BLUE TEAM

> UTM <

Configuración de la máquina virtual:

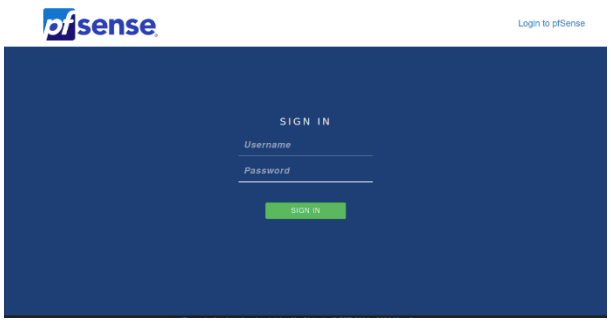
- BSD
- FreeBSD 64 bits
- RAM 2Gb
- Crear disco nuevo
- HDD 20 Gb
- Seleccionar el disco de instalación del firewall (pfSense en este caso)
- Configurar 3 redes:
    - Adaptador puente, conexión internet
    - Red interna, IT
    - Red interna, DMZ

Instalación de pfSense:

- Install
- Configuración del teclado
- Partición del disco > ZFS
- Opciones de configuración > Install
- Tipo de disco > stripe
- Espacio para seleccionar el disco a utilizar
- Aviso de formateo del disco > YES
- Reboot
- Deja que se reinicie, después desmontar la imagen del disco y resetear la maquina

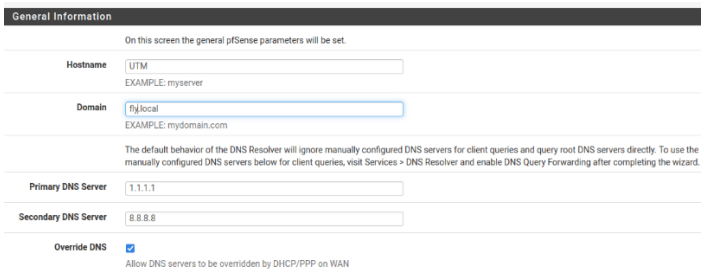
Configuración pfSense

Configurar la red de otra maquina a la Red interna – IT. Desde esa maquina abrir el navegador y acceder a pfSense en la IP **192.168.1.1**



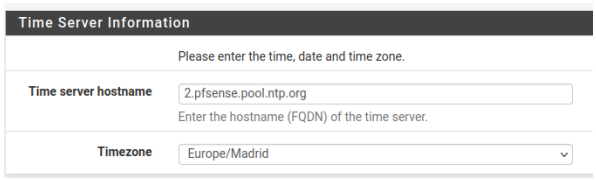
Iniciar sesión con **admin/pfsense**.

Establecer nombre del host, dominio y servidores dns.

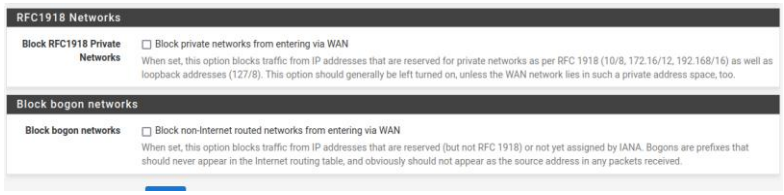


DNS 1.1.1.1 de cloudfare y 8.8.8.8 de Google.

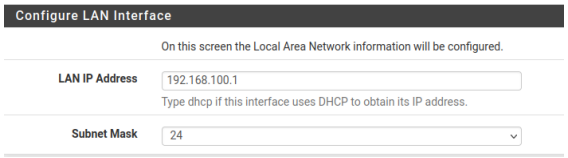
Establecer zona horaria.



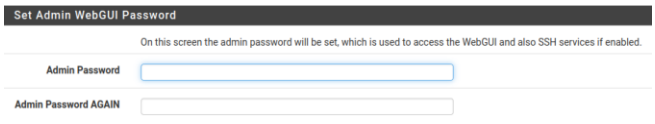
Configuración WAN > DHCP. Desbloquear opciones de RFC1918 y bogon.



