

# Relatório Suricata

## GRUPO

Caio Juliano – 0210971923035  
Leonardo Khenafes Zaccarelli Jubran – 0210971923014  
Webert Ferreira – 0210971923017

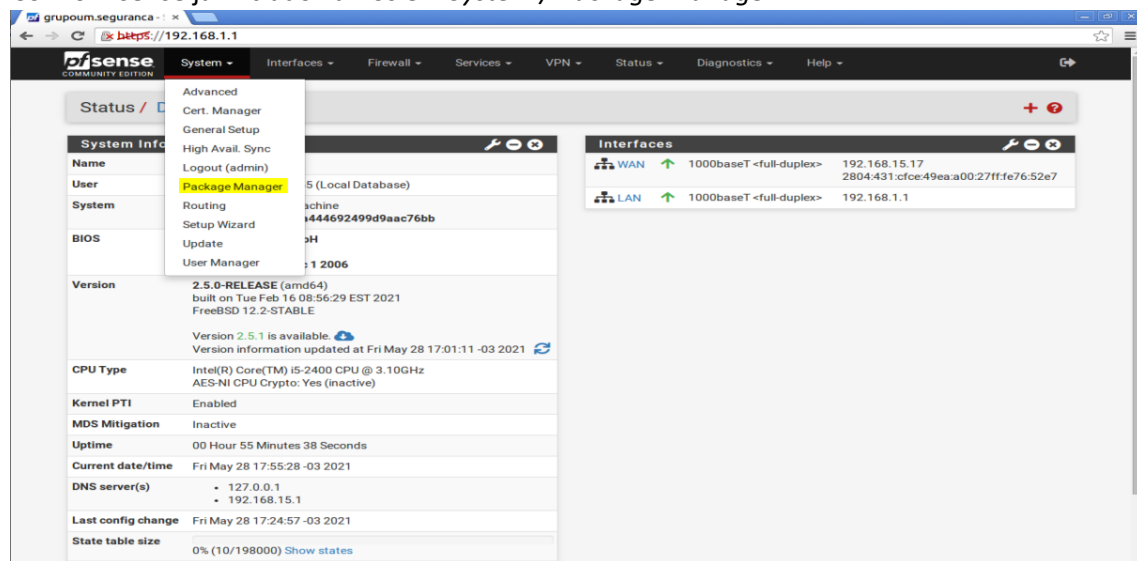
## Sobre o Suricata

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

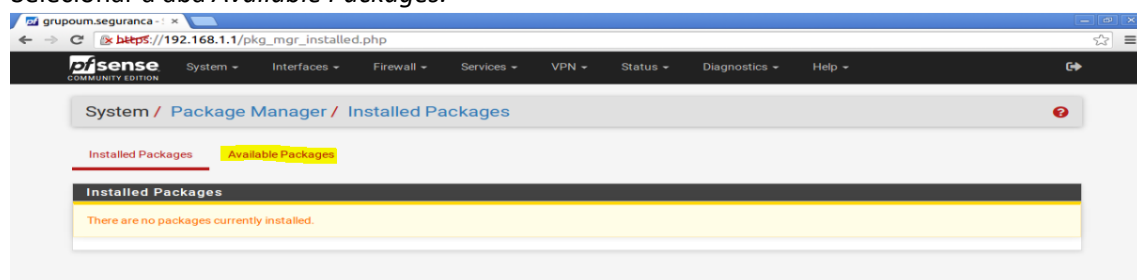
## Instalação Suricata

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

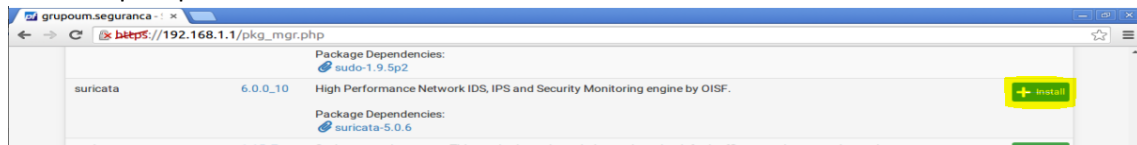
Com o Pfsense já iniciado vamos em *System / Package Manager*.



