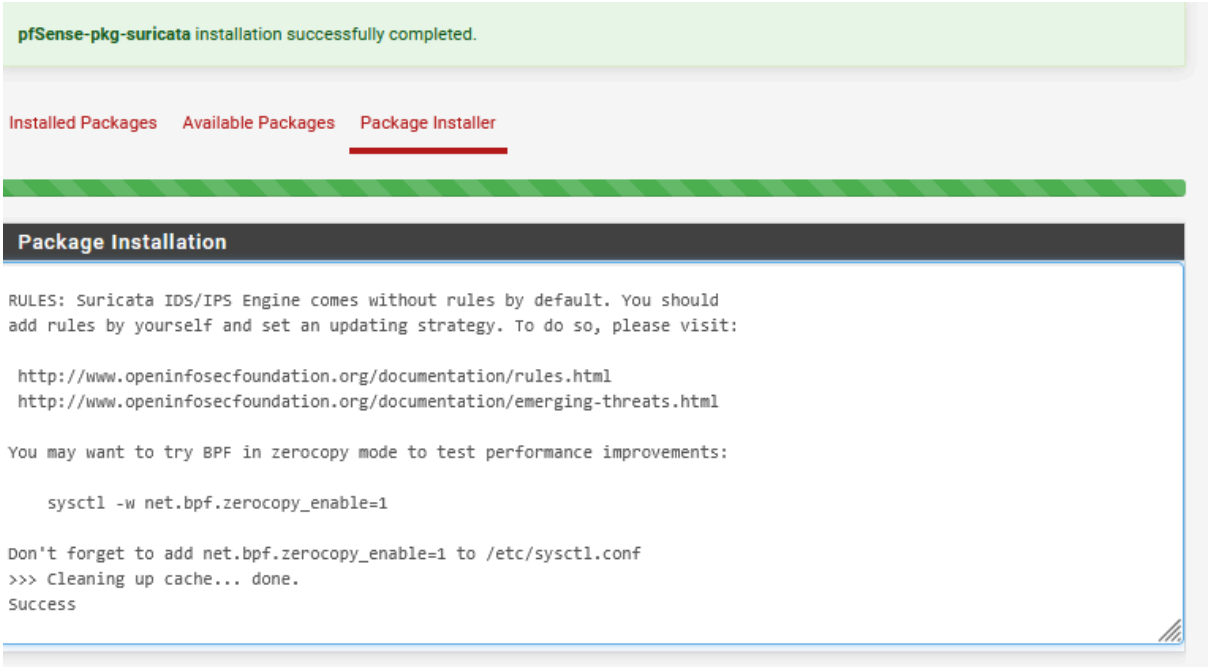
Mise en place de la détection d’intrus

Installation du Paquet

Menu : **System > Package Manager > Available Packages**

Dans la barre de recherche, tape `suricata`

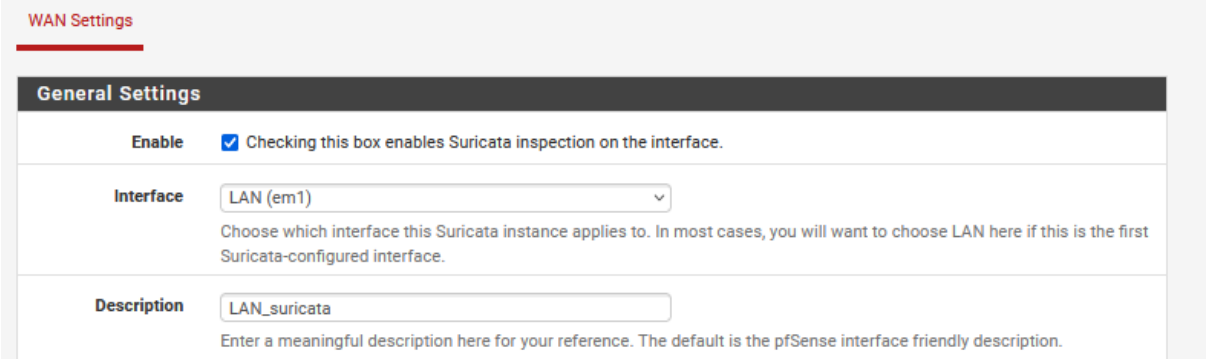
Clique sur Install à côté de Suricata

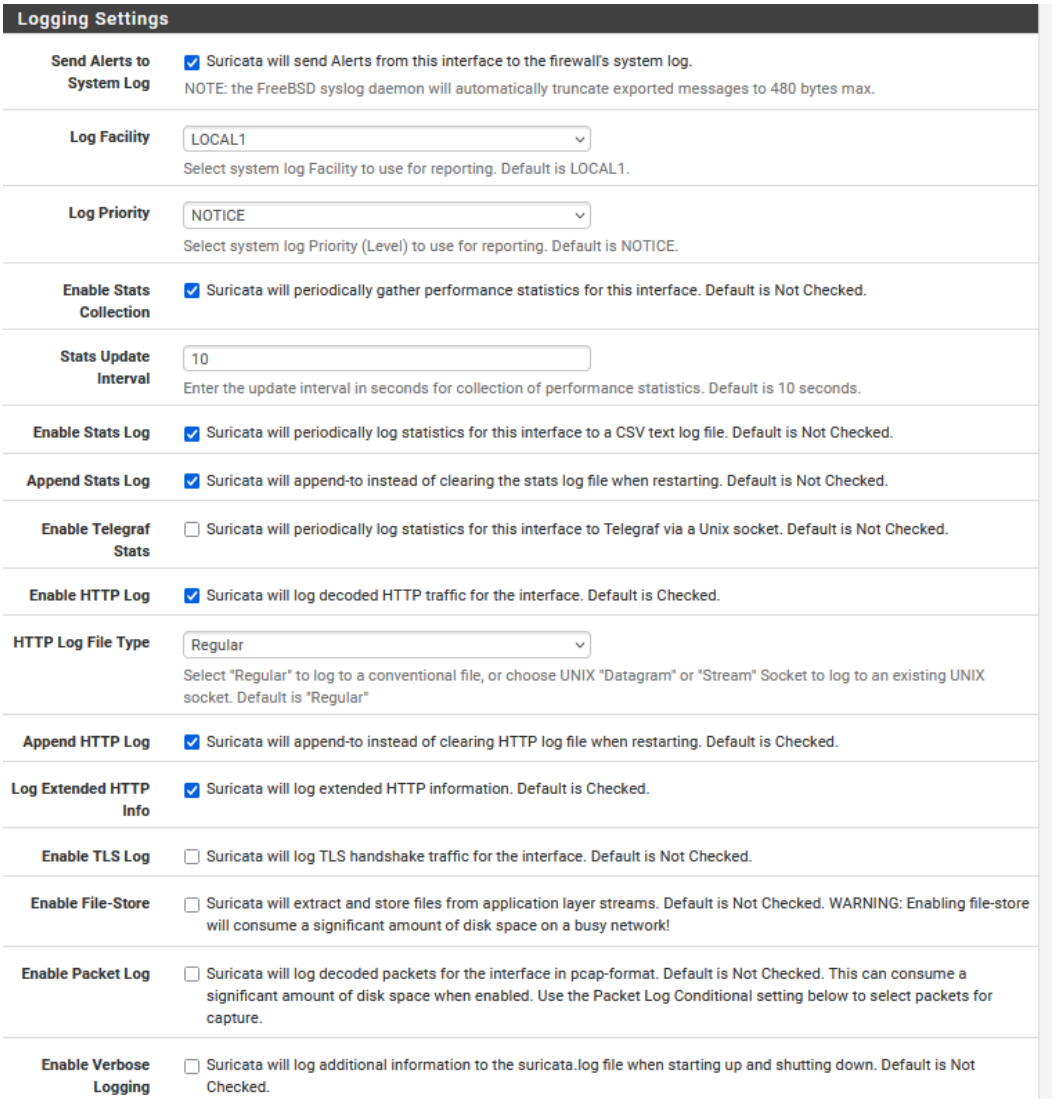


Activer Suricata sur l’interface LAN

Menu : **Services > Suricata**

Cliquez sur Add





EVE Output Settings

EVE JSON Log

☐ Suricata will output selected info in JSON format to a single file or to syslog. Default is Not Checked.

Alert and Block Settings

Block Offenders

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

IPS Mode

Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata 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 Suricata 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 include: bnxt, cc, cxgbe, cxl, 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

☑ Checking this option will kill firewall states for the blocked IP. Default is Checked.

Which IP to Block

BOTH

Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value.

Block On DROP Only

☐ Checking this option will insert blocks only when rule signatures having the DROP action are triggered. When not checked, any rule action (ALERT or DROP) will generate a block of the offending host. Default is Not Checked.

IP Pass List

default View List

Choose the Pass List you want this interface to use.
