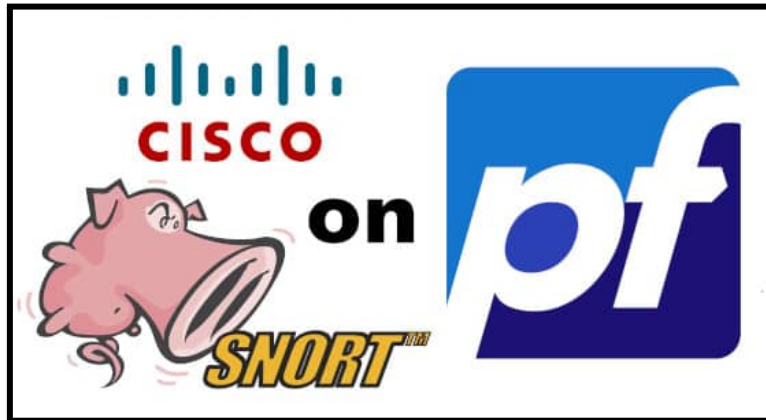


Guía de Snort: Introducción al Sistema de Detección y Prevención de Intrusiones



¿Qué es Snort?

Snort es una herramienta de código abierto diseñada para monitorear el tráfico de red y detectar amenazas. Funciona como un **IDS (Sistema de Detección de Intrusiones)** y un **IPS (Sistema de Prevención de Intrusiones)**, ofreciendo protección en tiempo real.

¿Para qué sirve Snort?

1. **Detección de Intrusiones (IDS):**
 - **Propósito:** Monitorea el tráfico de red buscando patrones sospechosos que coincidan con reglas predefinidas.
 - **Aplicación:** Usado para alertar a los administradores cuando se detectan ataques.
2. **Prevención de Intrusiones (IPS):**
 - **Propósito:** No solo detecta, sino que también bloquea el tráfico malicioso de manera proactiva.
 - **Aplicación:** Se utiliza para evitar que un ataque ocurra bloqueando paquetes maliciosos en tiempo real.
3. **Registro de Tráfico:**
 - **Propósito:** Guarda el tráfico de red para análisis posteriores.
 - **Aplicación:** Utilizado para auditoría, análisis forense, y revisión de incidentes de seguridad.

Puntos Claves para Entender Snort

1. Modos de Operación:

- **Sniffer:**
 - **Propósito:** Muestra los paquetes que pasan por la red en tiempo real.
 - **Aplicación:** Se usa para observar el tráfico sin aplicar reglas ni análisis.
- **Logger:**
 - **Propósito:** Guarda los paquetes capturados en un archivo para su análisis posterior.
 - **Aplicación:** Ideal para auditoría de tráfico o análisis forense.
- **IDS/IPS:**
 - **Propósito:** Detecta o bloquea el tráfico en base a reglas configuradas.
 - **Aplicación:** Es el modo principal utilizado para la detección y prevención de ataques.

2. Reglas de Snort:

- **Estructura:**
 - **Propósito:** Definen cómo debe comportarse Snort ante tráfico sospechoso.
 - **Aplicación:** Las reglas permiten a Snort decidir si generar una alerta, registrar el tráfico o bloquearlo.
- **Opciones de las Reglas:**
 - **Propósito:** Permiten especificar condiciones más detalladas como contenido, flags TCP, y otros parámetros.
 - **Aplicación:** Refinar las reglas para detectar comportamientos más específicos o patrones avanzados.

3. Preprocesadores:

- **Propósito:** Analizan y preparan el tráfico antes de que las reglas se apliquen.
- **Aplicación:** Mejoran la capacidad de detección al procesar tráfico como fragmentación IP, reensamblaje de TCP, o inspección de protocolos como HTTP.

4. Alertas y Logs:

- **Propósito:** Generar notificaciones en tiempo real y registrar datos de los paquetes que cumplen con las reglas configuradas.
- **Aplicación:** Las alertas son utilizadas para monitorear la red en tiempo real, y los logs son guardados para análisis más detallado.

5. Interfaces de Salida:

- **Propósito:** Permiten integrar Snort con otras plataformas como dashboards o bases de datos.
- **Aplicación:** Las alertas y los logs pueden visualizarse en herramientas externas como **Snorby**, **BASE**, o **Kibana** para obtener una visión más clara y gestionable de las detecciones.

