



## Suricata + PfSense

Inicialmente precisaremos realizar o download do pacote Suricata

System / [Package Manager](#) / [Installed Packages](#)

[Installed Packages](#) [Available Packages](#)

Installed Packages				
Name	Category	Version	Description	Actions
✓ suricata	security	6.0.0_10	High Performance Network IDS, IPS and Security Monitoring engine by OISF.	 
Package Dependencies: <a href="#">suricata-5.0.6</a>				

Desativaremos Hardware Checksum indo em System > Advanced > Networking

**Network Interfaces**

**Hardware Checksum Offloading** ☒ Disable hardware checksum offload

Checking this option will disable hardware checksum offloading.  
Checksum offloading is broken in some hardware, particularly some Realtek cards. Rarely, drivers may have problems with checksum offloading and some specific NICs. This will take effect after a machine reboot or re-configure of each interface.

Dentro de Services > Suricata iniciaremos as configurações em Global Settings. É necessário ter em mãos o Oinkmaster e o nome do arquivo de regras do Snort, ambos serão encontrados em [snort.org](https://snort.org)

**Install Snort rules** ☒ Snort free Registered User or paid Subscriber rules ☐ Use a custom URL for Snort rule downloads

[Sign Up for a free Registered User Rules Account](#)  
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

Enabling the custom URL option will force the use of a custom user-supplied URL when downloading Snort Subscriber rules.

**Snort Rules Filename**

Enter the rules tarball filename (filename only, do not include the URL.)  
Example: snortrules-snapshot-29151.tar.gz  
DO NOT specify a Snort3 rules file! Snort3 rules are incompatible with Suricata and will break your installation!











**Snort Oinkmaster Code**

Obtain a snort.org Oinkmaster code and paste it here.

**Install 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. ☐ Use a custom URL for Snort GPLv2 rule downloads

This ruleset is updated daily and is a subset of the subscriber ruleset. If you are a Snort Subscriber Rules customer (paid subscriber), the community ruleset is already built into your download of the Snort Subscriber rules, and there is no benefit in adding this rule set separately.

Criaremos duas interfaces

Interface Settings Overview						
	Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/>	WAN (em0)	  	AUTO	INLINE IPS	WAN	 
<input type="checkbox"/>	LAN (em1)	  	AUTO	INLINE IPS	LAN	 

Nos dois casos as configurações são idênticas, vejamos a seguir:  
Primeiro será necessário habilitar a interface e seleccionar se será WAN ou LAN

**General Settings**

Enable

☒ Checking this box enables Suricata inspection on the interface.

Interface

WAN (em0)

Choose which interface this Suricata instance applies to. In most cases, you will want to use WAN here.

Description

WAN

Enter a meaningful description here for your reference. The default is the interface name.

Habilitaremos os logs

Enable HTTP Log

☒ Suricata will log decoded HTTP traffic for the interface. Default is Checked.

Append HTTP Log

☒ Suricata will append-to instead of clearing HTTP log file when restarting. Default is Checked.

Log Extended HTTP Info

☒ Suricata will log extended HTTP information. Default is Checked.

Selecionaremos a opção Block Offenders que bloqueará hosts que gerarem alertas, e a opção Inline Mode para que o Suricata apenas monitore antes de tomar qualquer providencia

**Alert and Block Settings**

Block Offenders

☒ Checking this option will automatically block hosts that generate a Suricata alert.

IPS Mode

Inline Mode

Depois de ambas interfaces criadas e iniciadas, os logs ja passam a aparecer na aba Alerts

05/22/2021 00:07:03		3	TCP	Not Assigned	192.168.31.176	50596	35.244.247.133	443	1:2210059	SURICATA STREAM pkt seen on wrong thread
05/22/2021 00:07:03		3	TCP	Not Assigned	192.168.31.176	50594	35.244.247.133	443	1:2210059	SURICATA STREAM pkt seen on wrong thread
05/22/2021 00:06:51		3	TCP	Not Assigned	192.168.31.176	49152	52.114.128.9	443	1:2210059	SURICATA STREAM pkt seen on wrong thread

