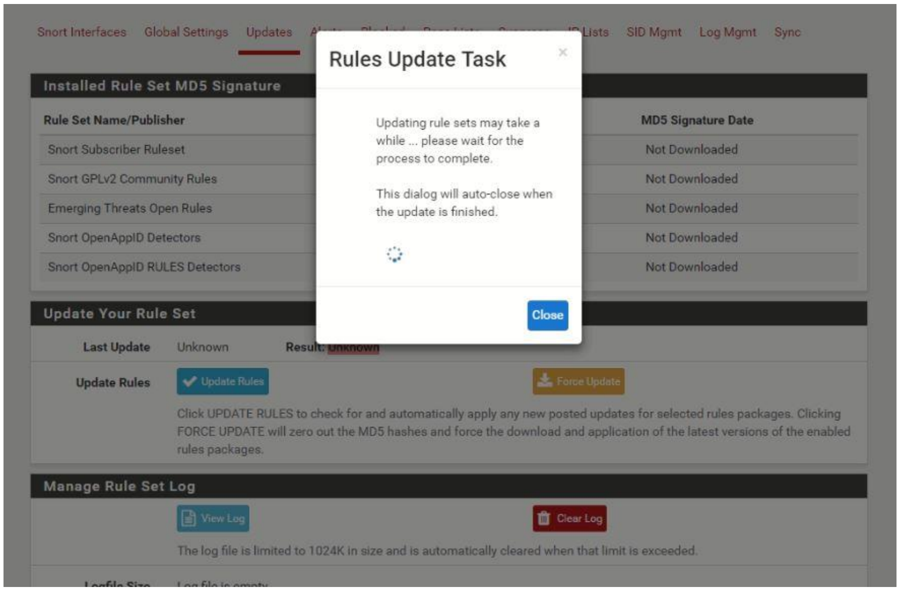
Update Rules

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.

- Once the rules start download it will be indicated in the “Installed Rule Set MD5 Signature” in the form of “date and time”. Downloading rules can take a couple of minutes depending upon the internet connection.



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.

Installed Rule Set MD5 Signature

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

Update Your Rule Set

Last Update Unknown Result: Unknown

Update Rules

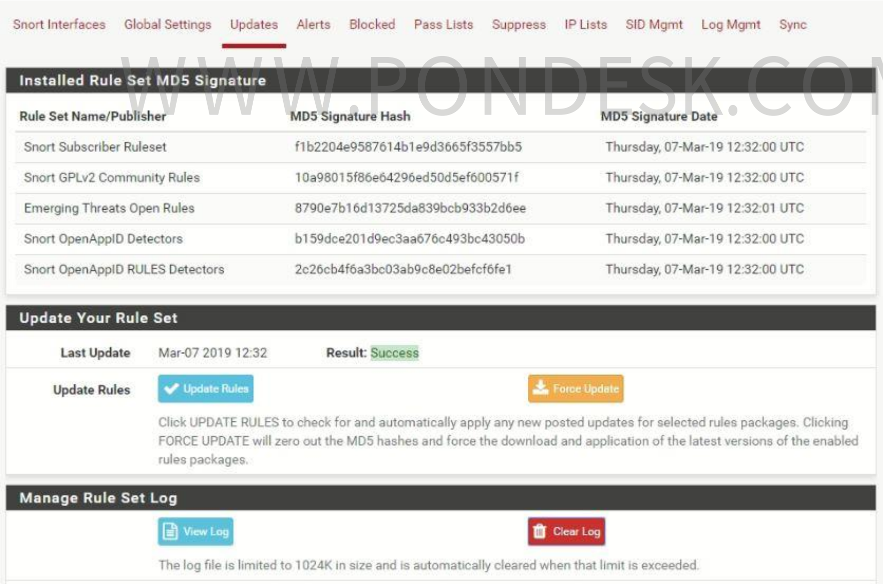
Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

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

- Successful downloading of rules.



Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	f1b2204e9587614b1e9d3665f3557bb5	Thursday, 07-Mar-19 12:32:00 UTC
Snort GPLv2 Community Rules	10a98015f86e64296ed50d5ef600571f	Thursday, 07-Mar-19 12:32:00 UTC
Emerging Threats Open Rules	8790e7b16d13725da839bcb933b2d6ee	Thursday, 07-Mar-19 12:32:01 UTC
Snort OpenAppID Detectors	b159dce201d9ec3aa676c493bc43050b	Thursday, 07-Mar-19 12:32:00 UTC
Snort OpenAppID RULES Detectors	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Thursday, 07-Mar-19 12:32:00 UTC

Update Your Rule Set

Last Update Mar-07 2019 12:32 Result: Success

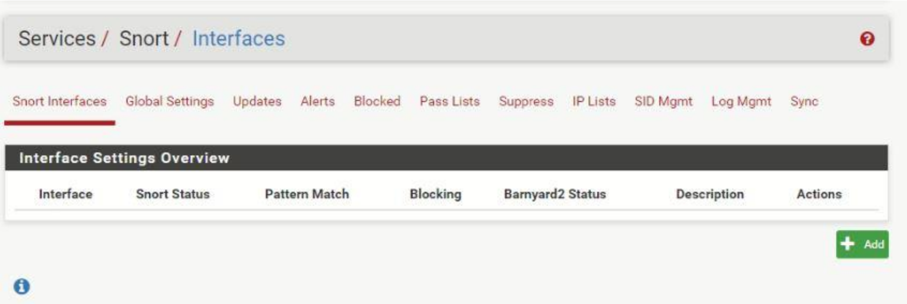
Update Rules

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.

- Now we need to define the interface for which we wish to setup Snort. Select “Add”.

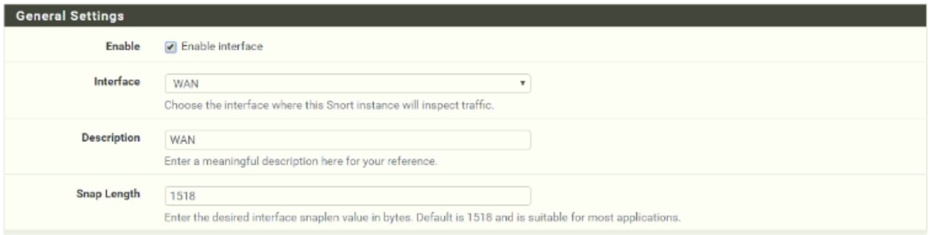


Services / Snort / Interfaces

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions

- You can set this up for either WAN or LAN depending upon your requirement.



General Settings

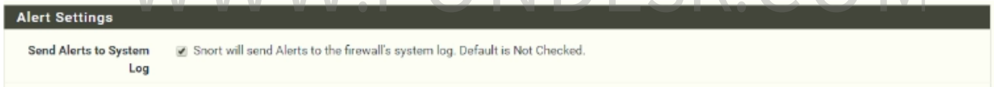
Enable ☑ Enable interface

Interface: WAN
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.

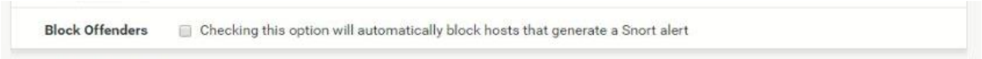
- In the alert settings you need to select "Send alerts to system logs" so that you have a firsthand idea of snort working or not.



Alert Settings

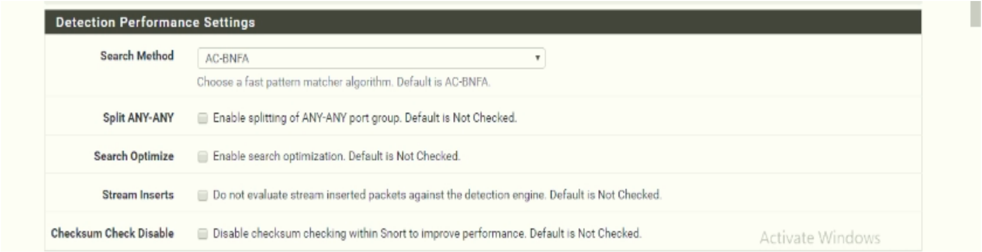
Send Alerts to System Log ☑ Snort will send Alerts to the firewall's system log. Default is Not Checked.

- In the alert settings there is an option to "block offenders that generate a snort alert". By default, its disabled but if you are experienced with snort then enable this option else leave it be.