Addresses in a Pass List are never blocked. Select "none" to prevent use of a Pass List.

The default Pass List adds Gateways, DNS servers, locally-attached networks, the WAN IP, VPNs and VIPs. Create a Pass List with an alias to customize whitelisted IP addresses. This option will only be used when block offenders is on. Choosing "none" will disable Pass List generation.

Enable Passlist Debugging Log

☐ Checking this option will enable detailed Passlist operations logging to file /var/log/suricata/suricata_em024779/passlist_debug.log. Default is Not Checked.

Performance and Detection Engine Settings

Run Mode

Workers

Choose a Suricata run mode setting. Default is "AutoFP" and is the recommended setting for IDS-only and Legacy Blocking Mode. "Workers" uses multiple worker threads, each of which processes the packets it acquires through all the decode and detect modules. "Workers" runmode is preferred for Inline IPS Mode blocking because it offers superior performance in that configuration. "Single" uses only a single thread for all operations, and is intended for use only in testing or development instances.

Max Pending Packets

1024

Enter number of simultaneous packets to process. Default is 1024.
This controls the number of simultaneous packets the engine can handle. Setting this higher generally keeps the threads more busy. The minimum value is 1 and the maximum value is 65,000.
Warning: Setting this too high can lead to degradation and a possible system crash by exhausting available memory.

