**Guia Administrador**

**Objetivo.**

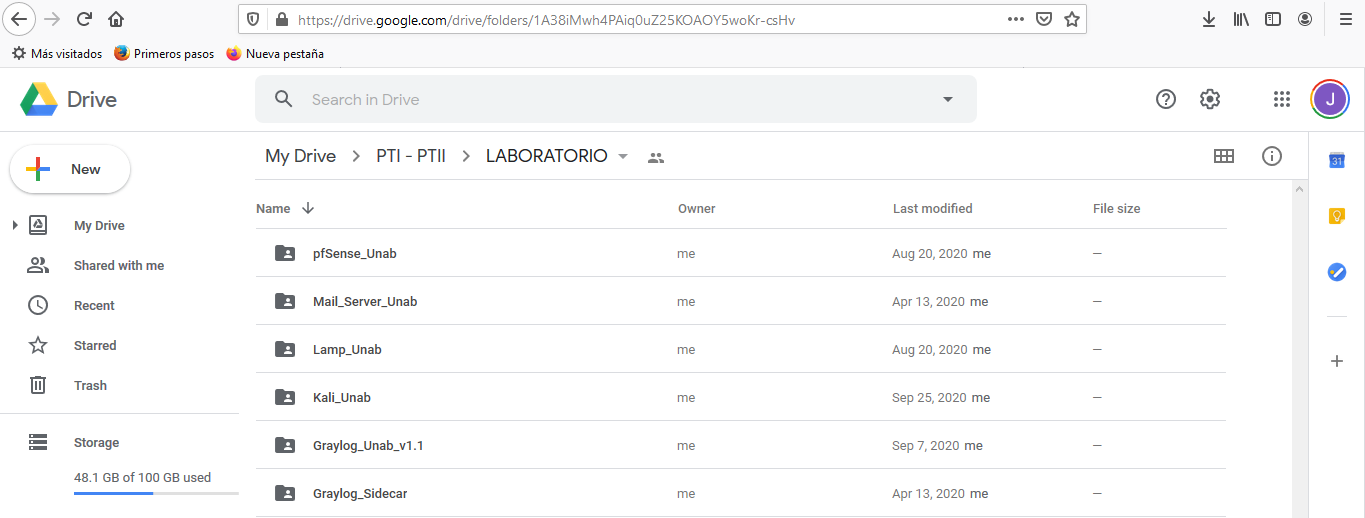
El presente anexo busca entregar los pasos necesarios para que el sistema de deteccion y categorización de posibles amenazas en una red sea implementado sin problemas en una o mas redes.

**Desarrollo.**

A continuación se indicaran los pasos para desplegar el sistema:

1. En primer lugar debemos descargar los archivos alojados en el siguiente Drive (demora bastante la descarga, considerar que son alrededor de 50 Gb en total):

<https://drive.google.com/open?id=1A38iMwh4PAiq0uZ25KOAOY5woKr-csHv>



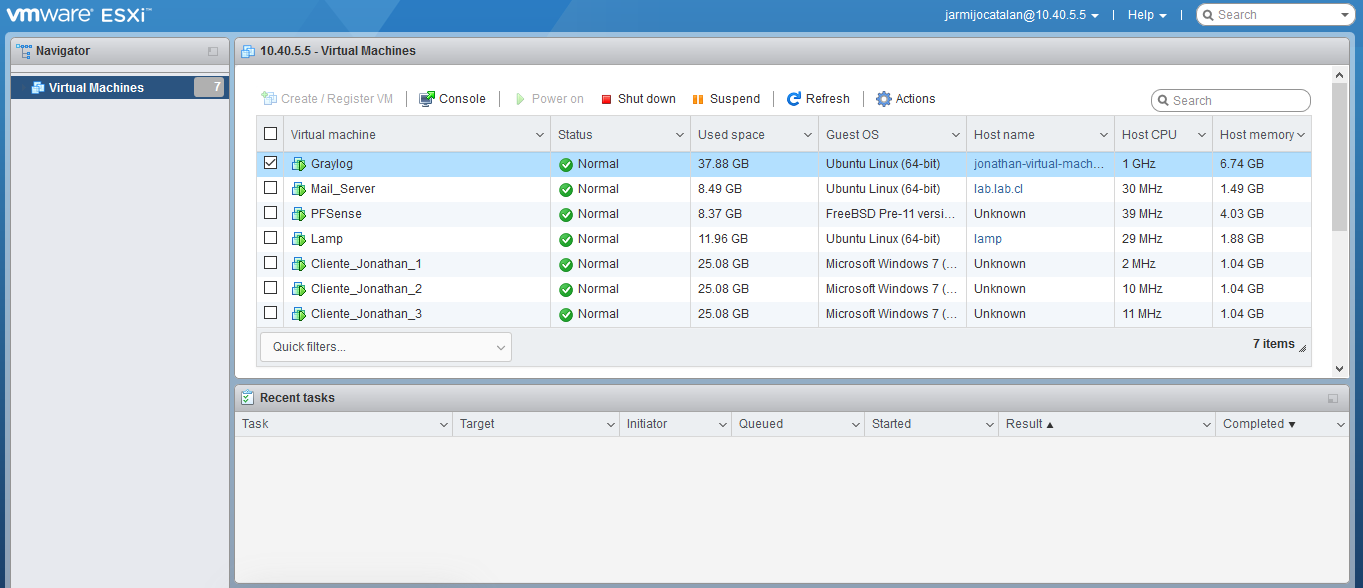
**Figura 1: Maquinas virtuales provistas**

1. Posterior a esto o en paralelo debemos realizar es tener dentro de la red un Servidor con “Vmware ESXi”, desde este servidor se administraran las maquinas virtuales y el sistema en general.
2. Luego hacemos doble click y cargamos las maquinas virtuales de acuerdo a siguiente detalle:
3. Mail\_Server\_Unab
4. pfSense\_Unab
5. Graylog\_Unab\_v1.1
6. Lamp\_Unab
7. Kali\_Unab

Se debe tener presente que como son maquinas OVF, estas ya vienen con una configuracion de red previa, esta puede ser cambiada por el encargado de red, de acuerdo a sus requerimientos.

Objeto evitar posibles fallas en el despliegue de las maquinas virtuales, lo importante es instalarlas una a una, esperando que todo su proceso de instalacion termine de forma correcta.

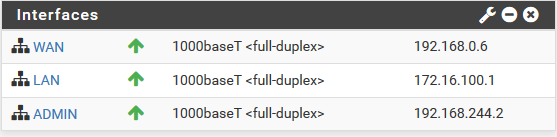
1. Adicionalmente a estas maquinas debieran existir “Equipos\_Clientes” o dipositivos de conectividad (Firewall, Router, Switch, etc.), dependiendo la realidad de cada red, estos seran los encargados en conjunto con pfsense de alimentar el sistema.



**Figura 2: Maquinas virtuales montadas**

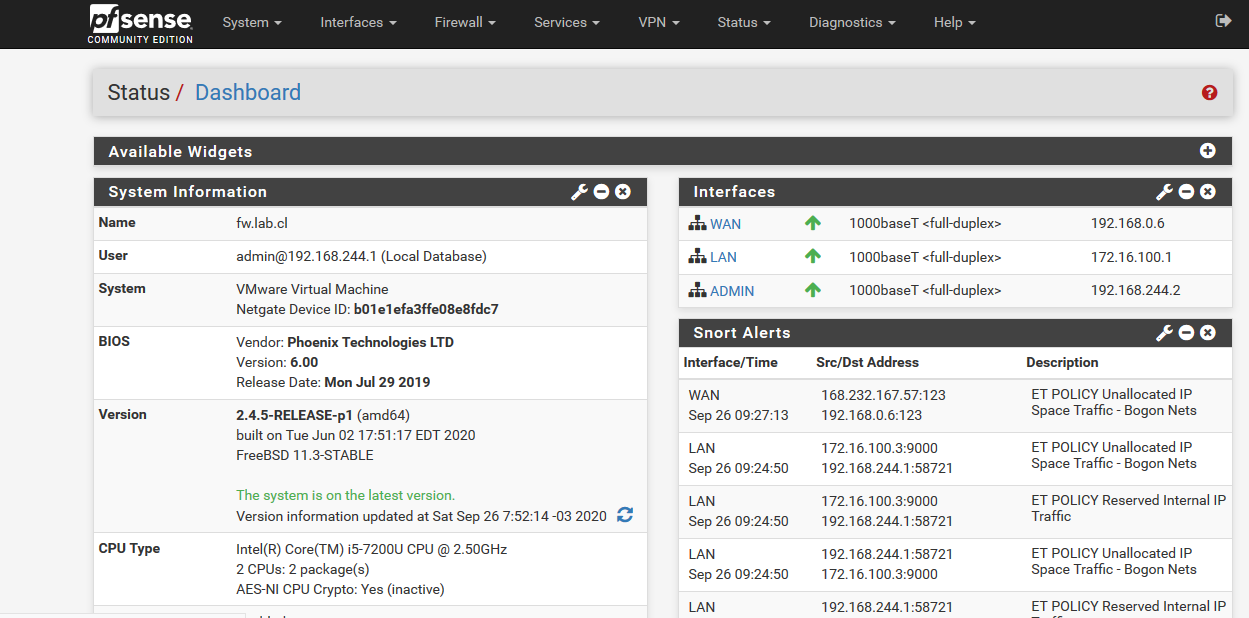
Como muestra la Figura 2, debieran quedar desplegadas las maquinas virtuales provistas.

1. Posterior a esto hay un proceso de configuracion de la red, esto va a ir variando dependiendo de la realidad de cada implementación, pero en general, lo que se busca es que:
2. Todo el trafico de la red pase y se gestione a traves de pfSense. Para esto deberiamos tener una interfax del PfSense como red WAN (La que da hacia fuera de mi red) y otra interfax como LAN (Dentro de mi red), adicionalmente se puede agregar una tercera interfax como ADMIN (Esto es opcional), objeto de esto es que todas estas maquinas se puedan visualizar entre ellas e intercambiar datos.



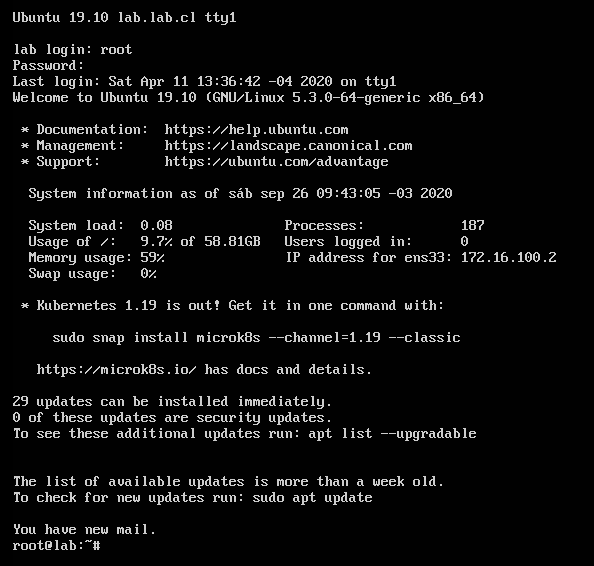
**Figura 3: Interfaces pfSense**

1. Debemos tener en cuenta que pfSense tiene un servicio DHCP habilitado para su LAN, a raiz de esto todas las maquinas que esten tomadas de esa interfax recibiran un direccionamiento IP que sera asignado por pfSense. Esto se realiza objeto gestionar de mejor forma todos los equipos que pasen por pfSense, esto se puede desabilitar.
2. Visualizaciones de las maquinas operando en forma normal:
3. **pfSense\_Unab**



