**Relatório Suricata**

**GRUPO**

Caio Juliano – 0210971923035

Leonardo Khenaifes Zaccarelli Jubran – 0210971923014

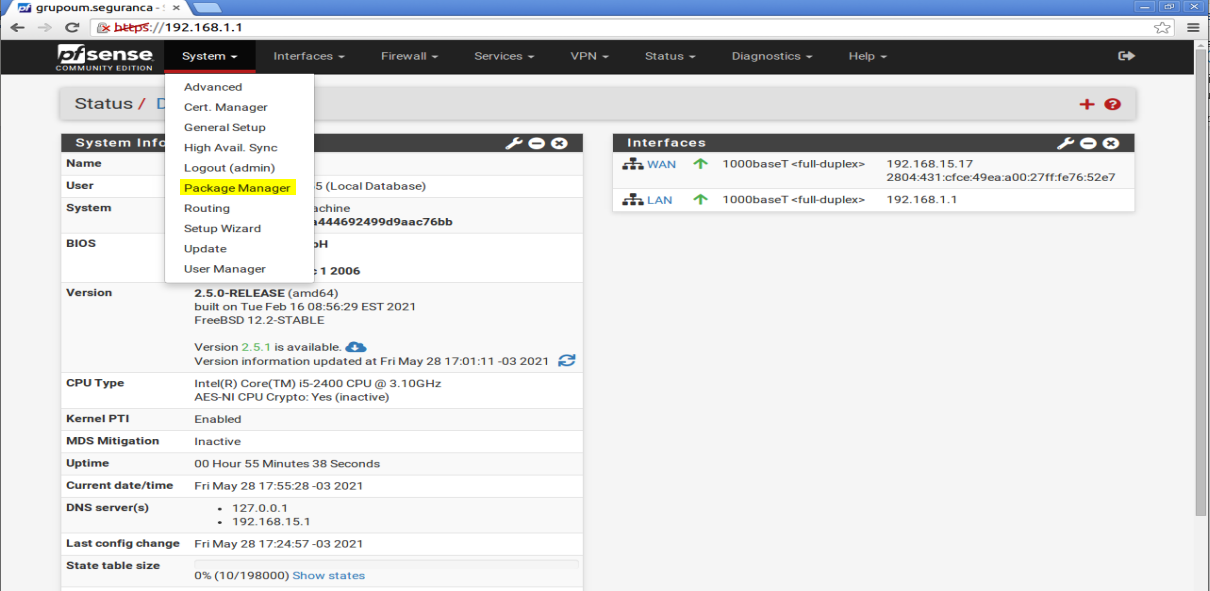
Webert Ferreira – 0210971923017

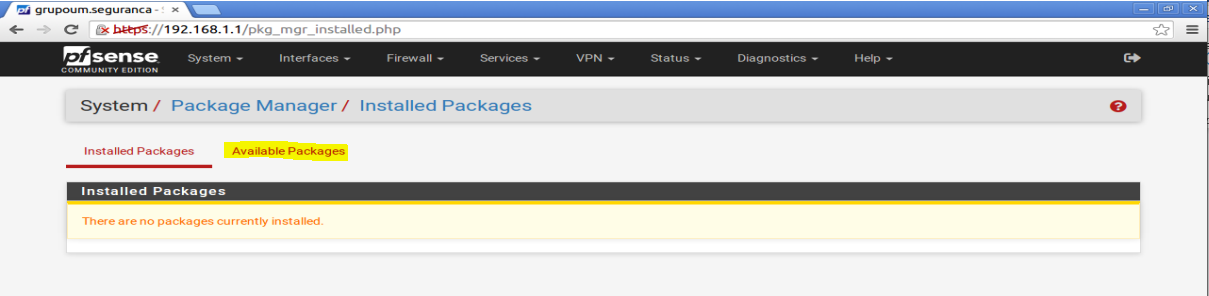
**Sobre o Suricata**

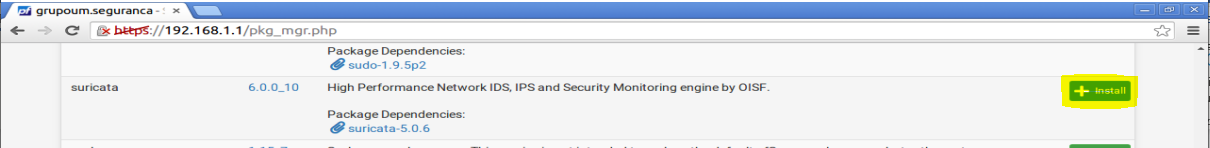
É um sistema de detecção e prevenção de intrusão, funciona inspecionando o tráfego de rede com regras e assinaturas.