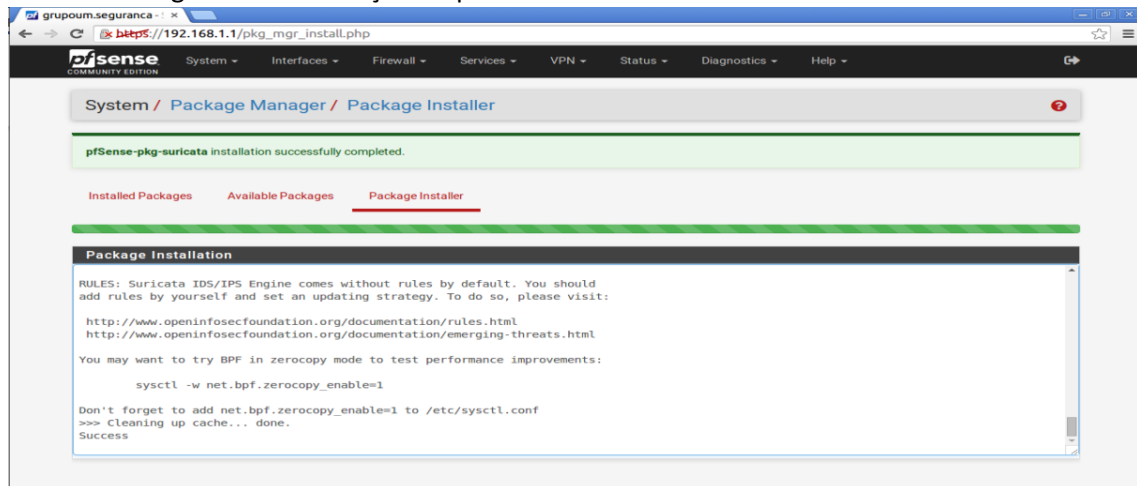
Selecionar a aba *Available Packages*.



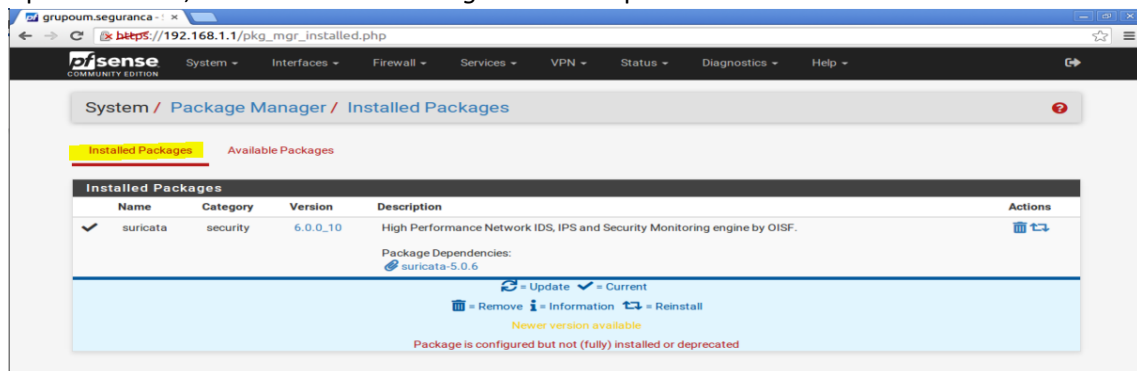
Procurar pelo pacote *Suricata* e ir em *Install*.



Confirmar e aguardar a instalação do pacote.

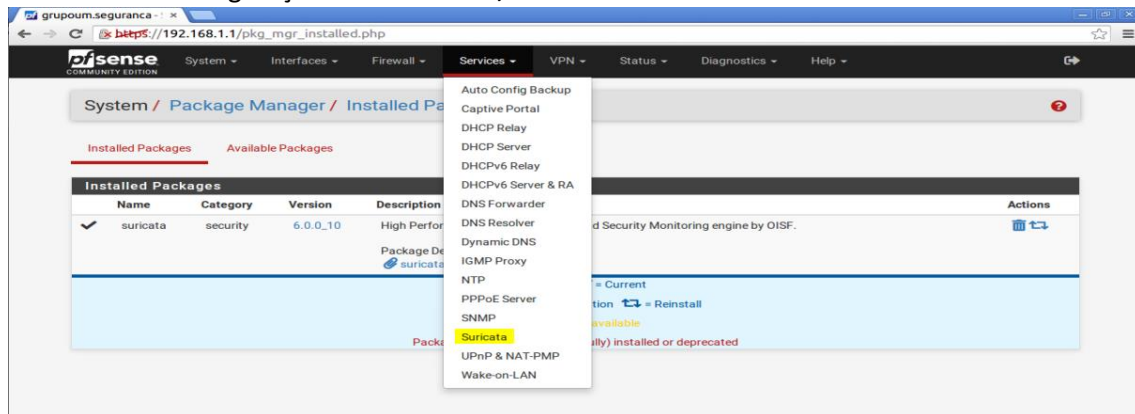


Após instalado, na aba *Installed Packages* mostra o pacote instalado.