## INDO MAIS A FUNDO

Indo em cada uma das interfaces e seleccionando a guia Categories é possível seleccionar todas regras e aplica-las

**Select the rulesets (Categories) Suricata 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

Enabled

Ruleset: Snort GPLv2 Community Rules

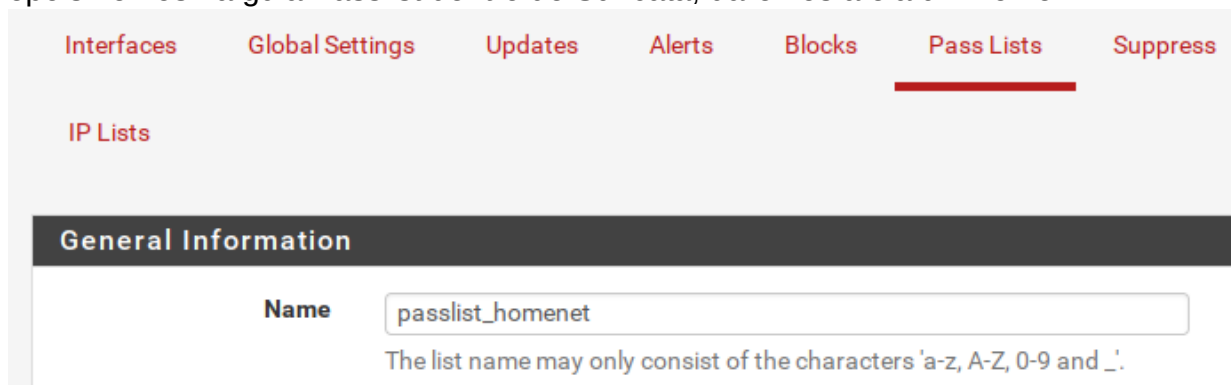
☒

Snort GPLv2 Community Rules (Talos-certified)

É possível também criar um Alias com host permissivos, e fazer destes hosts nossa homenet.

