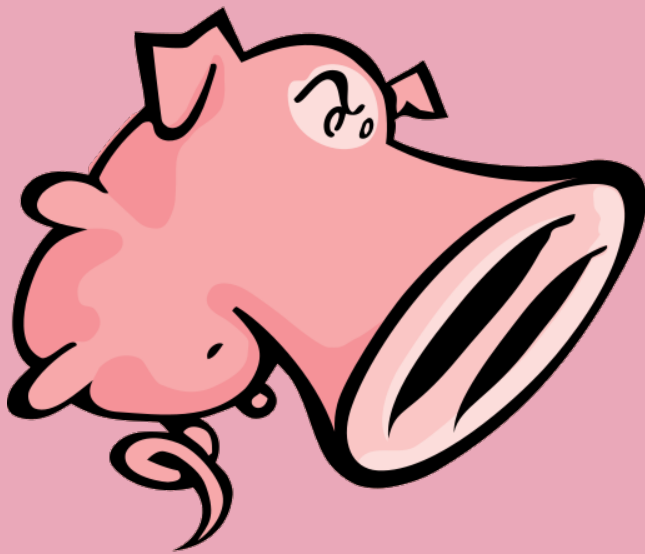


CONFIGURACIÓN DE SNORT CON PFSENSE



SEGURIDAD INFORMÁTICA
JUAN CARLOS NAVIDAD GARCÍA

1. Configuración de Pfsense:

```
Pfsense [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.3.2-RELEASE amd64 Tue Jul 19 12:44:43 CDT 2016
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.103.129/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

Enter an option: 
```

Una vez iniciado **Pfsense**, nos encontraremos con que nos listará unas opciones, de las cuáles solo tocaremos la **segunda**.

La **segunda opción** sirve para **configurar y asignar las direcciones IP** a los adaptadores de red.

De los cuales tenemos dos, uno que nos proporcionará **conexión a internet y que está conectado mediante DHCP** y otro adaptador conectado a un **segmento de LAN que sería equivalente a una red NAT en VirtualBox**, este adaptador se configuraría con la **IP estática**.

Así que, como ya he dicho, escribiremos el número **dos** para seleccionar la opción.

Enter an option: 2

Nos preguntará por la interfaz de red que queremos configurar, en nuestro caso solo configuraremos la segundo, la **LAN**, está es la interfaz por la que va a salir el servidor **Pfsense**.

Seleccionaremos la interfaz también escribiendo el número **2**:

```
Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

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

Continuando, nos pedirá la **dirección IP** que le queremos asignar a la interfaz, le podemos asignar cualquier dirección, en mi caso le he asignado la **192.168.1.1** que pertenece a la red interna.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.1
```

Después, nos pedirá la **máscara de subred** en la que nos encontramos, como ya he dicho es la **/24**, así que escribiremos **24**:

```
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
```

En las opciones "**For a LAN, press <Enter> for none**" y "**Enter the new LAN IPv6 address, press <Enter> for none**" pulsaremos **Enter** para saltar, ya que no a configurar las **direcciones IPv6**.

```
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:
>
```

Por último, nos preguntará si queremos configurar el **servidor DHCP**, en nuestro caso lo necesitaremos para que funcione el **portal cautivo**, así que lo configuraremos.

Para habilitarlo pulsaremos la tecla "**Y**", e introduciremos el rango de **IPs** que puede asignar nuestro **servidor DHCP**:

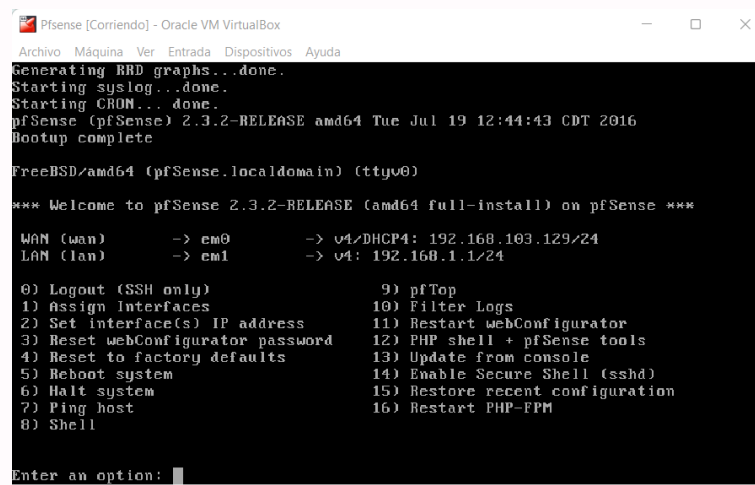
```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.100
Enter the end address of the IPv4 client address range: 192.168.1.200
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

Finalmente, nos preguntará si queremos que el **protocolo Web** sea **HTTP** y le diremos que si dando a la tecla "**Y**".

Después de todo, acabaremos con la configuración de la interfaz y podremos acceder a **Pfsense**.

