

Memoria Ciberseguridad

Evaluación BlueTeam



Nombre del Auditor: Kacper Mariusz Koper Mielczarek

Fecha: 19/01/2025

Índice

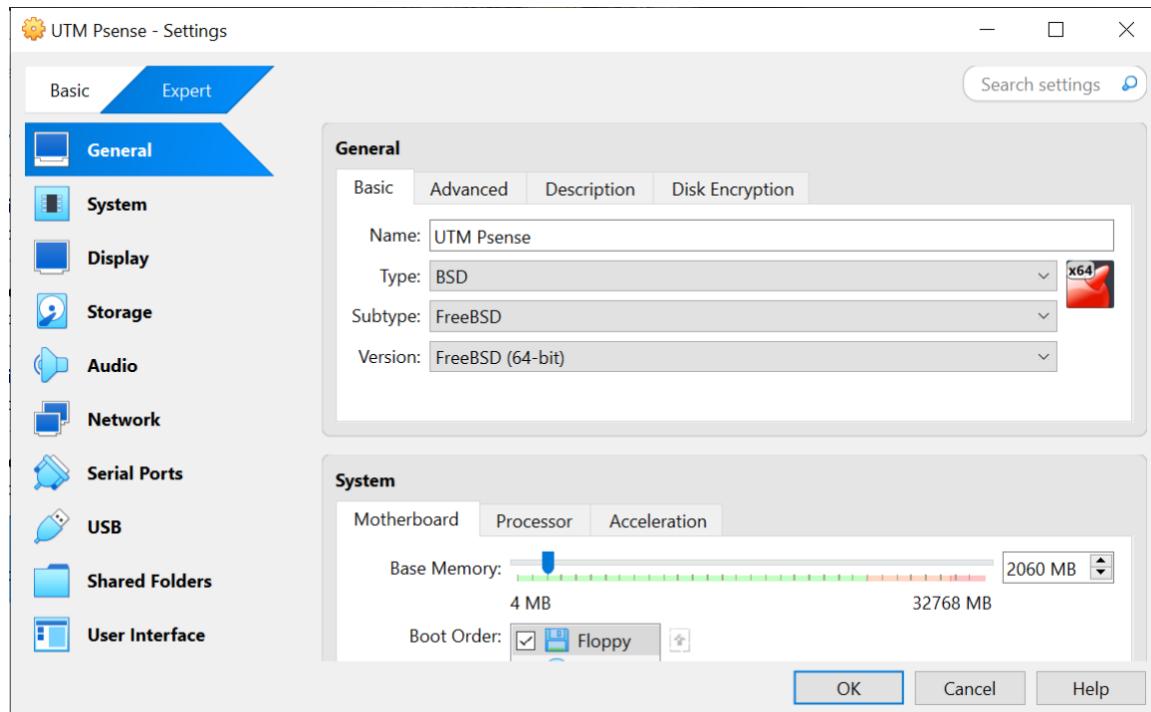
<i>Memoria Ciberseguridad.....</i>	1
1. Instalar y Configurar PfSense.....	3
1.1. Instalación	3
1.2. Configuración.....	18
1.3. IPS y DHCP.....	23
1.3.1. DNS	24
1.3.2. DHCP de la red LAN.....	26
1.3.2. Añadir red DMZ.....	28
1.3.3 Añadir red DMZ2	31
1.3.4 Comprobar redes añadidas	32
1.3.5 Rango DMZ	33
1.3.6 Rango DMZ2	35
1.4. Firewall	37
1.4.1 Alias a puertos	37
1.4.2. Reglas Firewall DMZ	38
1.4.3. Reglas Firewall LAN	44
1.4.4. Reglas firewall DMZ2.....	45
1.4.5. Reglas firewall WAN	49
1.5. Definir IPs estáticas.....	50
1.5.1 DMZ.....	50
1.5.2 DMZ2	52
1.5.3 LAN.....	53
2. Honeypots.....	54
3. Suricata.....	56
4. Elastic.....	67
4.1. Suricata	68
4.2. HoneyPot	86
4.3. Windows	97
5. Propuesta de mejora.....	108

