**Anexo Observaciones**

**Sprint 3**

A continuación detallare algunas observaciones detectadas al realizar las pruebas de aceptación del producto en este Sprint 3.

**Precondiciones:**

1. Máquina virtual **“Mail\_Unab”**:

Debe estar encendida, esto ya que brinda los servicios de MX (correo) y DNS.

1. Máquina virtual **“pfSense\_Unab”**:

Debe estar encendida, esto ya que esta máquina es la que rutea, sensa, detecta e informa todo lo que circula por las redes de este laboratorio.

1. Máquina virtual **“LAMP\_Unab”**:

Debe estar encendida, esto ya que esta máquina tiene instalado Apache, MySql, Php y Mutillidae (Herramienta para generar ataque a servicios web), además como mutillidae brinda un servicio web, es la victima elegida para efectuar las pruebas de Stress.

1. Máquina virtual **“Graylog\_Unab”**:

Debe estar encendida, ya que este es el correlacionador de eventos y es aquí donde se reportaran los diferentes logs de pfSense\_Unab y es donde se generara la visualización por parte del encargado de Seguridad TI o quien cumpla esta función.

Pasos para realizar prueba:

1. Ingresamos a la plataforma Graylog, de acuerdo a siguiente detalle:

URL : <http://172.16.100.3:9000/>

User : admin

Pass : Temeracbeta2020

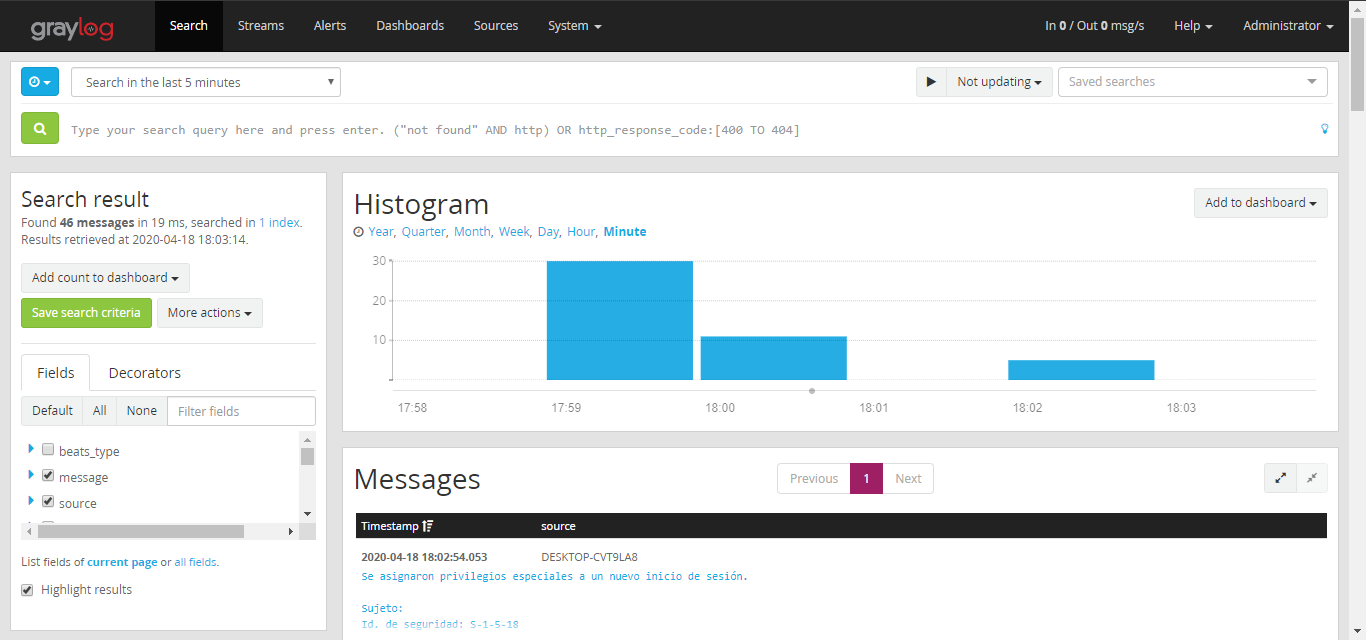


Figura N° 1 “Search”

Una visualización como la figura N° 1 se desplegara en su navegador.

1. A continuación nos dirigimos al símbolo de “Play”, donde debe tener la opción “Not updating” y le damos click y seleccionamos la opción que necesitemos, esto le da la instrucción al sistema de que actualice sus datos y log en el tiempo configurado.