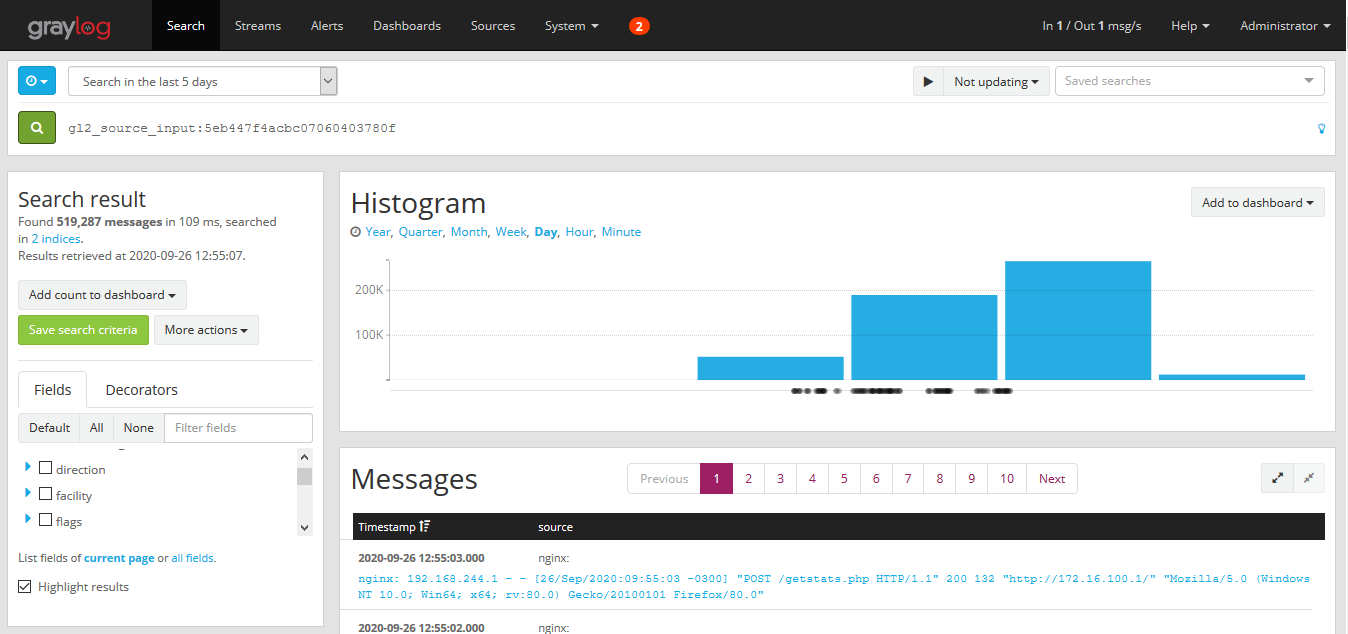
**Figura 4: Visualizacion pfSense**

1. **Mail\_Server\_Unab**



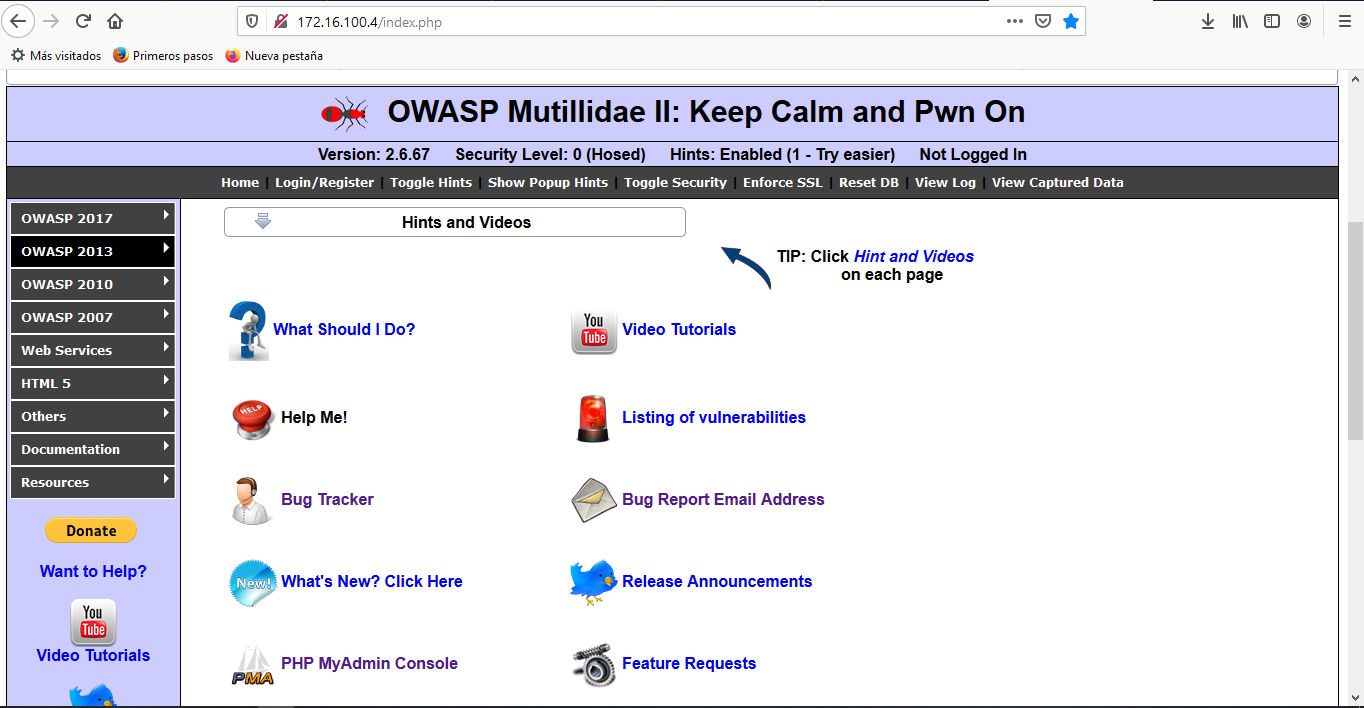
**Figura 5: Visualización Mail / Dns Server**

1. **Graylog\_Unab**



**Figura 6:Visualización Graylog**

1. **Lamp\_Unab**



**Figura 7: Lamp con Servicio Mutillidae II**

1. Credenciales del equipamiento:
2. Mail\_Server\_Unab

User: root

Pass: test

1. pfSense\_Unab

User: admin

Pass: Unab.2020

1. Lamp\_Unab

User: root

Pass: Unab.2020

1. Graylog\_Unab

User: root

Temerac2018

Web

User: admin

Pass: Temeracbeta2020

1. Posterior a esto, encendemos las 2 maquinas virtuales “Graylog\_Unab” y “Mail\_Server\_Unab”, dejamos de que ambas maquinas finalicen su proceso de encendido.
2. Luego ingresamos a “Graylog\_Unab” a través del usuario “jonathan”, en donde la password es “Temerac2018”.
3. Estando dentro de esta abriremos una ventana terminal. A través del comando “ifconfig” consultamos direccionamiento de red. Tomamos nota de la ip que aparece en ens33 “inet addr: 172.16.100.3” (en este caso), ya que esta debemos reemplazarla en el archivo que detallaremos mas adelante.
4. Posterior a esto nos dirigimos al archivo de configuración de Graylog, con el siguiente comando # sudo nano /etc./Graylog/server/server.conf. Ingresaremos nuevamente la pass “Temerac2018”.
5. Visualizaremos siguiente archivo, en donde nos debemos dirigir a “http\_”, esto lo podemos hacer mas rápido a través de “ctrl + w” y tipeamos “http\_bind\_address”, aquí debemos reemplazar el valor con la ip que habíamos copiado anteriormente (xxx.xxx.xxx.xxx:9000). Posterior a este cambio “ctrl + o” y enter para guardar.
6. Dentro del mismo archivo y con las teclas “ctrl + w” tipeamos “email transport” y enter, llegando a esta sección del archivo, debemos configurar la misma ip anterior, tal como se ve en la siguiente figura.
7. En la sección recién vista del archivo (#Email transport), también se efectúa la configuración del servidor de correo (dominio @lab.cl), con el cual se establecerá la comunicación, en este caso la configuración ya esta realizada y solo se debe cambiar la ip de la Uri, de acuerdo a lo solicitado en el pto. 11. Posterior a esto presionamos “ctrl + o” y enter para guardar, luego “ctrl + x” para salir.
8. Posterior a esto reiniciamos el correlacionador, con el comando #sudo systemctl restart graylog-server
9. Ahora instalaremos y configuraremos Graylog-Sidecar (agente) en un equipo(s) Windows, lo primero que haremos en equipo Windows será ejecutar el archivo graylog\_sidecar\_installer\_1.0.2-1, el cual estará junto a las maquinas virtuales, dejamos que el proceso de instalación termine.
10. Posterior a esto buscamos CMD y lo ejecutamos como “administrador”.
11. Estando dentro de CMD vamos al archivo de configuración de Graylog-Sidecar, con el siguiente comando notepad.exe C:\Program Files\Graylog\sidecar\sidecar.yml. Aquí seteamos la dirección ip de Graylog\_Unab en la línea server\_url: http://xxx.xxx.xxx.xxx:9000/api, como aparece en la figura de abajo. Luego “ctrl + g” para guardar y cerramos el archivo.
12. Creamos un API Token para este input desde System/Autenthication aquí seleccionamos provider setting del panel izquierdo y le damos un nombre al nuevo Token, posterior a esto lo copiamos y reemplazamos en este archivo ya editado de configuración de Graylog\_Sidecar.

Nota: Ya hay creado un Api Token “Windows\_Token\_Sidecar\_Unab”, también se puede copiar este y reemplazar en el archivo ya editado.

server\_api\_token: "d52sfsoiridmrk8ju25q2s1u2p93flm9qmv1okm2qt802nn1noj" (Token ejemplo).

1. Luego dentro de CMD ejecutamos siguientes comandos:

"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service install

"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service start

En el caso de que el proceso estuviera corriendo, ejecutamos:

"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service stop y luego:

"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service start

1. Luego ingresamos a Graylog http://ipa.ddr.ess.ss:9000/ y nos dirigimos a System/Sidecard/Configuration y en el archivo de configuración en host seteamos la ip de Graylog\_Unab, como muestra la figura de abajo (hosts: ["ipa.ddr.ess.sss:5044"]) (en este caso es esa ip). Luego abajo le damos “Update”.
2. Posterior a estos nos dirigimos a “Alertas”, menú que se encuentra en el panel superior y vamos a “Notifications”, luego en “Alerta de seguridad” le damos click a “More actions” y le damos a “edit”.
3. Debemos dejar siguiente configuración, en E-mails receivers dejaremos la cuenta jonathan@lab.cl que es el receptor y una de las cuentas configuradas en el servidor de correo “Mail\_Server\_Unab”, le damos “Save” con la cual guardaremos dicha configuración.
4. Ahora instalaremos en otros equipo (Que seria el equipo donde efectuare el monitoreo y donde recibiré los correos) un gestor de correo, las pruebas e implementación se realizaron con Thunderbird, posterior a la instalación configuraremos 2 cuentas de correos en este gestor, de acuerdo a siguiente detalle:

Cuenta 1.

Nombre: jonathan@lab.cl

Cuenta 2.

Nombre: graylog@lab.cl

Ambas cuentas deben que configuradas de acuerdo a las figuras (figura 1 – figura 2) de mas abajo.

