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

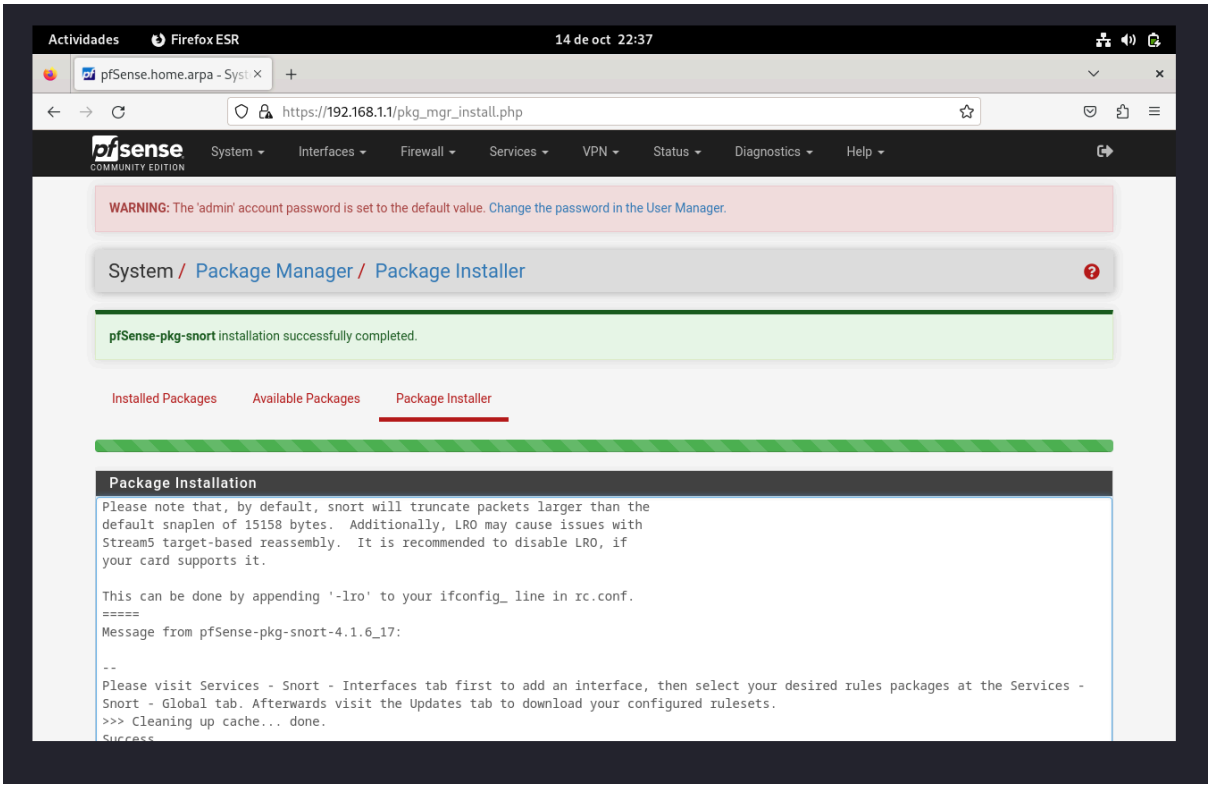
1. **Modos de Operación**:
    - **Sniffer**:
        - **Propósito**: Muestra los paquetes que pasan por la red en tiempo real.
        - **Aplicación**: Se usa para observar el tráfico sin aplicar reglas ni análisis.
    - **Logger**:
        - **Propósito**: Guarda los paquetes capturados en un archivo 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

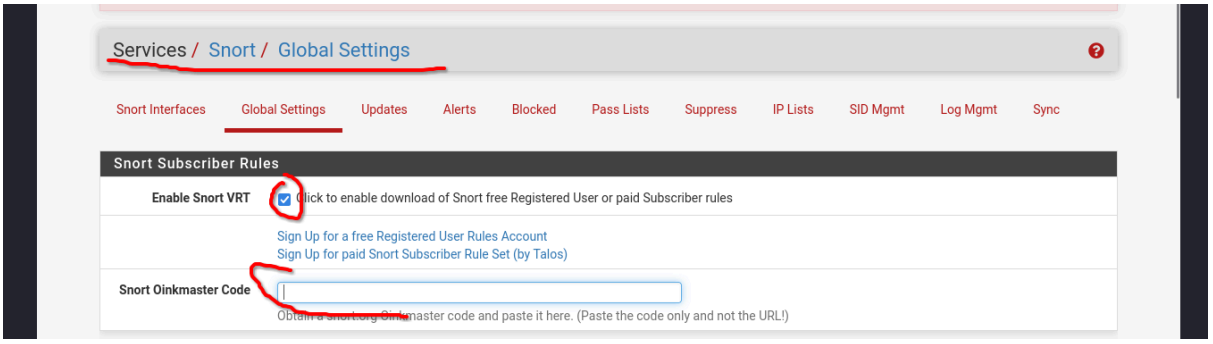
1. **Configuración de Reglas**:
    - **Propósito**: Definir cómo Snort debe comportarse ante tráfico específico.
    - **Aplicación**: Las reglas determinan qué tipo de tráfico genera alertas o es bloqueado.
2. **Falsos Positivos/Negativos**:
    - **Propósito**: Gestionar la precisión del sistema.
    - **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