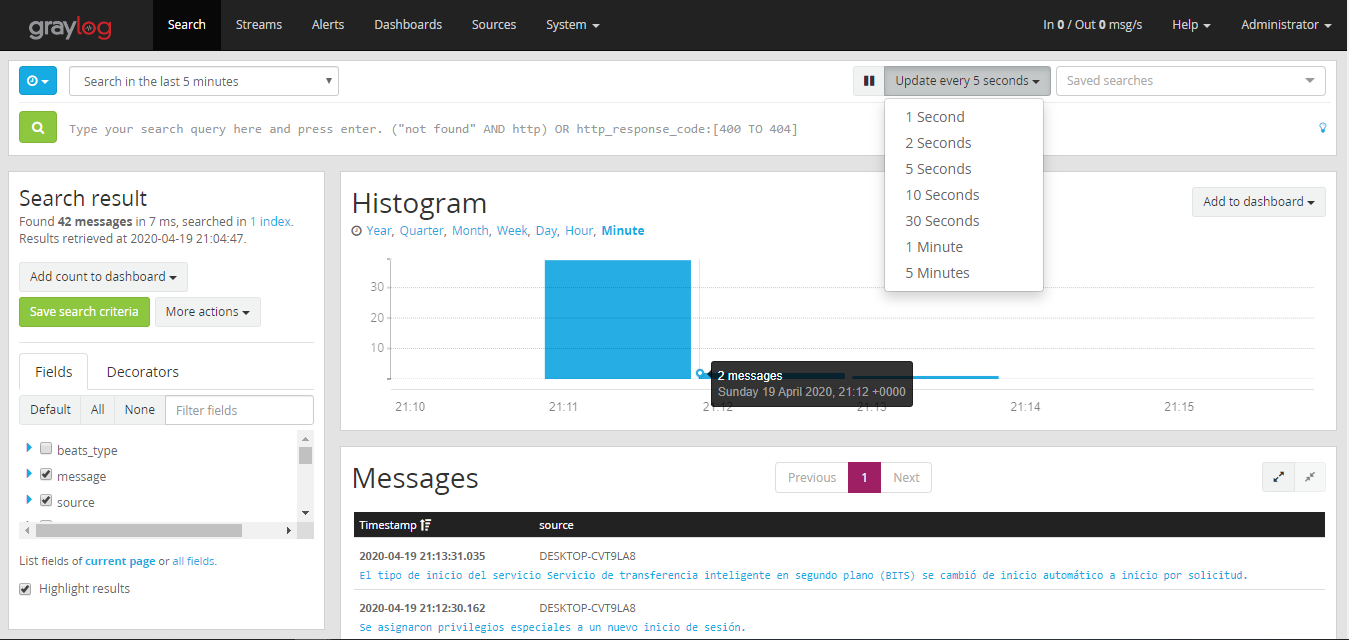


Figura N° 2

1. Posterior a esto verificamos que pfSense\_Unab este funcionando de manera correcta.

Ingresamos a la plataforma pfSense\_Unab, de acuerdo a siguiente detalle:

URL : http://172.16.100.1

User : admin

Pass : Unab.2020

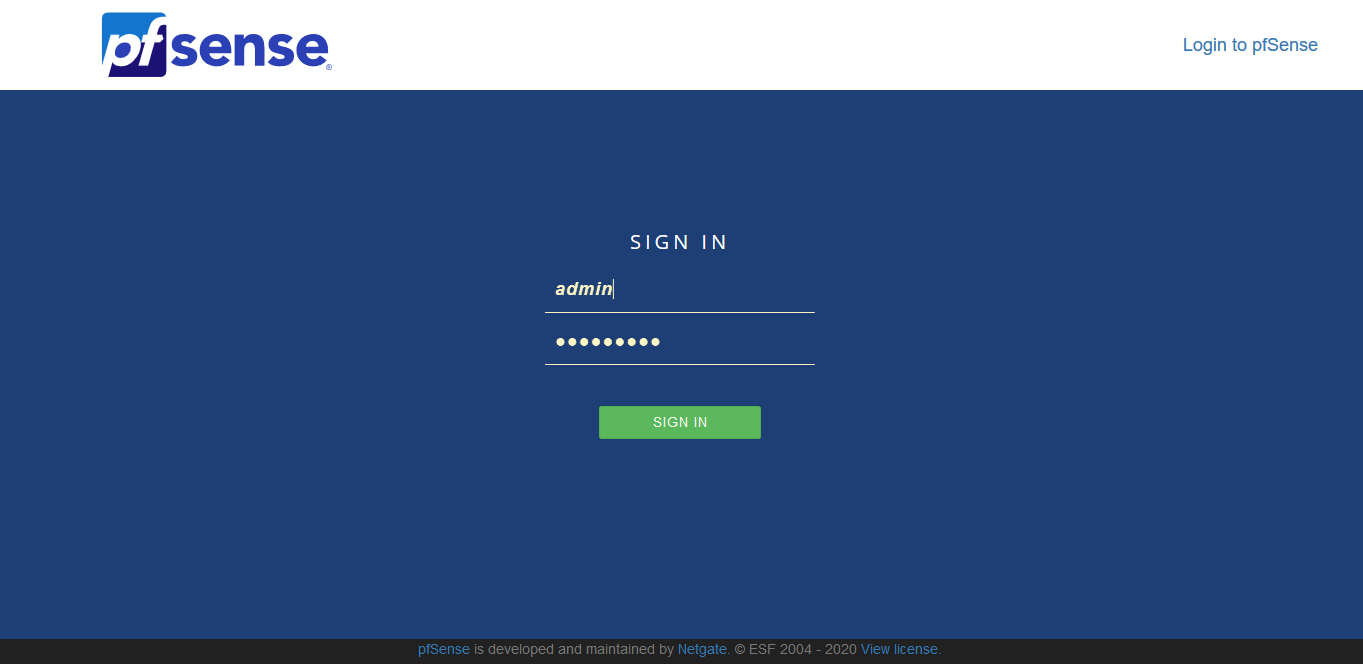


Figura N° 3 “Login pfSense”

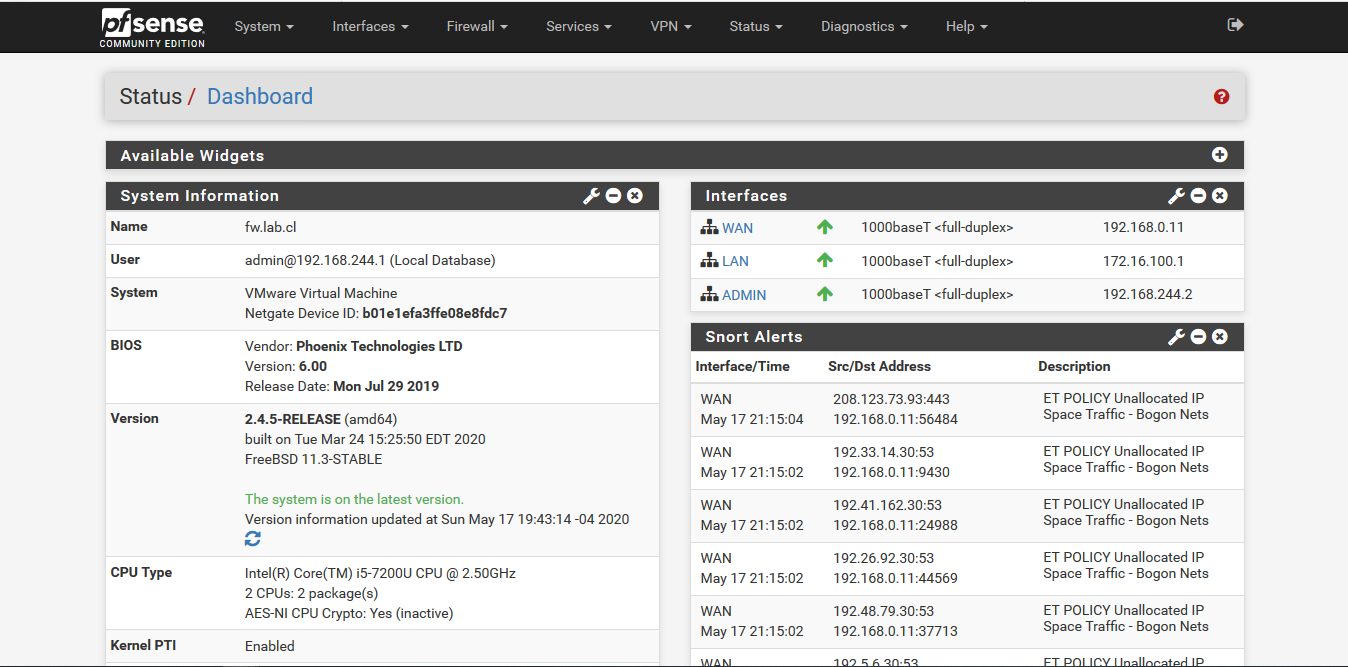


Figura N° 4 “Dashboard pfSense”

A través de la figura N° 4, podemos darnos cuenta que pfSense esta funcionando de manera normal, ya que visualizamos sus interfaces arriba y a través de “System Information” no se visualizan errores.