Conceptos Importantes

1. Configuración de Reglas:

- **Propósito:** Definir cómo Snort debe comportarse ante tráfico específico.
- **Aplicación:** Las reglas determinan qué tipo de tráfico genera alertas o es bloqueado.

2. Falsos Positivos/Negativos:

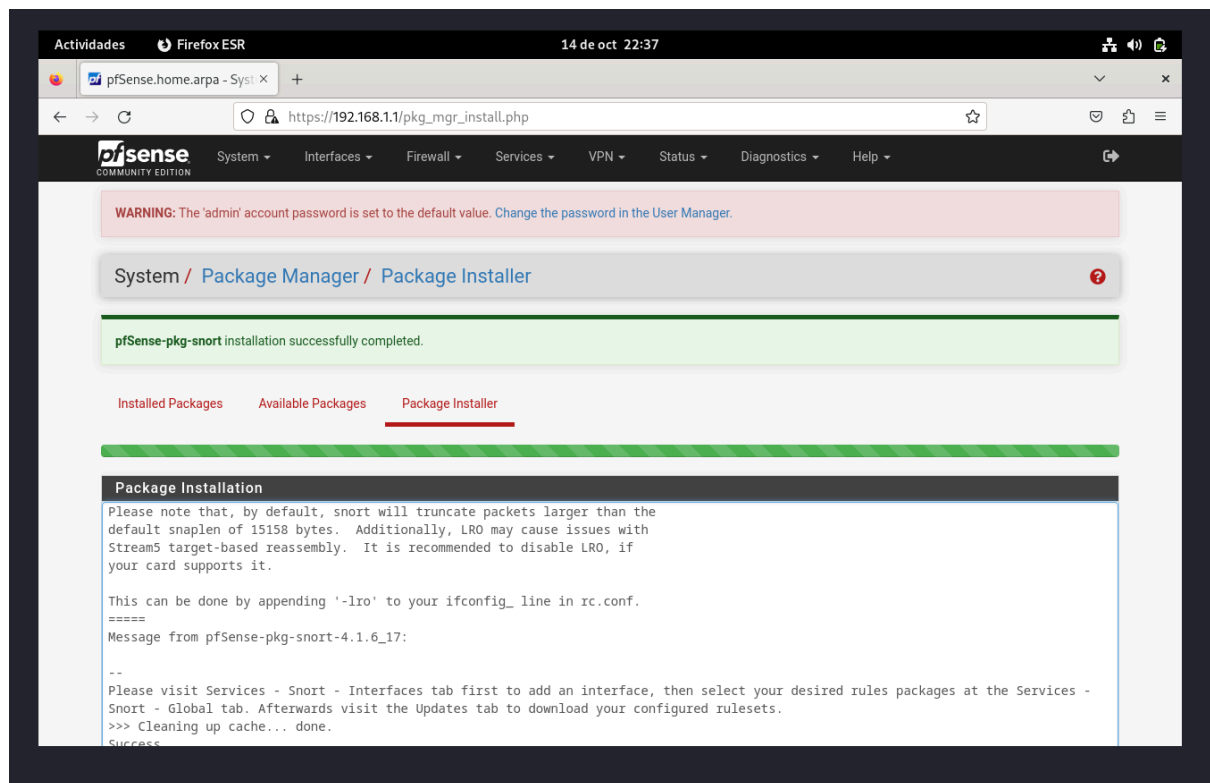
- **Propósito:** Gestionar la precisión del sistema.
- **Aplicación:** Es fundamental ajustar las reglas y preprocesadores para minimizar errores.