Detect-Engine Profile

Medium

Choose a detection engine profile. Default is Medium.
MEDIUM is recommended for most systems because it offers a good balance between memory consumption and performance. LOW uses less memory, but it offers lower performance. HIGH consumes a large amount of memory, but it offers the highest performance.

Multi-Pattern Matcher Algorithm

Auto

Choose a multi-pattern matcher (MPM) algorithm. Auto is the default, and is the best choice for almost all systems. Auto will use hyperscan if available.

Single-Pattern Matcher Algorithm

Auto

Choose a single-pattern matcher (SPM) algorithm. Auto is the default, and is the best choice for almost all systems. Auto will use hyperscan if available.

Signature Group Header MPM Context

Auto

Choose a Signature Group Header multi-pattern matcher context. Default is Auto.
AUTO means Suricata selects between Full and Single based on the MPM algorithm chosen. FULL means every Signature Group has its own MPM context. SINGLE means all Signature Groups share a single MPM context. Using FULL can improve performance at the expense of significant memory consumption.

Inspection Recursion Limit

3000

Enter limit for recursive calls in content inspection code. Default is 3000.
When set to 0 an internal default is used. When left blank there is no recursion limit.

Delayed Detect

☐ Suricata will build list of signatures after packet capture threads have started. Default is Not Checked.

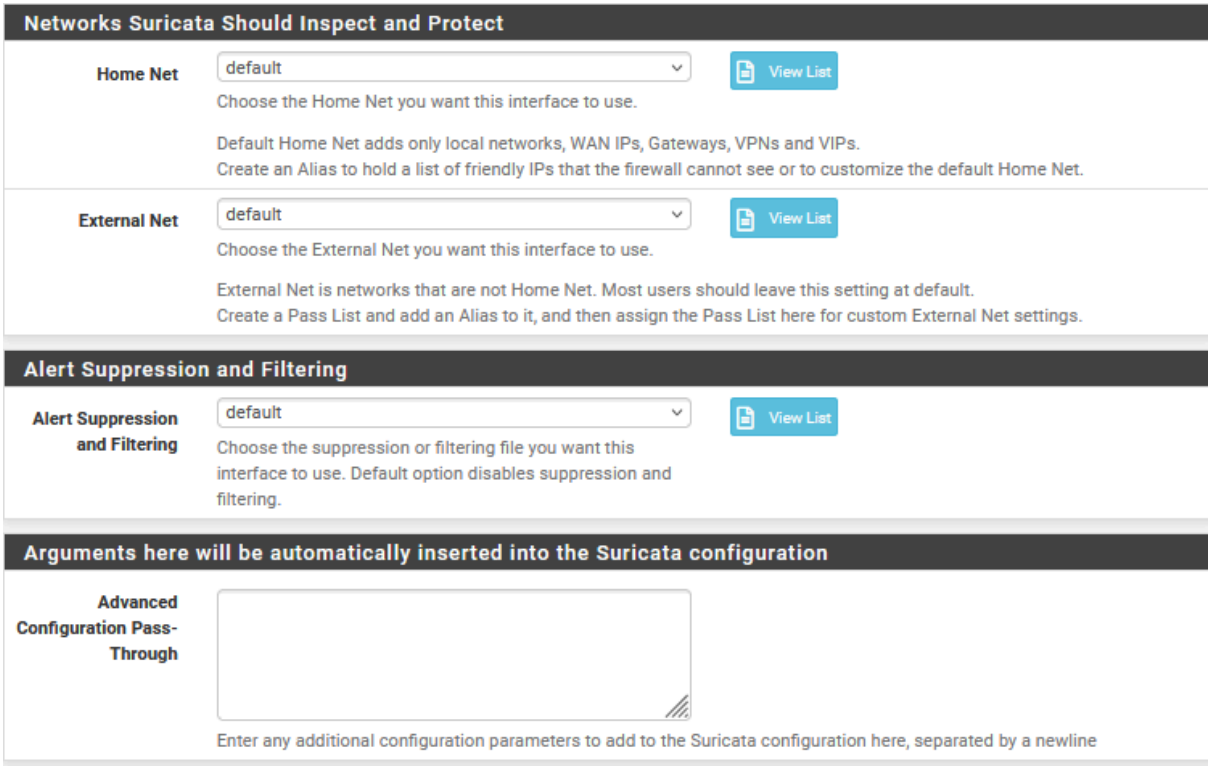
Promiscuous Mode

☑ Suricata will place the monitored interface in promiscuous mode when checked. Default is Checked.

Interface PCAP Snaplen

1518

Enter value in bytes for the interface PCAP snaplen. Default is 1518. This parameter is only valid when IDS or Legacy Mode IPS is enabled


Networks Suricata Should Inspect and Protect
Home Net
default
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
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.
Alert Suppression and Filtering
Alert Suppression and Filtering
default
View List
Choose the suppression or filtering file you want this interface to use. Default option disables suppression and filtering.
Arguments here will be automatically inserted into the Suricata configuration
Advanced Configuration Pass-Through
Enter any additional configuration parameters to add to the Suricata configuration here, separated by a newline