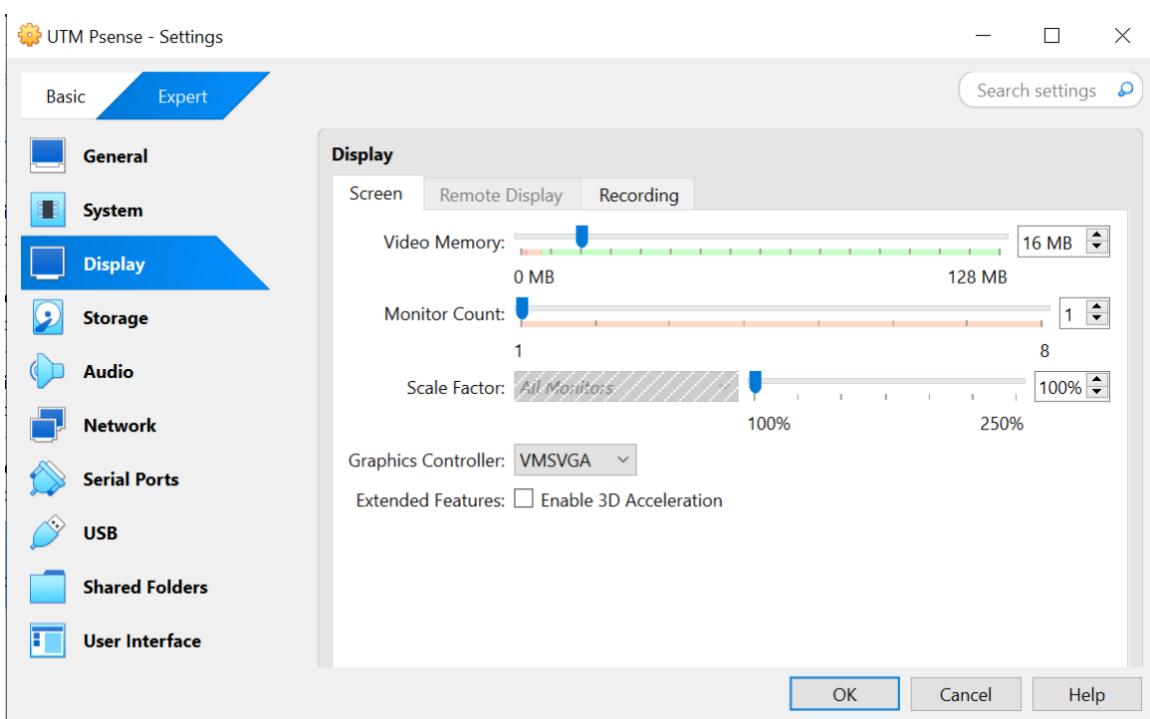
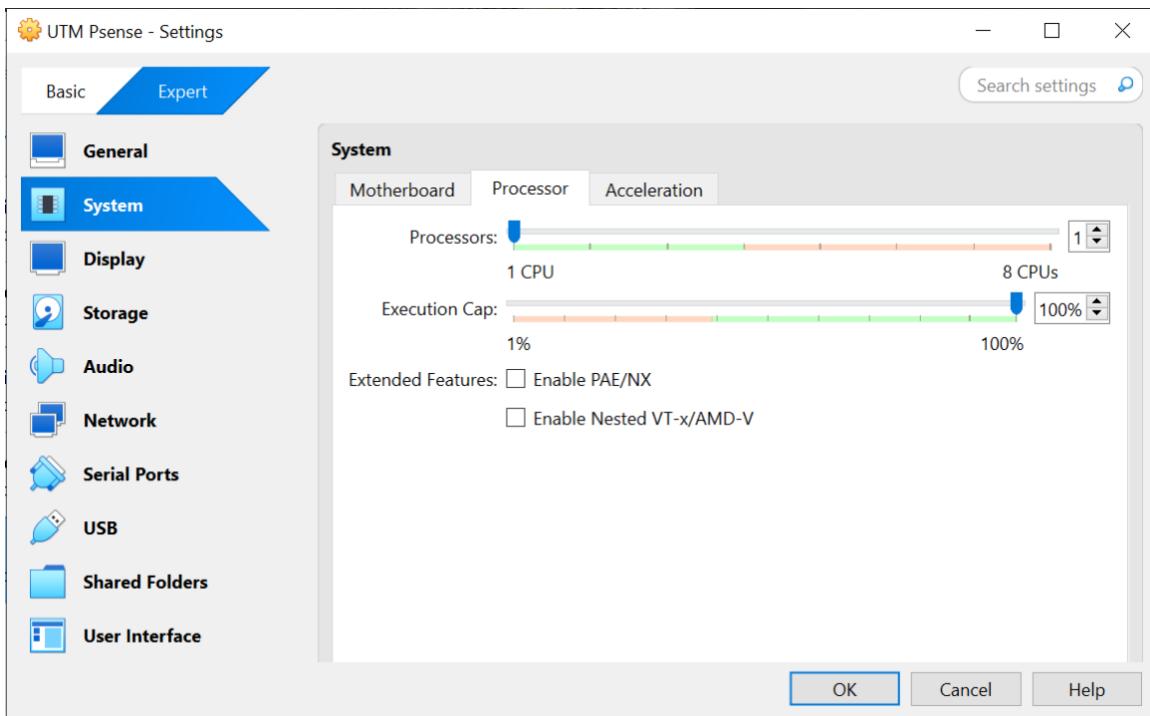
1. Instalar y Configurar PfSense