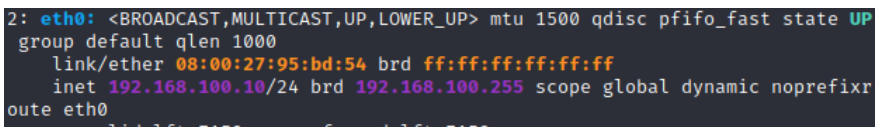
Establecer IP, diferente a la local para que no haya problemas.



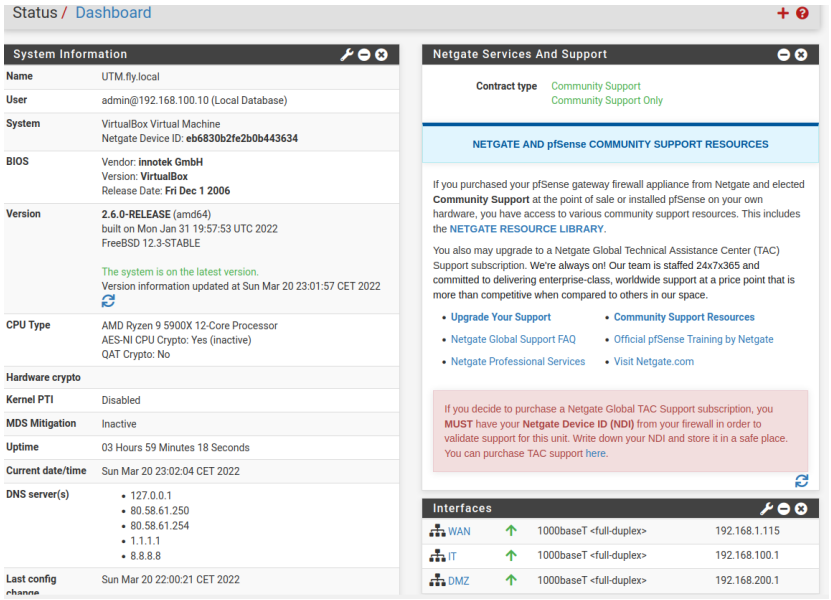
Establecer nueva contraseña.



Comprobar que tenemos la nueva IP.

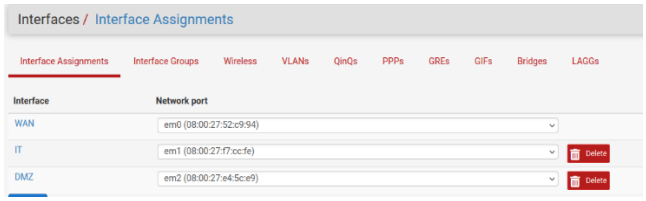


Acceder con las nuevas credenciales e IP.



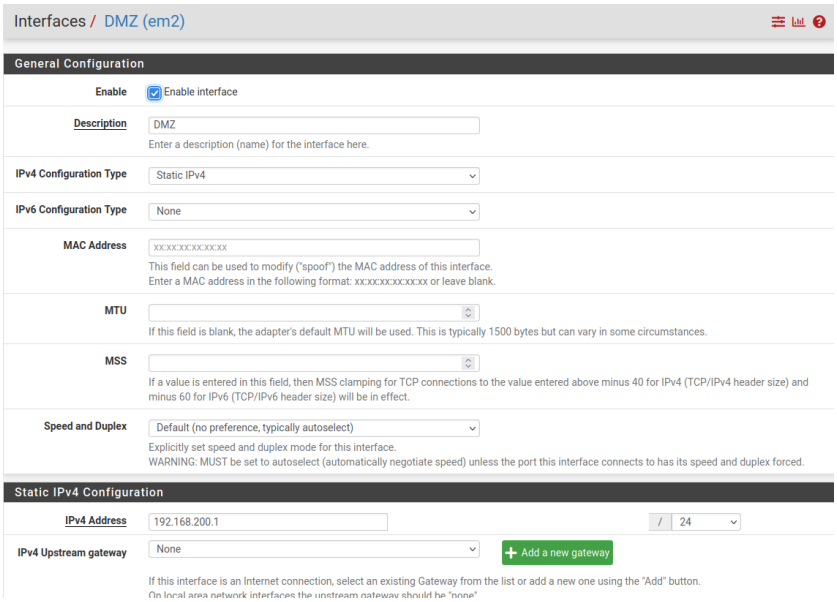
Interfaces > Assignments. Renombrar LAN a IT.