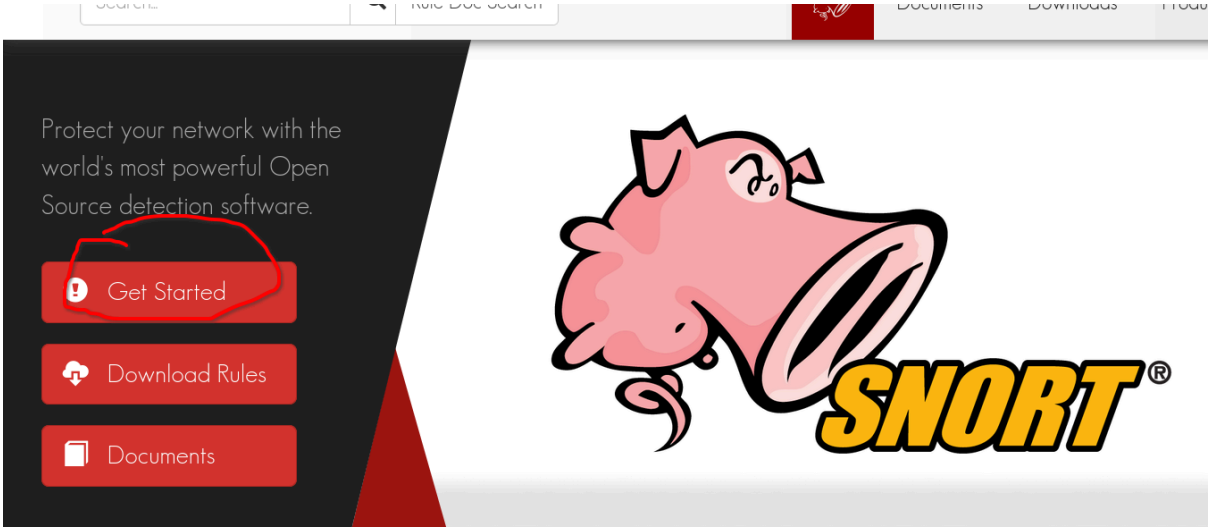
Para instalar Snort en pfSense, ve a **System** > **Package Manager**, luego dirígete a la pestaña **Available Packages**. Busca **Snort** en la lista de paquetes disponibles y haz clic en **Install**. Espera a que se complete la instalación para comenzar a configurarlo.