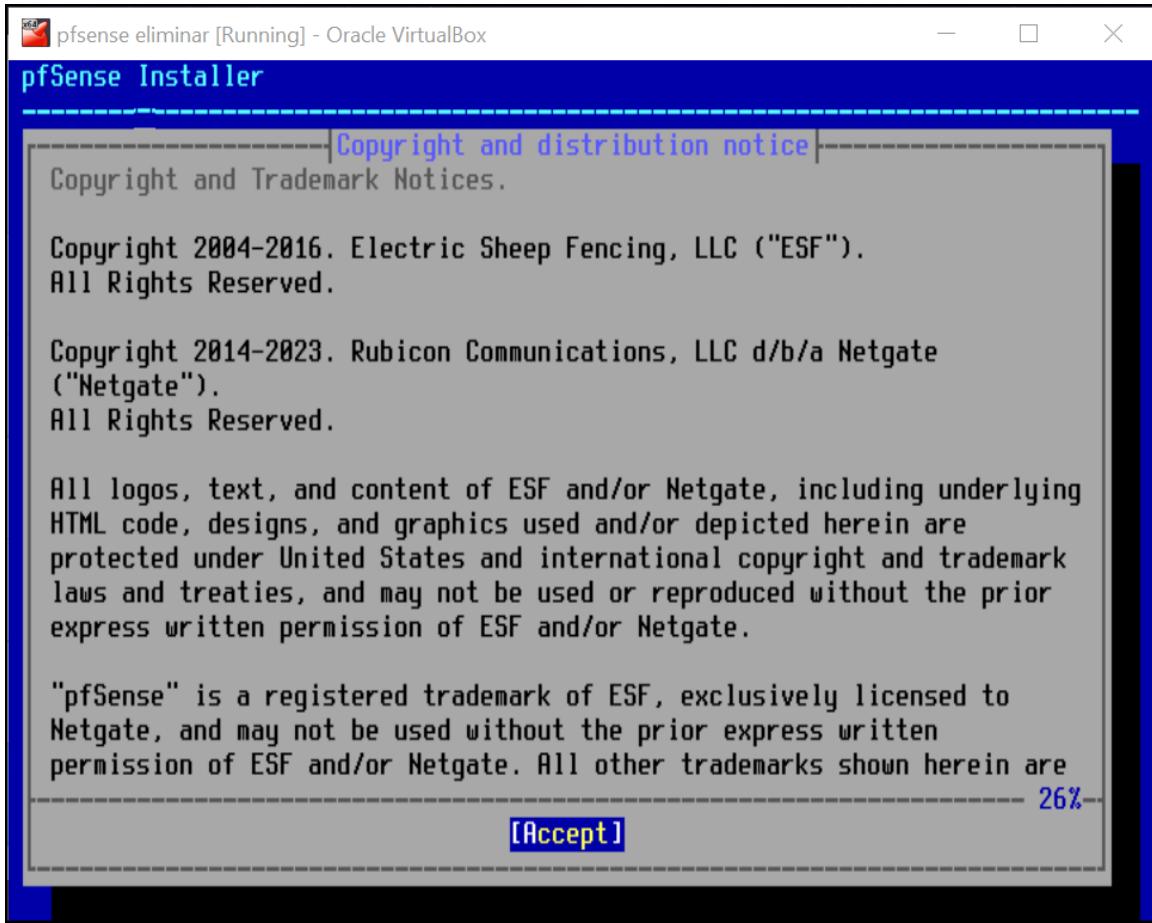
1.1. Instalación

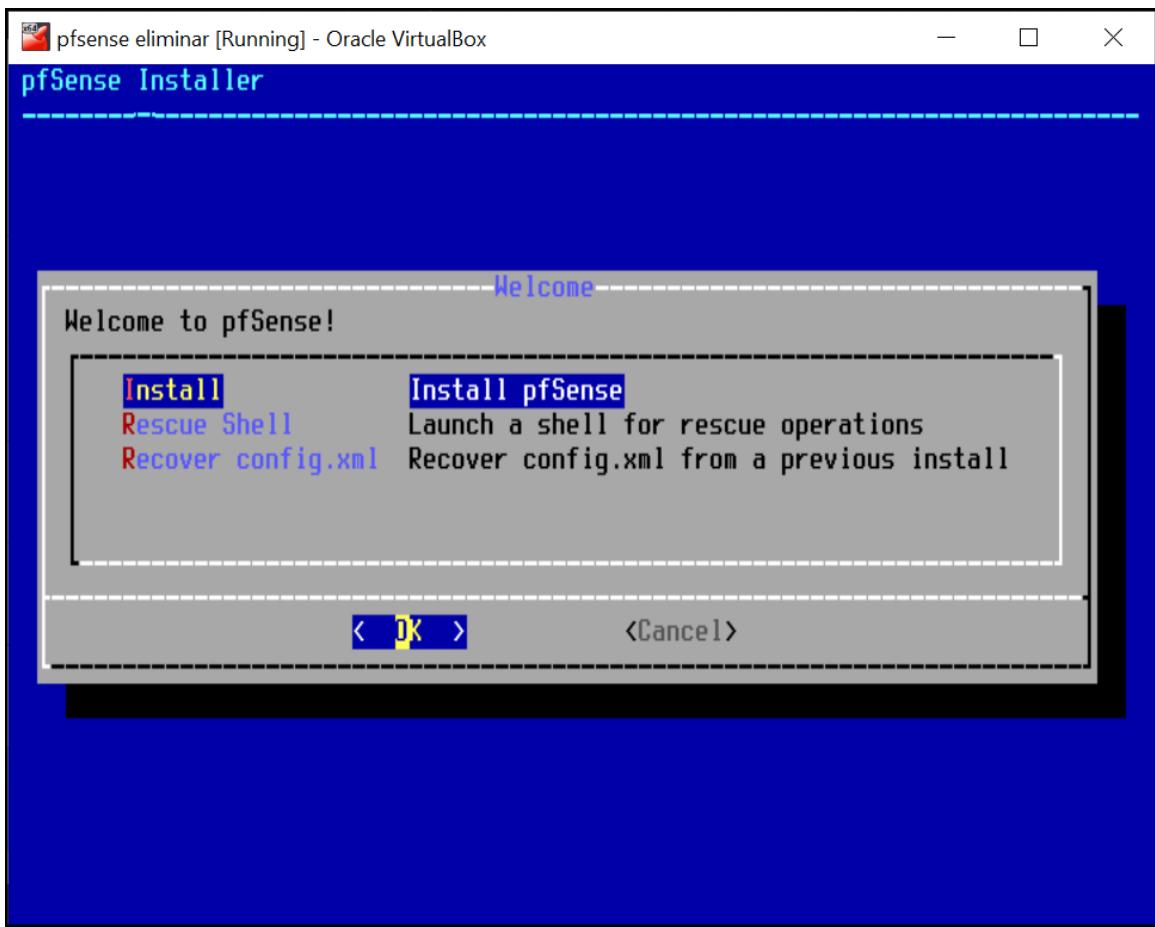
En esta primera etapa de la práctica, se realizó la instalación y configuración inicial de **PfSense**, un sistema UTM (Unified Threat Management) utilizado para gestionar y controlar el tráfico de red de los equipos conectados. Inicialmente, se procedió con la instalación del sistema y la configuración básica, asignando las interfaces correspondientes para las redes internas (**LAN**) y externas (**WAN**). Este proceso permitió establecer los parámetros iniciales para obtener conexión en red.

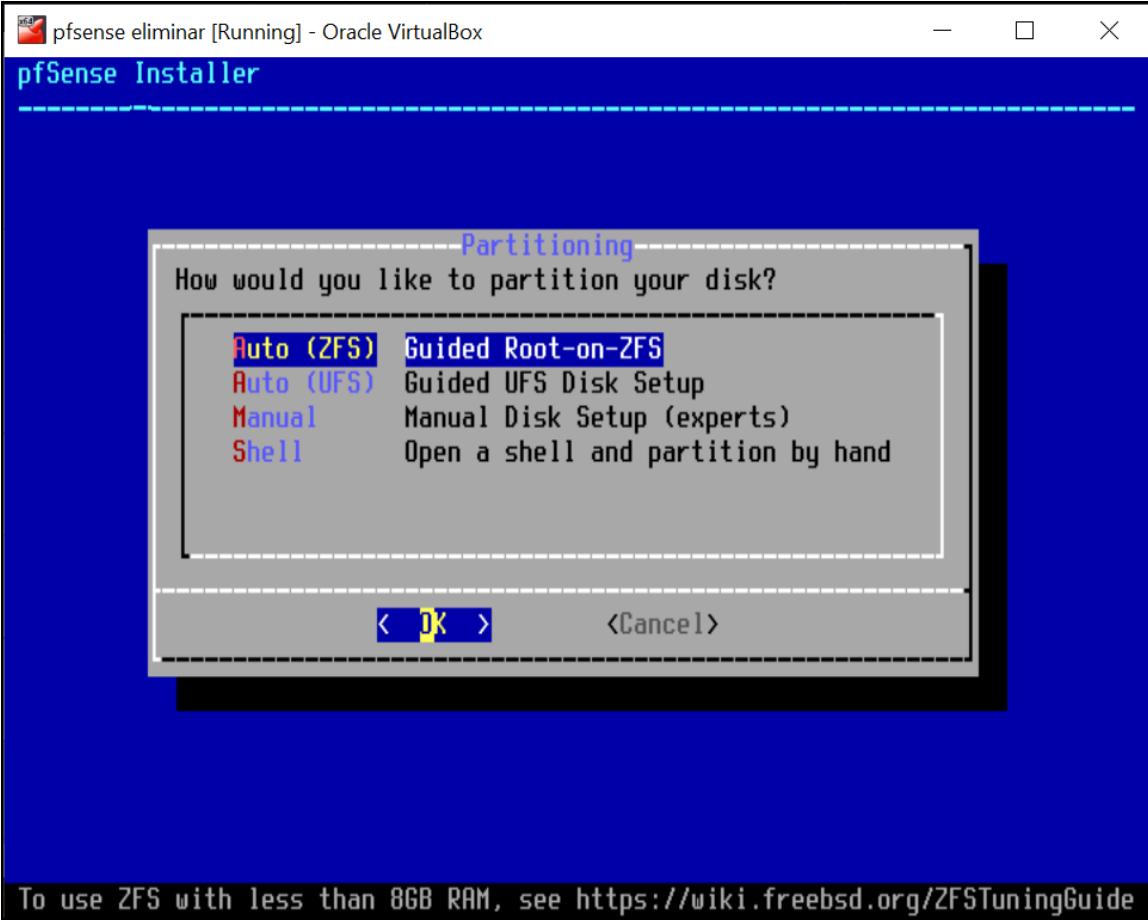
Finalmente, se verificó el correcto funcionamiento de la máquina, comprobando que las interfaces asignadas operan según lo esperado. Se obtuvo con éxito el dato de las direcciones asignadas a la **WAN** y la **LAN**, confirmando que el sistema está preparado para proceder a gestionar las diferentes reglas del PfSense.

