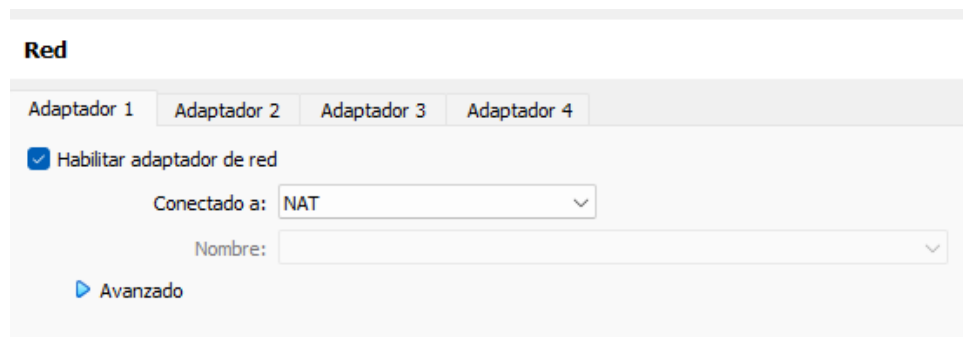


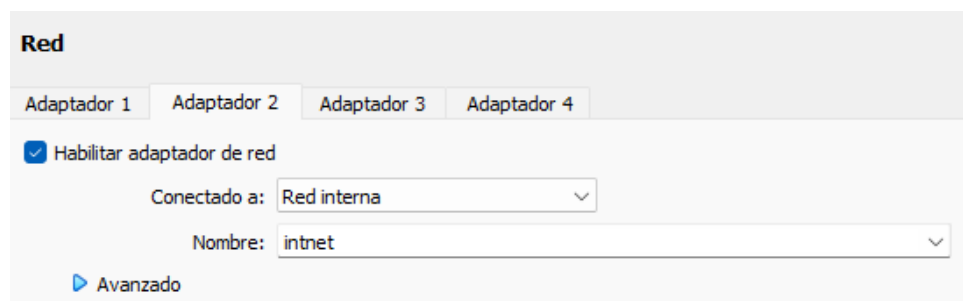
# Lab 3. Bastionado del área perimetral

## CREACION MÁQUINA PFSENSE:

- Lo primero que haremos para iniciar la práctica, será crear la máquina Pfsense. En mi caso la iniciaré desde Virtual Box. Para instalar pfsense tenemos varias opciones. Yo escogeré la del repositorio de GitHub.  
[https://github.com/CloudSentralDotNet/iso\\_pfsense/releases](https://github.com/CloudSentralDotNet/iso_pfsense/releases)
- Una vez creada la máquina, editaremos la configuración de red. En este caso habilitamos dos adaptadores una en NAT y otra en red interna. Como se ve en las siguientes fotos:



The screenshot shows the 'Red' (Network) configuration window for a virtual machine. At the top, there are four tabs: 'Adaptador 1', 'Adaptador 2', 'Adaptador 3', and 'Adaptador 4'. The 'Adaptador 1' tab is selected. Below the tabs, there is a checkbox labeled 'Habilitar adaptador de red' which is checked. Underneath, there is a dropdown menu labeled 'Conectado a:' with 'NAT' selected. Below that is a text field labeled 'Nombre:' which is empty. At the bottom left, there is a blue play button icon followed by the text 'Avanzado'.



The screenshot shows the 'Red' (Network) configuration window for a virtual machine. At the top, there are four tabs: 'Adaptador 1', 'Adaptador 2', 'Adaptador 3', and 'Adaptador 4'. The 'Adaptador 2' tab is selected. Below the tabs, there is a checkbox labeled 'Habilitar adaptador de red' which is checked. Underneath, there is a dropdown menu labeled 'Conectado a:' with 'Red interna' selected. Below that is a text field labeled 'Nombre:' with 'intnet' entered. At the bottom left, there is a blue play button icon followed by the text 'Avanzado'.