```
The IPv4 LAN address has been set to 192.168.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.1.1/
Press <ENTER> to continue.
```

Reiniciaremos la máquina para que se apliquen bien los cambios y nos daremos cuenta de que, al reiniciar, nos saldrá la dirección IP que le hemos asignado a la interfaz "**LAN**":



```
PfSense [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.3.2-RELEASE amd64 Tue Jul 19 12:44:43 CDT 2016
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.103.129/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

Enter an option:
```

Esta dirección IP será la que utilizaremos para acceder al **configurador Web de Pfsense**.

2. Configuración inicial de Pfsense:

Para crear el **portal cautivo** y realizar las diversas configuraciones que quedan en **Pfsense** necesitaremos otra máquina (cliente) en la misma red.

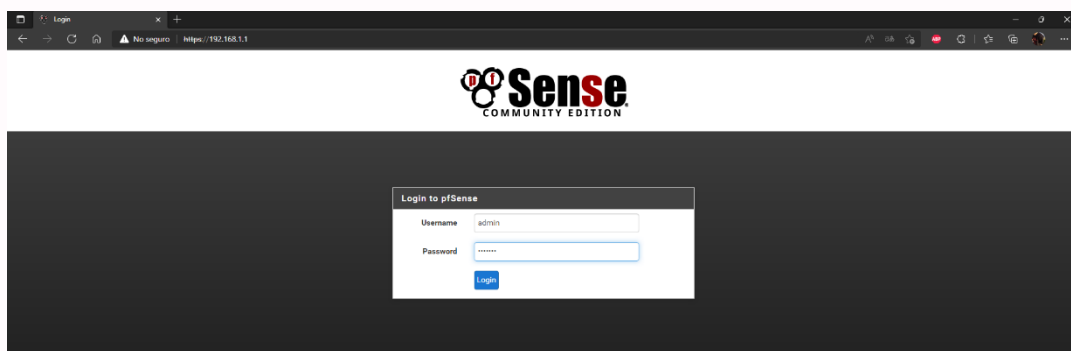
Para esto he utilizado una máquina virtual con **Windows 10** también configurada la red como "**Red Interna**".



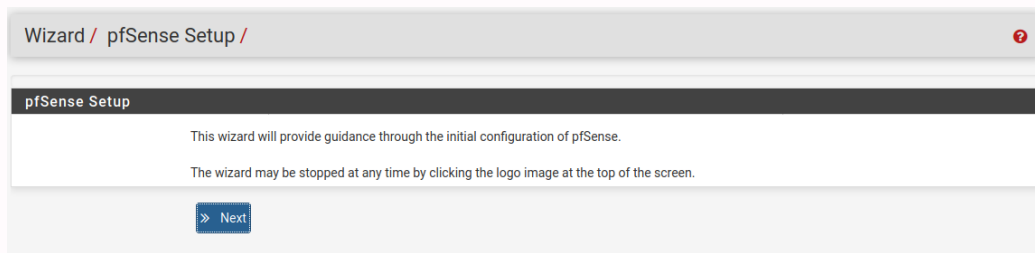
Iniciaremos la máquina virtual e ingresaremos en el navegador;

En la barra de búsqueda insertaremos la **IP configurada anteriormente**, en mi caso la **192.168.1.1**.

Una vez dentro nos pedirá **iniciar sesión**, el usuario y la contraseña por defecto son **usuario: admin ; contraseña: pfsense**



Una vez iniciada la sesión, comenzará el **setup** de la configuración web de **Pfsense**:



Wizard / pfSense Setup /

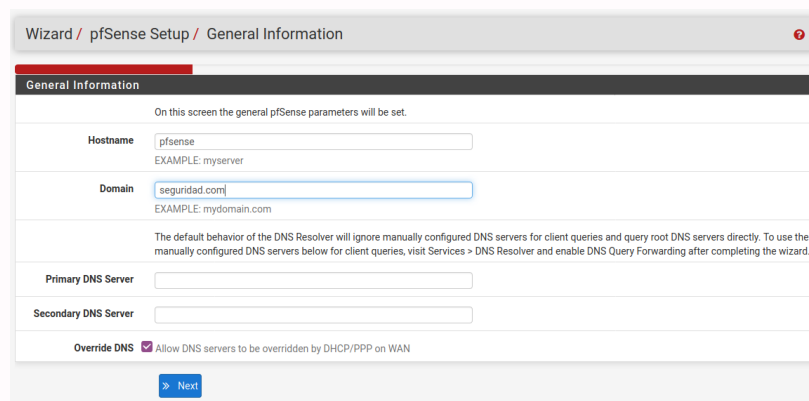
pfSense Setup

This wizard will provide guidance through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

» Next

Lo primero sería darle un **nombre de dominio a Pfsense**, no tendríamos que tocar nada más de esa pantalla, aunque si queremos podemos añadir **direcciones DNS**, aunque no es necesario.



Wizard / pfSense Setup / General Information

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfsense
EXAMPLE: myserver

Domain: seguridad.com
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.

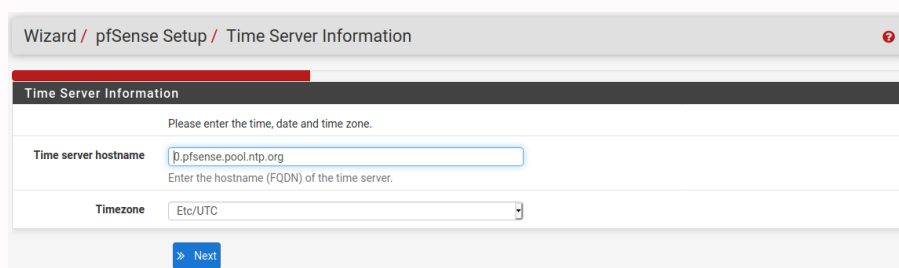
Primary DNS Server:

Secondary DNS Server:

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

» Next

A continuación, nos aparecerá la selección del **servidor de horario** y nuestra **zona horaria**, todo lo dejaremos **por defecto**, no tocaremos nada.