Se debe tener presente para ambas cuentas:

a) Your name: El que desee.

b) Email address: jonathan@lab.cl (cuenta 1) y graylog@lab.cl (cuenta 2).

c) Password: test2020

d) Server hostname: Es la dirección ip del servidor de correo “Mail\_Server\_Unab”.

e) Puerto IMAP: 143

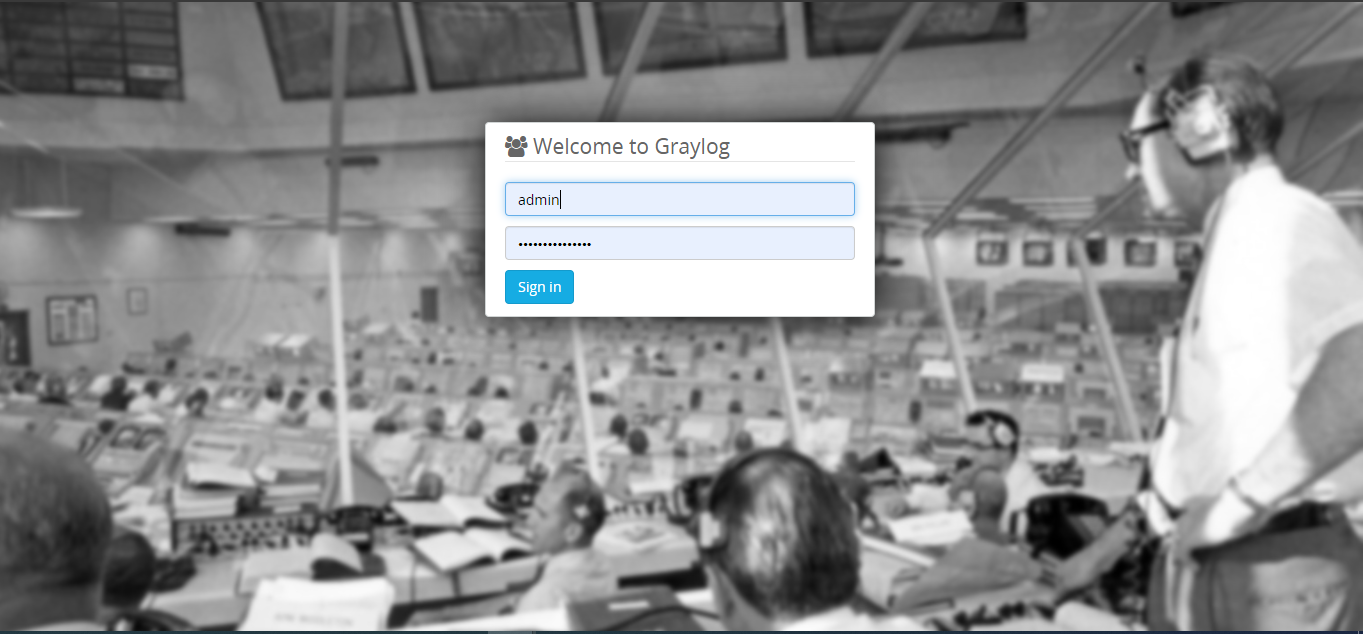
f) Puerto SMTP: 25

1. Posterior a esto nos vamos a la maquina “Graylog\_Unab” y seteamos como DNS de esta la direccion ip del servidor de correo “Mail\_Server\_Unab”, también como se muestra en las figuras siguientes se recomienda dejar direccionamiento IP en “Manual” y setera mismos datos ya asignados (#ifconfig).
2. Objeto ver si configuración esta correcta y las alertas (correos) quedaron bien seteados, nos dirigimos a “Alert”, dentro de este nos vamos a “Notifications” y buscamos la alerta configurada que lleva por nombre “Alerta de Seguridad”, aquí hacemos click en el boton “Test”, si esta todo bien nos debiera llegar un correo a la cuenta [jonathan@lab.cl](mailto:jonathan@lab.cl).
3. Mientras usted se encuentra trabajando en otras actividades frente al computador, las notificaciones deben aparecer como pop-up.
4. Respecto al servidor de correo “Mail\_Server\_Unab”, las credenciales para ingresar son las siguientes:

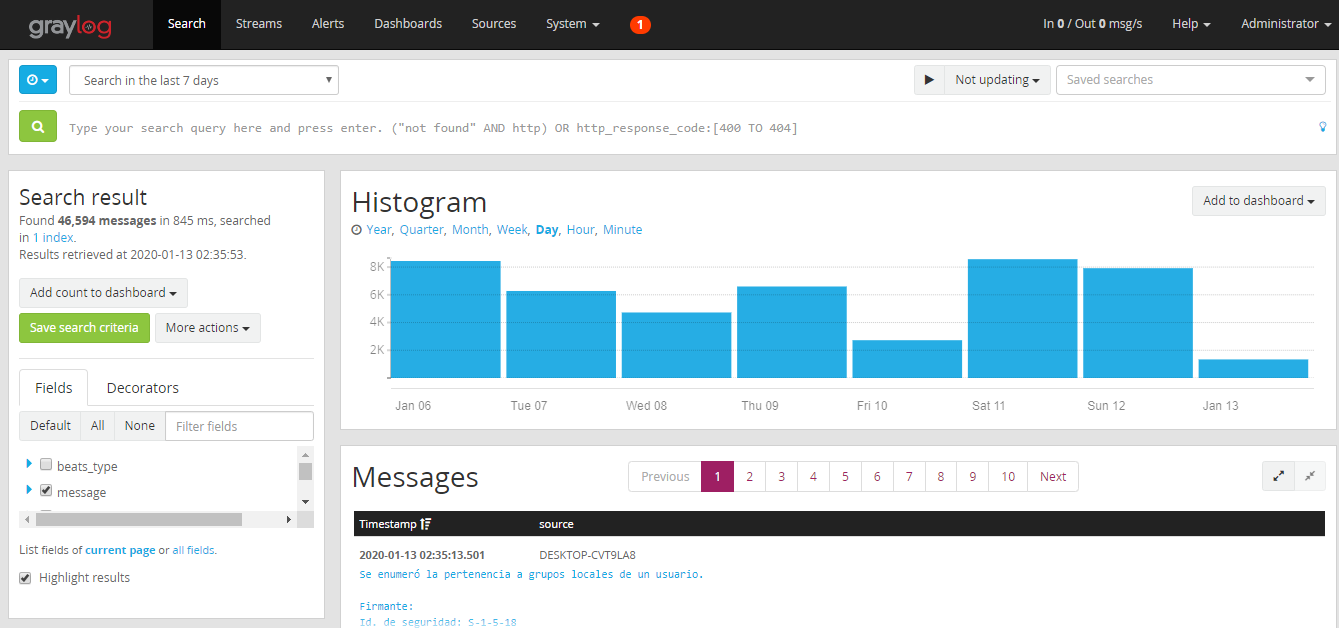
User: root / Pass: test

User: test / Pass: test

1. En el caso de que servidor de correo presente problemas, se debe verificar a través del comando #nano etc/bind/db.lab.cl que las ip´s que tiene configuradas son las asignadas (misma ip del servidor de correo).
2. A continuación se despliega la visualización del sistema de correlación.

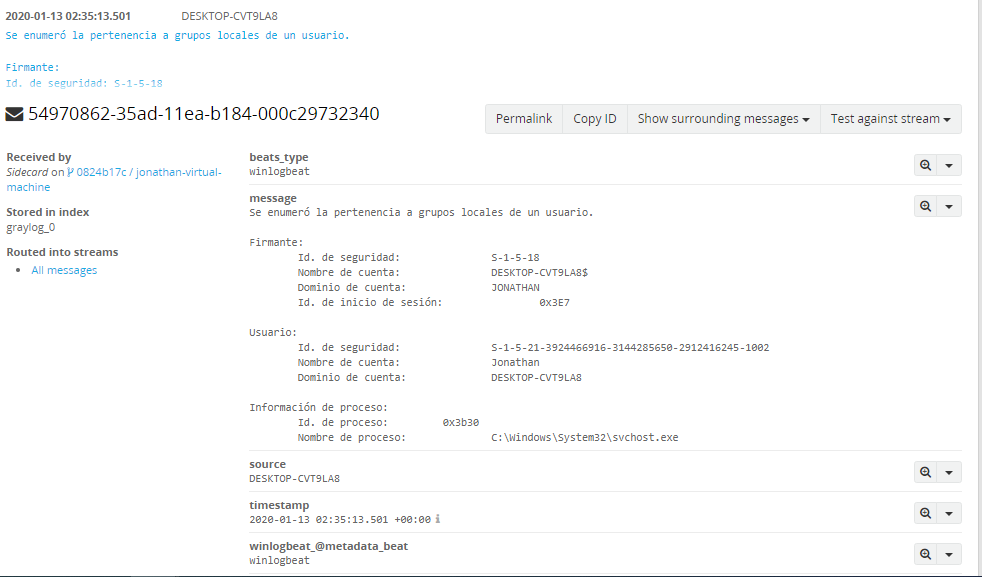


Esta es la visualización que debemos ver para hacer ingreso al correlacionador de eventos Graylog, con las credenciales entregadas.



Una de las primeras visualizaciones que tendremos es esta en donde podemos ver el Histograma, en donde se pueden apreciar los eventos que están ingresando al sistema.

En el costado derecho podemos visualizar la cantidad de eventos recolectada y la cantidad de tiempo empleada en esta, lo cual nos hace ver que efectivamente el flujo de datos es considerable.



Si hacemos clic sobre uno de los eventos que se encuentran bajo el Histograma, notaremos que se despliega este evento y se pueden visualizar todos los componentes que forman parte de ese determinado log. Esto quita una gran carga de trabajo a los encargados de Seguridad TI, ya que podemos apreciar de forma rápida y certera quien es el origen del evento, su dominio, dependencia, hora de ocurrencia y otros datos que son de vital importancia para en caso lo requiera mitigar un incidente informático.

1. A continuacion se incluye un paso a paso de como operar Graylog:
2. Ingresamos a la plataforma Graylog, de acuerdo a siguiente detalle:

URL : <http://xxx.xxx.xxx.xxx:9000/>

User : admin

Pass : Temeracbeta2020

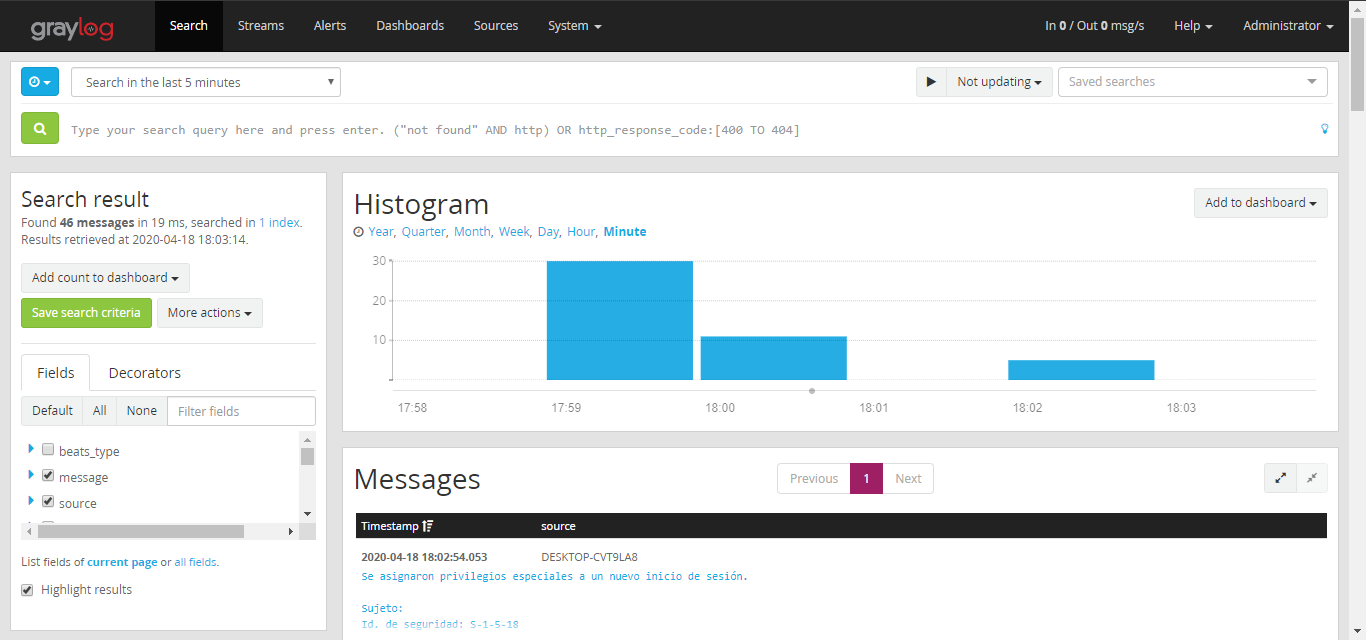
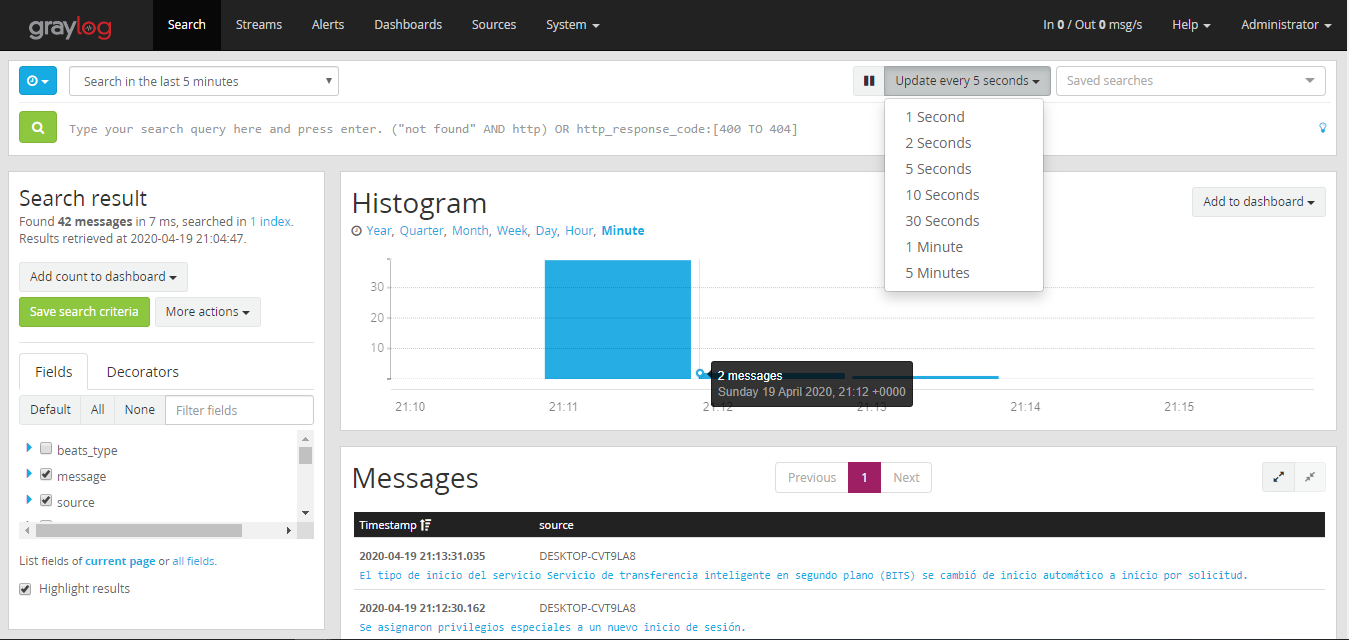