- Cuando este todo listo, iniciaremos la máquina y seguiremos los pasos de la instalación de la máquina. Virtual box tiene la peculiaridad de que una vez instalado la máquina, hay que quitar el archivo iso ya que eso solo sirve para la instalación. Nos tendría que quedar algo como esto:

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 4f21ade07711a06ba6a3

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

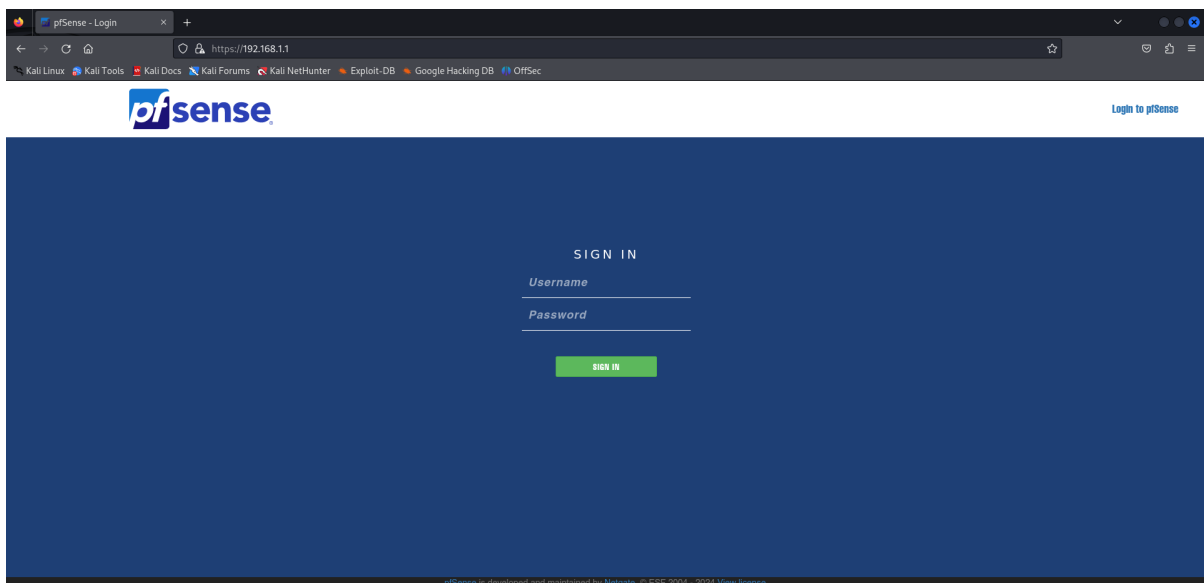
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 