Wizard / pfSense Setup / Time Server Information

Time Server Information

Please enter the time, date and time zone.

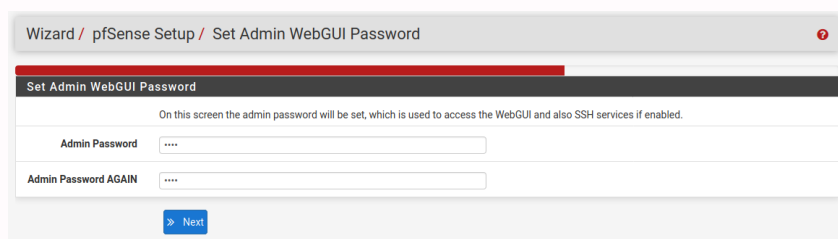
Time server hostname: p.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone: Etc/UTC

» Next

Los siguientes dos apartados serán sobre la **configuración de las interfaces de red**, las cuales ya hemos configurado **manualmente** en pasos anteriores. Así que también se dejará todo tal cual está.

Para finalizar, nos hará introducir una **nueva contraseña para el usuario administrador**, para que no se quedé la contraseña por defecto.



Wizard / pfSense Setup / Set Admin WebGUI Password

Set Admin WebGUI Password

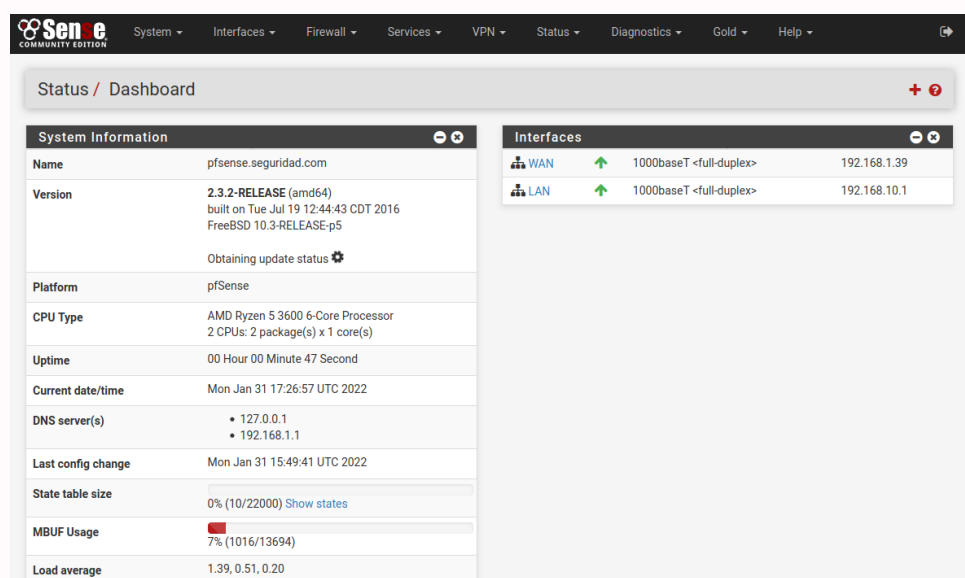
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password:

Admin Password AGAIN:

[Next](#)

Una vez introducida la nueva contraseña, se nos abrirá el **panel principal de Pfsense**:



Status / Dashboard

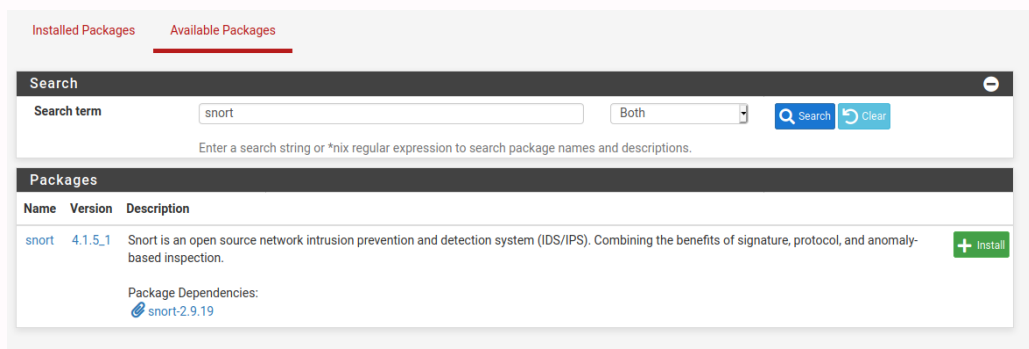
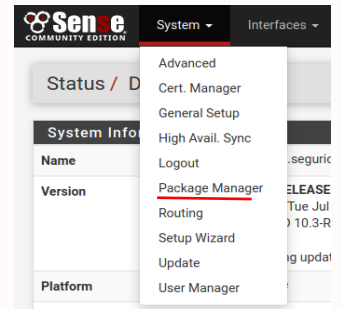
System Information	
Name	pfsense.seguridad.com
Version	2.3.2-RELEASE (amd64) built on Tue Jul 19 12:44:43 CDT 2016 FreeBSD 10.3-RELEASE-p5 Obtaining update status
Platform	pfSense
CPU Type	AMD Ryzen 5 3600 6-Core Processor 2 CPUs: 2 package(s) x 1 core(s)
Uptime	00 Hour 00 Minute 47 Second
Current date/time	Mon Jan 31 17:26:57 UTC 2022
DNS server(s)	• 127.0.0.1 • 192.168.1.1
Last config change	Mon Jan 31 15:49:41 UTC 2022
State table size	0% (10/22000) Show states
MBUF Usage	7% (1016/13694)
Load average	1.39, 0.51, 0.20

Interfaces	
WAN	1000baseT <full-duplex> 192.168.1.39
LAN	1000baseT <full-duplex> 192.168.10.1

3. Instalación del paquete Snort:

Snort no viene directamente incluido en **Pfsense**, por lo que hay que instalarlo desde el administrador de paquetes.

Entonces nos iremos a **sistema → Administrador de paquetes**. Y dentro del administrador de paquetes nos iremos a paquetes disponibles. Buscaremos **Snort** y le daremos a instalar:

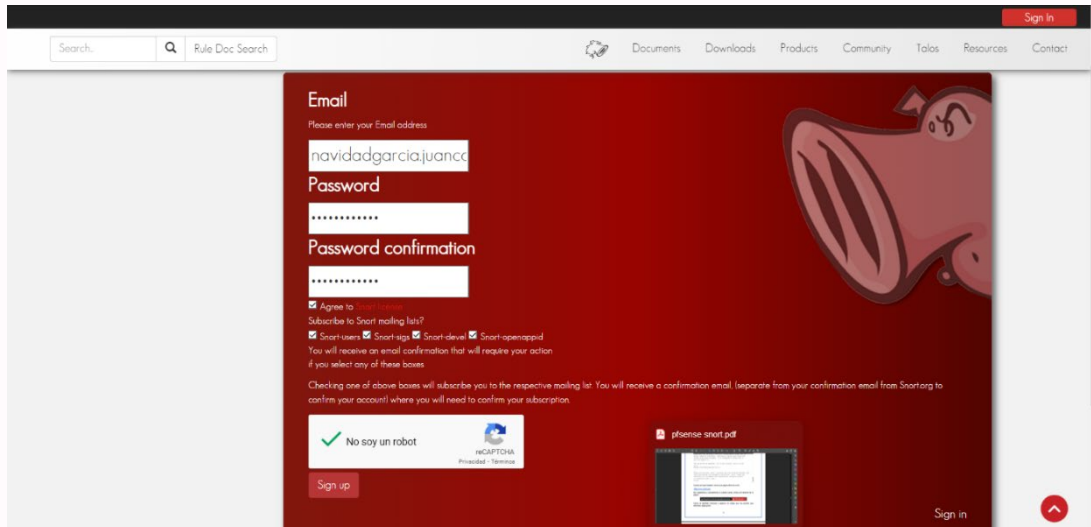


Una vez esté instalado, el **Snort** se va a encontrar en el apartado de Servicios como **Snort**.

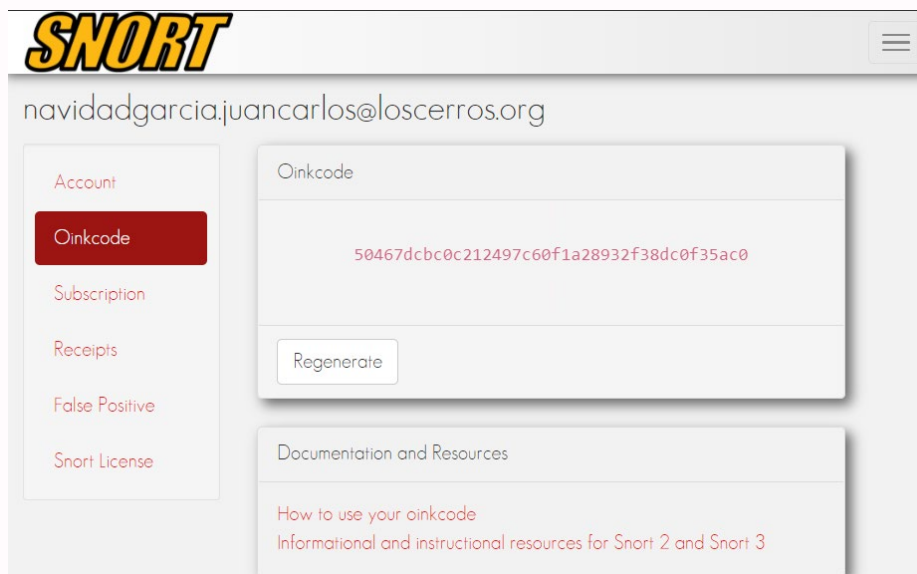
4. Registro en Snort:

Para poder descargar las **reglas** y poder utilizar completamente **Snort**, tenemos que registrarnos en su página web y utilizar **un código de licencia gratuito** que nos ofrece.