## Configuração Suricata

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

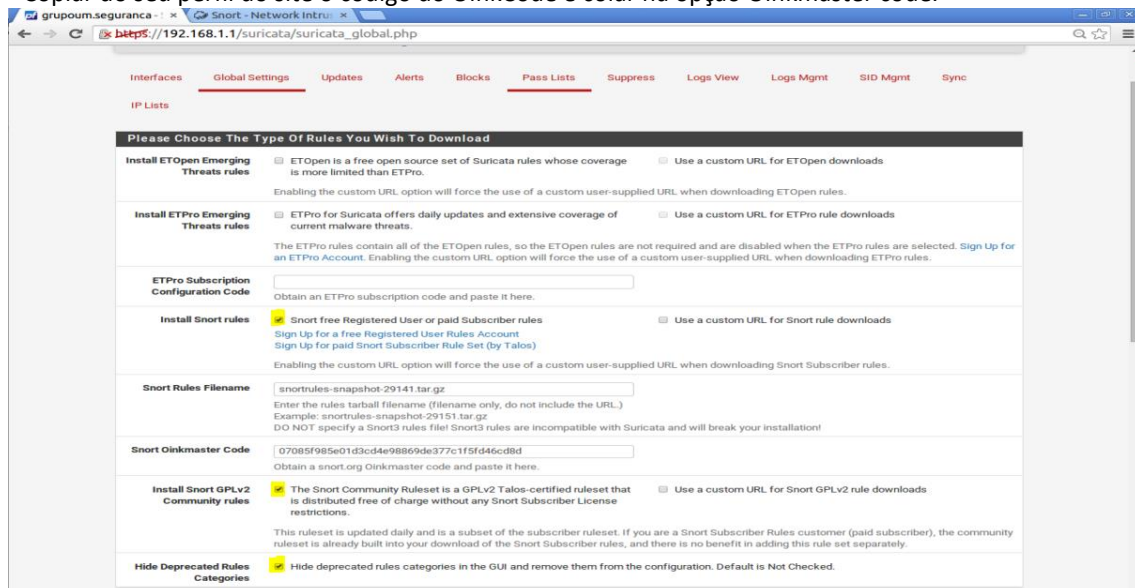


Na aba **Global Settings** marcar os itens indicados.

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 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.

The screenshot shows the 'Global Settings' page for Suricata. The 'Rules Update Settings' section is expanded, showing the following configuration:

- Update Interval:** 1 DAY (selected from a dropdown menu). A hint below states: 'Please select the interval for rule updates. Choosing NEVER disables auto-updates. Hint: In most cases, every 12 hours is a good choice.'
- Update Start Time:** 00:30. A hint below states: '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.'
- Live Rule Swap on Update:** ☒ Enable "Live Swap" reload of rules after downloading an update. Default is Not Checked. When enabled, Suricata will perform a live load of the new rules following an update instead of a hard restart. If issues are encountered with live load, uncheck this option to perform a hard restart of all Suricata instances following an update.
- GeoLite2 DB Update:** ☒ Enable downloading of free GeoLite2 Country IP Database updates. Default is Not Checked. When enabled, Suricata will automatically download updates for the free GeoLite2 country IP database. If you have a subscription for more current GeoIP2 updates, uncheck this option and instead create your own process to place the required database file in /usr/local/share/suricata/GeoLite2/.
- GeoLite2 DB License Key:** Enter your MaxMind GeoLite2 License Key. To utilize the free MaxMind GeoLite2 GeoIP functionality, you must register for a free MaxMind user account. Use the GeoIP Update version 3.1.1 or newer registration option.