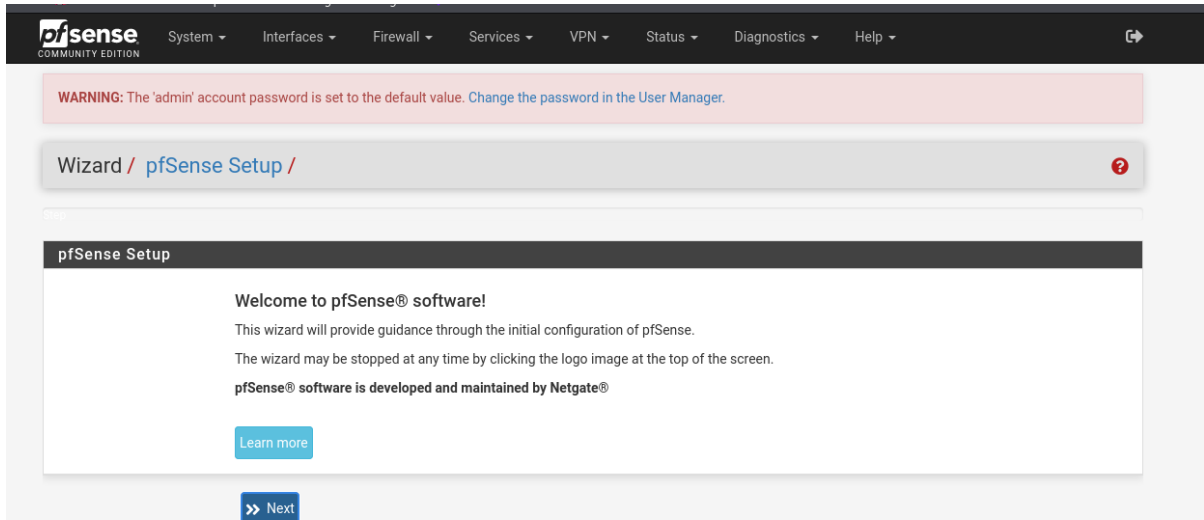
```

- A continuación, nos meteremos a una máquina en la que configuraremos la red interna como hemos hecho en la máquina Pfsense y nos meteremos a la ip de la red interna desde firefox por ejemplo

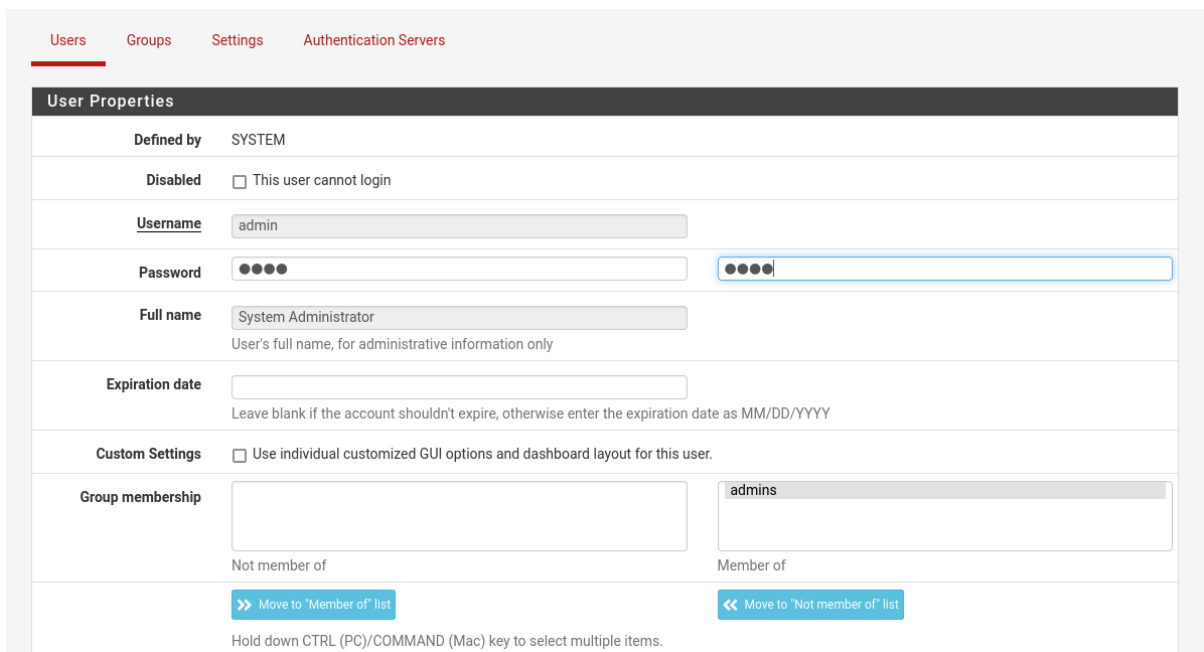


- Nos saldría la interfaz de pfsense donde tenemos que poner las credenciales por defecto.



- Usuario: admin
- Contraseña: pfsense



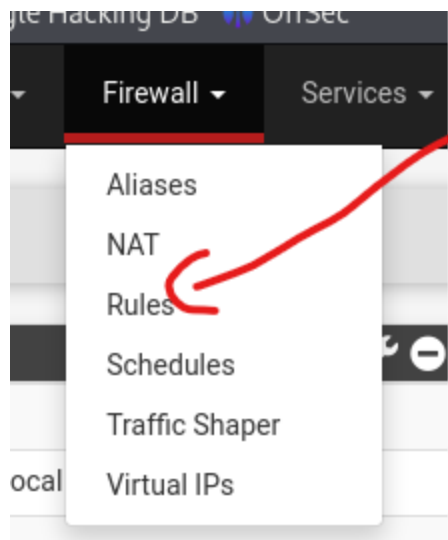
- Esto sería el set up por defecto y lo tendremos que configurar como lo ha hecho la máquina. Lo primero que haremos será cambiar la contraseña de administrador.



- Si no tenemos configuradas las interfaces, las configuraremos. En mi caso ya las tengo configuradas. Tendría que salir algo como esto:

Interfaces <span>🔧 - ✕</span>			
 WAN	↑	1000baseT <full-duplex>	10.0.2.15
 LAN	↑	1000baseT <full-duplex>	192.168.1.1

- Ahora configuraremos el firewall que se encuentra en la pestaña Firewall/Rules



- Como se puede ver en la siguiente imagen nos saldrán una serie de apartados. Donde tendremos que configurarlos. Añadiremos esta serie de reglas:
  - LAN:
    - Action: Pass
    - Source: Lan net
    - Destination: Wan net
    - Protocol: Any

Firewall / Rules / Edit

### Edit Firewall Rule

**Action** Pass  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** WAN  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** Any  
Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match LAN net Source Address /

**Destination**

**Destination** ☐ Invert match WAN net Destination Address /

- WAN:
  - Action: Pass
  - Source: Lan net
  - Destination: Wan net
  - Protocol: Any

**Edit Firewall Rule**

**Action** Pass  
 Choose what to do with packets that match the criteria specified below.  
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
 Set this option to disable this rule without removing it from the list.

**Interface** WAN  
 Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
 Select the Internet Protocol version this rule applies to.

**Protocol** TCP  
 Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match any Source Address /   
Display Advanced  
 The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

**Destination**

**Destination** ☐ Invert match WAN address Destination Address /

**Destination Port Range** (other)  (other)   
 From Custom To Custom  
 Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

- Añadiremos una regla aparte en la WAN para bloquear todo el tráfico

**Edit Firewall Rule**

**Action** Block  
 Choose what to do with packets that match the criteria specified below.  
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
 Set this option to disable this rule without removing it from the list.

**Interface** WAN  
 Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
 Select the Internet Protocol version this rule applies to.

**Protocol** Any  
 Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match any Source Address /

**Destination**

**Destination** ☐ Invert match any Destination Address /

**Extra Options**

**Log** ☐ Log packets that are handled by this rule  
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description** block traffic  
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

- Aplicamos los cambios y nos saldrá este mensaje:

The changes have been applied successfully. The firewall rules are now reloading in the background.  
[Monitor](#) the filter reload progress.

## SURICATA:

- Instalaremos suricata en el ubuntu server. Yo ya tengo un ubuntu server de una práctica anterior así que la reutilizaré. Para instalar suricata se utiliza este comando:

```
sudo apt-get install suricata
```

## WAZUH:

- Volveremos a instalar un ubuntu server nuevo que contenga el servidor Wazuh. Las especificaciones de Wazuh serán las mismas que para el servidor de Suricata.
- Añadiremos un repositorio con este comando:

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

```
wazuh-install.sh
root@alvaro:/home/alvaro# bash ./wazuh-install.sh -a
23/10/2024 18:13:58 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.1
23/10/2024 18:13:58 INFO: Verbose logging redirected to /var/log/wazuh-install.log
23/10/2024 18:14:01 INFO: Verifying that your system meets the recommended minimum hardware requirements.
23/10/2024 18:14:01 INFO: Wazuh web interface port will be 443.
23/10/2024 18:14:07 INFO: --- Dependencies ---
23/10/2024 18:14:07 INFO: Installing apt-transport-https.
23/10/2024 18:14:10 INFO: Installing debhelper.
```

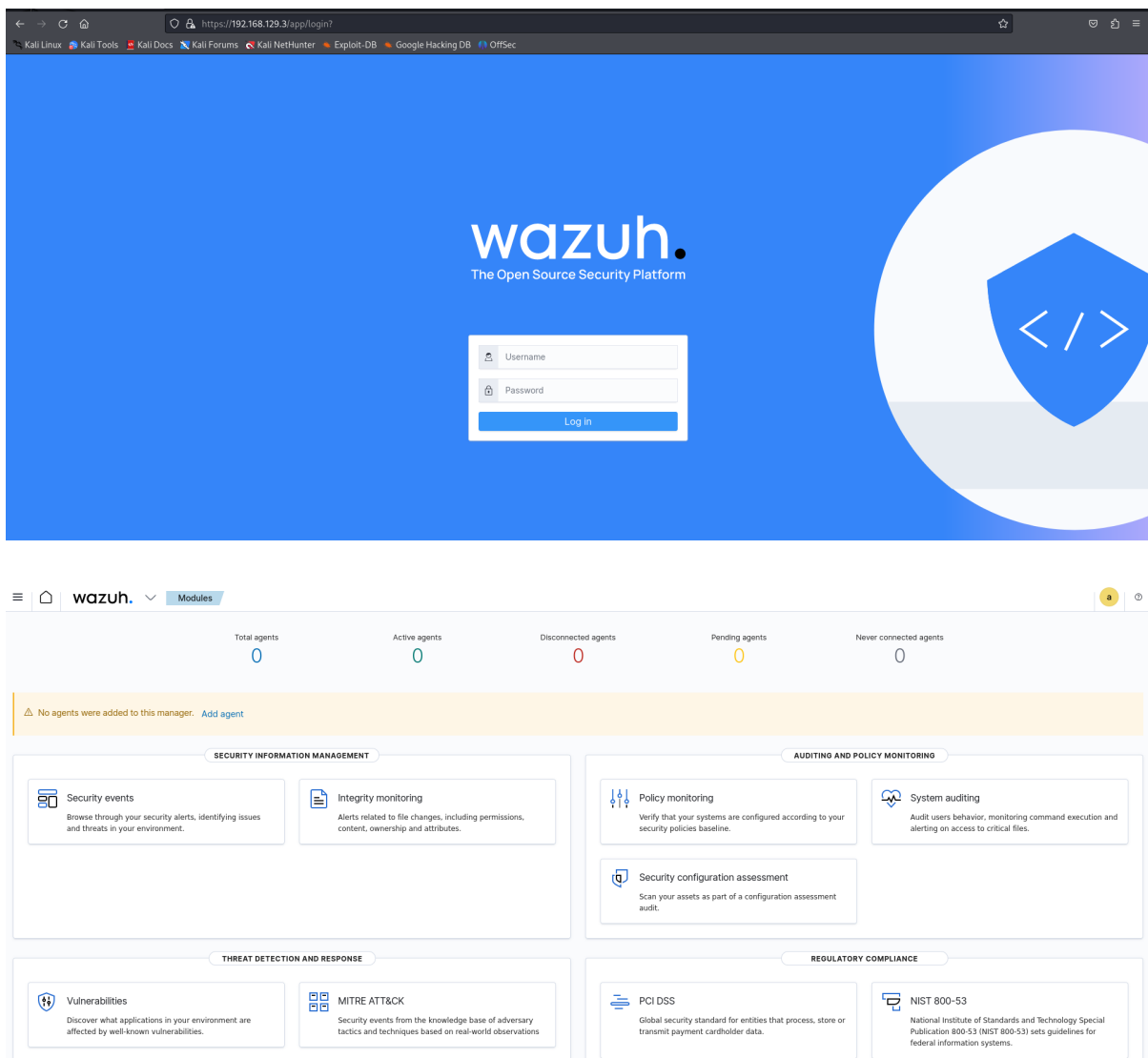
- Una vez creado el repositorio lo instalaremos