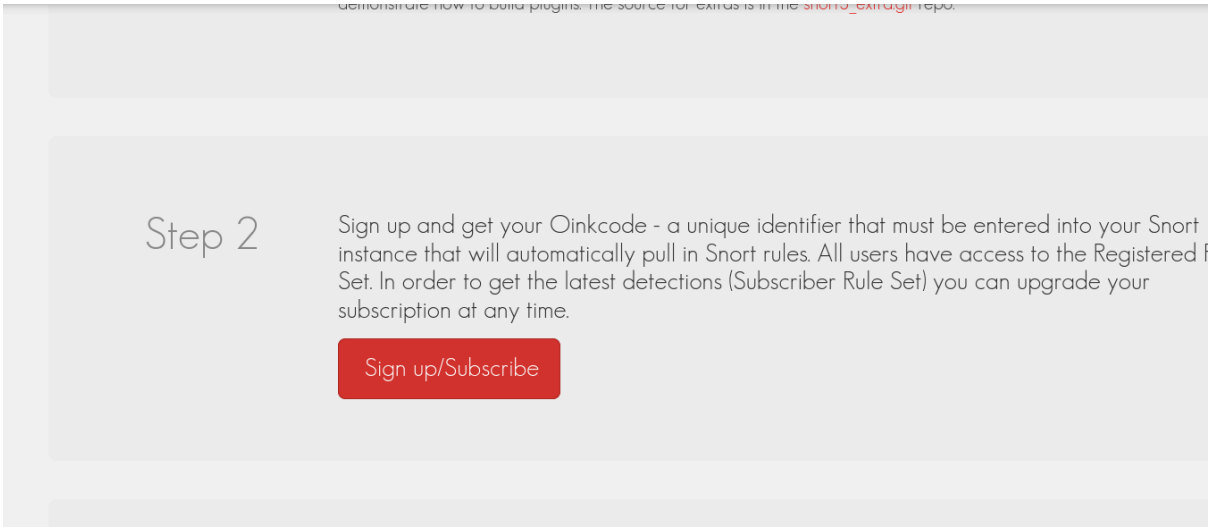


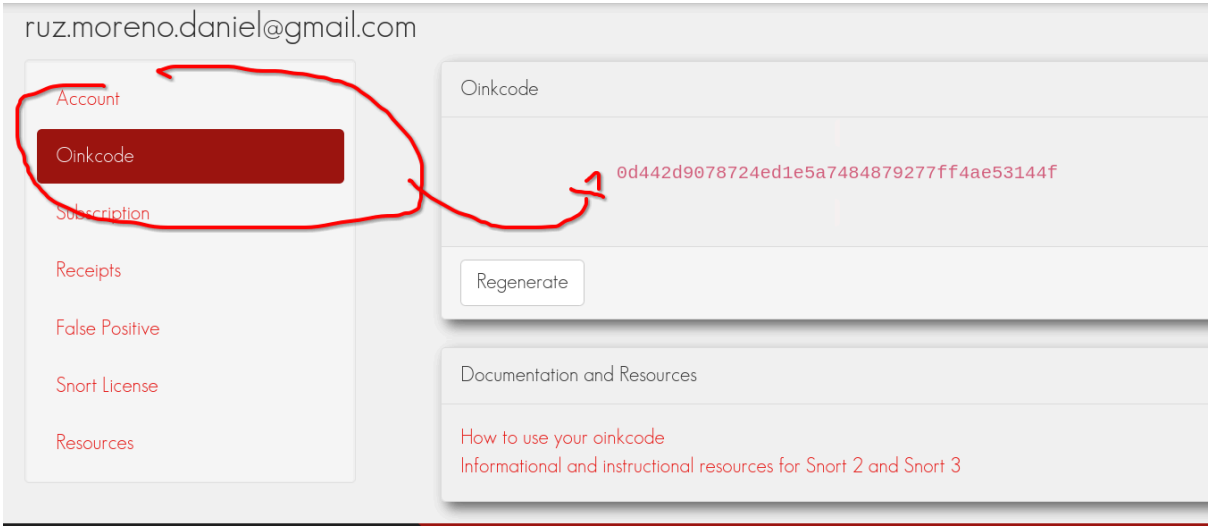
configuración de snort



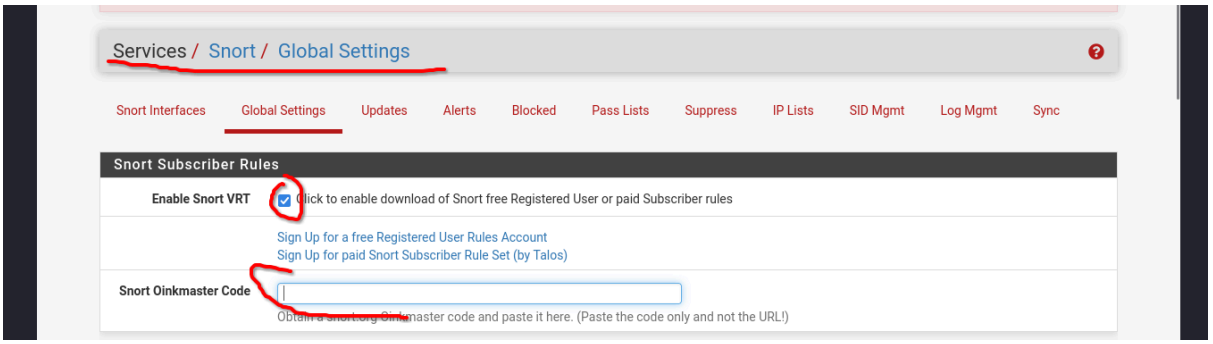
Para instalar Snort en pfSense, ve a **System** > **Package Manager**, luego dirígete a la pestaña **Available Packages**. Busca **Snort** en la lista de paquetes disponibles y haz clic en **Install**. Espera a que se complete la instalación para comenzar a configurarlo.