Añadir una nueva red que será para DMZ.



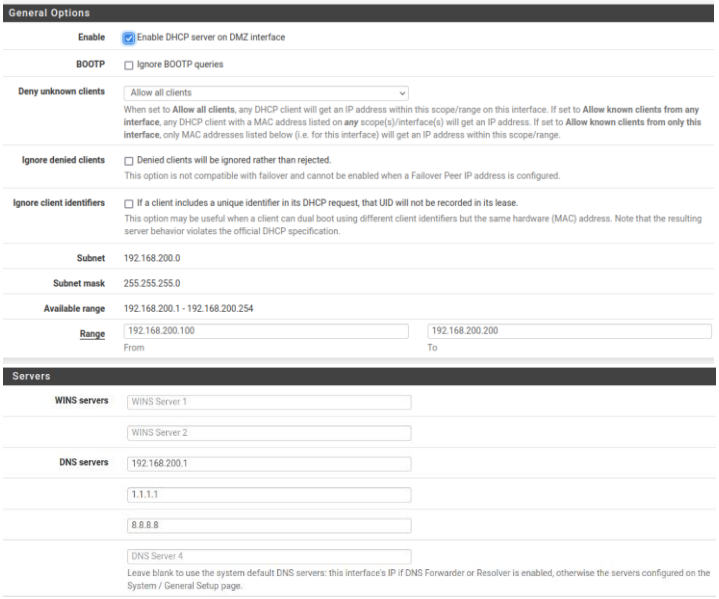
Configuración de la red DMZ:

- IP estatica
- IP6 > None
- Dirección IP > 192.168.200.1/24



Configuración servidor DHCP:

- Rango de IP > 192.168.200.100 – 192.168.200.200
- Servidor DNS > 192.168.200.1 / 1.1.1.1 / 8.8.8.8
- Puerta de enlace > 192.168.200.1



> SURICATA <

Instalación de suricata:

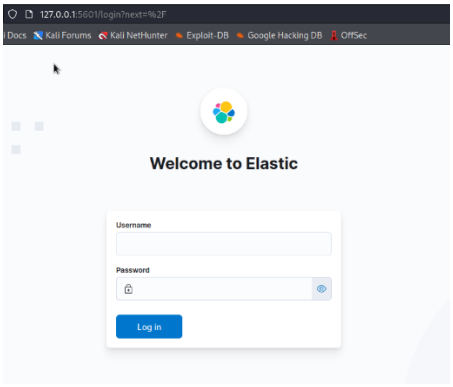
- En la maquina de IT
- sudo apt-get install suricata
- sudo suricata-update (para descargar todas las reglas de suricata)
- Archivo de configuración suricata.yml > /etc/suricata/
- Para crear nuevas reglas, crearlas en /etc/suricata/rules y añadirlas al archivo suricata.yml, en el apartado rule-files.
- Para comprobar el funcionamiento, comprobar los logs con tail -f fast.log y > curl http://testmynids.org/uid/index.html

```
└─$ tail -f fast.log
03/19/2022-20:20:20.947422  [**] [1:2022973:1] ET POLICY Possible Kali Linux
hostname in DHCP Request Packet [**] [Classification: Potential Corporate Pri
vacy Violation] [Priority: 1] {UDP} 192.168.100.10:68 → 192.168.100.1:67
03/19/2022-20:48:22.124584  [**] [1:2013028:6] ET POLICY curl User-Agent Outb
ound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 19
2.168.100.10:47720 → 13.224.106.44:80
03/19/2022-20:48:22.133338  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check r
eturned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TC
```