La página es www.snort.org, dentro de la página nos iremos a **Sign Up** para registrarnos:



Cuando nos hayamos **registrado**, **iniciaremos sesión** y nos iremos a **OinkCode**:



Finalmente copiaremos ese **código** para utilizarlo en el siguiente apartado.

5. Configuración de Snort:

Ahora, nos iremos a **Snort** desde **Pfsense**, recuerdo que se encuentra en el apartado de servicios.

Una vez dentro nos iremos al apartado de **Global Settings** y habilitamos **Snort VRT** y debajo pegamos el **código**:

Snort Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync
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="50467dcbc0c212497c60f1a28932f38dc0f35ac0"/>										
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)										

Aparte de añadir el **código**, habilitaremos las siguientes opciones:

Snort GPLv2 Community Rules	
Enable Snort GPLv2	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> Click to enable download of Emerging Threats Pro rules
Sign Up for an ETPro Account ETPro for Snort offers daily updates and extensive coverage of current malware threats.	
Sourcefire OpenAppID Detectors	
Enable OpenAppID	<input checked="" type="checkbox"/> 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	Installed Detection Package Version=352
Enable AppID Open Text Rules	<input checked="" type="checkbox"/> 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 .	

Posteriormente, nos iremos al apartado **Updates** y le daremos a **Update Rules** para actualizar todas las **reglas** que habilitaremos posteriormente:

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	080cfe4d054dc7818c0e8c3736029569	Thursday, 17-Feb-22 17:27:57 UTC
Snort GPLv2 Community Rules	2ca9eb52b0b30f8e8824d9ac77c287b3	Thursday, 17-Feb-22 17:27:57 UTC
Emerging Threats Open Rules	7adcd3b1dce781af55f484ca4bc86e2	Thursday, 17-Feb-22 17:27:58 UTC
Snort OpenAppID Detectors	5f660e60ad199bd5e2dbcaec8a7b2165	Thursday, 17-Feb-22 17:27:57 UTC
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Thursday, 17-Feb-22 17:27:57 UTC
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update: Feb-17 2022 17:27 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.

Nos debe de aparecer **Result: Success**.

Una vez tengamos las **reglas actualizadas**, habilitaremos las **interfaces**, para eso nos iremos a **Snort Interfaces**:

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
-----------	--------------	---------------	---------------	-------------	---------

La primera en añadir será la interfaz **WAN**, la cual la configuraremos de la siguiente manera:

WAN Settings

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.

Detection Performance Settings

Search Method:
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.

Ahora nos iremos a **WAN Categories** y habilitaremos las dos primeras casillas:

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

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 Connectivity

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!

Debajo tendremos todas las reglas de **Snort**, le daremos a seleccionar todas

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)

Enable	Ruleset: ET Open Rules	Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules	Enable	Ruleset: Snort OPENAPPID Rules
<input checked="" type="checkbox"/>	emerging-activex.rules	<input type="checkbox"/>	snort_app-detect.rules	<input type="checkbox"/>	snort_browser-chrome.so.rules	<input checked="" type="checkbox"/>	openappid-ads.rules
<input checked="" type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_attack-responses.rules	<input type="checkbox"/>	snort_browser-ie.so.rules	<input checked="" type="checkbox"/>	openappid-browser_plugin.rules
<input checked="" type="checkbox"/>	emerging-botcc.portgrouped.rules	<input type="checkbox"/>	snort_backdoor.rules	<input type="checkbox"/>	snort_browser-other.so.rules	<input checked="" type="checkbox"/>	openappid-bussiness_applications.rules
<input checked="" type="checkbox"/>	emerging-botcc.rules	<input type="checkbox"/>	snort_bad-traffic.rules	<input type="checkbox"/>	snort_browser-webkit.so.rules	<input checked="" type="checkbox"/>	openappid-collaboration.rules
<input checked="" type="checkbox"/>	emerging-chat.rules	<input type="checkbox"/>	snort_blacklist.rules	<input type="checkbox"/>	snort_exploit-kit.so.rules	<input checked="" type="checkbox"/>	openappid-database.rules
<input checked="" type="checkbox"/>	emerging-ciarmy.rules	<input type="checkbox"/>	snort_botnet-cnc.rules	<input type="checkbox"/>	snort_file-executable.so.rules	<input checked="" type="checkbox"/>	openappid-file_storage.rules