Figura N° 1 “Search”

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

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

Figura N° 2

1. A continuacion le damos click al boton “Show alerts”, aquí visualizaremos todas las alertas que se han gatillado.

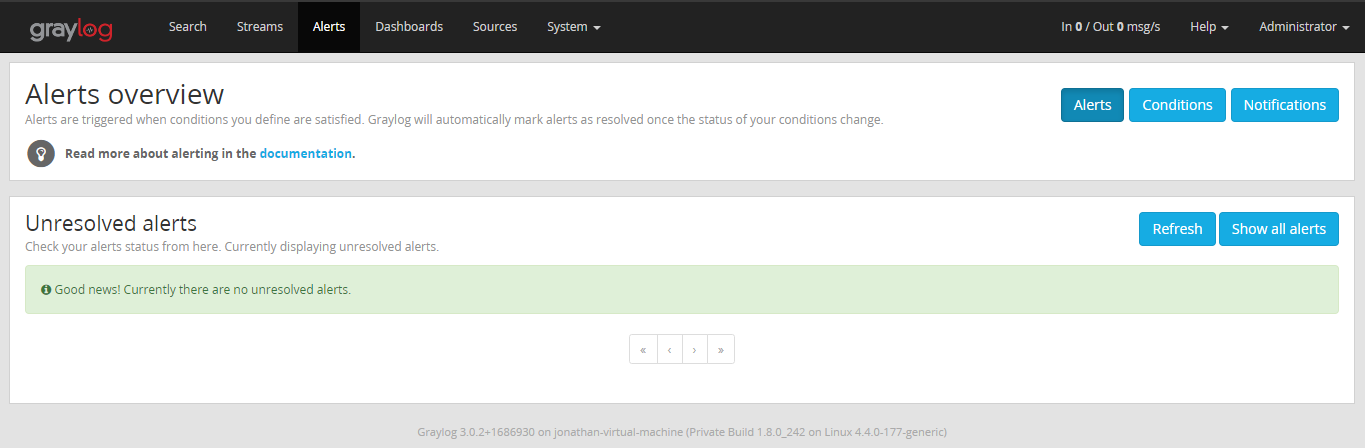


Figura N° 3

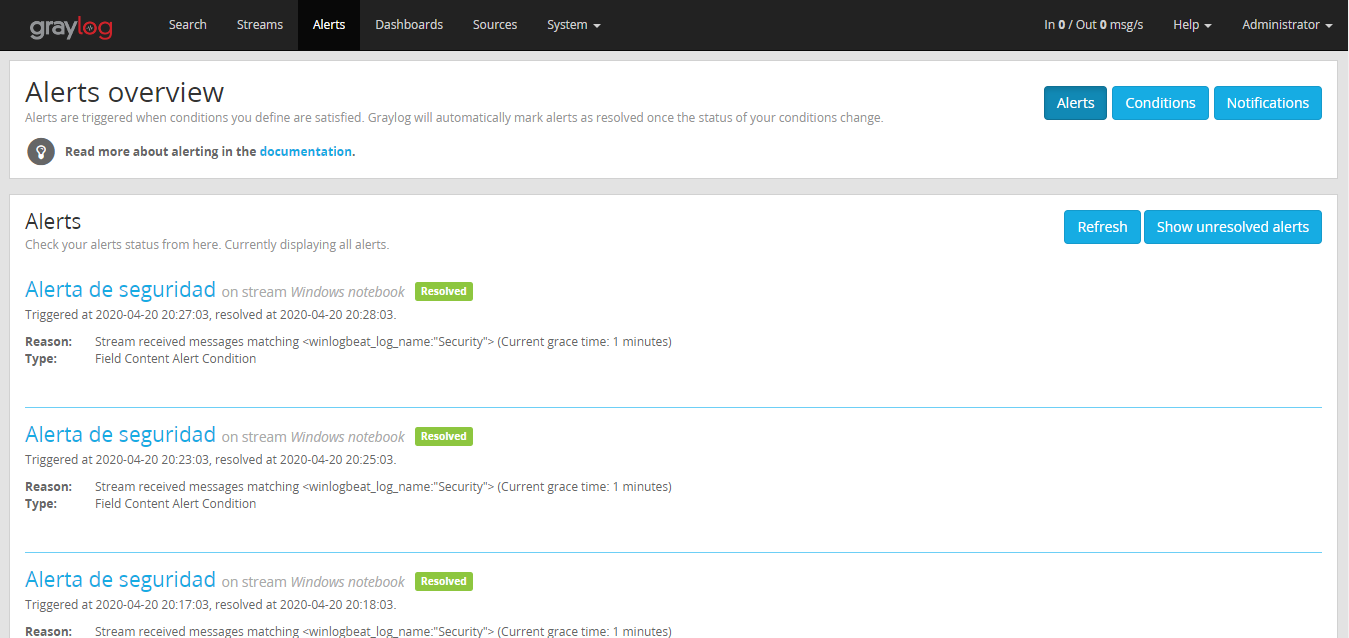


Figura N° 4

1. Posterior a estos nos dirigimos al menu “Alerts”, el cual se encuentra en el panel superior, vamos a “Notifications”, luego en “Alerta de seguridad” le damos click a “More actions” y le damos a “edit”.

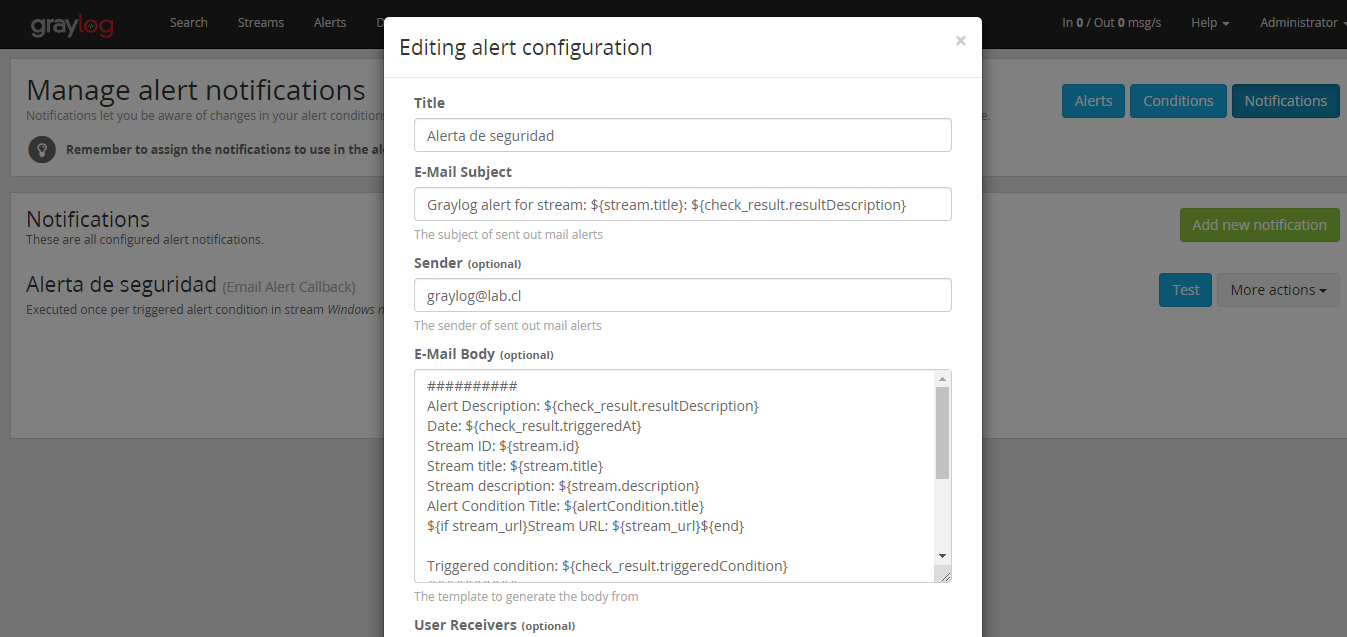


Figura N° 5

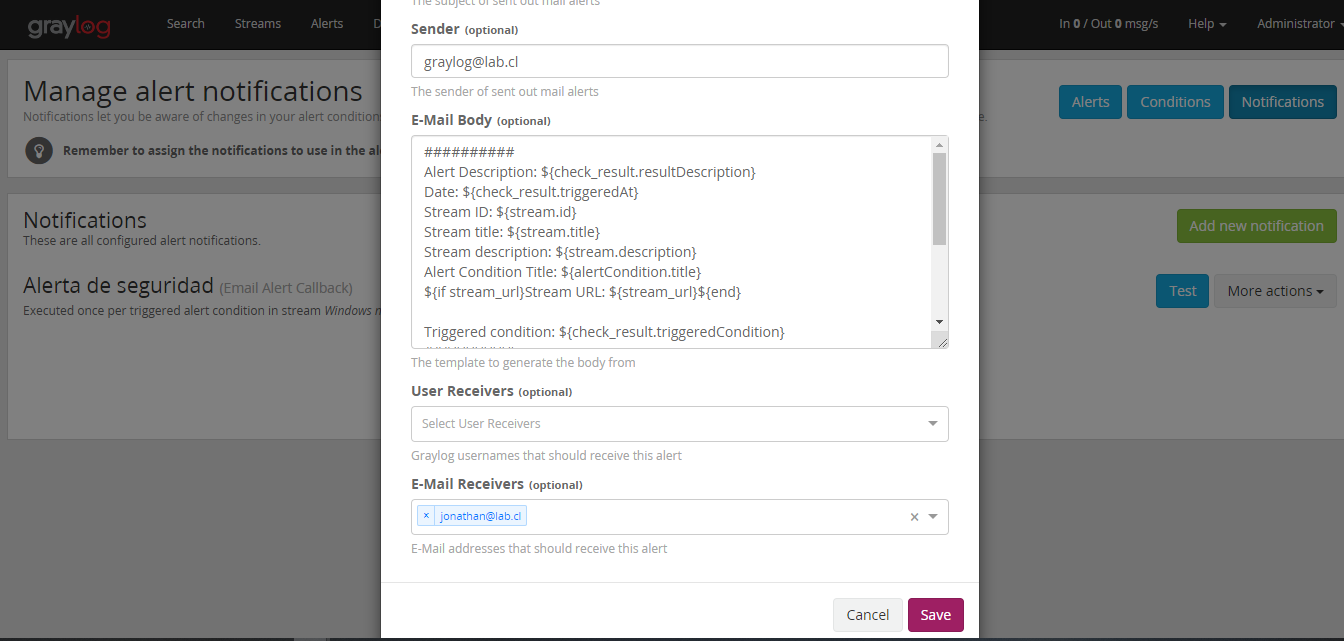


Figura N° 6

1. En las figura N° 5 y N° 6 podemos ver el originador y el destinatario de las cuentas de correo a la cual se enviara el correo con la notificacion de la alerta de seguridad. Esto con el objeto de que el personal de seguridad TI o el encargado tome las acciones de mitigación.
2. Si nuestra intencion es solo visualizar la configuración de la notificación y no efectuar cambios en esta dentro de la pestaña “Notifications”, hacemos click en “show configuration”, opcion que se encuentra en la parte inferior de Alerta de seguridad.