3. Actualización de Firmas:

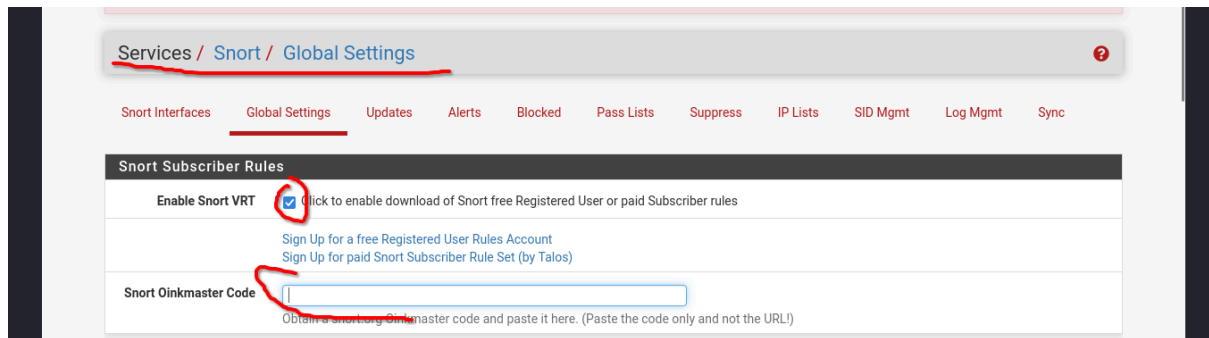
- **Propósito:** Mantener a Snort al día con las últimas amenazas.
- **Aplicación:** Las firmas de ataque deben actualizarse frecuentemente para detectar nuevas vulnerabilidades.

Instalación de snort en pfsense

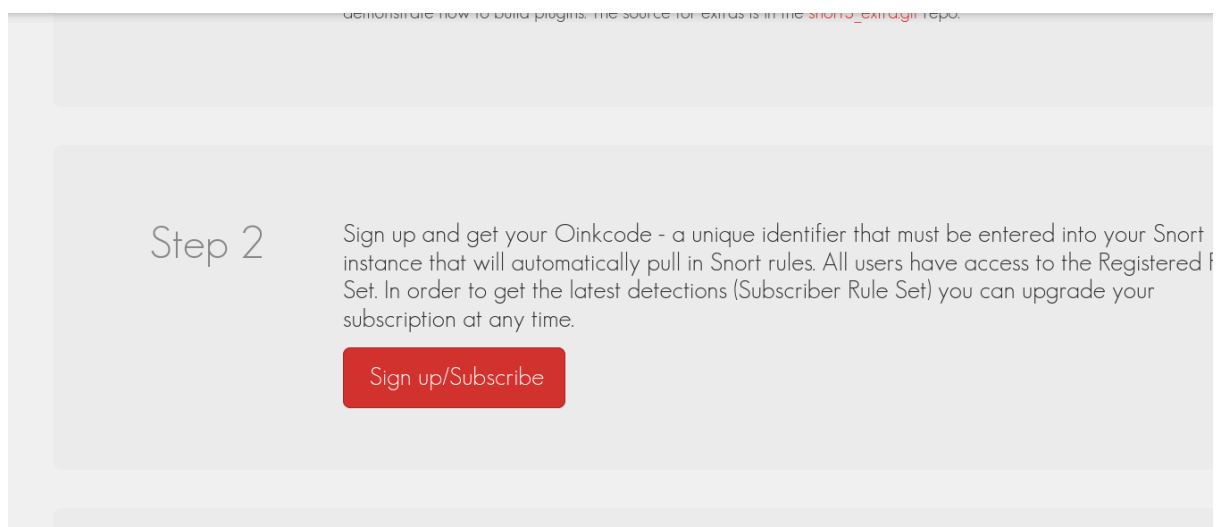
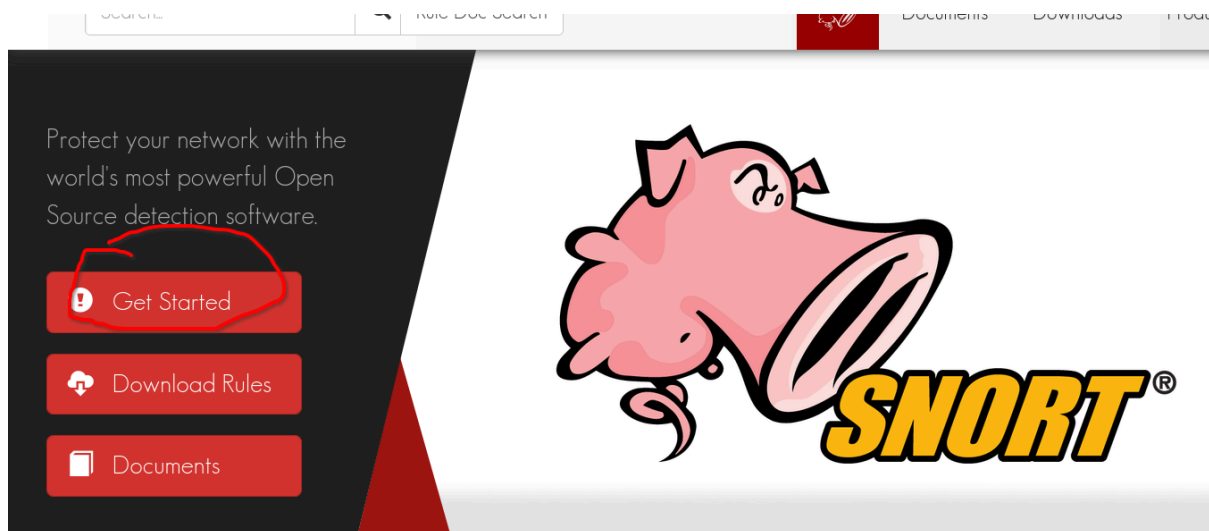
Para instalar Snort en pfSense, ve a **System > Package Manager**, luego dirígete a la pestaña **Available Packages**. Busca **Snort** en la lista de paquetes disponibles y haz clic en **Install**. Espera a que se complete la instalación para comenzar a configurarlo.