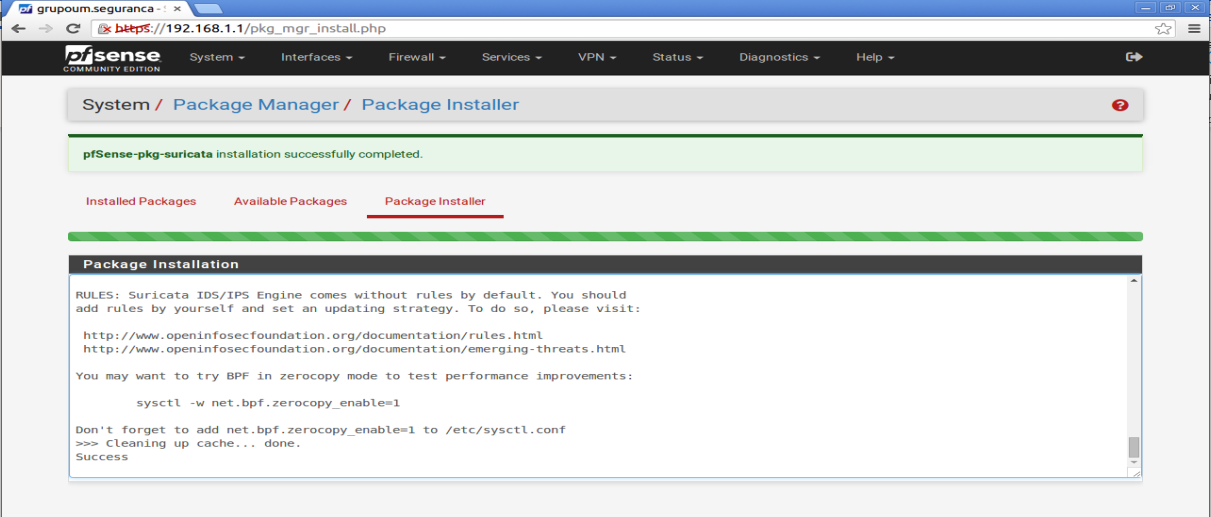
**Instalação Suricata**

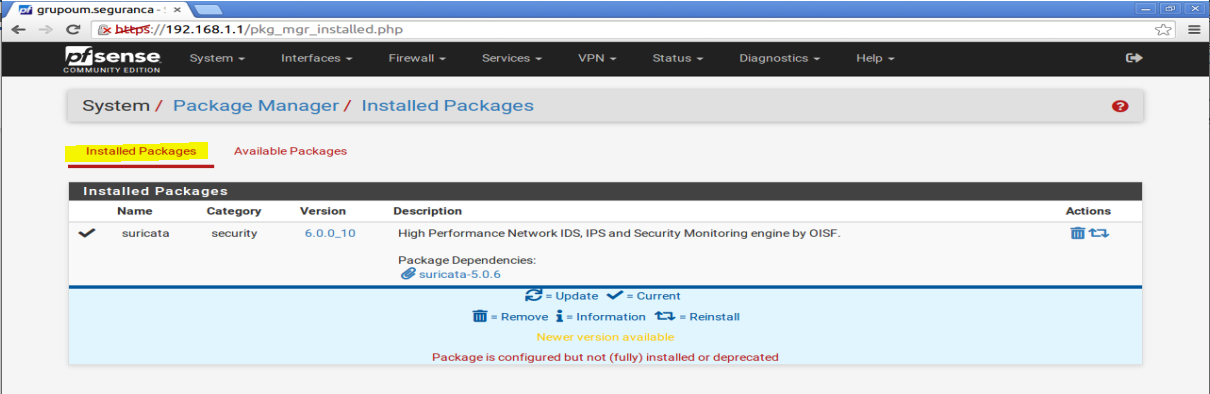
O Suricata pode ser configurado diretamente dentro do Pfsense, e para isso é feito a instalação do pacote correspondente ao serviço.