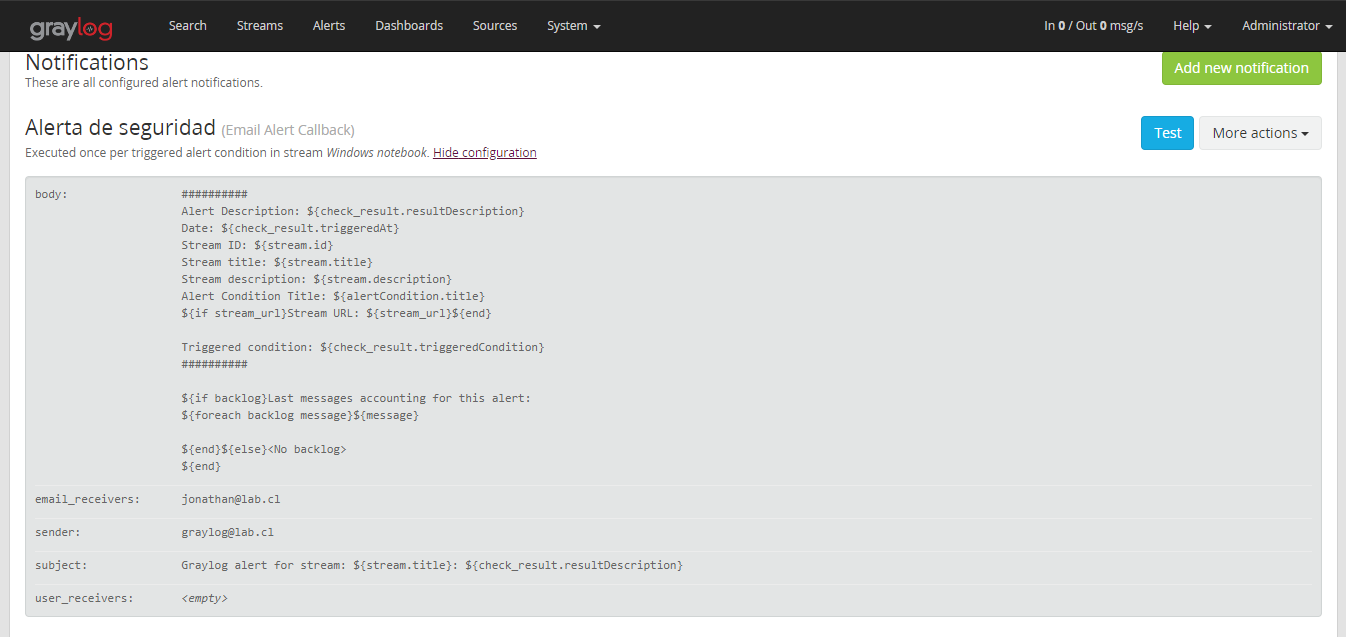


Figura N° 7

1. En el equipo destinado para monitoreo se configuro un gestor de correo (Thunderbird) la cuenta para la recepción de las notificaciones ([jonathan@lab.cl](mailto:jonathan@lab.cl), para pruebas), esta cuenta sera la encargada de recibir los distintos correos con notificaciones de Alertas de Seguridad.

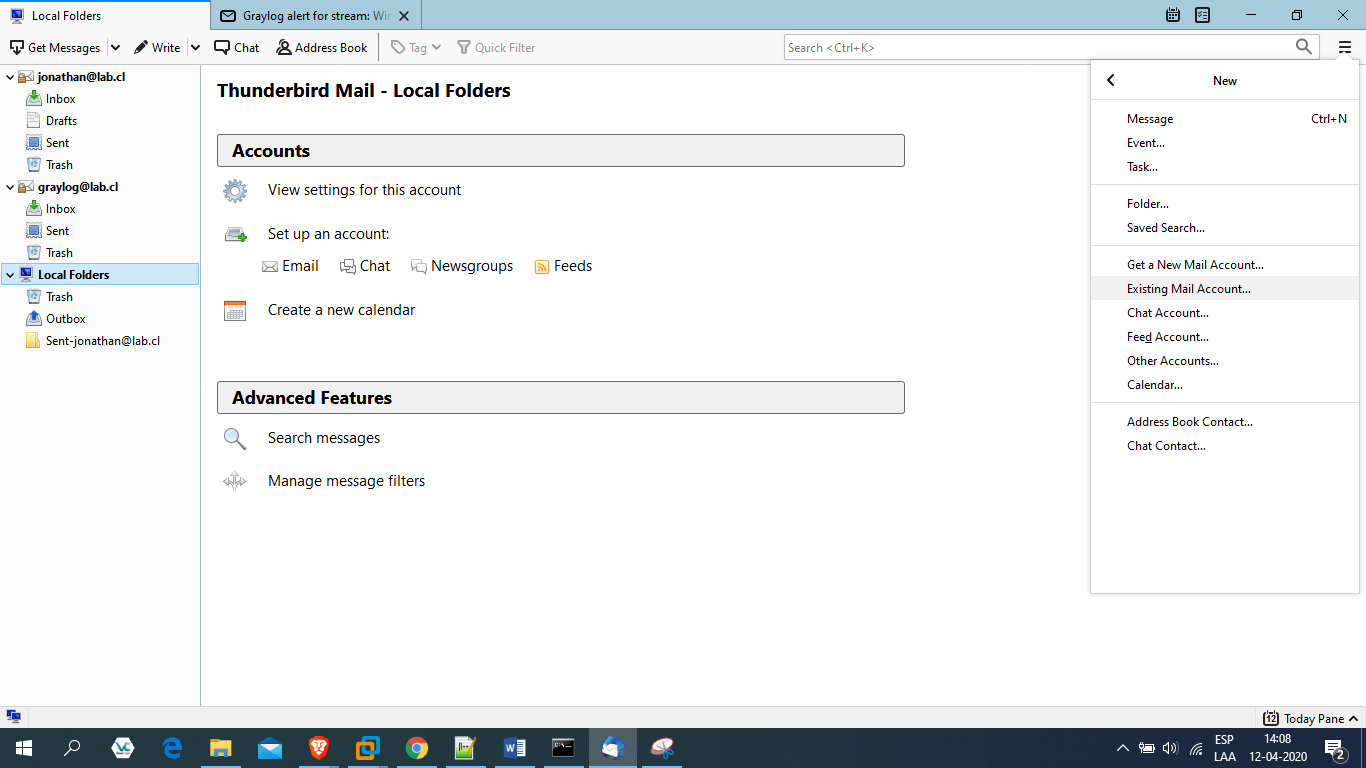


Figura N° 8

Cuenta 1.

Nombre: [jonathan@lab.cl](mailto:jonathan@lab.cl)

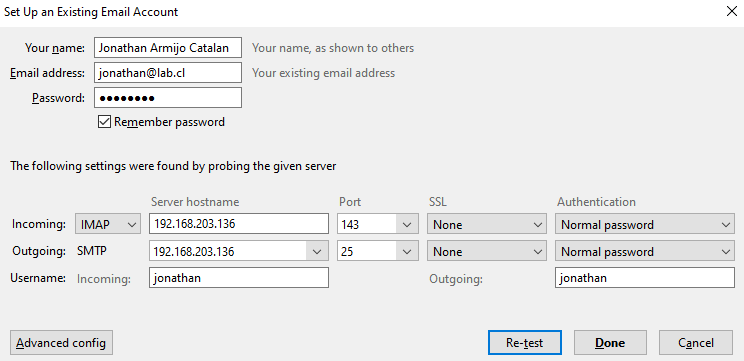
Cuenta 2.

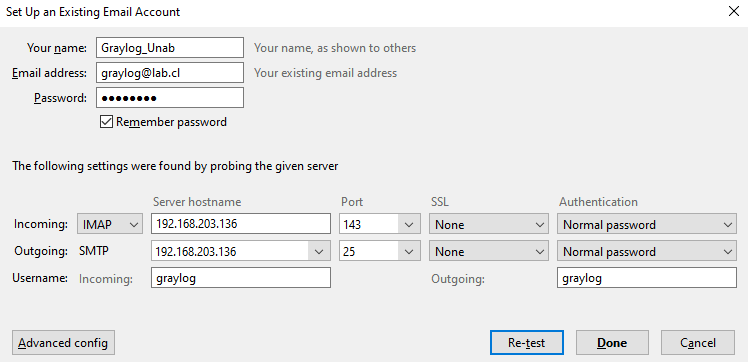
Nombre: [graylog@lab.cl](mailto:graylog@lab.cl)

Ambas cuentas deben que configuradas de acuerdo a las figuras (figura 1 – figura 2) de mas abajo.

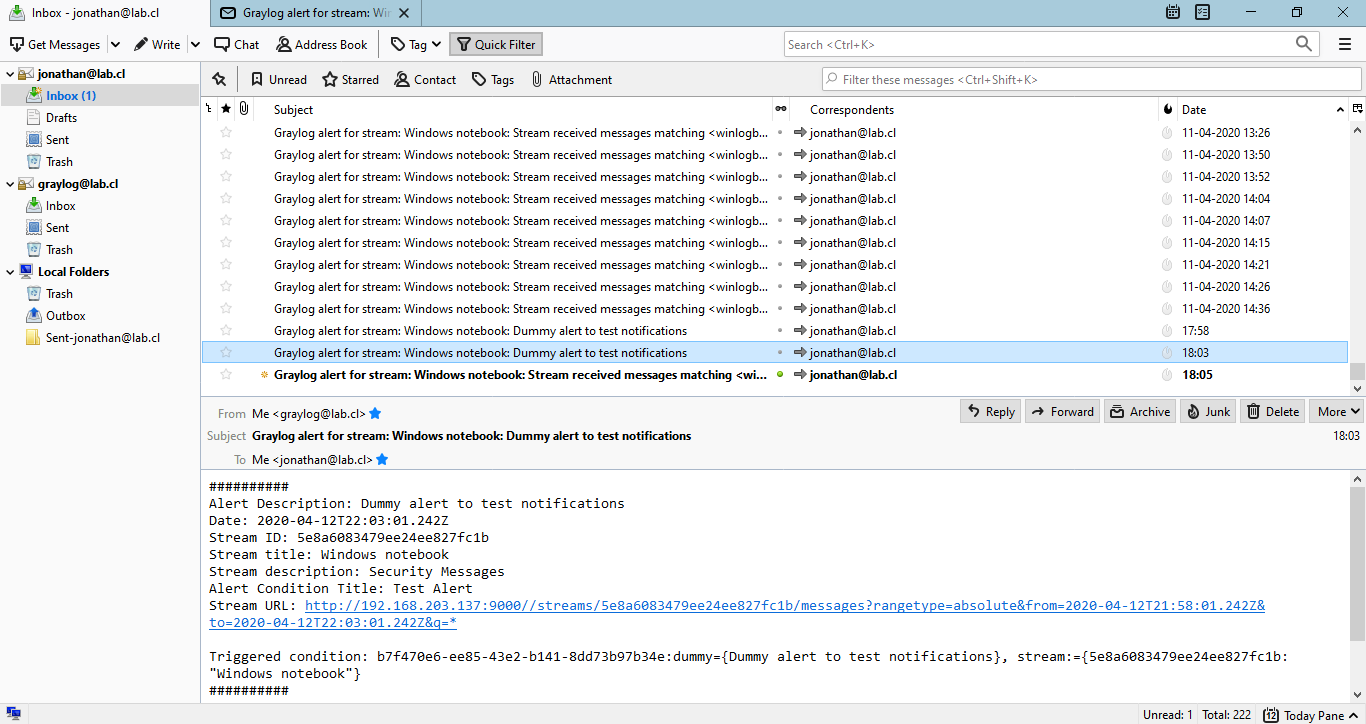
Se debe tener presente para ambas cuentas:

1. Your name: Jonathan Armijo (Ejemplo).
2. Email address: [jonathan@lab.cl](mailto:jonathan@lab.cl) (cuenta 1) y [graylog@lab.cl](mailto:graylog@lab.cl) (cuenta 2).
3. Password: **test2020**
4. Server hostname: Es la direccion ip del servidor de correo “Mail\_Server\_Unab”.
5. Puerto IMAP: 143
6. Puerto SMTP: 25

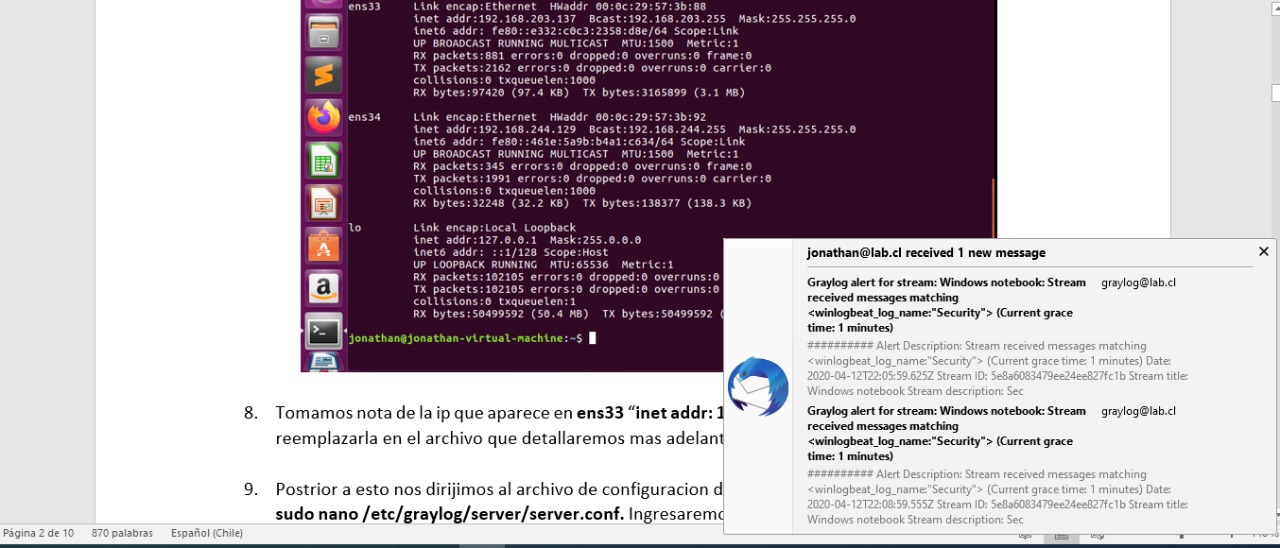




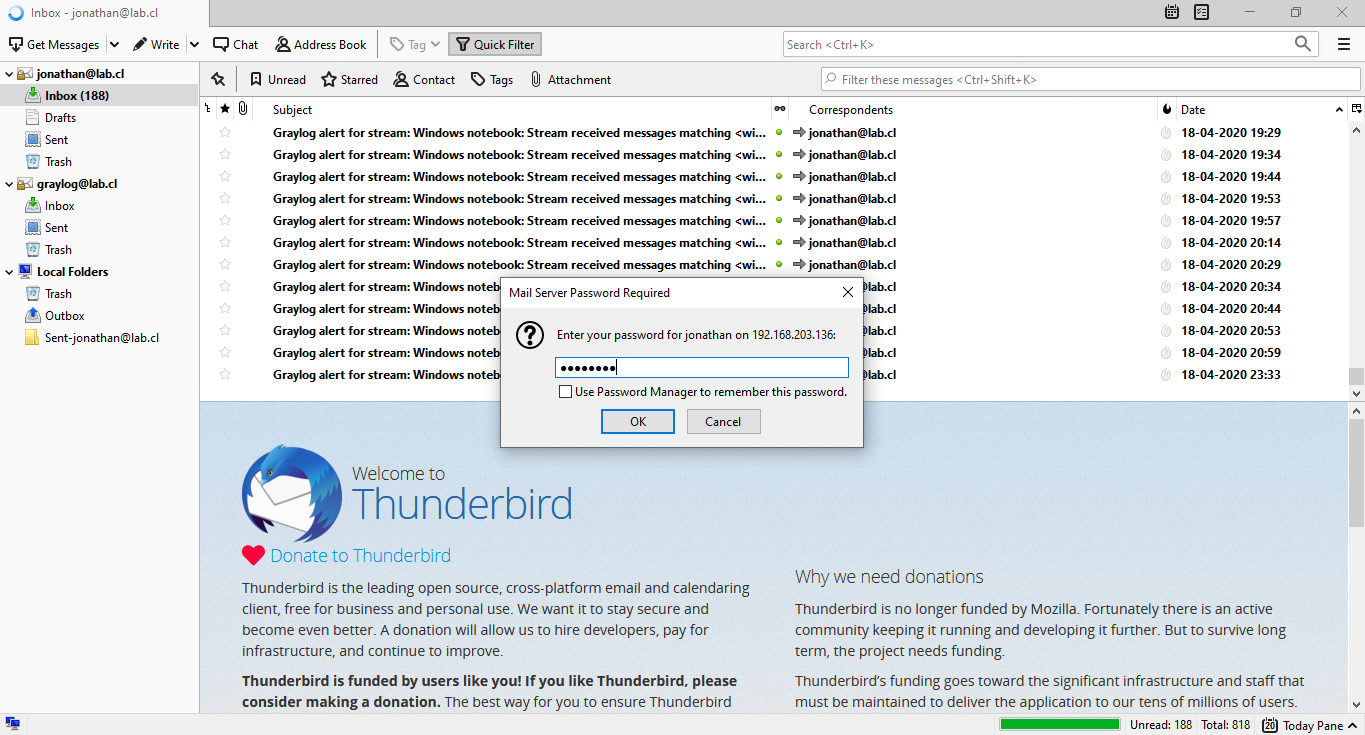
1. Objeto ver si configuracion esta correcta y las alertas (correos) quedaron bien seteados, nos dirigimos a “Alert”, dentro de este nos vamos a “Notifications” y buscamoos la alerta configurada que lleva por nombre “Alerta de Seguridad”, aquí hacemos click en el boton “Test”, si esta todo bien nos debiera llegar un correo a la cuenta [jonathan@lab.cl](mailto:jonathan@lab.cl).



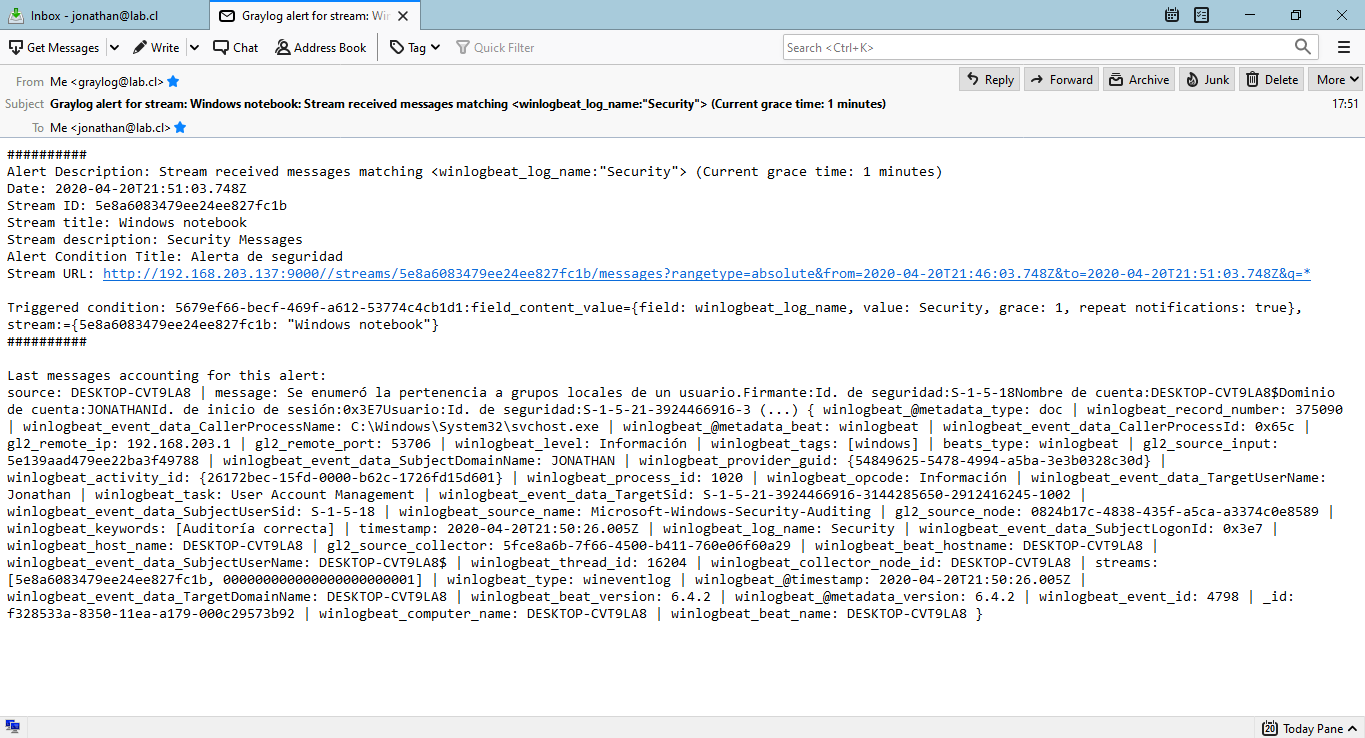
1. Mientras usted se encuentra trabajando en otras actividades frente al computador, las notificaciones deben aparecer como indica la siguiente figura:



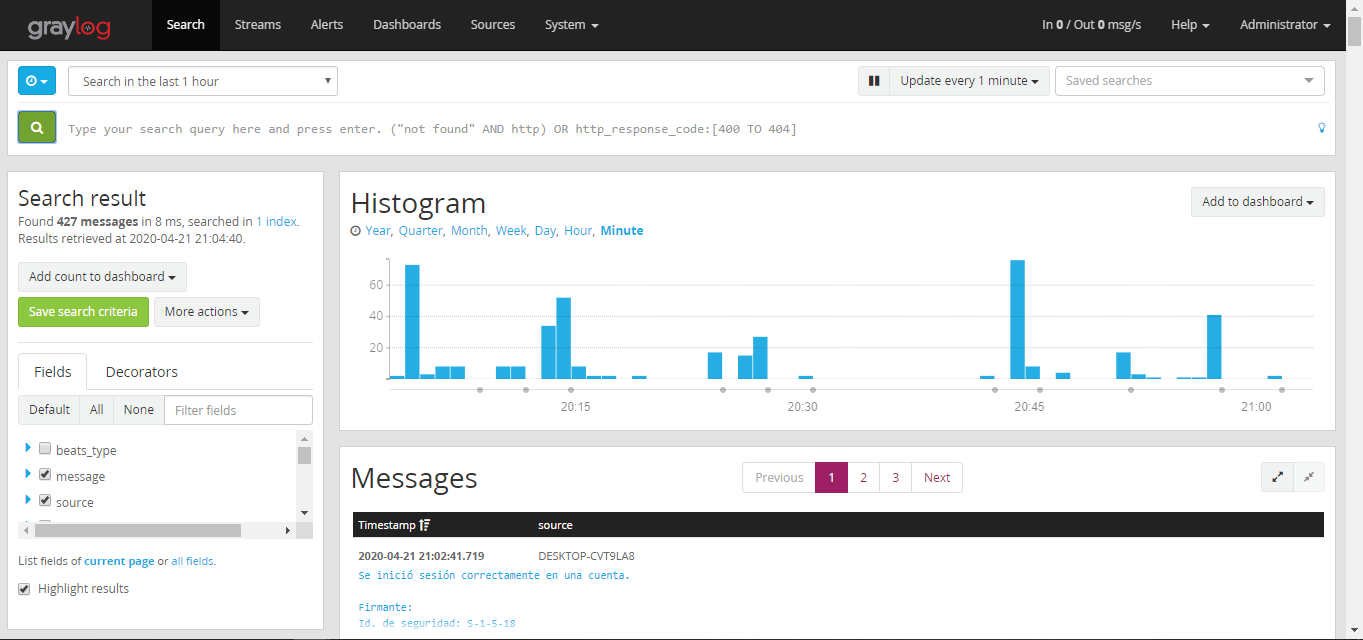
1. Al abrir el gestor de correo, este le solicitara la password del usuario, esta es **test2020**, ingresamos esta password y le damos ok.