1. Verificamos “Mail\_Unab”, objeto detectar errores.

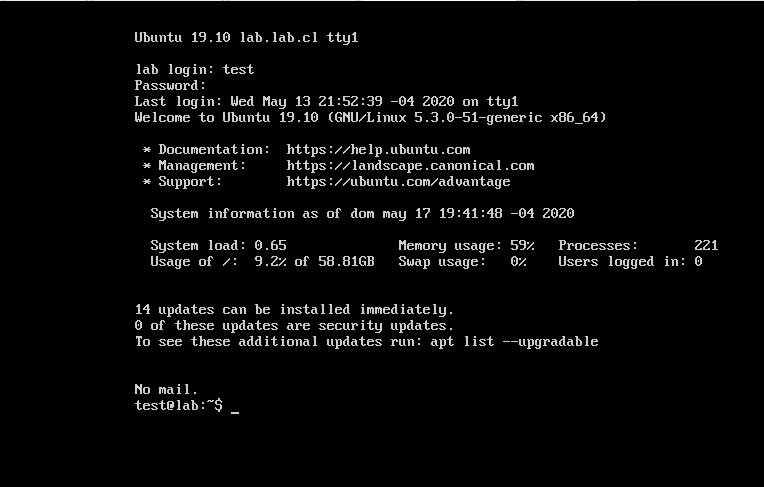


Figura N° 5 “Servicio de correo”

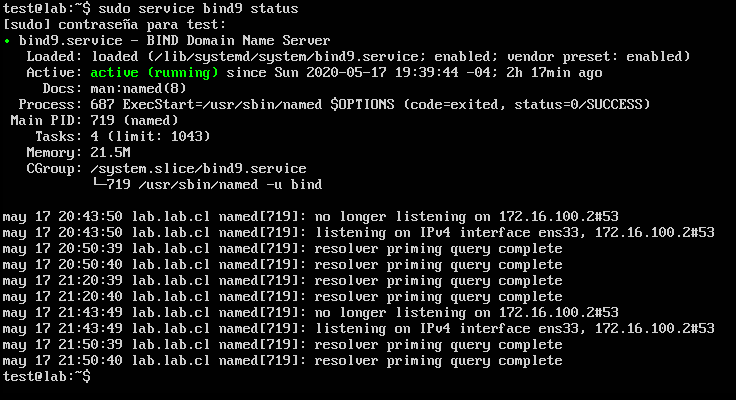


Figura N° 6 “Servicio DNS”

1. A través de la Figura N° 5, nos damos cuenta de que el servicio de correo esta operando de manera correcta.
2. A través de la Figura N° 6, nos damos cuenta de que el servicio de DNS se encuentra activo y operando sin errores.
3. Posterior a esto verificamos “LAMP\_Unab”.