Com o Pfsense já iniciado vamos em *System / Package Manager.*

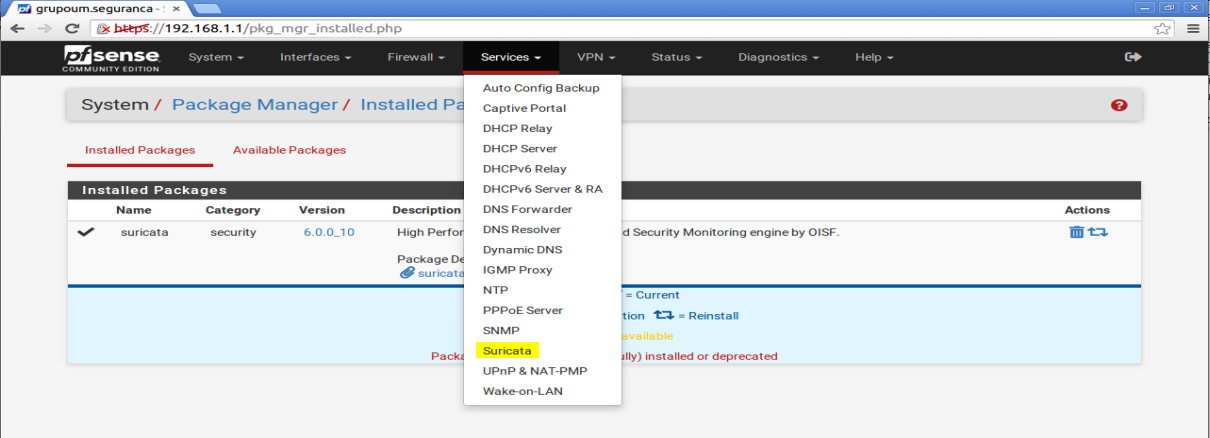
Selecionar a aba *Avaliable Packages.*

Procurar pelo pacote *Suricata* e ir em *Install.*

Confirmar e aguardar a instalação do pacote.

Após instalado, na aba *Installed Packages* mostra o pacote instalado.

**Configuração Suricata**

Para iniciar a configuração ir até *Services / Suricata*. 

Na aba *Global Settings* marcar os itens indicados.

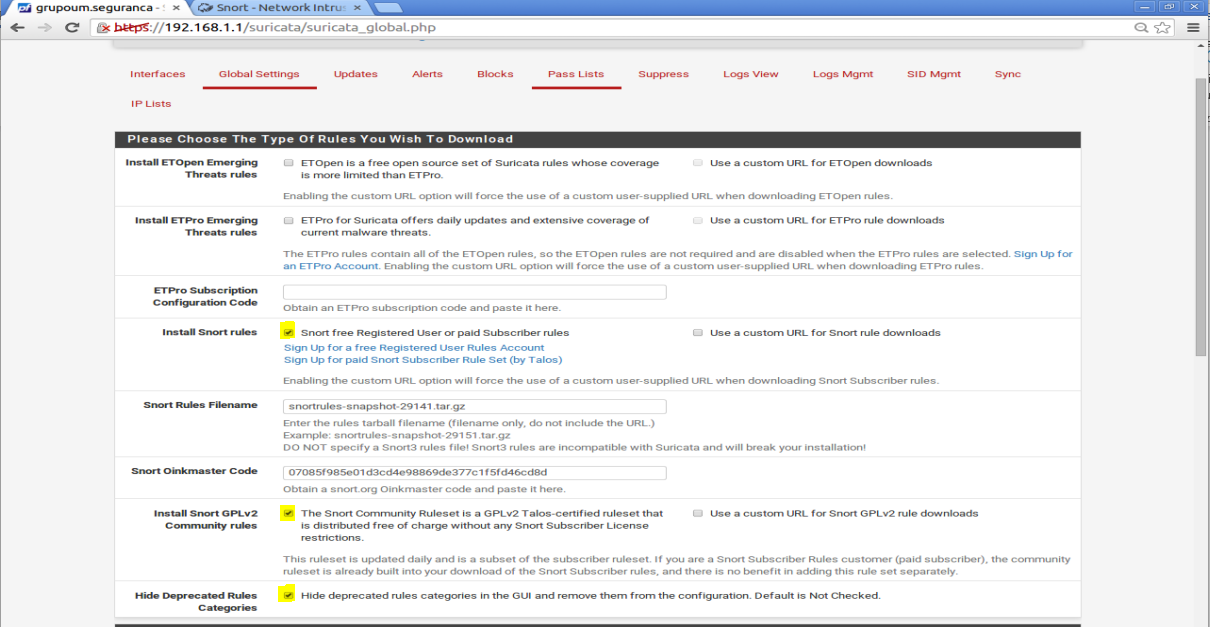
Nesse caso iremos fazer uma adição de assinaturas de regras utilizando o Snort.