1. Al recibir un correo electronico con el detalle de una alerta de seguridad, lo que procederemos a realizar es hacer click en esta alerta desplegando los detalles de esta, si los detalles que se aprecian en este no son convincentes de que efectivamente estamos frente a un incidente informatico, haremos click en el link “Stream URL” inserto en el mismo correo, este link nos redigira hacia el sistema de correlacion de eventos, desde donde fue gatillada y enviada la alerta. Aquí podremos revisar en detalle la alerta enviada por el sistema

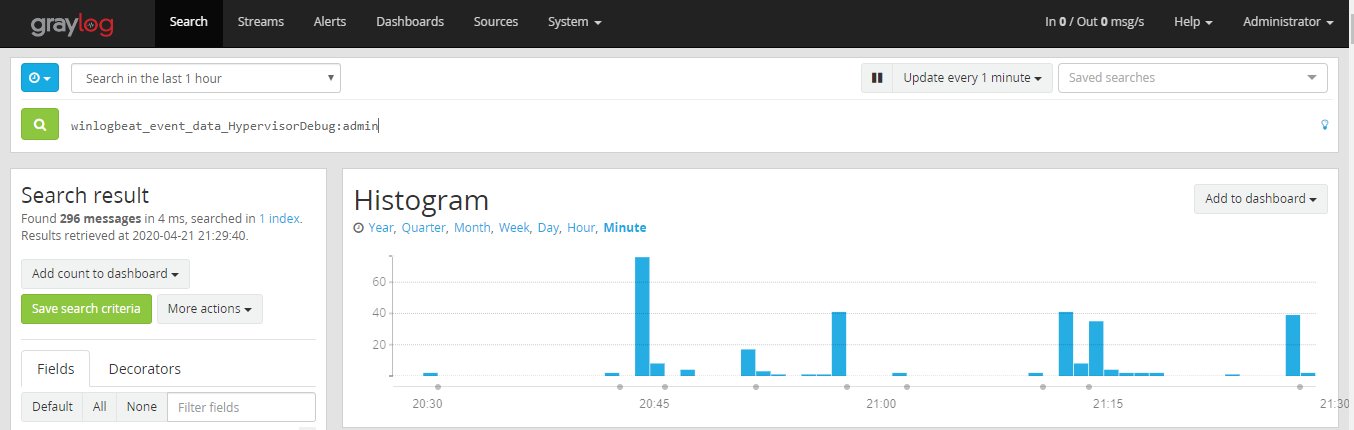


1. Normalmente el operador de seguridad o la persona encargada de informatica, en el caso que tenga la diponibilidad para monitorear la red debiera mantener en visual este dashboard, el cual muestra bastante detalles de lo que esta circulando por la red.

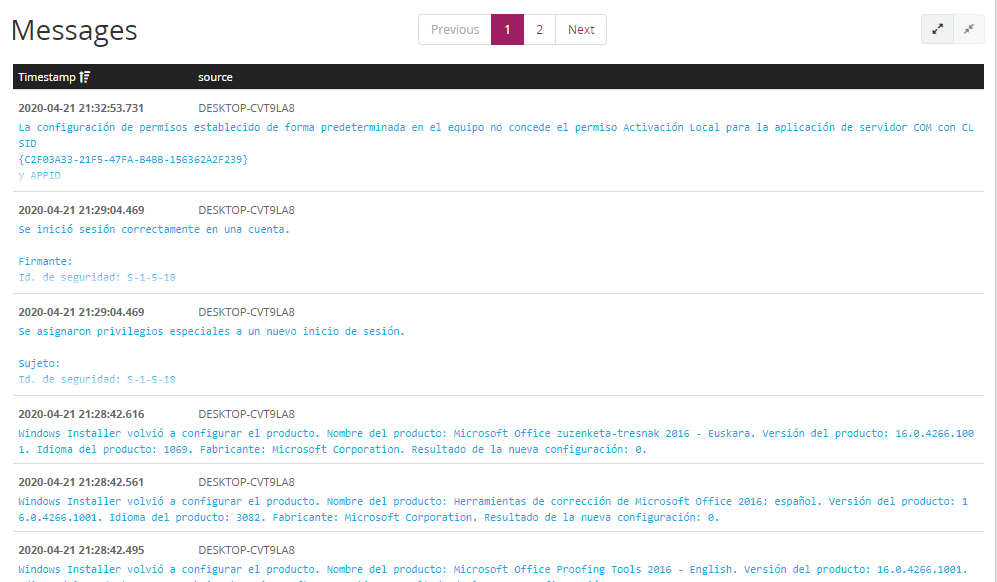


Desde este Dashboard podemos visualizar y realizar siguientes acciones:

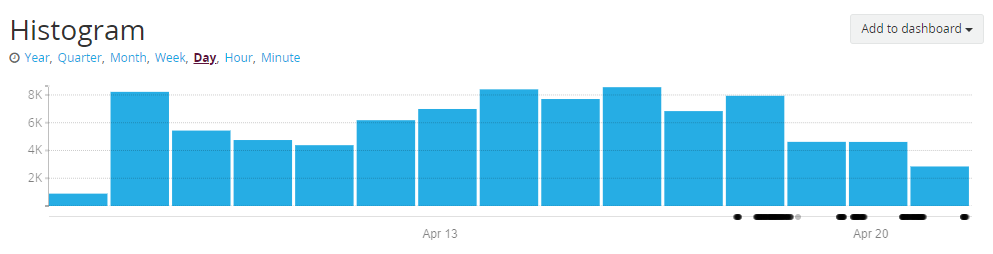
1. Busqueda de eventos o logs (Type your search…..)



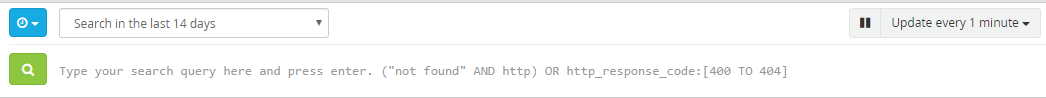
1. Visualizacion de los distintos mensajes (Messages)



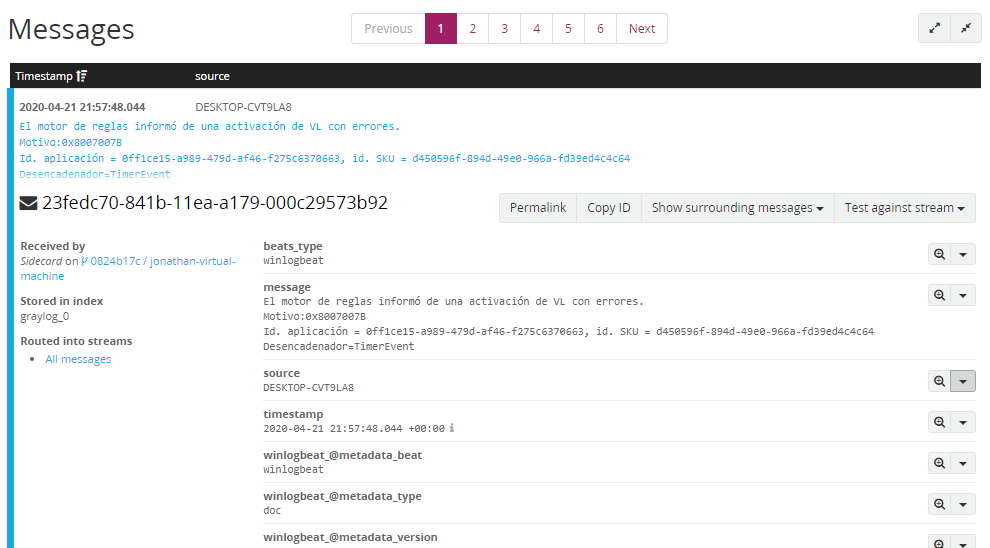
1. Peak de eventos (Histogram)



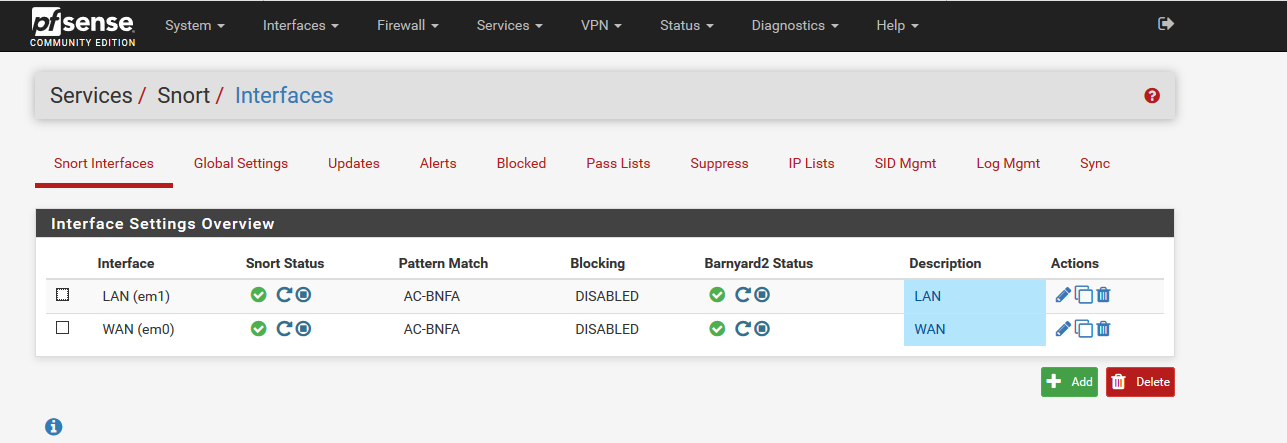
1. Busqueda historica e en tiempo real (Search in the last….)



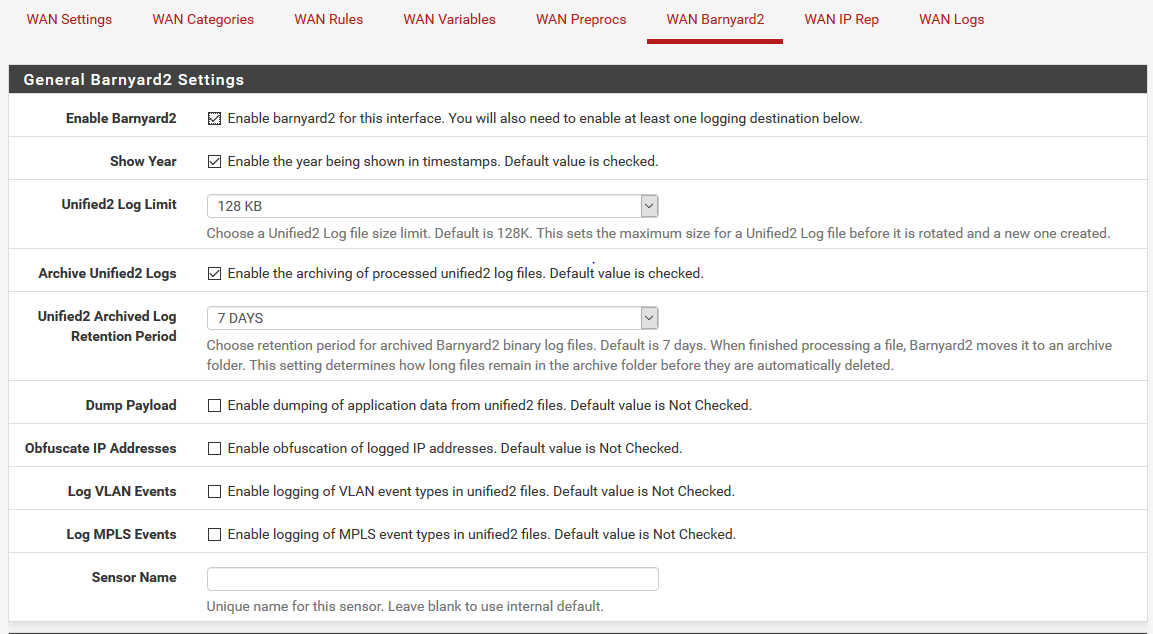
1. Despliegue en detalle de los distintos eventos (Click en messages)