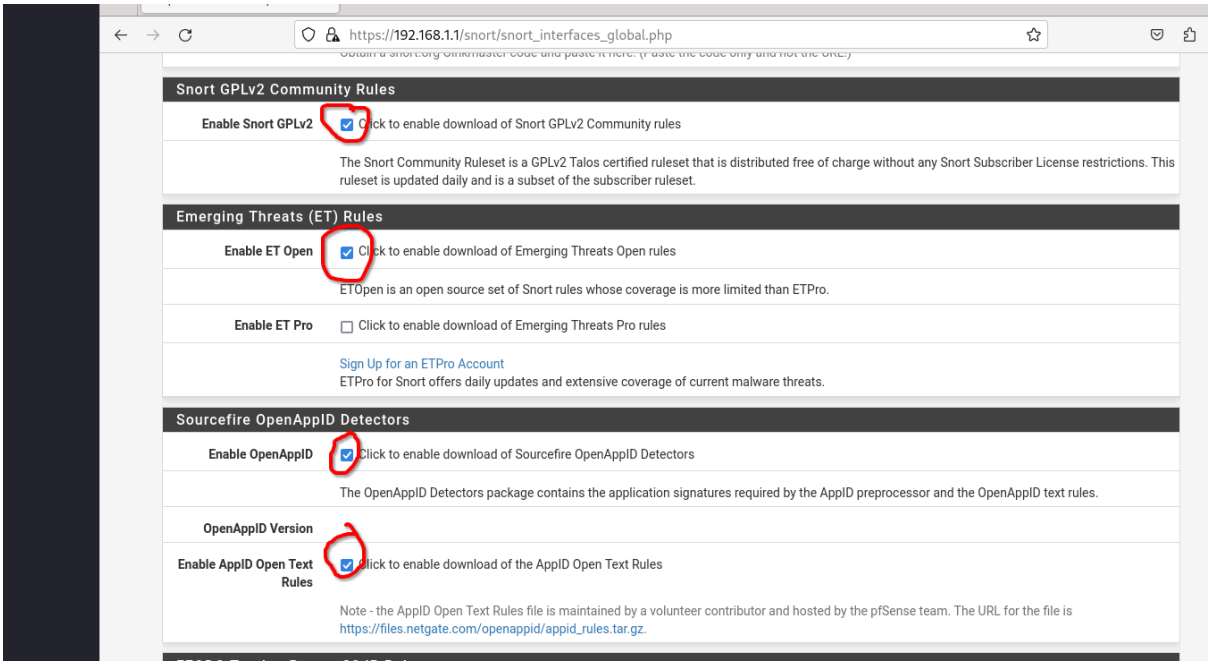


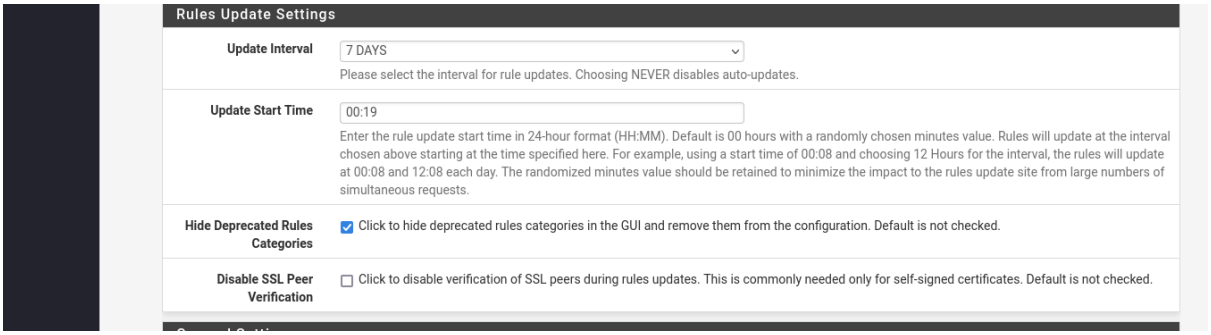


copiamos el código