O processo para incorporar essas regras são:

- Entrar no Site do Snort, fazer o cadastro e autenticar no site.

- Fazer o download das regras, versão 29141 e copiar apenas o nome do arquivo na opção filename.

- Copiar do seu perfil do site o código do OinkCode e colar na opção Oinkmaster code.

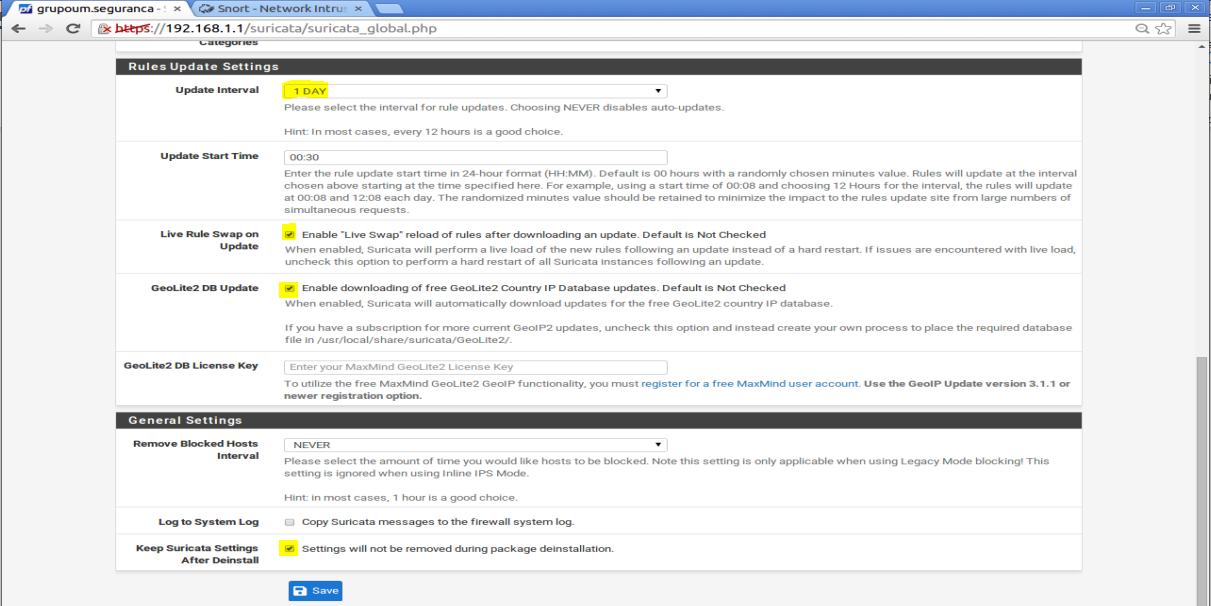


Ainda na aba *Global Settings* marcar os itens indicados e salvar.

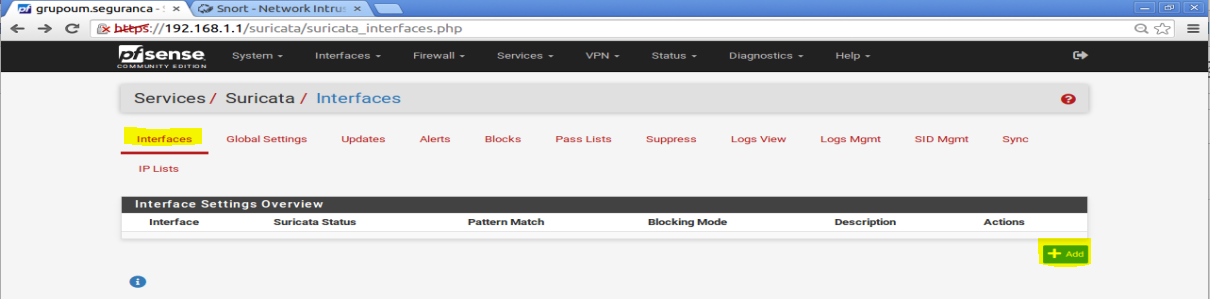
Update Interval: Intervalo de atualização

Live rule Swap on Update: Utilizado para não forçar o reinício do serviço.