Block Offenders □ Checking this option will automatically block hosts that generate a Snort alert

- In the "Detection Performance Settings" the default search method is "AC-BNFA" but you can choose another method as per your requirement and leave the other options to default. These methods are processor and memory intensive so choose one which suits your device configuration.



Detection Performance Settings

Search Method: AC-BNFA
Choose a fast pattern matcher algorithm. Default is AC-BNFA.

Split ANY-ANY □ Enable splitting of ANY-ANY port group. Default is Not Checked.

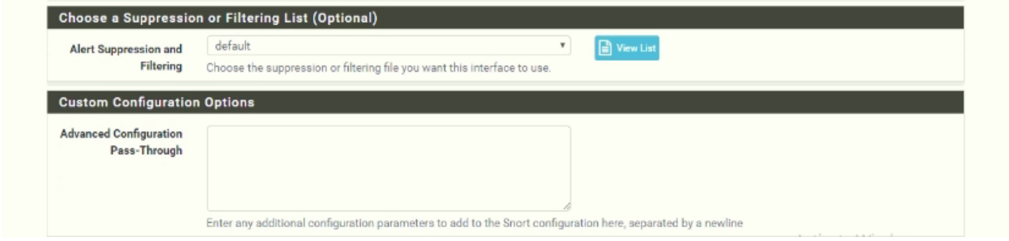
Search Optimize □ Enable search optimization. Default is Not Checked.

Stream Inserts □ Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.

Checksum Check Disable □ Disable checksum checking within Snort to improve performance. Default is Not Checked.

- “Choose the networks snort should inspect and whitelist” leave this option to default.

- “Choose a suppression or filtering list (optional)” should be set to default.



Choose a Suppression or Filtering List (Optional)

Alert Suppression and Filtering: default

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

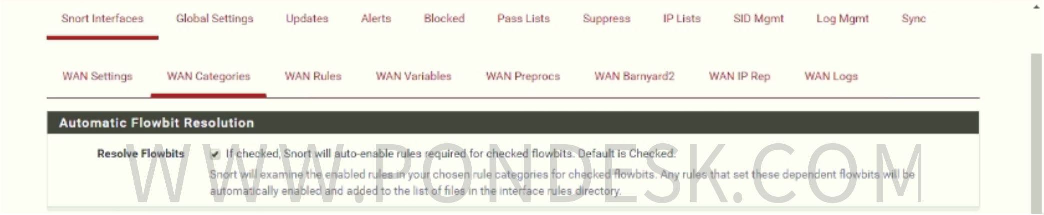
Custom Configuration Options

Advanced Configuration Pass-Through:

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

- Now select “Save”.

- Now select “WAN Categories” and put a check mark on “Resolve flowbits”.



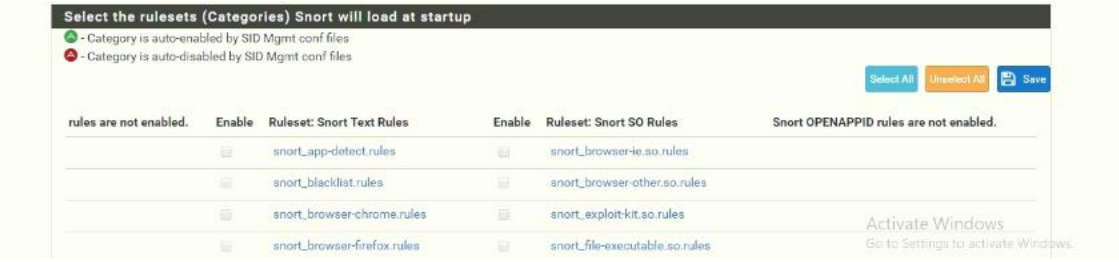
Automatic Flowbit Resolution

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.

- In the “Snort Subscriber IPS Policy Selection” put a check mark on “Use IPS Policy”. Enabling this option will allow you to bypass the downloaded rules and set snort’s built-in IPS policy to kick in. There are three policies to choose from “Connectivity”, “Balanced”, “Security” and “Max-Detect”. It is best to go for either connectivity or balanced as it’s recommended. If you are an experienced snort user then go for security.

- Now you need to enable the downloaded rules for snort which will be loaded at startup. It depends upon your requirement which rules you wish to enable. You can put a check mark on the ones you wish to enable and select “save”.