Primeiro criamos o Alias em Firewall > Aliases

Depois iremos na guia Passlist dentro de Suricata, daremos a ela um nome



Interfaces Global Settings Updates Alerts Blocks **Pass Lists** Suppress

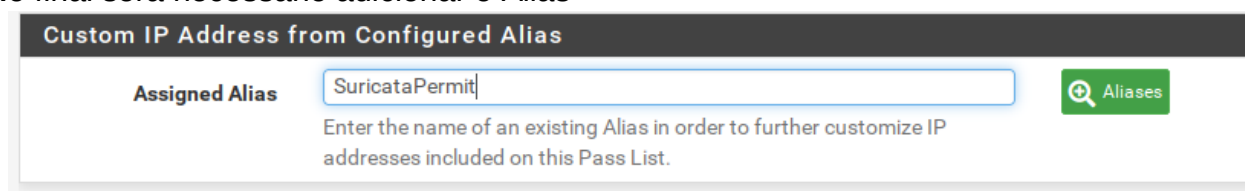
IP Lists

### General Information


**Name**

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

No final será necessário adicionar o Alias

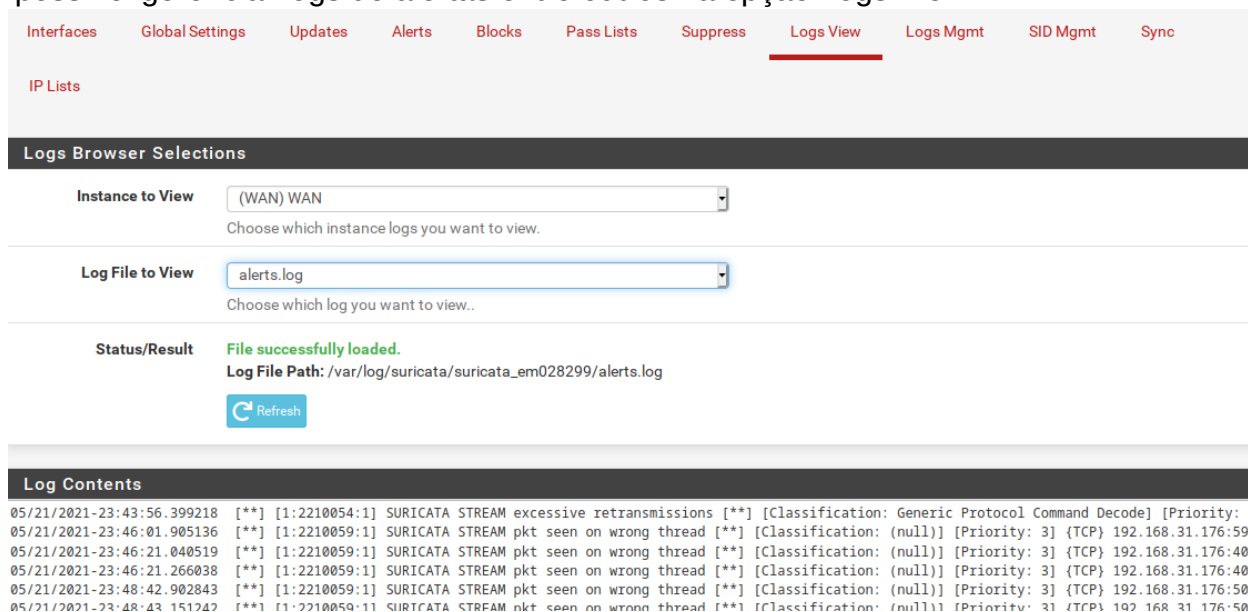


**Custom IP Address from Configured Alias**

**Assigned Alias**  

Enter the name of an existing Alias in order to further customize IP addresses included on this Pass List.

É possível gerenciar logs de alertas entre outros na opção Logs View




Interfaces Global Settings Updates Alerts Blocks Pass Lists Suppress **Logs View** Logs Mgmt SID Mgmt Sync

IP Lists

### Logs Browser Selections

**Instance to View**   
Choose which instance logs you want to view.

**Log File to View**   
Choose which log you want to view..

**Status/Result** **File successfully loaded.**  
**Log File Path:** /var/log/suricata/suricata\_em028299/alerts.log  


### Log Contents

```
05/21/2021-23:43:56.399218  [**] [1:2210054:1] SURICATA STREAM excessive retransmissions [**] [Classification: Generic Protocol Command Decode] [Priority:
05/21/2021-23:46:01.905136  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.31.176:59
05/21/2021-23:46:21.040519  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.31.176:40
05/21/2021-23:46:21.266038  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.31.176:40
05/21/2021-23:48:42.902843  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.31.176:50
05/21/2021-23:48:43.151242  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.31.176:50
```

É possível também alterar um alerta para que ele passe a “dropar” atividades

The screenshot shows a security dashboard with an alert log and a modal dialog for selecting rule actions.

**Alert Log View Filter**

Last 250 Alert Entries. (Most recent first)

Note: Alerts triggered by DROP rules that have been triggered by a rule that is currently in a 'DROP' state.

Date	Action	Pri	Proto	Not Assigned	192.168.31.176	42122	142.250.218.168	443	1:2210059	SURICATA STREAM pkt seen on wrong thread
05/22/2021 00:35:24	⚠	3	TCP	Not Assigned	192.168.31.176	42122	142.250.218.168	443	1:2210059	SURICATA STREAM pkt seen on wrong thread
05/22/2021 00:35:23	⚠	3	TCP	Not Assigned	192.168.31.176	54996	72.52.94.234	443	1:2210059	SURICATA STREAM pkt seen on wrong thread
05/22/2021 00:35:23	⚠	3	TCP	Not Assigned	192.168.31.176	54994	72.52.94.234	443	1:2210059	SURICATA STREAM pkt seen on wrong thread
05/22/2021	⚠	3	TCP	Not Assigned	192.168.31.176	54992	72.52.94.234	443	1:2210059	SURICATA STREAM pkt seen on wrong thread

**Rule Action Selection**

Choose desired rule action from selections below:

☐ Default ☐ ALERT ☒ DROP ☐ REJECT

Choosing 'Default' will return the rule action to the original value specified by the rule author. Note this is usually ALERT.

Save Cancel