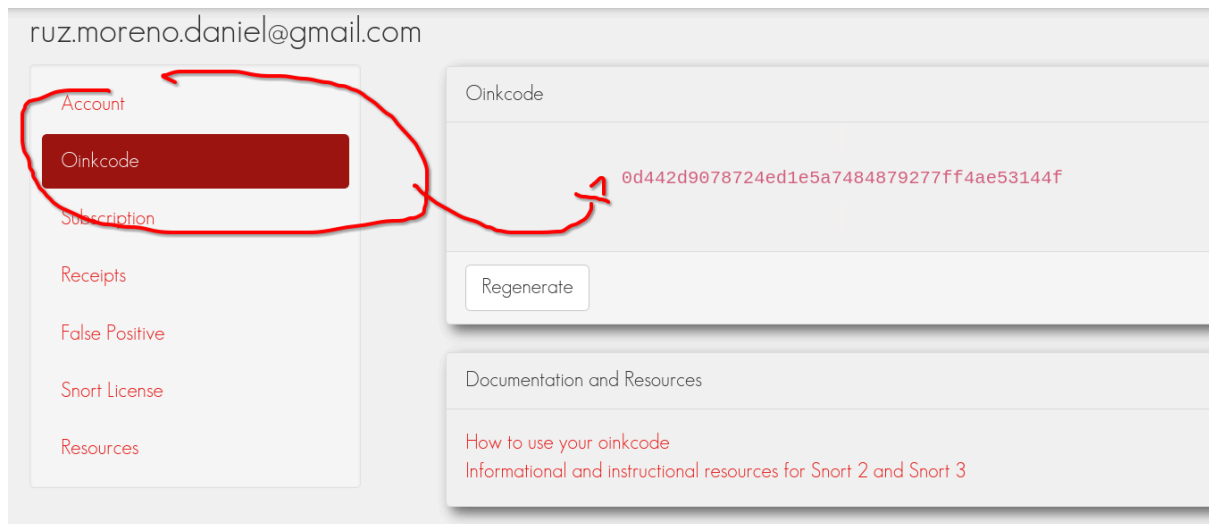


configuración de snort

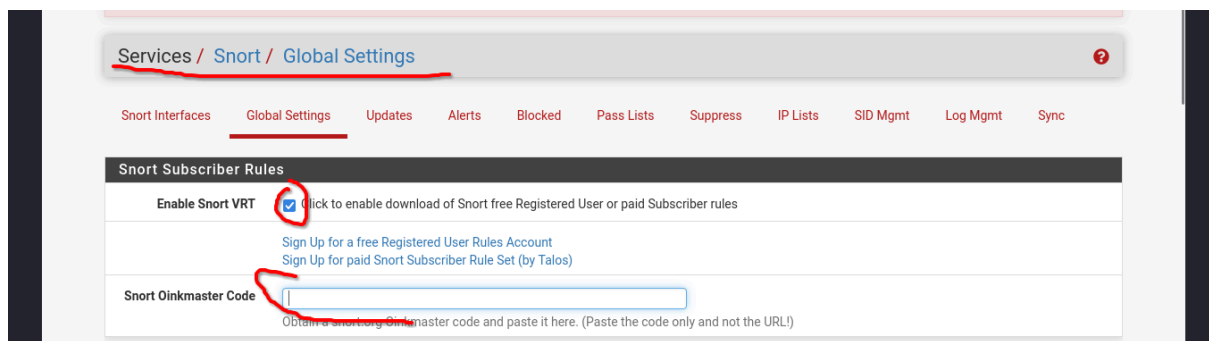


Para instalar Snort en pfSense, ve a **System > Package Manager**, luego dirígete a la pestaña **Available Packages**. Busca **Snort** en la lista de paquetes disponibles y haz clic en **Install**. Espera a que se complete la instalación para comenzar a configurarlo.

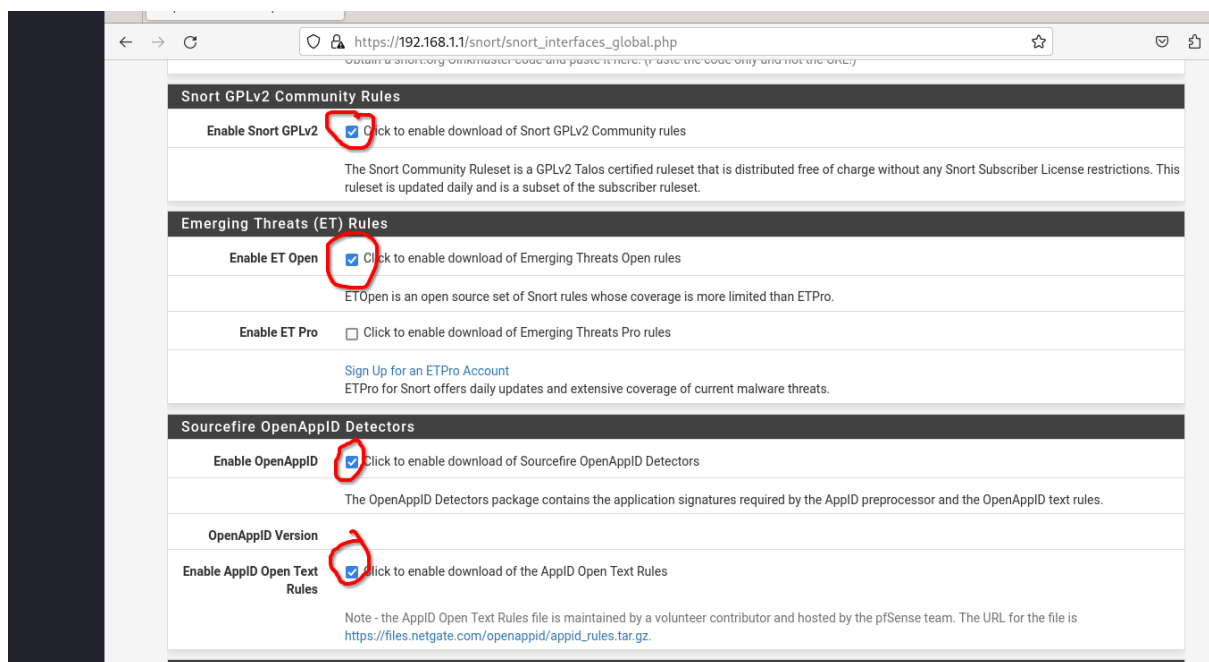




copiamos el código



luego marcamos las casillas como están en la imagen



Rules Update Settings

Update Interval

7 DAYS

Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Update Start Time

00:19

Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.

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.

Guardamos los cambios y actualizamos la lista de reglas.

prisen.se.norne.arpa - Serv

https://192.168.1.1/snort/snort_download_updates.php

130%

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	ae5f927cb858094d7930ce36283a99a5	Tuesday, 15-Oct-24 02:01:40 UTC
Snort GPLv2 Community Rules	81e6abdf1b243c116738f689f7a6a9d	Tuesday, 15-Oct-24 02:01:40 UTC
Emerging Threats Open Rules	f8cc0754aac53e9c8f182adb538710a5	Tuesday, 15-Oct-24 02:01:40 UTC
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Tuesday, 15-Oct-24 02:01:40 UTC
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Tuesday, 15-Oct-24 01:59:56 UTC
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update

Oct-15 2024

Update Rules

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.