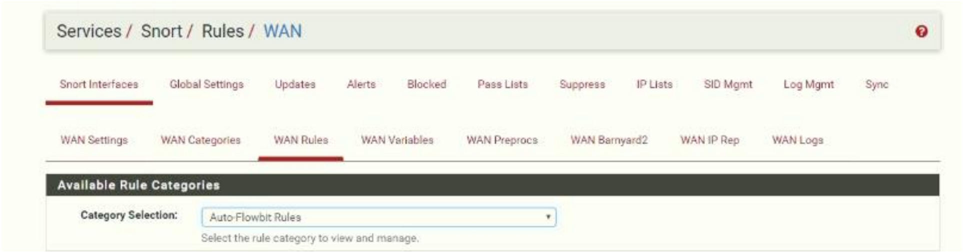
Select the rulesets (Categories) Snort will load at startup

🟢 - Category is auto-enabled by SID Mgmt conf files

🔴 - Category is auto-disabled by SID Mgmt conf files

rules are not enabled.	Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules	Snort OPENAPPID rules are not enabled.
	□	snort_app-detect.rules	□	snort_browser-ie.so.rules	
	□	snort_blacklist.rules	□	snort_browser-other.so.rules	
	□	snort_browser-chrome.rules	□	snort_exploit-kit.so.rules	
	□	snort_browser-firefox.rules	□	snort_file-executable.so.rules	

- Now select “WAN Rules” and here select “Auto Flowbit rules” or any of the three preconfigured policies “Connectivity or Balanced or Security”.

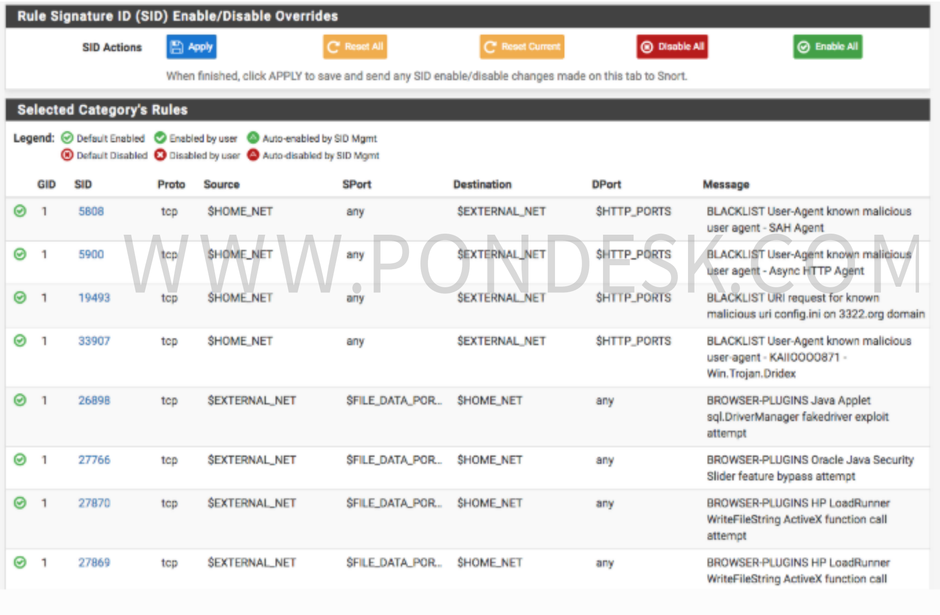


Available Rule Categories

Category Selection: Auto-Flowbit Rules

Select the rule category to view and manage.

- In the selected rules category, you can enable or disable the rules depending upon your requirement and select “apply” afterwards.



Rule Signature ID (SID) Enable/Disable Overrides

SID Actions

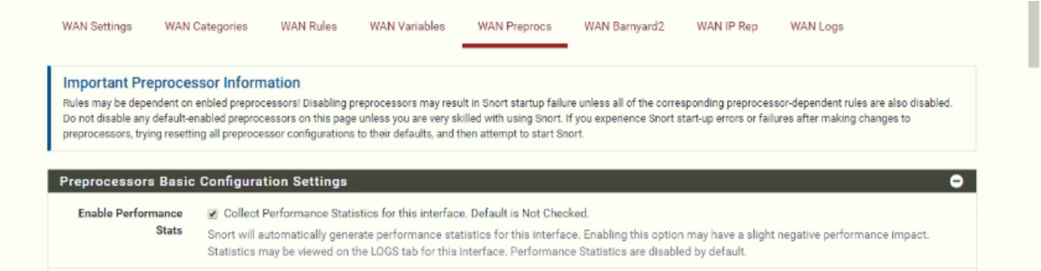
When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.