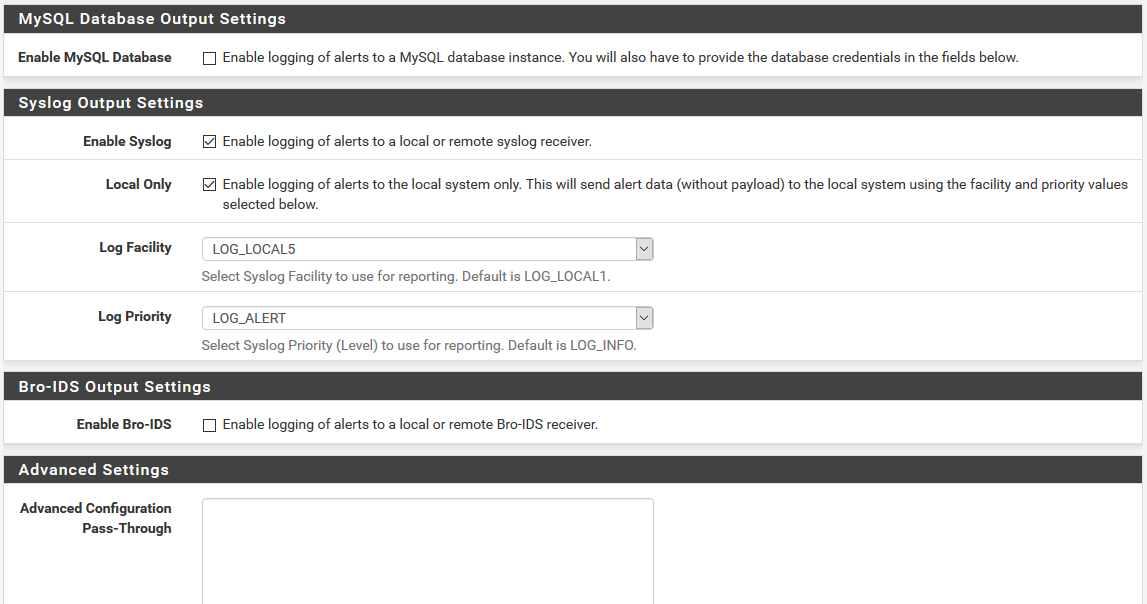


1. Para cargar reglas Snort a pf Sense, nos dirgimos al siguiente menu

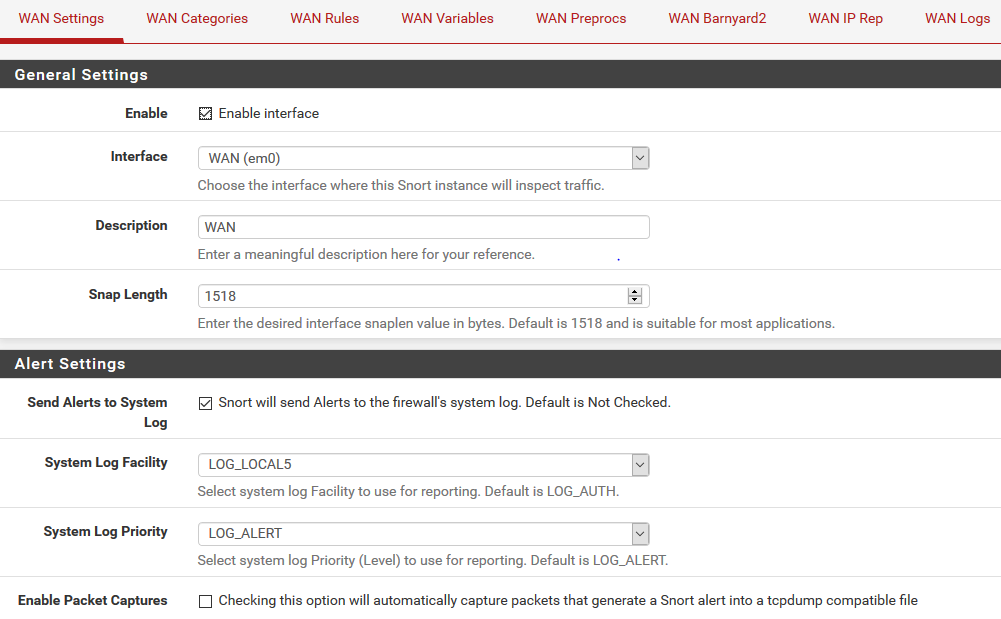


Seleccionamos WAN Barnyard2 y siguiente configuración:

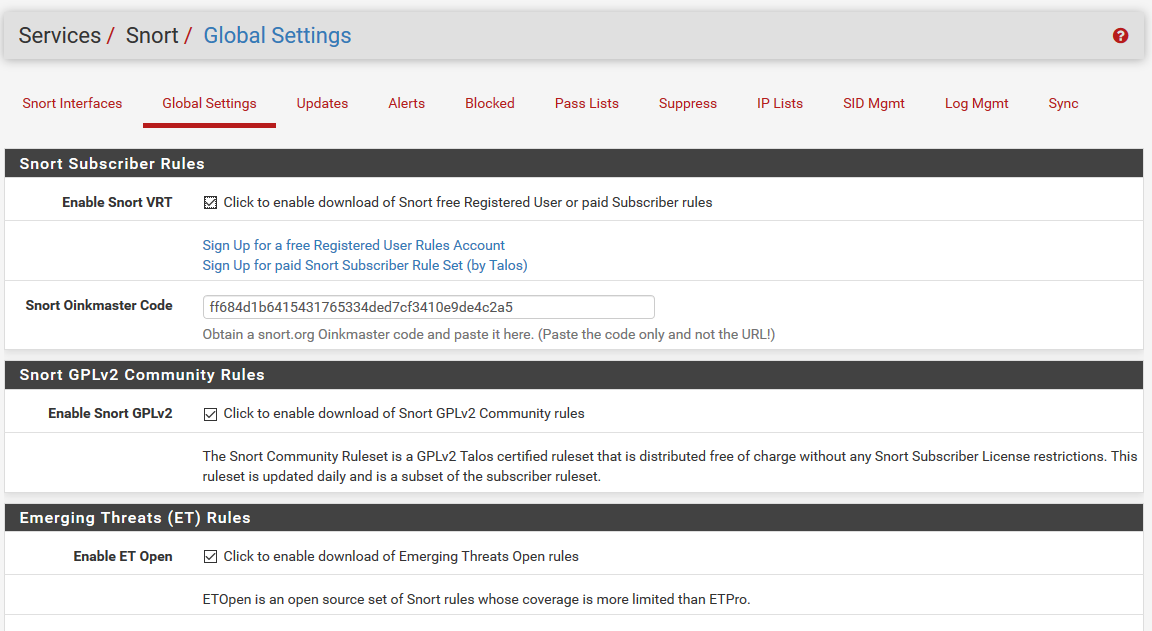




Vamos a WAN Settings y realizamos siguiete configuración.

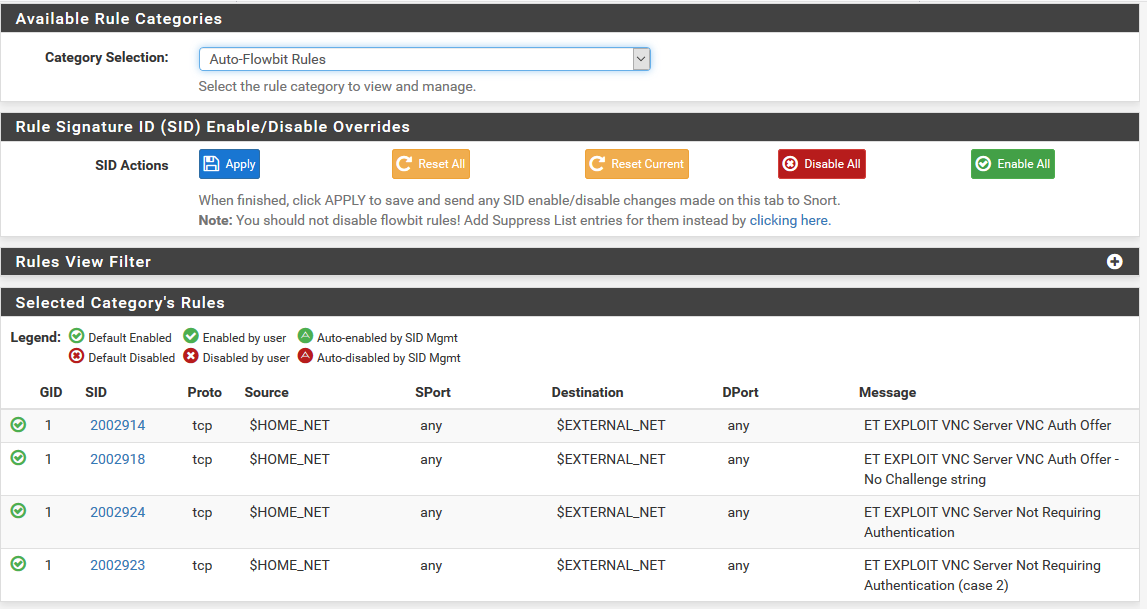


Luego al menu de “Global Settings”



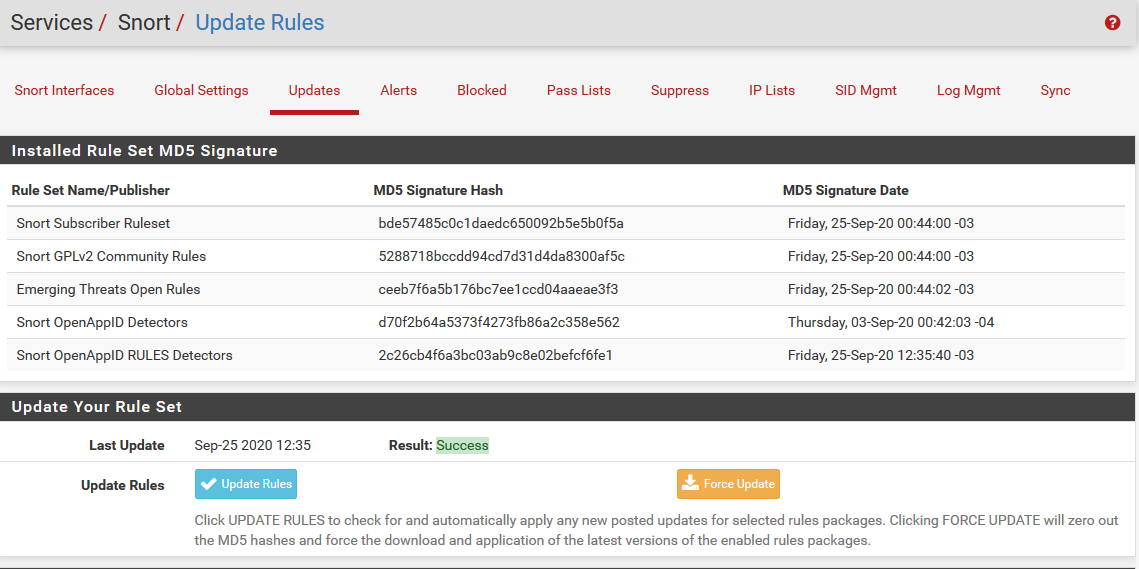
Ahí se nos solicitara un codigo “oinkmaster”, el cual getionar a través de el link adjunto.

Luego vamos a WAN rules



Son bastantes y variadas las reglas Snort que se nos presentan.

Vamos a Update rule, aquí podemos ver las actualizaciones de las reglas



1. Dentro de Graylog esta creado un “Panel”, el cual muestra todos los eventos gatillados de posibles amenazas, las cuales han sido enviadas por pf Sense.