GeoLite2 DB Update: Baixa a geolocalização dos Ip’s baseados nos países.

Keep Suricata Settings: Para ser mantida as configurações após atualizações de pacote.

**Configurando as Interfaces**

Na aba *Interfaces* vamos selecionar *add* para configurar a primeira interface que sera a WAN.

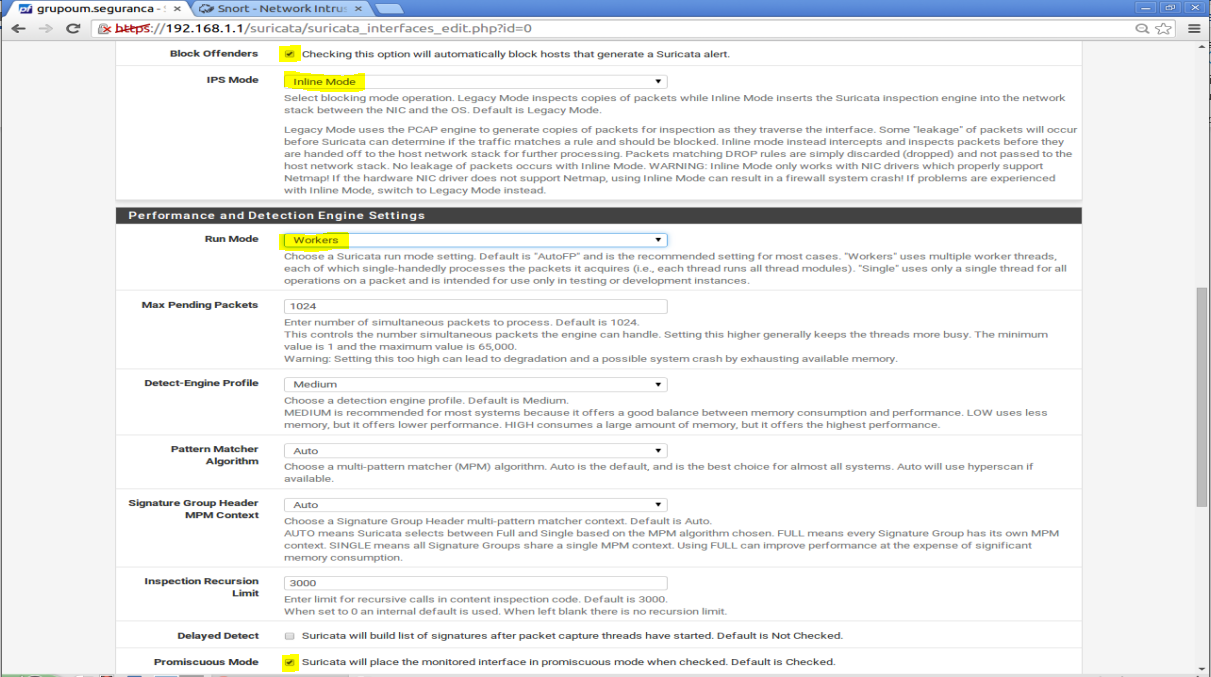
Selecionar os itens conforme indicado para a interface WAN.

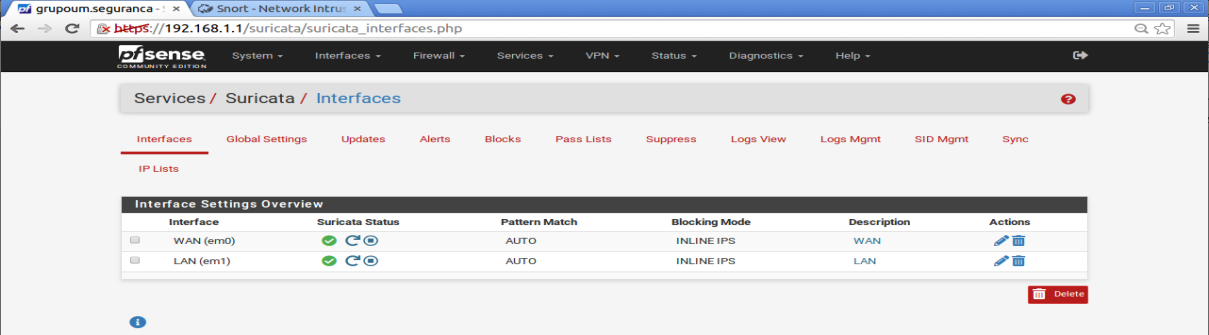
Block Offenders: Opção de bloqueio e alerta de hosts.