Selected Category's Rules

Legend: ✓ Default Enabled ✓ Enabled by user ✓ Auto-enabled by SID Mgmt
⊗ Default Disabled ⊗ Disabled by user ⊗ Auto-disabled by SID Mgmt

	GID	SID	Proto	Source	SPort	Destination	DPort	Message
✓	1	5808	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST User-Agent known malicious user agent - SAH Agent
✓	1	5900	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST User-Agent known malicious user agent - Async HTTP Agent
✓	1	19493	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST URI request for known malicious uri config.ini on 3322.org domain
✓	1	33907	tcp	$HOME_NET	any	$EXTERNAL_NET	$HTTP_PORTS	BLACKLIST User-Agent known malicious user-agent - KAI0000871 - Win.Trojan.Dridex
✓	1	26898	tcp	$EXTERNAL_NET	$FILE_DATA_POR...	$HOME_NET	any	BROWSER-PLUGINS Java Applet sql.DriverManager fakedriver exploit attempt
✓	1	27766	tcp	$EXTERNAL_NET	$FILE_DATA_POR...	$HOME_NET	any	BROWSER-PLUGINS Oracle Java Security Slider feature bypass attempt
✓	1	27870	tcp	$EXTERNAL_NET	$FILE_DATA_POR...	$HOME_NET	any	BROWSER-PLUGINS HP LoadRunner WriteFileString ActiveX function call attempt
✓	1	27869	tcp	$EXTERNAL_NET	$FILE_DATA_POR...	$HOME_NET	any	BROWSER-PLUGINS HP LoadRunner WriteFileString ActiveX function call

- Select “WAN Preprocs” and put a check mark on “Enable performance Stats”. Performance stats are disabled by default as it creates a negative impact as it consumes disk space. If you have a big enough disk then its fine else leave it unchecked. Leave the other options in “Preprocessors Basic Configuration Settings” to default.



Important Preprocessor Information

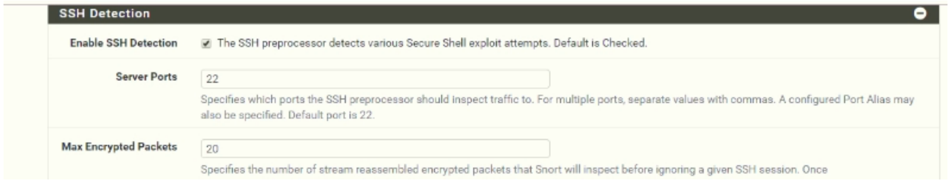
Rules may be dependent on enbled preprocessors! Disabling preprocessors may result in Snort startup failure unless all of the corresponding preprocessor-dependent rules are also disabled. Do not disable any default-enabled preprocessors on this page unless you are very skilled with using Snort. If you 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.

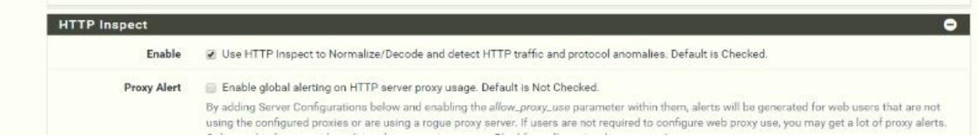
- Now depending upon your requirement, you can enable other options as well. Detecting SSH attempts is a good option.