The 'General Settings' section is also visible below:

- Remove Blocked Hosts Interval:** NEVER (selected from a dropdown menu). A hint below states: 'Please select the amount of time you would like hosts to be blocked. Note this setting is only applicable when using Legacy Mode blocking! This setting is ignored when using Inline IPS Mode. Hint: In most cases, 1 hour is a good choice.'
- Log to System Log:** ☐ Copy Suricata messages to the firewall system log.
- Keep Suricata Settings After Deinstall:** ☒ Settings will not be removed during package deinstallation.

A 'Save' button is located at the bottom of the settings form.

## Configurando as Interfaces

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

The screenshot shows the 'Interfaces' page in the Suricata web interface. The breadcrumb navigation shows 'Services / Suricata / Interfaces'. The 'Interfaces' tab is selected in the top navigation bar. Below the navigation bar, there is a section for 'Interface Settings Overview' with a table that has the following columns: Interface, Suricata Status, Pattern Match, Blocking Mode, Description, and Actions. A green '+ Add' button is located at the bottom right of the table.

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.

The screenshot shows the Suricata configuration page in the Snort Network Intrusion Detection System (NIDS) web interface. The page is titled "Suricata Interfaces Edit" and contains several sections for configuring the engine.

- Block Offenders:** A checkbox labeled "Checking this option will automatically block hosts that generate a Suricata alert." is checked.
- IPS Mode:** A dropdown menu is set to "Inline Mode". Below it, a text box explains that 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. A warning states: "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 DROPT 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! If the hardware NIC driver does not support Netmap, using Inline Mode can result in a firewall system crash! If problems are experienced with Inline Mode, switch to Legacy Mode instead."
- Performance and Detection Engine Settings:**
  - Run Mode:** A dropdown menu is set to "Workers". Below it, a text box explains that "Workers" uses multiple worker threads, each of which single-handedly processes the packets it acquires (i.e., each thread runs all thread modules). "Single" uses only a single thread for all operations on a packet and is intended for use only in testing or development instances.
  - Max Pending Packets:** A text box contains the value "1024". Below it, a text box explains: "Enter number of simultaneous packets to process. Default is 1024. This controls the number 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:** A dropdown menu is set to "Medium". Below it, a text box explains: "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."
  - Pattern Matcher Algorithm:** A dropdown menu is set to "Auto". Below it, a text box explains: "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."
  - Signature Group Header MPM Context:** A dropdown menu is set to "Auto". Below it, a text box explains: "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:** A text box contains the value "3000". Below it, a text box explains: "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:** A checkbox labeled "Suricata will build list of signatures after packet capture threads have started. Default is Not Checked." is unchecked.
  - Promiscuous Mode:** A checkbox labeled "Suricata will place the monitored interface in promiscuous mode when checked. Default is Checked." is checked.

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

The screenshot shows the Suricata configuration page in the Snort Network Intrusion Detection System (NIDS) web interface, specifically the "Interface Settings Overview" table. The table lists the configuration for the WAN and LAN interfaces.

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
WAN (em0)		AUTO	INLINE IPS	WAN	
LAN (em1)		AUTO	INLINE IPS	LAN	

At the bottom right of the table, there is a "Delete" button.

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

The screenshot shows the Suricata web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled 'Services / Suricata / Update Rules Set Files'. Below this, there are tabs for Interfaces, Global Settings, Updates (selected), Alerts, Blocks, Pass Lists, Suppress, Logs View, Logs Mgmt, SID Mgmt, and Sync. The 'Updates' tab is active, showing a table of installed rule sets and a section to update the rule set.

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	Not Enabled	Not Enabled
Snort Subscriber Rules	Not Downloaded	Not Downloaded
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded

**UPDATE YOUR RULE SET**

Last Update: Unknown  
Result: Unknown

[Update](#) [Force](#)

**MANAGE RULE SET LOG**

[View Log](#)  
Log is empty.

The log file is limited to 1024K in size and automatically clears when the limit is exceeded.

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

The screenshot shows the Suricata web interface after a successful update. The 'Updates' tab is still active, and the table of installed rule sets now shows MD5 hashes and dates for the rule sets. The 'UPDATE YOUR RULE SET' section shows the last update was successful on May 28, 2021, at 19:03.