Ingresamos a la plataforma LAMP\_Unab, a través de la url <http://172.16.100.4>

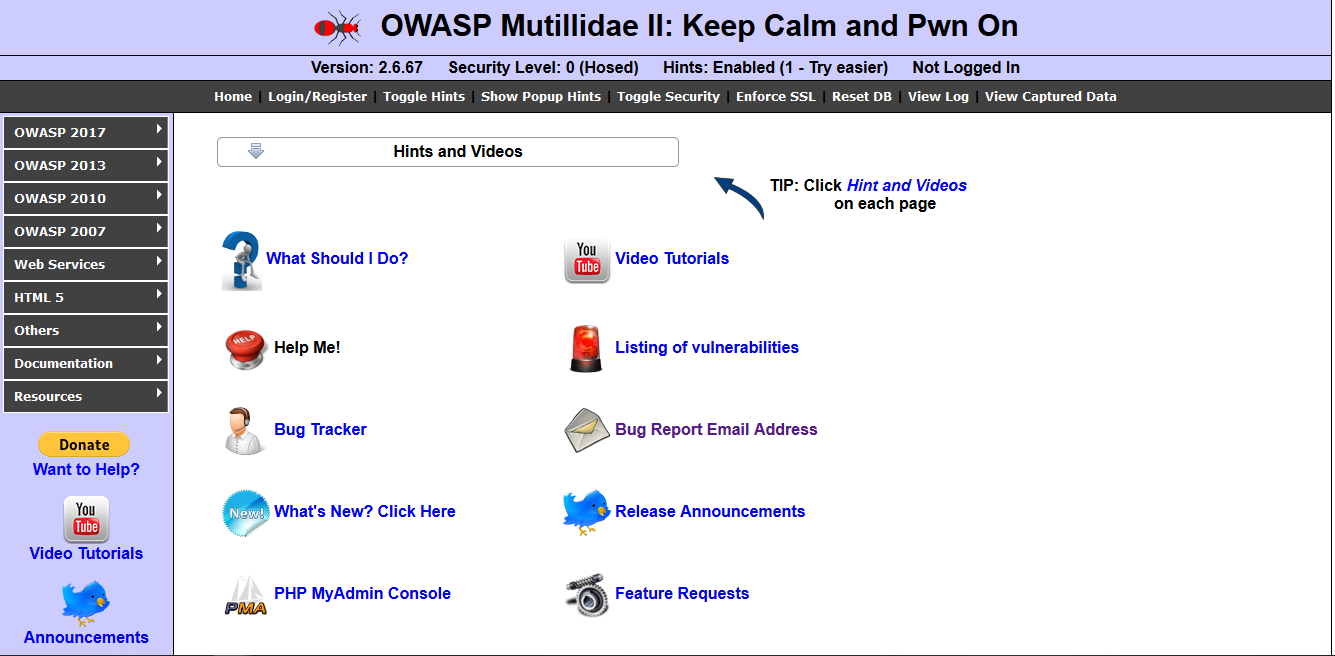


Figura N° 7 “Mutillidae”

A través de la Figura N° 7 “Mutillidae”, nos damos cuenta de que el servicio web esta operando de manera correcta.

1. Posterior a esto se preparo herramienta para generar ataques del tipo “Web Stress” hacia servidor LAMP\_Unab.
2. Se verificaron antes del ataque el uso de CPU y alertas Snort gatilladas en “pfSense\_Unab”

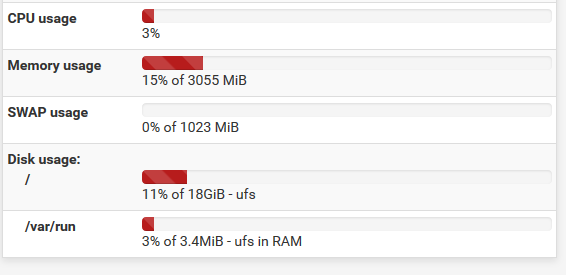


Figura N° 8 “CPU pfSense”

A través de la Figura N° 8, se aprecia que pfSense esta operando bajo rangos muy por bajo de lo normal (3%) de su capacidad.

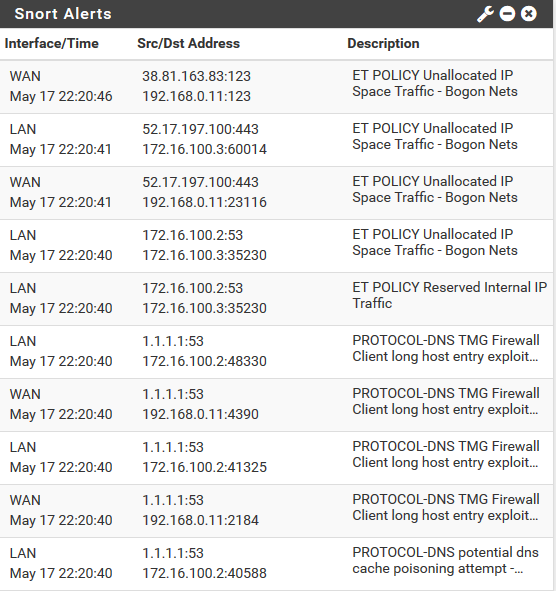


Figura N° 9 “Alertas Snort”

A través de la Figura N° 9, se pueden apreciar alertas Snort normales dentro del laboratorio establecido.