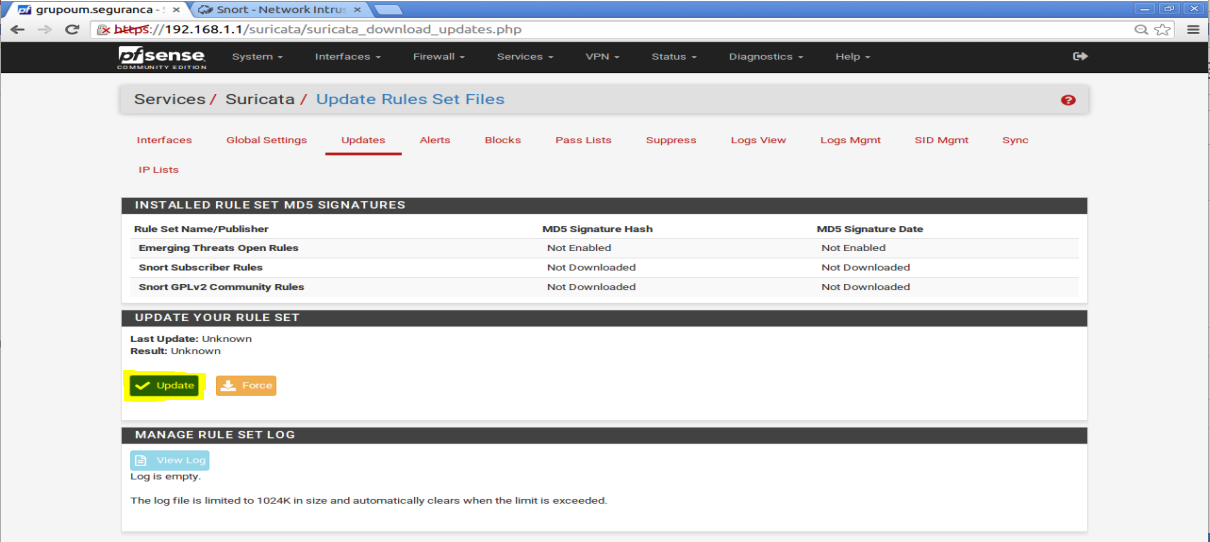
IPS Mode: Selecionando Inline mode para bloquear o tráfego de rede fazendo o alerta para depois fazer manualmente as prevenções.

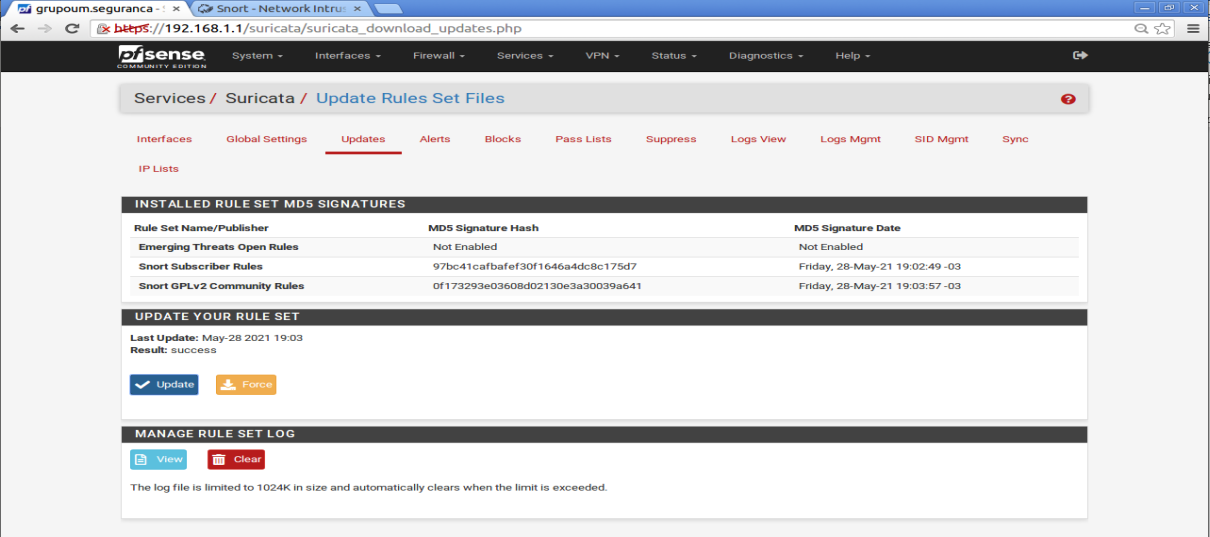
Run Mode: Selecionando Workers para utilização de múltiplas threads.