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	Not Enabled	Not Enabled
Snort Subscriber Rules	97bc41cafbafe30f1646a4dc8c175d7	Friday, 28-May-21 19:02:49 -03
Snort GPLv2 Community Rules	0f173293e03608d02130e3a30039a641	Friday, 28-May-21 19:03:57 -03

**UPDATE YOUR RULE SET**

Last Update: May-28 2021 19:03  
Result: success

[Update](#) [Force](#)

**MANAGE RULE SET LOG**

[View](#) [Clear](#)

The log file is limited to 1024K in size and automatically clears when the limit is exceeded.

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

The screenshot shows the Suricata Alerts page in the pfSense web interface. The page has a navigation bar with tabs for Interfaces, Global Settings, Updates, Alerts (selected), Blocks, Pass Lists, Suppress, Logs View, Logs Mgmt, SID Mgmt, and Sync. Below the navigation bar, there's a section for Alert Log View Settings, including a dropdown for Instance to View (WAN), a Download button, a Clear button, a Save button, and a Refresh checkbox. The main section is titled 'Alert Log View Filter' and displays a table of the last 250 alert entries. The table has columns for Date, Action, Pri, Proto, Class, Src, SPort, Dst, DPort, GID:SID, and Description. Two entries are visible, both showing 'Generic Protocol Command Decode' and 'SURICATA STREAM excessive retransmissions'.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
05/28/2021 19:07:39	Alert	3	TCP	Generic Protocol Command Decode	2804:431:cfe:49ea:a00:27ff:fe76:52e7	30097	2607:ee80:10:119:41	443	1:2210054	SURICATA STREAM excessive retransmissions
05/28/2021 19:07:36	Alert	3	TCP	Generic Protocol Command Decode	2607:ee80:10:119:41	443	2804:431:cfe:49ea:a00:27ff:fe76:52e7	30093	1:2210054	SURICATA STREAM excessive retransmissions

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

The screenshot shows the Suricata Alerts page with a 'Rule Action Selection' dialog box open. The dialog box prompts the user to choose a desired rule action from selections below: Deny, Alert, Reject, and Ignore. It also includes a note: 'Choosing 'Default' will return the rule action to the original value specified by the rule author. Note this is usually ALERT.' The background shows the same alert log table as the previous screenshot, but the first entry's Action column now shows a yellow alert icon.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
05/28/2021 19:07:39	Alert	3	TCP	Generic Protocol Command Decode	2804:431:cfe:49ea:a00:27ff:fe76:52e7	30097	2607:ee80:10:119:41	443	1:2210054	SURICATA STREAM excessive retransmissions
05/28/2021 19:07:36	Alert	3	TCP	Generic Protocol Command Decode	2607:ee80:10:119:41	443	2804:431:cfe:49ea:a00:27ff:fe76:52e7	30093	1:2210054	SURICATA STREAM excessive retransmissions

Tela onde mostra o pacote com tráfego negado.

The screenshot shows the Suricata Alerts page in a web browser. The browser address bar shows the URL: [https://192.168.1.1/suricata/suricata\\_alerts.php?instance=0](https://192.168.1.1/suricata/suricata_alerts.php?instance=0). The page has a navigation menu with options: Interfaces, Global Settings, Updates, Alerts (selected), Blocks, Pass Lists, Suppress, Logs View, Logs Mgmt, SID Mgmt, and Sync. Below the navigation menu, there is a section for 'Alert Log View Settings' with a dropdown for 'Instance to View' (set to '(WAN) WAN') and a 'Save or Remove Logs' button. Below this, there is a 'Save Settings' button and a 'Refresh' button. The 'Alert Log View Filter' section is also visible. The main content area displays a table of 'Last 250 Alert Entries'. The table has columns: Date, Action, Pri, Proto, Class, Src, SPort, Dst, DPort, GID:SID, and Description. Two entries are shown, both with a yellow warning icon in the Action column. The first entry is dated 05/28/2021 19:07:39 and the second is dated 05/28/2021 19:07:36. Both entries describe 'SURICATA STREAM excessive retransmissions'.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
05/28/2021 19:07:39	⚠	3	TCP	Generic Protocol Command Decode	2804:431:cfe:49ea:a00:27ff:fe76:52e7	30097	2607:ee80:10::119:41	443	1:2210054	SURICATA STREAM excessive retransmissions
05/28/2021 19:07:36	⚠	3	TCP	Generic Protocol Command Decode	2607:ee80:10::119:41	443	2804:431:cfe:49ea:a00:27ff:fe76:52e7	30093	1:2210054	SURICATA STREAM excessive retransmissions

## 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.