1. Posterior a esto y bajo los parámetros controlados se procede a efectuar el ataque “Web Stress”.

**Previo al Ataque:**

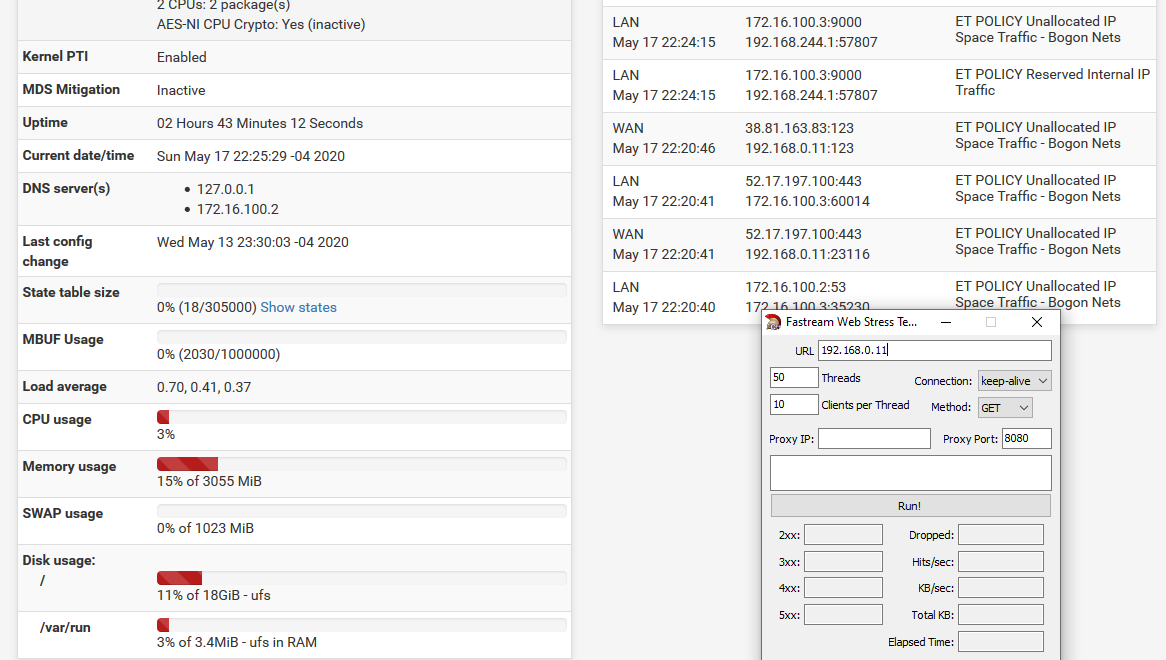


Figura N° 10 “CPU pfSense”

**Durante el ataque:**

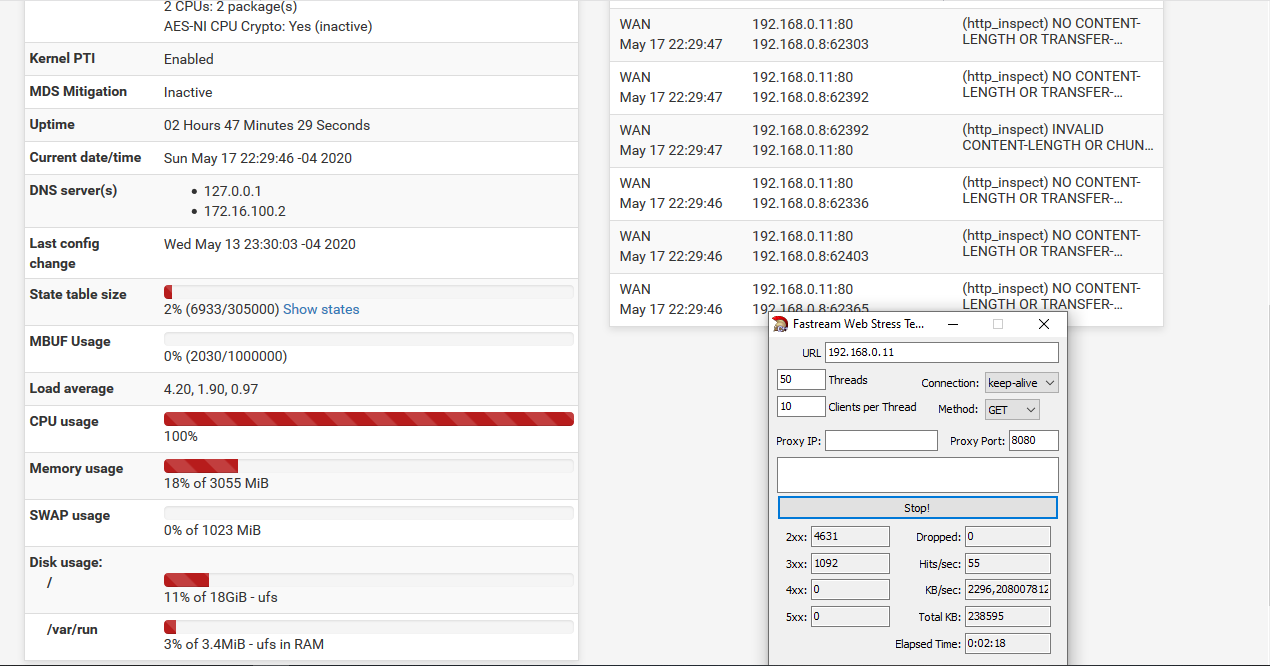


Figura N° 11 “CPU pfSense – Ataque Web Stress”

Aquí se puede apreciar que mientras se efectúa el ataque Web Stress, el uso de CPU aumenta considerablemente en pfSense, llegando hasta el 100%.

Esto produce una lentitud en la administración de pfSense y del sistema en general.