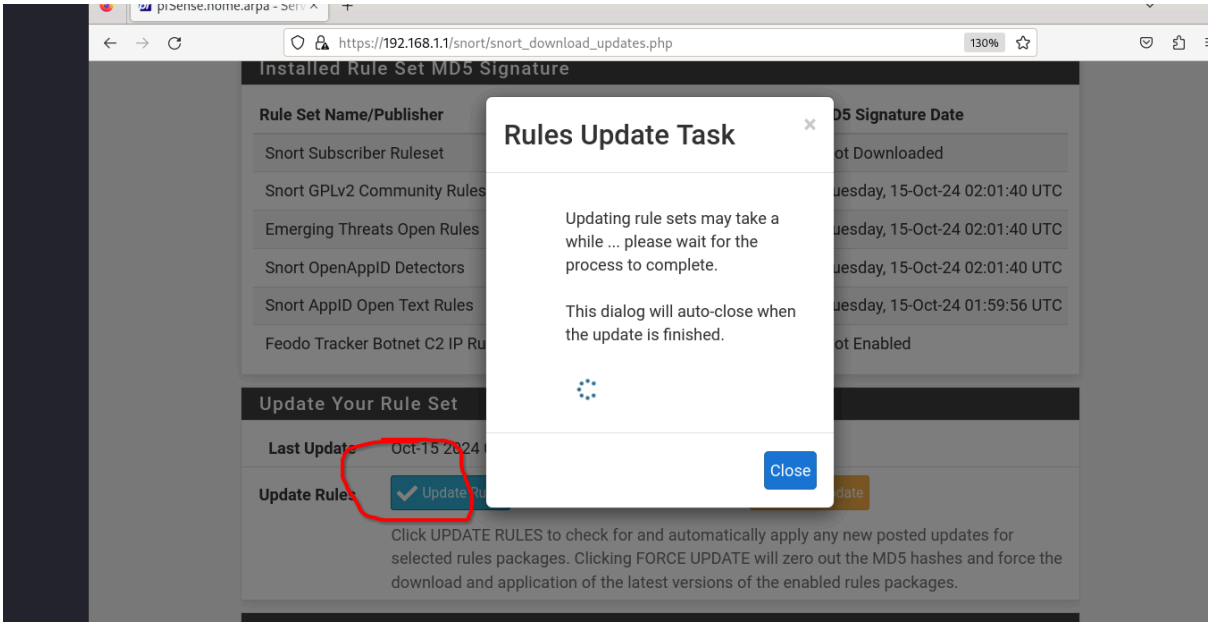


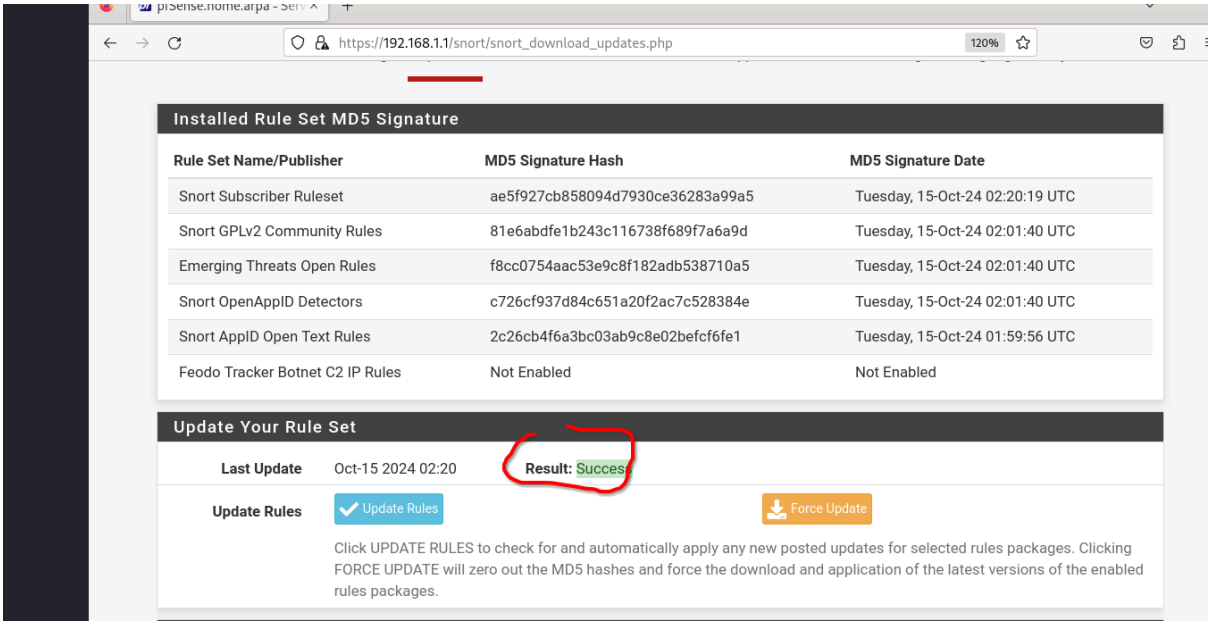
luego marcamos las casillas como están en la imagen