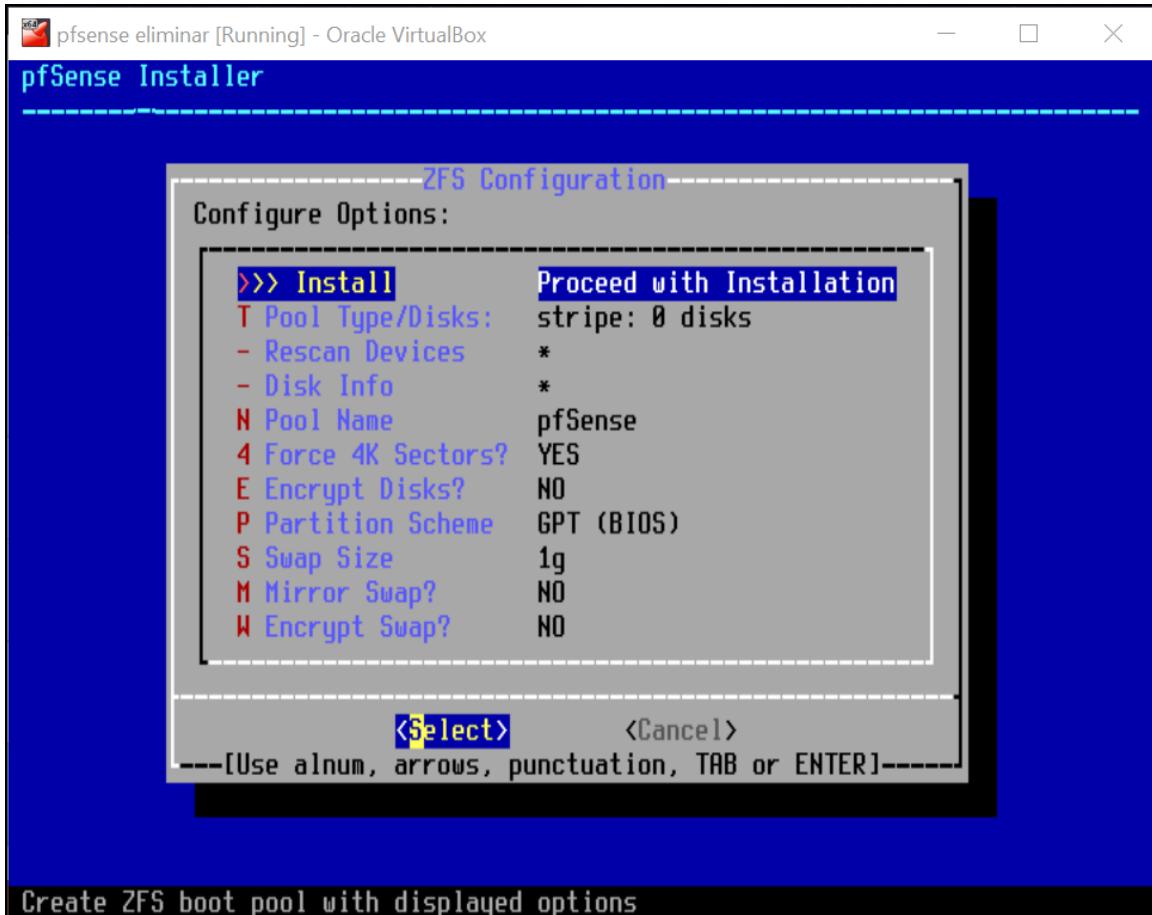


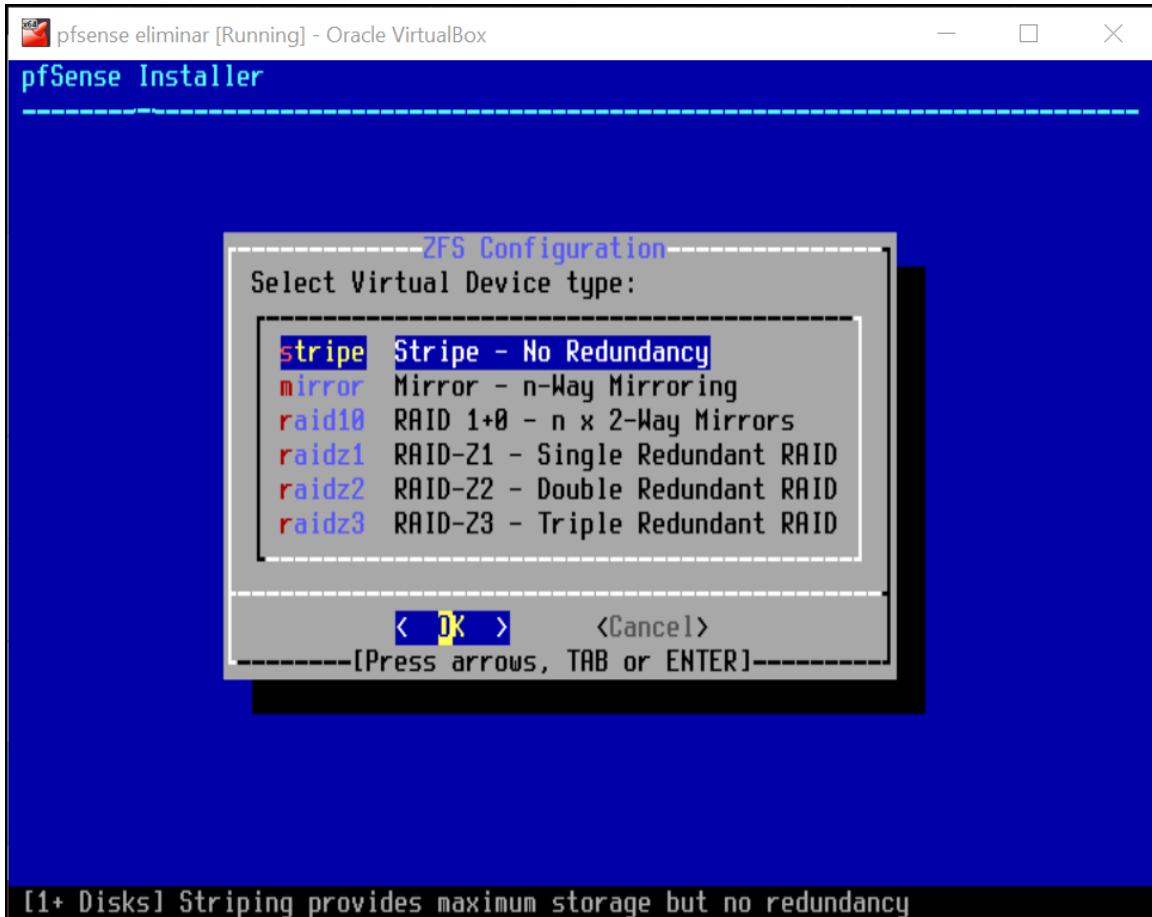