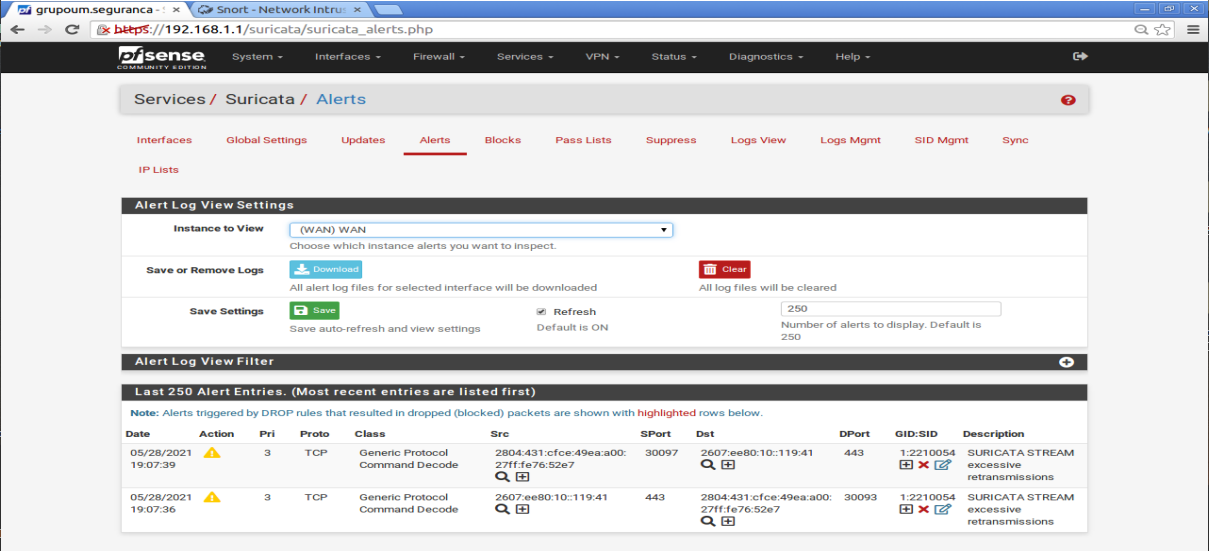
Promiscuous mode: monitorar a interface de modo promiscuo.