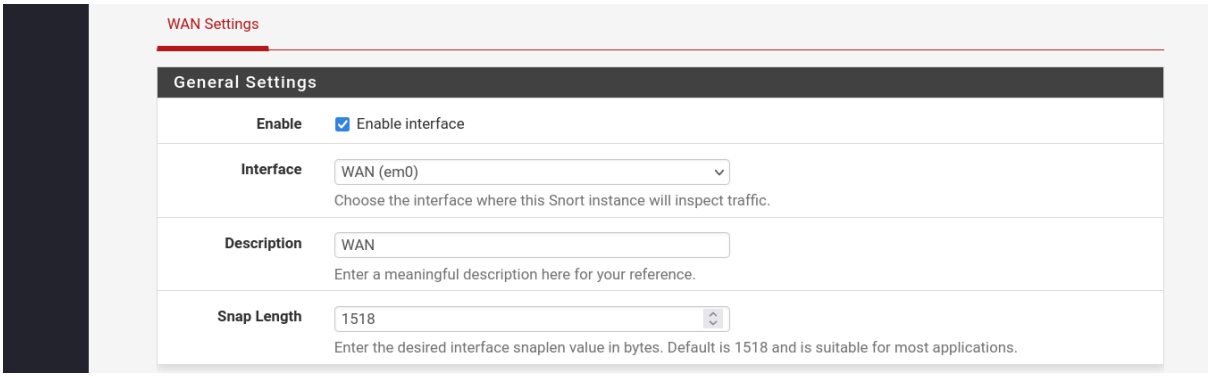


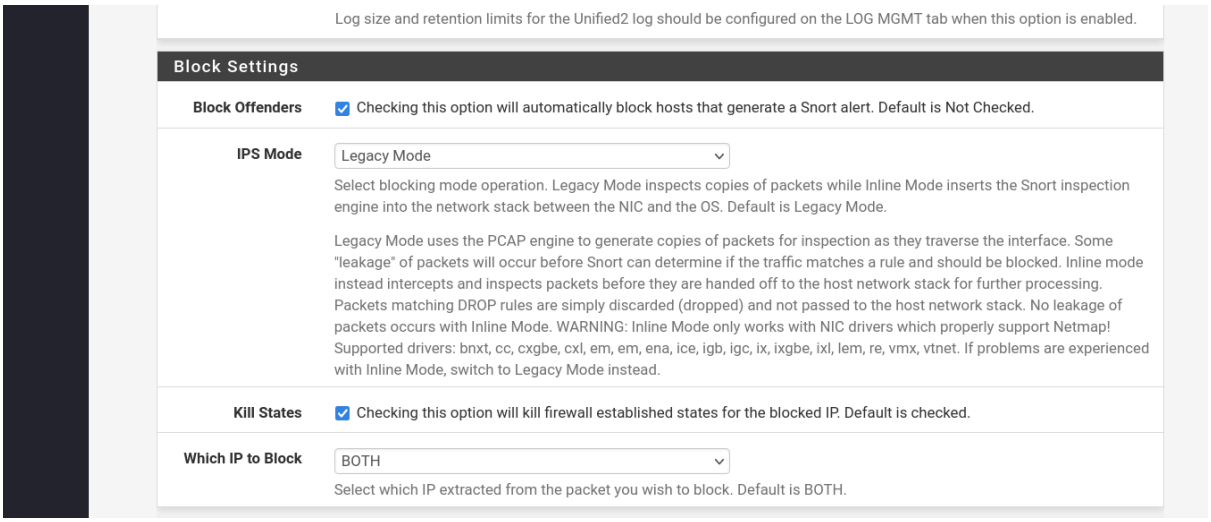
Guardamos los cambios y actualizamos la lista de reglas.