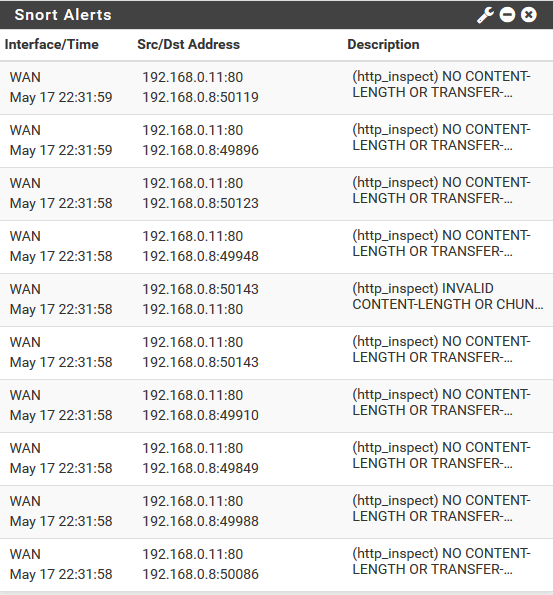


Figura N° 12 “Alertas snort”

A través de la Figura N° 12, podemos apreciar que se están gatillando las alertas snort, a través de **“http\_inspect”**

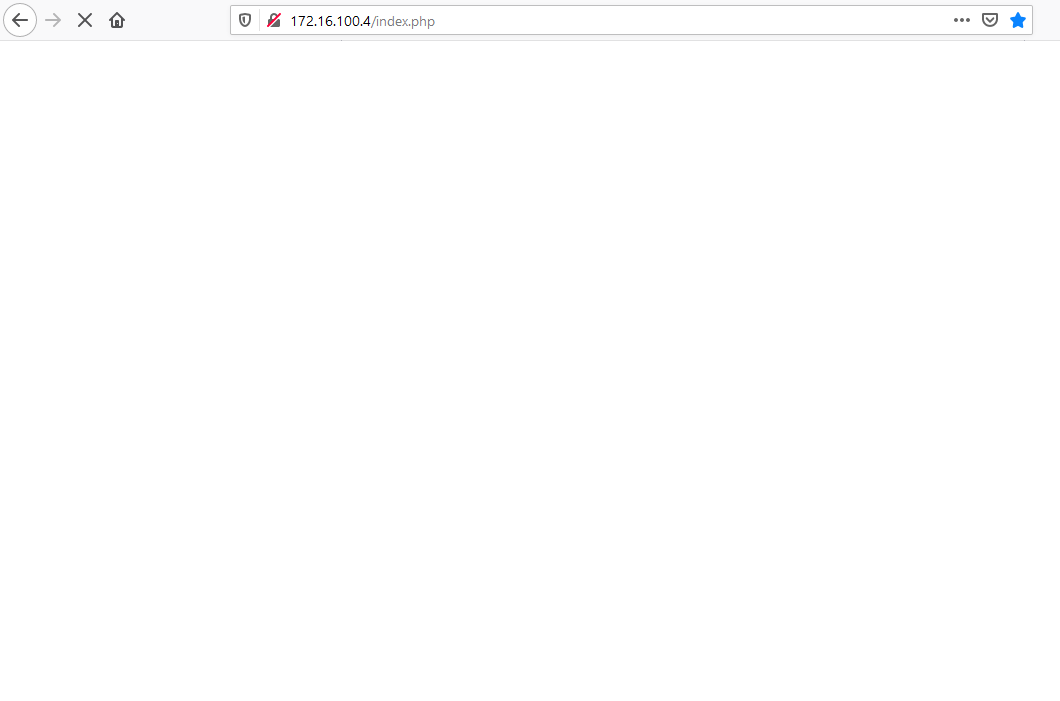


Figura N° 12 “Servicio web Mutillidae”

A través de la Figura N° 12, podemos visualizar que el servicio web de Mutillidae esta abajo y no tiene la capacidad de responder a nuestra solicitud.