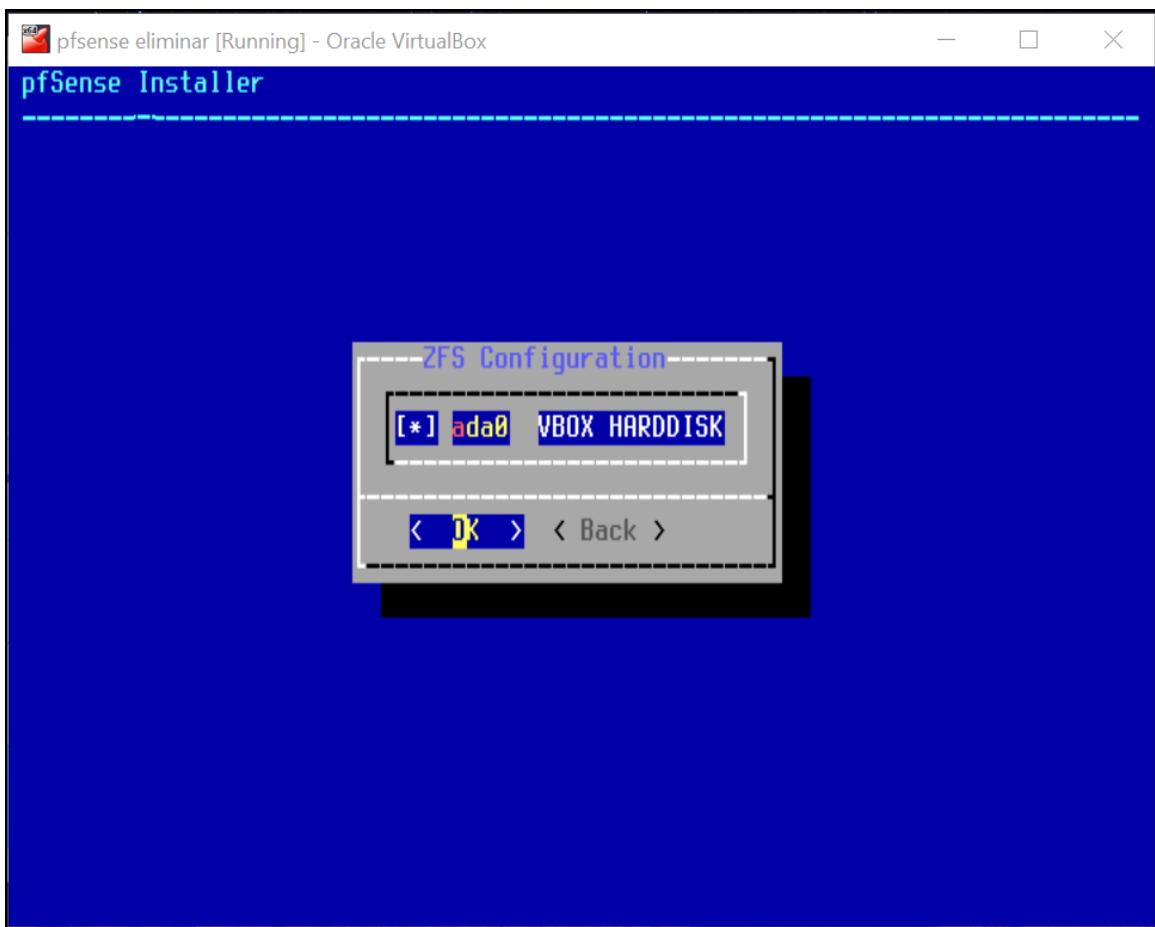


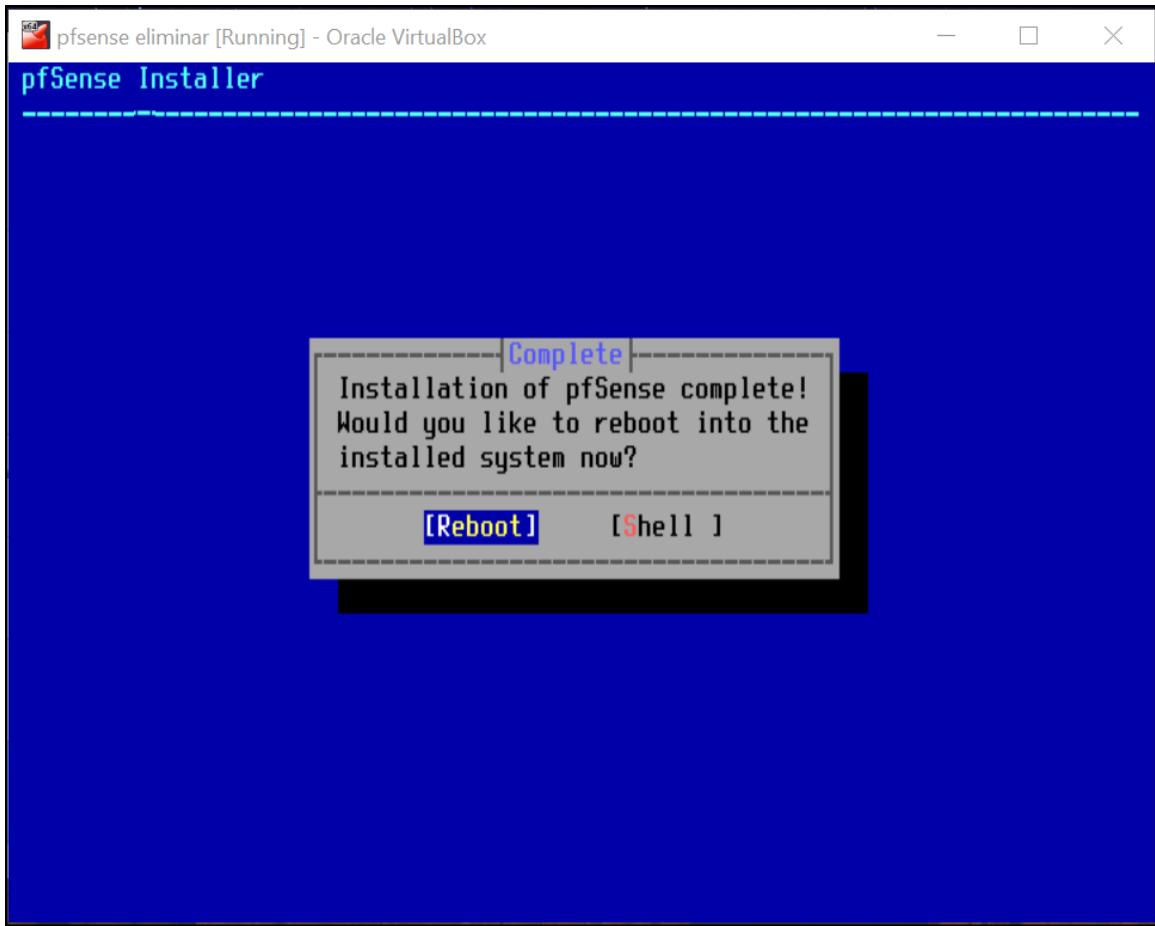