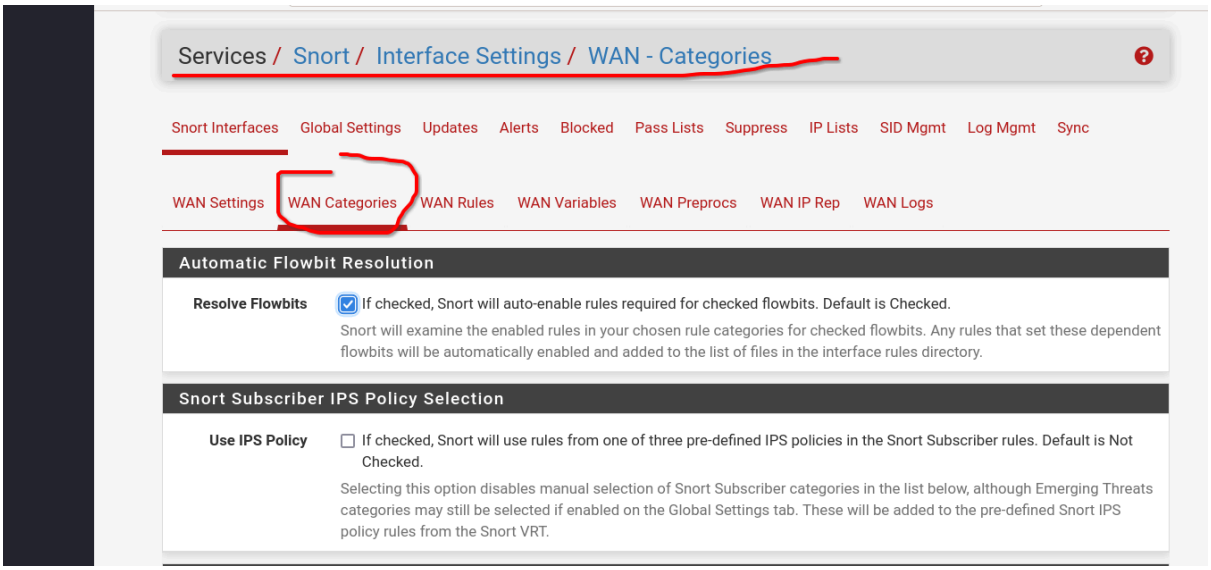


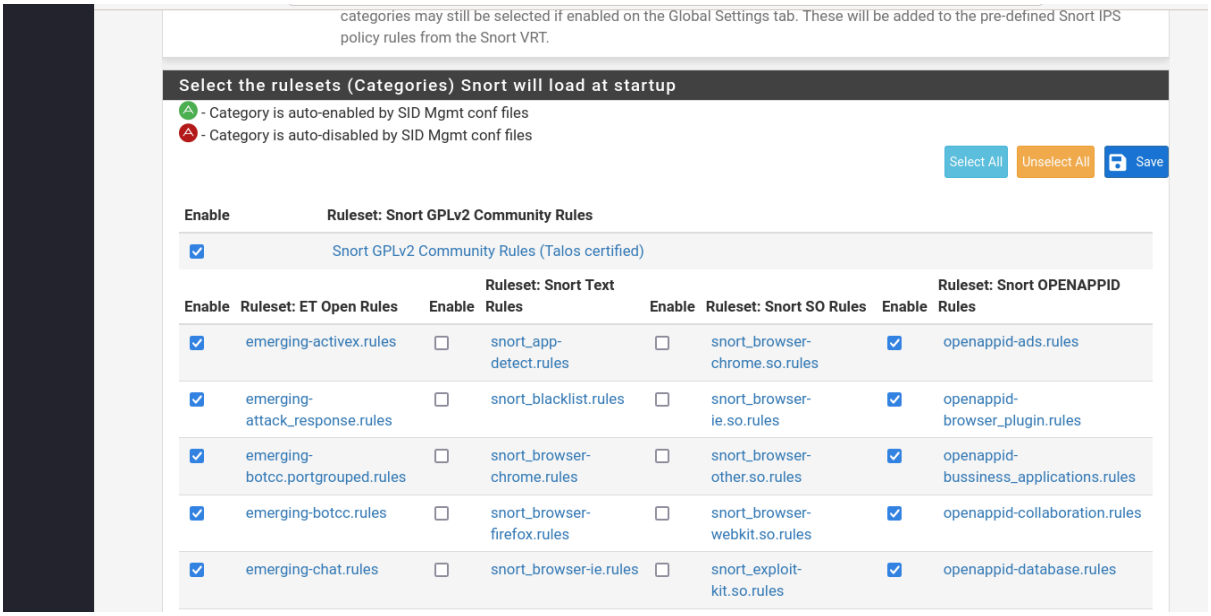
Para activar el modo **IPS** en Snort en **pfSense**, ve a **Services** > **Snort** y en la pestaña **Global Settings**, marca **Enable Block Offenders**. Luego, en la pestaña **Interfaces**, selecciona la interfaz deseada (como **WAN** o **LAN**) y habilita **Block Offenders** para esa interfaz específica.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