<input checked="" type="checkbox"/>	emerging-compromised.rules	<input type="checkbox"/>	snort_browser-chrome.rules	<input type="checkbox"/>	snort_file-flash.so.rules	<input checked="" type="checkbox"/>	openappid-file_transfer.rules
<input checked="" type="checkbox"/>	emerging-current_events.rules	<input type="checkbox"/>	snort_browser-firefox.rules	<input type="checkbox"/>	snort_file-image.so.rules	<input checked="" type="checkbox"/>	openappid-games.rules
<input checked="" type="checkbox"/>	emerging-deleted.rules	<input type="checkbox"/>	snort_browser-ie.rules	<input type="checkbox"/>	snort_file-java.so.rules	<input checked="" type="checkbox"/>	openappid-hacktools.rules
<input checked="" type="checkbox"/>	emerging-dns.rules	<input type="checkbox"/>	snort_browser-other.rules	<input type="checkbox"/>	snort_file-multimedia.so.rules	<input checked="" type="checkbox"/>	openappid-mail.rules
<input checked="" type="checkbox"/>	emerging-dos.rules	<input type="checkbox"/>	snort_browser-plugins.rules	<input type="checkbox"/>	snort_file-office.so.rules	<input checked="" type="checkbox"/>	openappid-messaging.rules
<input checked="" type="checkbox"/>	emerging-drop.rules	<input type="checkbox"/>	snort_browser-webkit.rules	<input type="checkbox"/>	snort_file-other.so.rules	<input checked="" type="checkbox"/>	openappid-mobile.rules
<input checked="" type="checkbox"/>	emerging-dshield.rules	<input type="checkbox"/>	snort_chat.rules	<input type="checkbox"/>	snort_file-pdf.so.rules	<input checked="" type="checkbox"/>	openappid-network_manager.rules
<input checked="" type="checkbox"/>	emerging-exploit.rules	<input type="checkbox"/>	snort_content-replace.rules	<input type="checkbox"/>	snort_indicator-shellcode.so.rules	<input checked="" type="checkbox"/>	openappid-network_monitor.rules

Por último, nos iremos a **WAN Preprocs** al apartado de **Application ID Detection**, habilitaremos las dos casillas:

Application ID Detection

Enable

☒ Use OpenAppID to detect various applications. Default is Not Checked.

Memory Cap

Memory (in MB) for App ID structures. Minimum is 32 and maximum is 3000 (3 GB). Default is 256 (256 MB).
 The memory cap in megabytes used by AppID internal structures in RAM.

AppID Stats Logging

☒ Enable OpenAppID statistics logging. Default is Checked. Log size and retention limits for AppID Stats Logging can be set on the LOG MGMT tab.