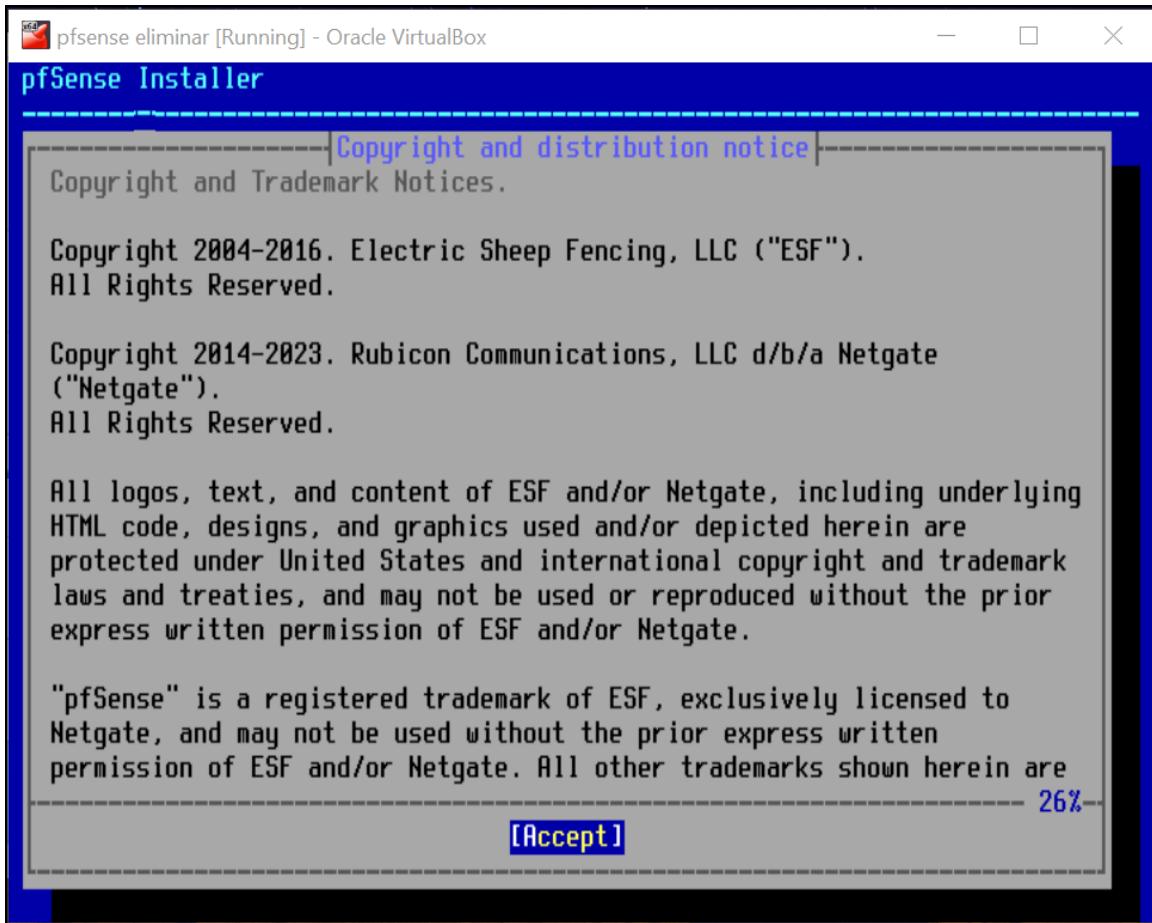


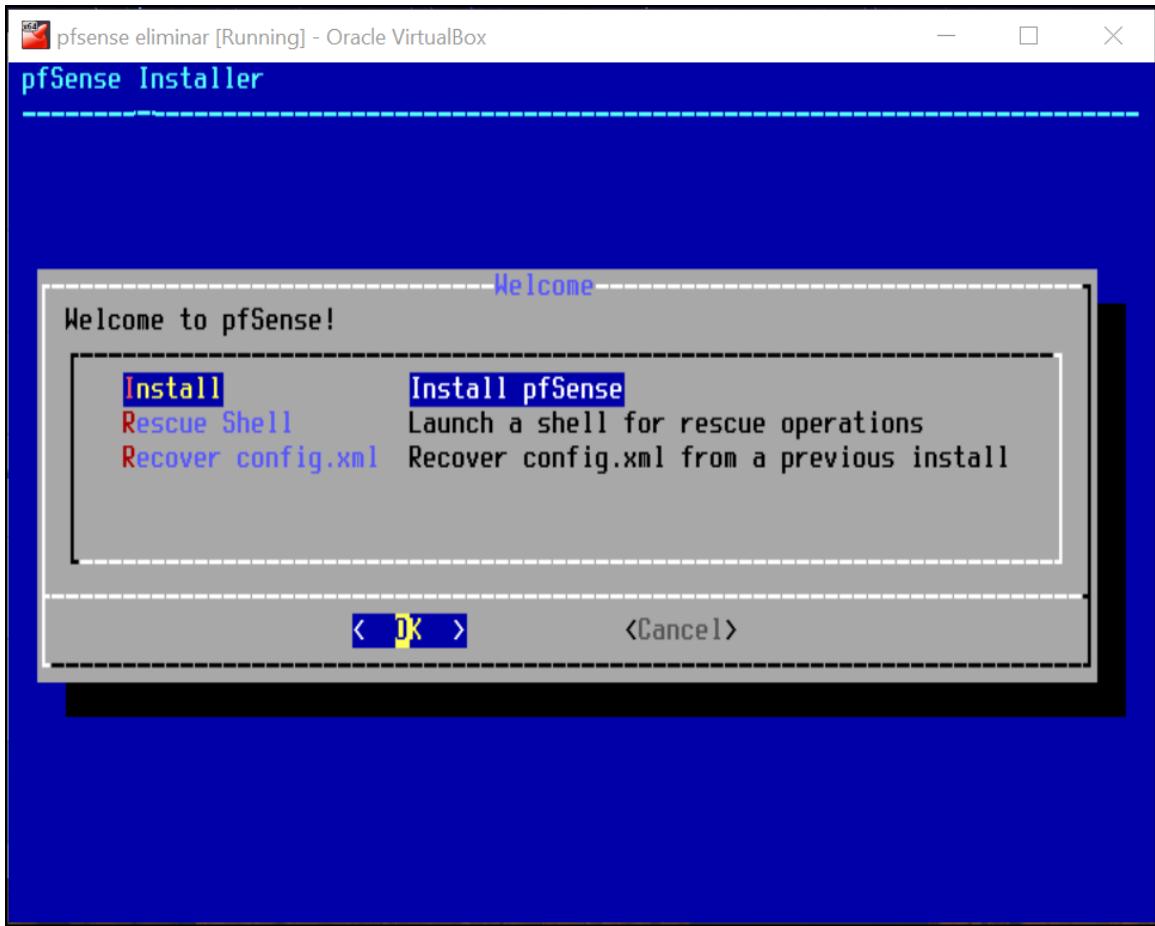


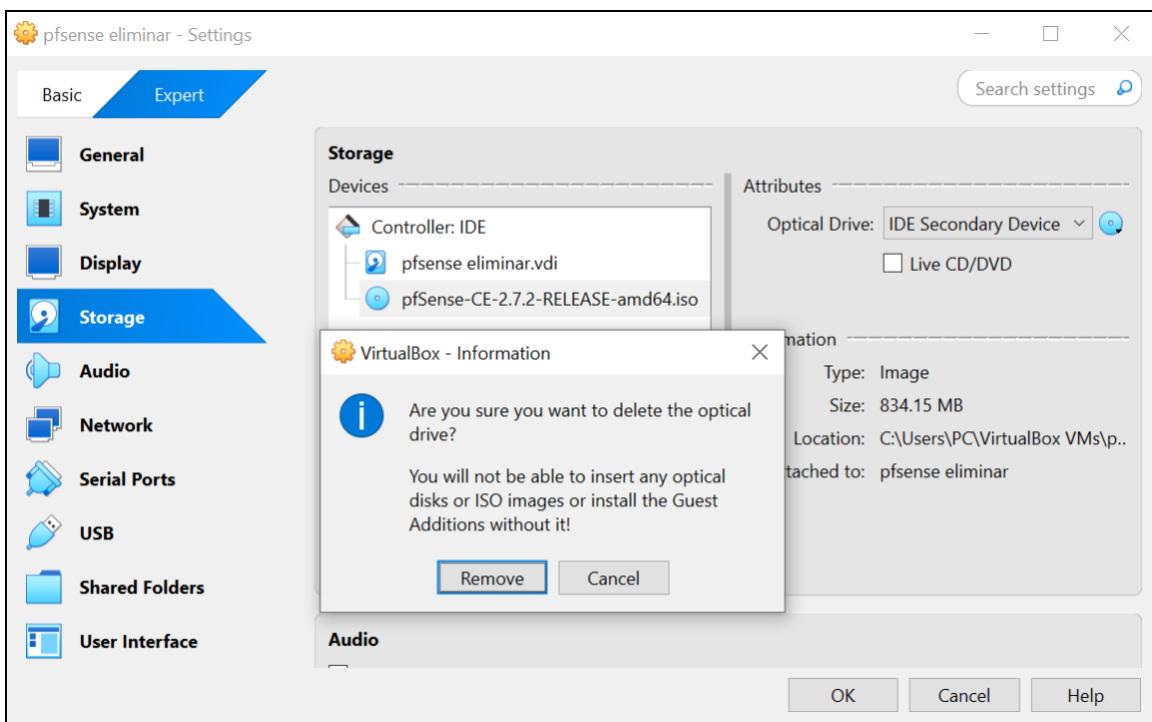