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.

Close

prisen.se.norne.arpa - Serv

https://192.168.1.1/snort/snort_download_updates.php

120%

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	ae5f927cb858094d7930ce36283a99a5	Tuesday, 15-Oct-24 02:20:19 UTC
Snort GPLv2 Community Rules	81e6abdf1b243c116738f689f7a6a9d	Tuesday, 15-Oct-24 02:01:40 UTC
Emerging Threats Open Rules	f8cc0754aac53e9c8f182adb538710a5	Tuesday, 15-Oct-24 02:01:40 UTC
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Tuesday, 15-Oct-24 02:01:40 UTC
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Tuesday, 15-Oct-24 01:59:56 UTC
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update

Oct-15 2024 02:20

Result: Success

Update Rules

Update Rules

Force Update

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.

Para activar el modo **IPS** en Snort en **pfSense**, ve a **Services > Snort** y en la pestaña **Global Settings**, marca **Enable Block Offenders**. Luego, en la pestaña **Interfaces**, selecciona la interfaz deseada (como **WAN** o **LAN**) y habilita **Block Offenders** para esa interfaz específica. Guarda los cambios y Snort bloqueará automáticamente el tráfico malicioso en las interfaces configuradas.

WAN Settings

General Settings

Enable

☒ Enable interface

Interface

WAN (em0)

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.

Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode

Legacy Mode

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

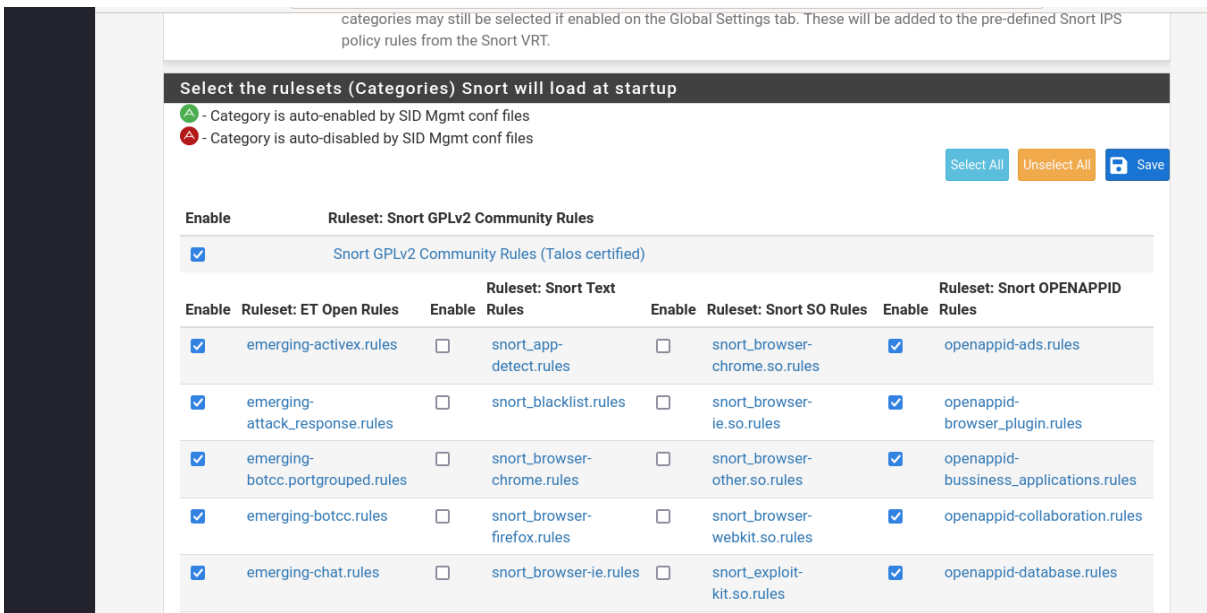
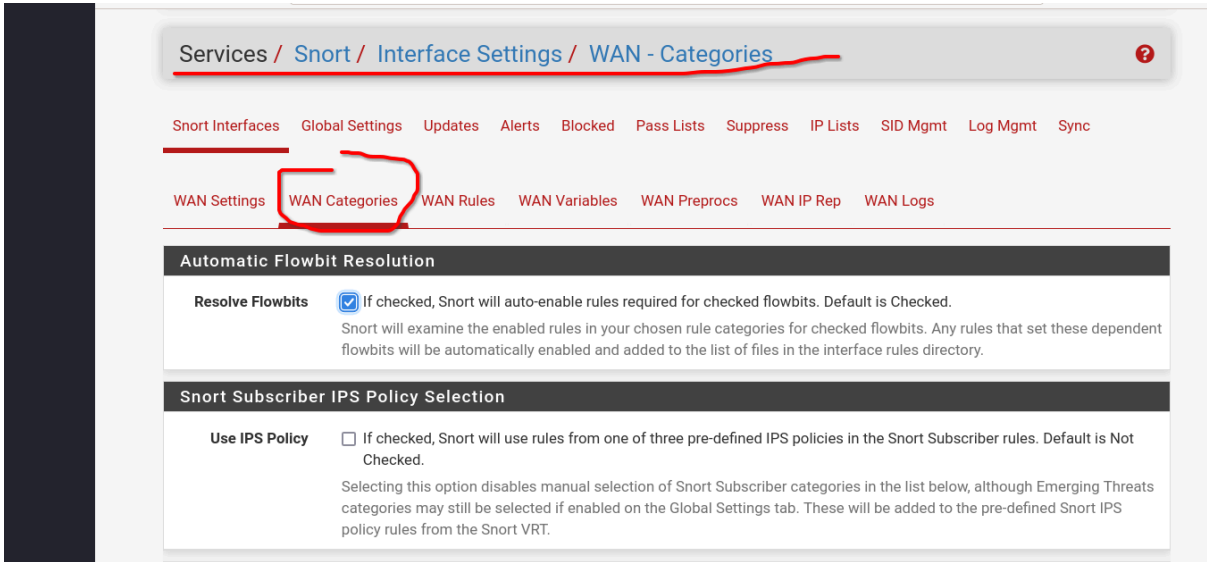
☒ Checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block