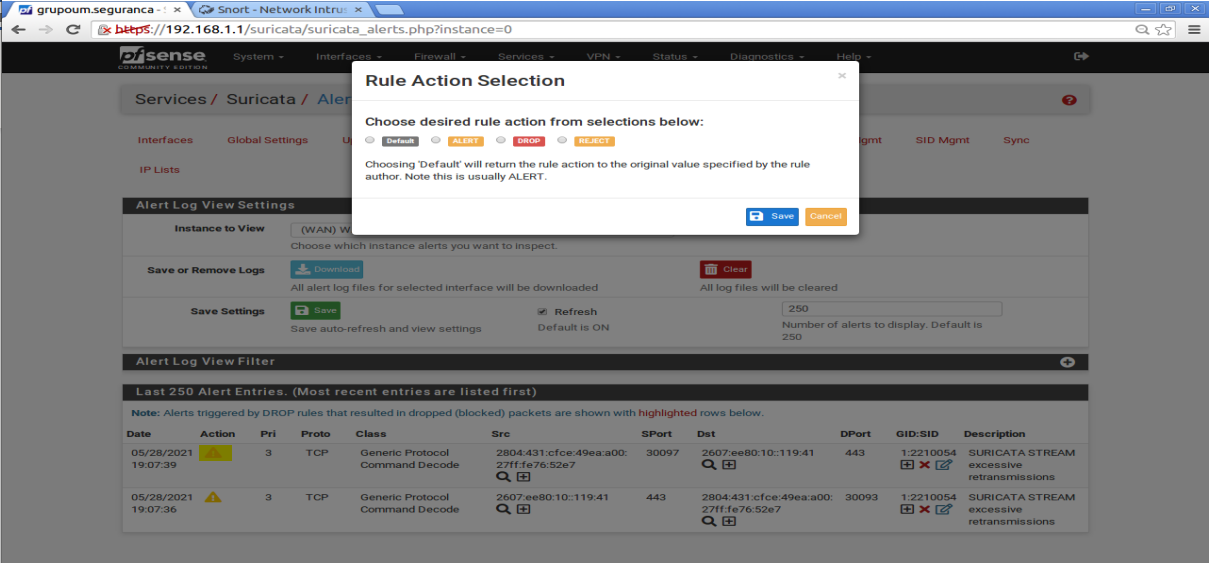


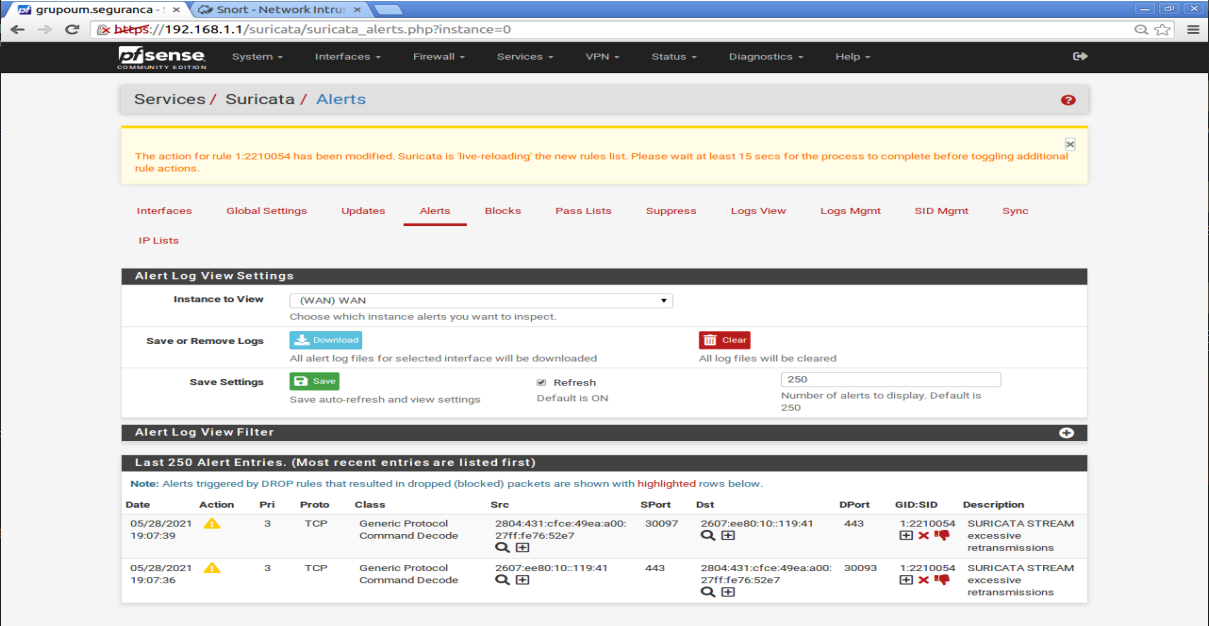
Duplicar as mesmas configurações da Interface WAN para a Interface LAN, ficando assim.

Na aba updates, selecionar update para fazer o processo de atualização das regras.

Na atualização ele fez o download das regras e já mostra os hash, indicando que as regras foram implementadas.

Na aba *Alerts* já podemos visualizar todos os alertas que o firewall vai detectar através do Suricata.

Clicando no Ícone de Alerta (!) podemos fazer a tratativa dos pacotes, podendo apenas bloquear o pacote ou rejeitar o host.

Tela onde mostra o pacote com tráfego negado.

**Considerações Finais**

O Suricata é uma poderosa ferramenta de detecção de intrusão, e uma ótima opção por ser open source, além de poder ser associada a outras ferramentas dando uma maior versatilidade a configuração das suas funções.