1. Vamos a visualizar nuestro correlacionador de eventos

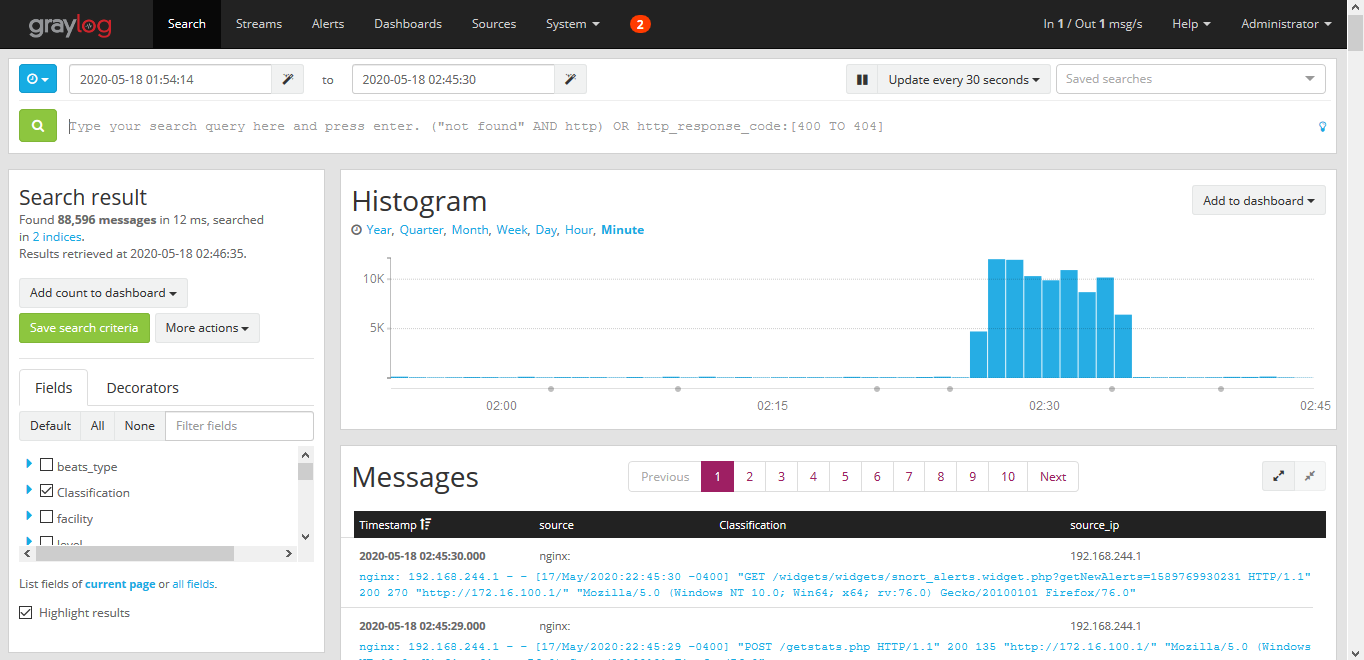


Figura N° 13 “Alertas en Graylog”

En esta Figura N° 13, podemos visualizar como se rompe en forma brutal el Baseline normal del comportamiento habitual, si uno se fija bien en el grafico del Histograma se ven pequeñas barras celestes antes de que se gatillen los ataques y mientras se efectúan los ataques se ven esas grandes columnas.

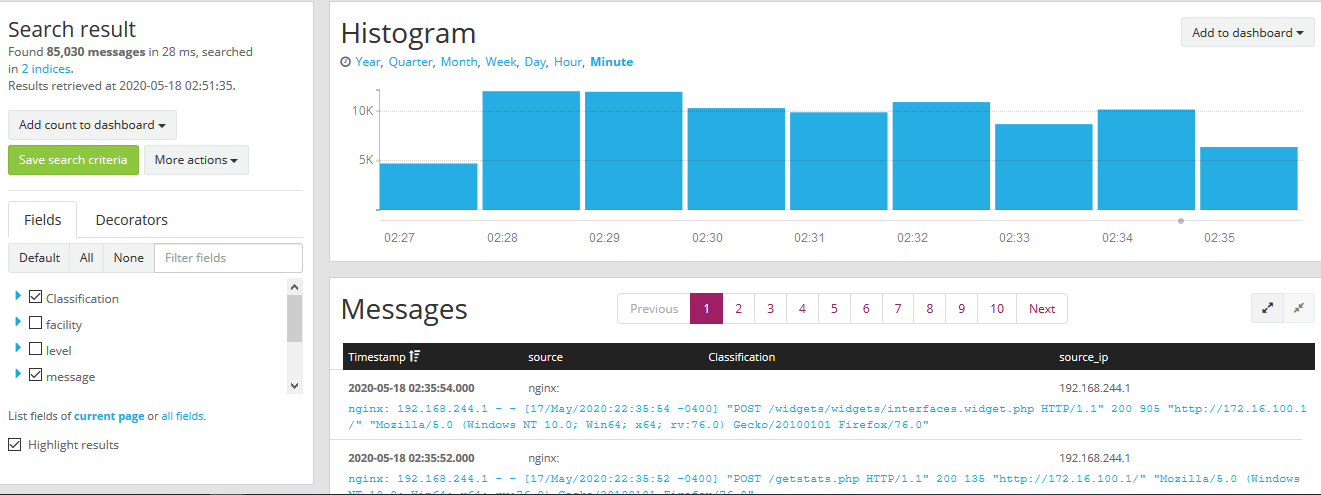


Figura N° 13 “Alertas Graylog”

A través de la Figura N° 13, se puede apreciar que en 7 minutos con 53 seg. se gatillaron alrededor de 85.000 eventos, los cuales fueron enviados desde pfSense a Graylog.

1. Posterior a estos ataques se extrajeron logs duros (Ro) y se enviaron a cuenta de correo de Vicente Martínez.