BOTH

Select which IP extracted from the packet you wish to block. Default is BOTH.

La opción WAN/LAN Category en Snort te permite especificar qué tipo de tráfico deseas que Snort inspeccione en la interfaz seleccionada, ya sea WAN (Wide Area Network) o LAN (Local Area Network). Al marcar las casillas correspondientes, puedes elegir analizar el tráfico entrante (Inbound), saliente (Outbound) o ambos (Both), lo que te permite personalizar el monitoreo de Snort y optimizar la detección de amenazas según las necesidades de tu red.



La opción **LAN/WAN Preprocessors** en Snort permite activar módulos que procesan el tráfico antes de que Snort lo analice en busca de amenazas. Estos módulos, como **Frag3** para reensamblar paquetes fragmentados o **Stream5** para rastrear conexiones, ayudan a mejorar la precisión de Snort y a detectar ataques más fácilmente. Al habilitar estos preprocessors en las interfaces **LAN** o **WAN**, Snort puede analizar mejor el tráfico y ofrecer una detección más eficiente.

Services / Snort / Interface Settings / WAN - Preprocessors and Flow

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

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

Important Preprocessor Information

Rules may be dependent on enabled 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

default all

Application ID Detection

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

Memory Cap 256
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 300
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.

Portscan Detection

Enable ☒ Use Portscan Detection to detect various types of port scans and sweeps. Default is Not Checked.

Protocol

Choose the Portscan protocol type to alert for (all, tcp, udp, icmp or ip). The default is *all*.

Scan Type

Choose the Portscan scan type to alert for. The default is *all*.

PORTSCAN: one->one scan; one host scans multiple ports on another host.

PORTSWEEP: one->many scan; one host scans a single port on multiple hosts.

DECOY_PORTSCAN: one->one scan; attacker has spoofed source address inter-mixed with real scanning address.

DISTRIBUTED_PORTSCAN: many->one scan; multiple hosts query one host for open services.

ALL: alerts for all of the above scan types.

Detection

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.



Save



Reset

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.