SSH Detection

Enable SSH Detection	☑ The SSH preprocessor detects various Secure Shell exploit attempts. Default is Checked.
Server Ports	22 Specifies which ports the SSH preprocessor should inspect traffic to. For multiple ports, separate values with commas. A configured Port Alias may also be specified. Default port is 22.
Max Encrypted Packets	20 Specifies the number of stream reassembled encrypted packets that Snort will inspect before ignoring a given SSH session. Once

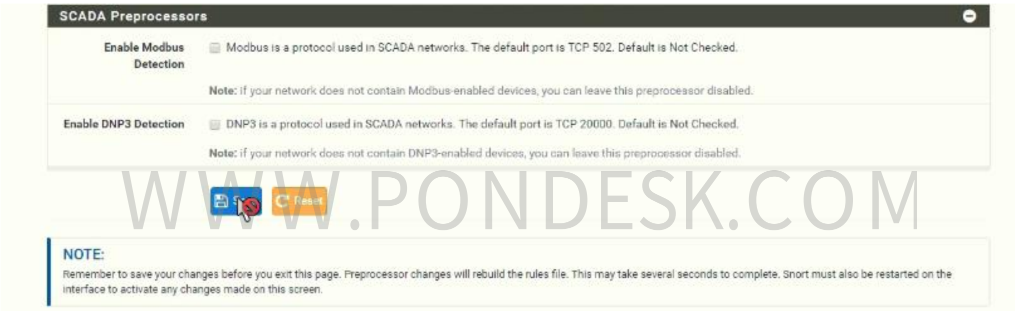
- “HTTP” traffic is enabled by default and should be left enabled.



HTTP Inspect

Enable	☑ Use HTTP Inspect to Normalize/Decode and detect HTTP traffic and protocol anomalies. Default is Checked.
Proxy Alert	□ Enable global alerting on HTTP server proxy usage. Default is Not Checked. By adding Server Configurations below and enabling the *allow_proxy_use* parameter within them, alerts will be generated for web users that are not using the configured proxies or are using a rogue proxy server. If users are not required to configure web proxy use, you may get a lot of proxy alerts.

- Leave the other options to default settings and select “save”.

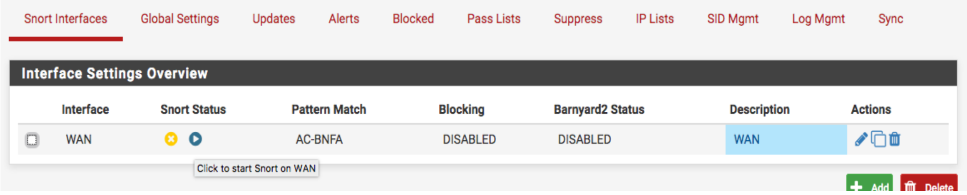


SCADA Preprocessors

Enable Modbus Detection	□ Modbus is a protocol used in SCADA networks. The default port is TCP 502. Default is Not Checked. **Note:** if your network does not contain Modbus-enabled devices, you can leave this preprocessor disabled.
Enable DNP3 Detection	□ DNP3 is a protocol used in SCADA networks. The default port is TCP 20000. Default is Not Checked. **Note:** if your network does not contain DNP3-enabled devices, you can leave this preprocessor disabled.

NOTE:
Remember to save your changes before you exit this page. Preprocessor changes will rebuild the rules file. This may take several seconds to complete. Snort must also be restarted on the interface to activate any changes made on this screen.

- Once this is done you are all set to start snort for the selected interface. Click on the play button to start the service.

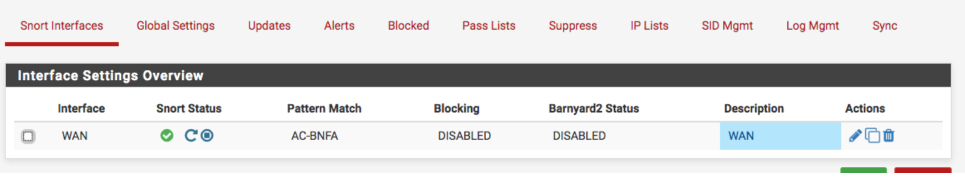


Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
□	WAN	⊗ ▶	AC-BNFA	DISABLED	DISABLED	WAN	✎ ⧉ 🗑

Click to start Snort on WAN

- Service has now successfully started.



Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
□	WAN	✓ ⟳ ◉	AC-BNFA	DISABLED	DISABLED	WAN	✎ ⧉ 🗑

NOTE: This is the basic setup for snort. Depending upon the free rules that are downloaded may or may not have any bugs. This happens from time to time and the netgate forum (https://forum.netgate.com) is the best place to report them and appropriate support if you have dedicated support then contact the support team.

THANK YOU

--

PONDESK SUPPORT TEAM
https://www.pondesk.com