AppID Stats Period

Bucket size in seconds for AppID stats. Minimum is 60 (1 min) and maximum is 3600 (1 hr). Default is 300 (5 mins).
 The bucket size in seconds used to collect AppID statistics.

De la misma manera añadiremos y configuraremos la segunda interfaz, la **LAN**.

6. Comprobación:

Para terminar, ya tendríamos todo configurado y solo nos quedaría **iniciar las interfaces** para que empiecen a **capturar el tráfico** de la red.

Para habilitarlas, desde **Snort Interfaces**, le damos al botón de iniciar en cada una:

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 (em0)		AC-BNFA	DISABLED	WAN	
<input type="checkbox"/> LAN (em1)		AC-BNFA	DISABLED	LAN	

Delete

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 (em0)		AC-BNFA	DISABLED	WAN	
<input type="checkbox"/> LAN (em1)		AC-BNFA	DISABLED	LAN	

Delete

El **tick verde** significaría que la **interfaz** está configurada correctamente y, por lo tanto, se ha arrancado.

Por último, para comprobar que **Snort** está capturando el **tráfico de la red**, nos iremos al apartado **Alerts** y escogeremos la **interfaz LAN**, podremos ver todo nuestro tráfico de red, en el caso de que no salga nada, es que **Snort** no está trabajando correctamente por algún fallo de configuración en específico:

Services / Snort / Alerts

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

Alert Log View Settings

Interface to Inspect: LAN (em1) ☒ Auto-refresh view 250 [Save](#)

Alert Log Actions [Download](#) [Clear](#)

Alert Log View Filter

Most Recent 250 Entries from Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2022-02-17 17:01:32		3	TCP	Misc activity	192.168.1.100	36410	216.58.215.131	80	1:70444	firefox
2022-02-17 17:01:32		3	TCP	Misc activity	192.168.1.100	36410	216.58.215.131	80	1:70473	http
2022-02-17 17:01:31		3	TCP	Misc activity	192.168.1.100	47140	93.184.220.29	80	1:70444	firefox
2022-02-17 17:01:31		3	TCP	Misc activity	192.168.1.100	47140	93.184.220.29	80	1:70473	http
2022-02-17 17:01:31		3	TCP	Misc activity	192.168.1.100	36420	216.58.215.131	80	1:70444	firefox
2022-02-17 17:01:31		3	TCP	Misc activity	192.168.1.100	36420	216.58.215.131	80	1:70473	http
2022-02-17 17:01:28		3	TCP	Misc activity	192.168.1.100	36406	216.58.215.131	80	1:70444	firefox
2022-02-17 17:01:28		3	TCP	Misc activity	192.168.1.100	36406	216.58.215.131	80	1:70473	http