

# BLUE TEAM

## > UTM <

Configuración de la máquina virtual:

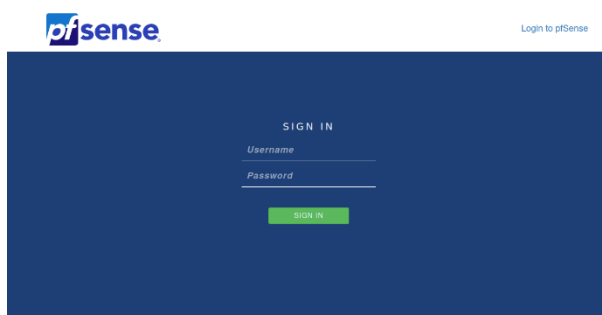
- BSD
- FreeBSD 64 bits
- RAM 2Gb
- Crear disco nuevo
- HDD 20 Gb
- Seleccionar el disco de instalación del firewall (pfSense en este caso)
- Configurar 3 redes:
  - Adaptador puente, conexión internet
  - Red interna, IT
  - Red interna, DMZ

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.

**General Information**

On this screen the general pfSense parameters will be set.

Hostname:   
EXAMPLE: myserver

Domain:   
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server:

Secondary DNS Server:

Override DNS: ☒  
Allow DNS servers to be overridden by DHCP/PPP on WAN

DNS 1.1.1.1 de cloudfare y 8.8.8.8 de Google.

Establecer zona horaria.

**Time Server Information**

Please enter the time, date and time zone.

Time server hostname:   
Enter the hostname (FQDN) of the time server.

Timezone:

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

**RFC1918 Networks**

Block RFC1918 Private Networks: ☐ Block private networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

**Block bogon networks**

Block bogon networks: ☐ Block non-Internet routed networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

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

**Configure LAN Interface**

On this screen the Local Area Network information will be configured.

LAN IP Address:   
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask:

Establecer nueva contraseña.

**Set Admin WebGUI Password**

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password:

Admin Password AGAIN:

Comprobar que tenemos la nueva IP.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:95:bd:54 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.10/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
```

Acceder con las nuevas credenciales e IP.

Status / Dashboard

System Information

Name

UTM.fly.local

User

admin@192.168.100.10 (Local Database)

System

VirtualBox Virtual Machine  
Netgate Device ID: eb6830b2fe2b0b443634

BIOS

Vendor: innotek GmbH  
Version: VirtualBox  
Release Date: Fri Dec 1 2006

Version

2.6.0-RELEASE (amd64)  
built on Mon Jan 31 19:57:53 UTC 2022  
FreeBSD 12.3-STABLE  

The system is on the latest version.  
Version information updated at Sun Mar 20 23:01:57 CET 2022

CPU Type

AMD Ryzen 9 5900X 12-Core Processor  
AES-NI CPU Crypto: Yes (inactive)  
QAT Crypto: No

Hardware crypto

Kernel PTI

Disabled

MDS Mitigation

Inactive

Uptime

03 Hours 59 Minutes 18 Seconds

Current date/time

Sun Mar 20 23:02:04 CET 2022

DNS server(s)

• 127.0.0.1

• 80.58.61.250

• 80.58.61.254

• 1.1.1.1

• 8.8.8.8

Last config

Sun Mar 20 22:00:21 CET 2022

Netgate Services And Support

Contract type

Community Support  
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

• Upgrade Your Support

• Community Support Resources

• Netgate Global Support FAQ

• Official pfSense Training by Netgate

• Netgate Professional Services

• Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support [here](#).

Interfaces

WAN

1000baseT <full-duplex>

192.168.1.115

IT

1000baseT <full-duplex>

192.168.100.1

DMZ

1000baseT <full-duplex>

192.168.200.1

Interfaces > Assignments. Renombrar LAN a IT.

Añadir una nueva red que será para DMZ.

Interfaces / Interface Assignments

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

Interface

Network port

WAN

em0 (08:00:27:52:c9:94)

IT

em1 (08:00:27:f7:cc:fe) 

Delete

DMZ

em2 (08:00:27:e4:5c:e9) 

Delete

Configuración de la red DMZ:

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

Interfaces / DMZ (em2)

General Configuration

Enable ☒ Enable interface

Description

DMZ

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xxxxxxxxxxxx

This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxxxxxxxxx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address

192.168.200.1

/ 24

IPv4 Upstream gateway

None

+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none"

## 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

General Options

Enable ☒ Enable DHCP server on DMZ interface

BOOTP

☐ Ignore BOOTP queries

Deny unknown clients

Allow all clients

When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients

☐ Denied clients will be ignored rather than rejected.

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers

☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet

192.168.200.0

Subnet mask

255.255.255.0

Available range

192.168.200.1 - 192.168.200.254

Range

192.168.200.100

192.168.200.200

From To

Servers

WINS servers

WINS Server 1

WINS Server 2

DNS servers

192.168.200.1

1.1.1.1

8.8.8.8

DNS Server 4

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

## > SURICATA <

Instalación de suricata:

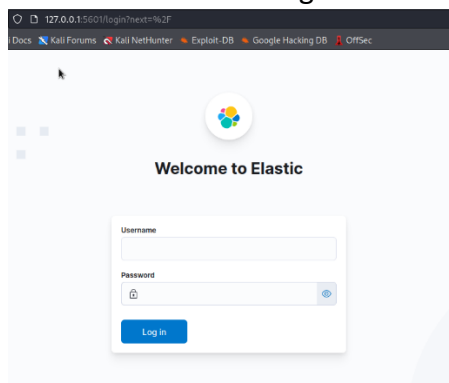
- En la maquina de IT
- `sudo apt-get install suricata`
- `sudo suricata-update` (para descargar todas las reglas de suricata)
- Archivo de configuración `suricata.yml` > `/etc/suricata/`
- Para crear nuevas reglas, crearlas en `/etc/suricata/rules` y añadirlas al archivo `suricata.yml`, en el apartado `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
```