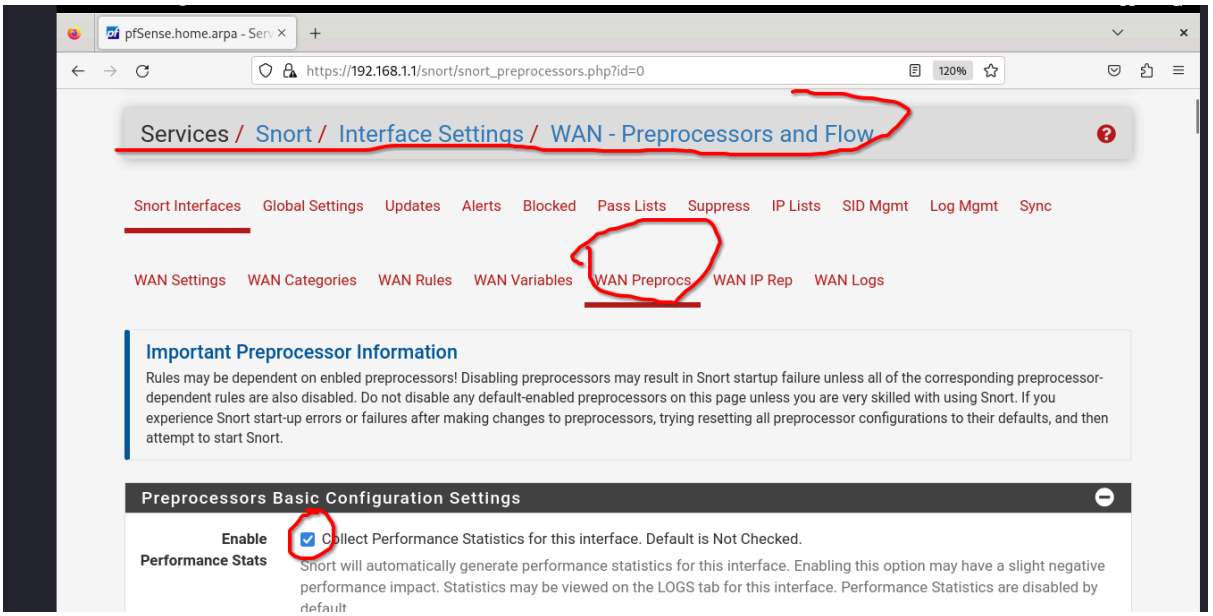


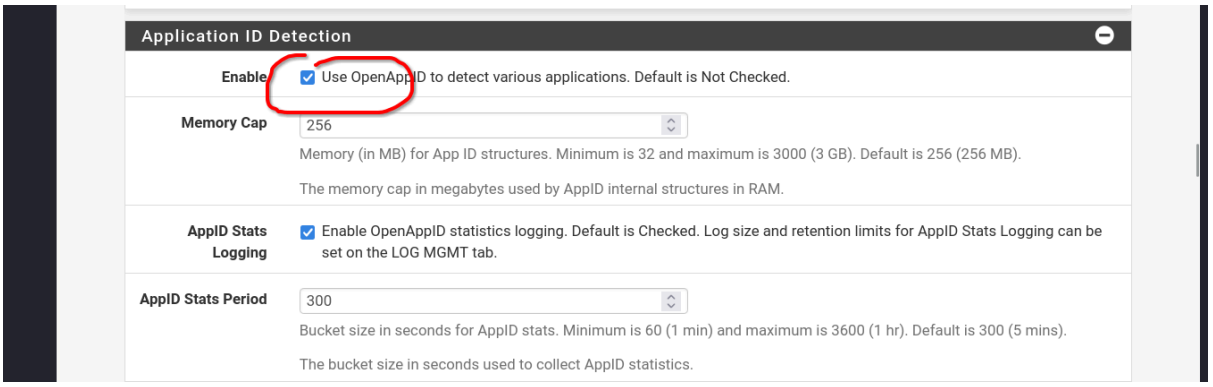
La opción WAN/LAN Category en Snort te permite especificar qué tipo de tráfico deseas que Snort inspeccione en la interfaz seleccionada, ya sea WAN (Wide Area Network) o LAN (Local Area Network). Al marcar las casillas correspondientes, puedes elegir analizar el tráfico entrante (Inbound), saliente (Outbound)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

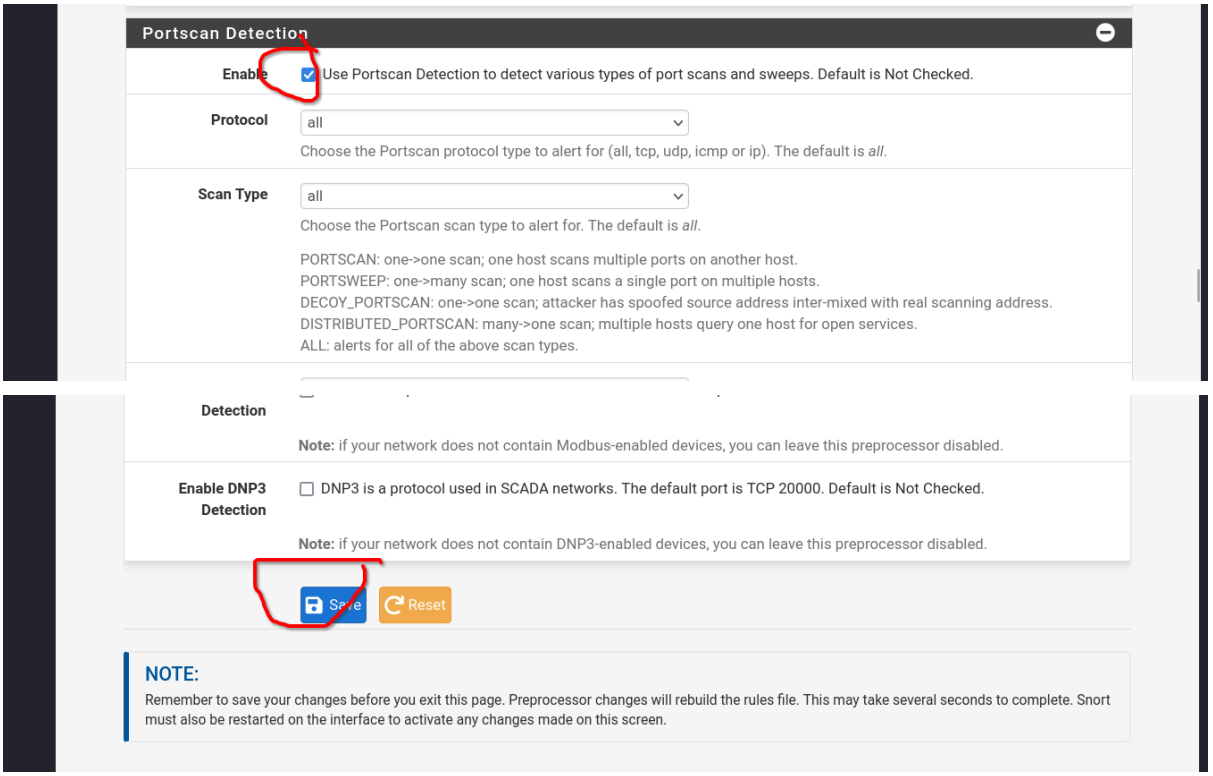




La opción **LAN/WAN Preprocessors** en Snort permite activar módulos que procesan el tráfico antes de que Snort lo analice en busca de amenazas. Estos módulos, como **Frag3** para reensamblar paquetes fragmentados o **Stream5** para rastrear conexiones, ayudan a mejorar la precisión de Snort y a detectar 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.







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.