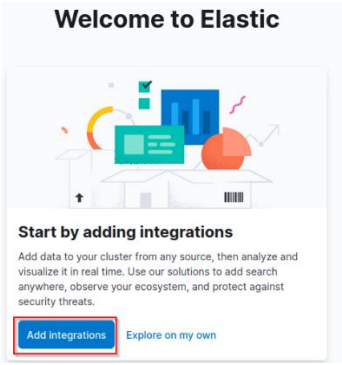
> ELASTICSEARCH <

Instalación de elasticsearch:

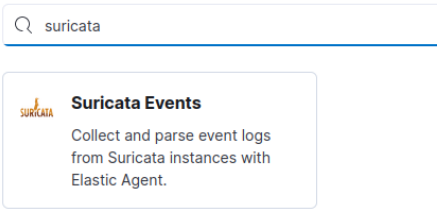
- En la maquina DMZ
- Requiere tener Docker instalado
- sudo git clone https://github.com/deviantony/docker-elk
- Desde la carpeta Docker-elk > Docker-compose up, para montar la app.
- Acceder desde el navegador > 127.0.0.1:5601 (puerto de elastichsearch)



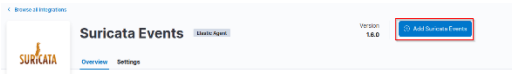
- Credenciales por defecto **elastic/ghangeme**
- Una vez logeado, seleccionar añadir integración.



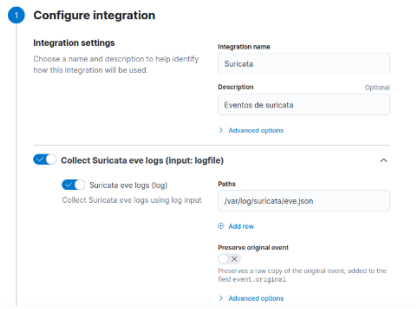
- Utilizar el buscador para encontrar la integración de suricata.



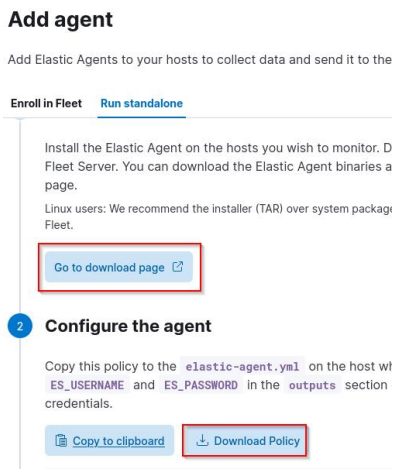
- Añadir eventos.



- Introducir opciones y los logs a recolectar.



- Configurar el agente para el host:
    - Seleccionar configuración individual.
    - Descargar el agente y la política de los enlaces correspondientes en el host de suricata.



- Descomprimir el agente.
- Al estar utilizando otro equipo, copiar el contenido de la política con la opción “Copy to clipboard” y crea el archivo de manera manual en el host. Cambiar las credenciales user y paswword del archivo por las de incio de sesión en elasticsearch.
- Copiar el archivo .yml dentro de la carpeta del agente.
- Ejecutar el agente > sudo ./elastic-agent install. (no instalar en modo Fleet)

```
└─$ sudo ./elastic-agent install
[sudo] password for kali:
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a servi
ce. Do you want to continue? [Y/n]:y
Do you want to enroll this Agent into Fleet? [Y/n]:n
Elastic Agent has been successfully installed.
```

- Una vez instalado todo, desde la maquina de elasticsearch, mostrara los eventos.