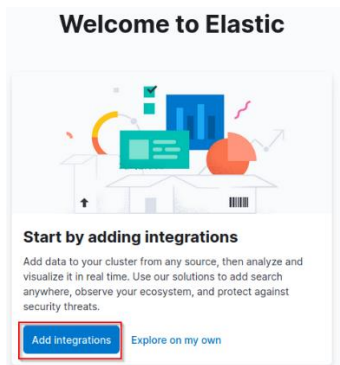
## > ELASTICSEARCH <

Instalación de elasticsearch:

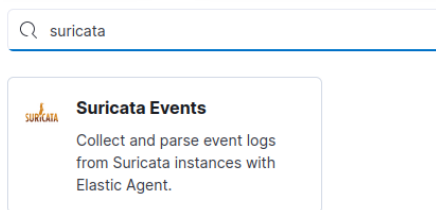
- En la maquina DMZ
- Requiere tener Docker instalado
- `sudo git clone https://github.com/deviantony/docker-elk`
- Desde la carpeta `Docker-elk` > `Docker-compose up`, para montar la app.
- Acceder desde el navegador > `127.0.0.1:5601` (puerto de elasticsearch)



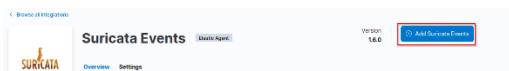
- Credenciales por defecto **elastic/ghangeme**
- Una vez logeado, seleccionar añadir integración.



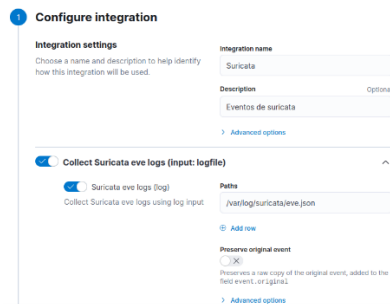
- Utilizar el buscador para encontrar la integración de suricata.



- 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.

## Add agent

Add Elastic Agents to your hosts to collect data and send it to the

Enroll in Fleet **Run standalone**

Install the Elastic Agent on the hosts you wish to monitor. Download the Elastic Agent binaries from the Elastic Agent download page.

Linux users: We recommend the installer (TAR) over system packages.

[Go to download page](#)

### 2 Configure the agent

Copy this policy to the `elastic-agent.yml` on the host with the `ES_USERNAME` and `ES_PASSWORD` in the `outputs` section.

[Copy to clipboard](#)

[Download Policy](#)

- 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 password del archivo por las de inicio 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 service. 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 máquina de elasticsearch, mostrara los eventos.