```
bash ./wazuh-install.sh
```

- Necesitaremos bastante espacio en el disco duro unos 50 GB. Una vez instalado nos quedaría así

```
23/10/2024 18:50:42 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: nUQ.D.x0+kFfqmayNVcD0sK32rfpSs4K
23/10/2024 18:50:42 INFO: Installation finished.
```

- Usuario: admin
- Contraseña: R10ZtvVTcNbZGLPPwEC2gSK\*4enO?c2y
  - Con Wazuh iniciado, nos meteremos a la IP de nuestro Ubuntu server y podremos ver el panel de inicio de Wazuh





- Ese sería el panel de control de Wazuh
- INSTALACION AGENTES WAZUH
  - Para instalar los agentes de wazuh, nos iremos al apartado que nos sale en la imagen de arriba "New Agent" y procederemos con la instalación

Deploy new agent

1 Select the package to download and install on your system:

**LINUX**

☐ RPM amd64   ☐ RPM aarch64  
☒ DEB amd64   ☐ DEB aarch64

**WINDOWS**

☐ MSI 32/64 bits

**macOS**

☐ Intel  
☐ Apple silicon

[For additional systems and architectures, please check our documentation.](#)

2 Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FDQN).

Assign a server address: [?](#)

Server address

- Para la dirección de servidor, utilizaremos la de wazuh

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FDQN).

Assign a server address: [?](#)

192.168.1.102

- Y para las opciones adicionales añadiremos el nombre de nuestro suricata

✓ **Optional settings:**

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: ?

Suricata

① The agent name must be unique. It can't be changed once the agent has been enrolled. ?

Select one or more existing groups: ?

default × |

- Una vez puesto todo, nos saldrán todos los comandos para poder hacerlo en nuestro suricata. Estos comandos los pegamos en nuestro ubuntu server donde está suricata instalado.

The screenshot shows the Wazuh dashboard interface. At the top, there's a navigation bar with 'wazuh.' and tabs for 'Agents' and 'Suricata'. Below this, there's a 'Modules' dropdown and links for 'Inventory data', 'Stats', and 'Configuration'. The main content area displays the agent's details for 'Suricata' (ID 001). It includes fields for Status (green dot), IP address (192.168.1.103), Version (Wazuh v4.7.5), Groups (default), Operating system (Ubuntu 24.04.1 LTS), and Cluster node (node01). Below these are 'Registration date' and 'Last keep alive' timestamps. The dashboard also features a 'MITRE' section with 'Top Tactics' (Defense Evasion) and a 'Compliance' section with a donut chart showing PCI DSS results (10.6.1 (4) and 10.2.6 (1)). At the bottom, there's a 'FIM: Recent events' table with columns for Time, Path, Action, Rule description, Rule Le..., and Rule id, currently showing 'No recent events'.

- Esto sería el agente instalado y conectado.