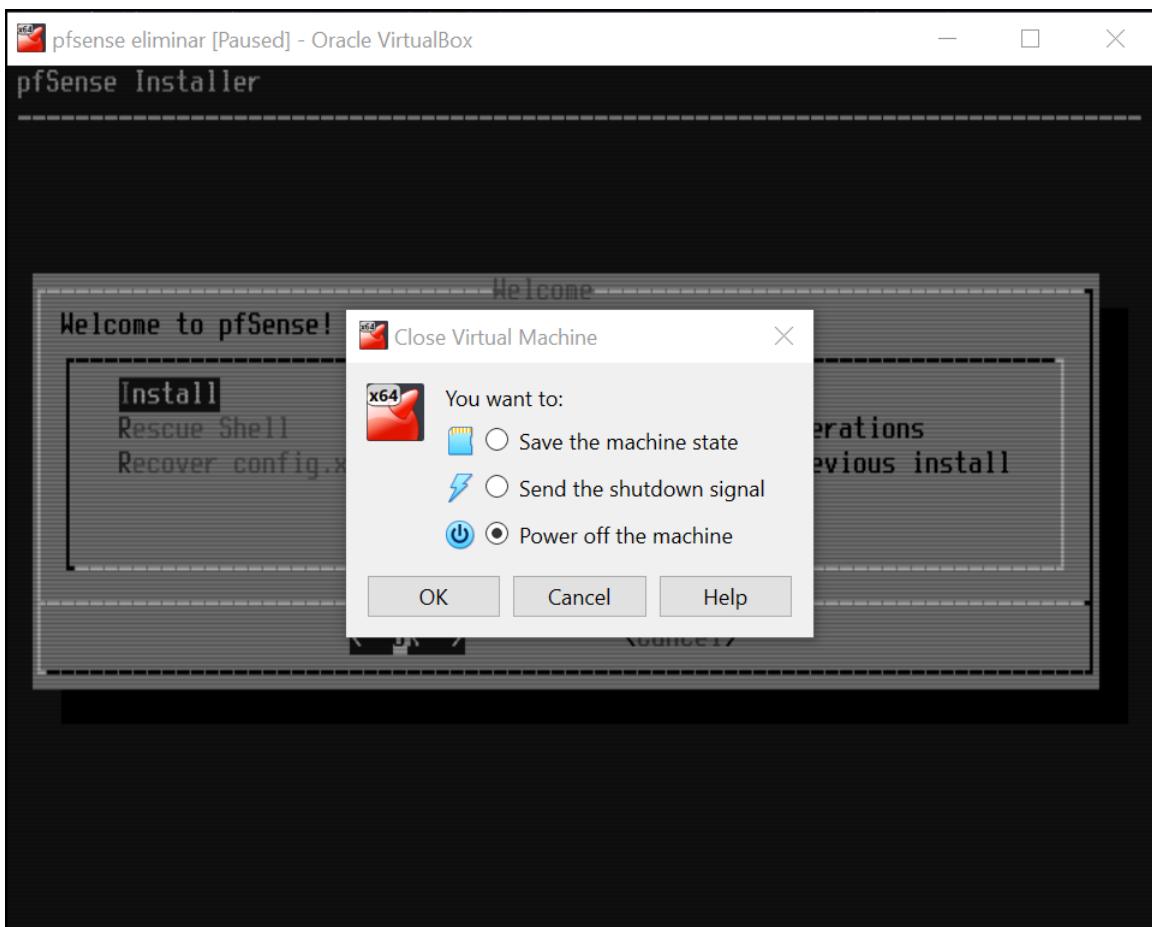


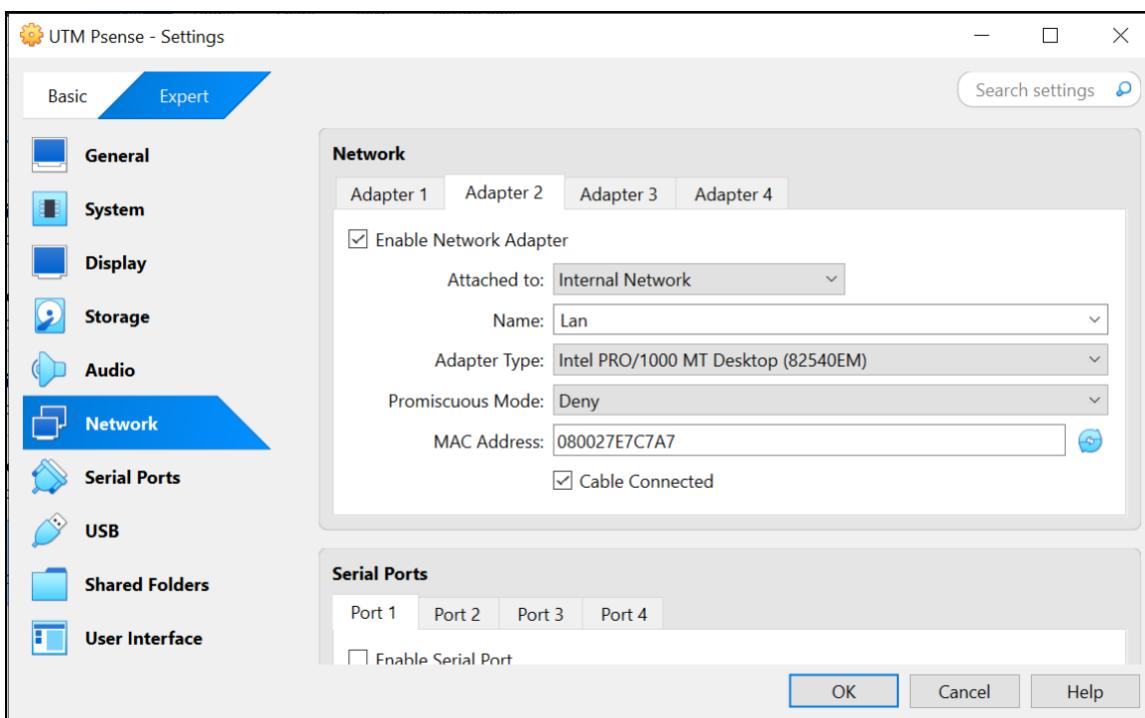
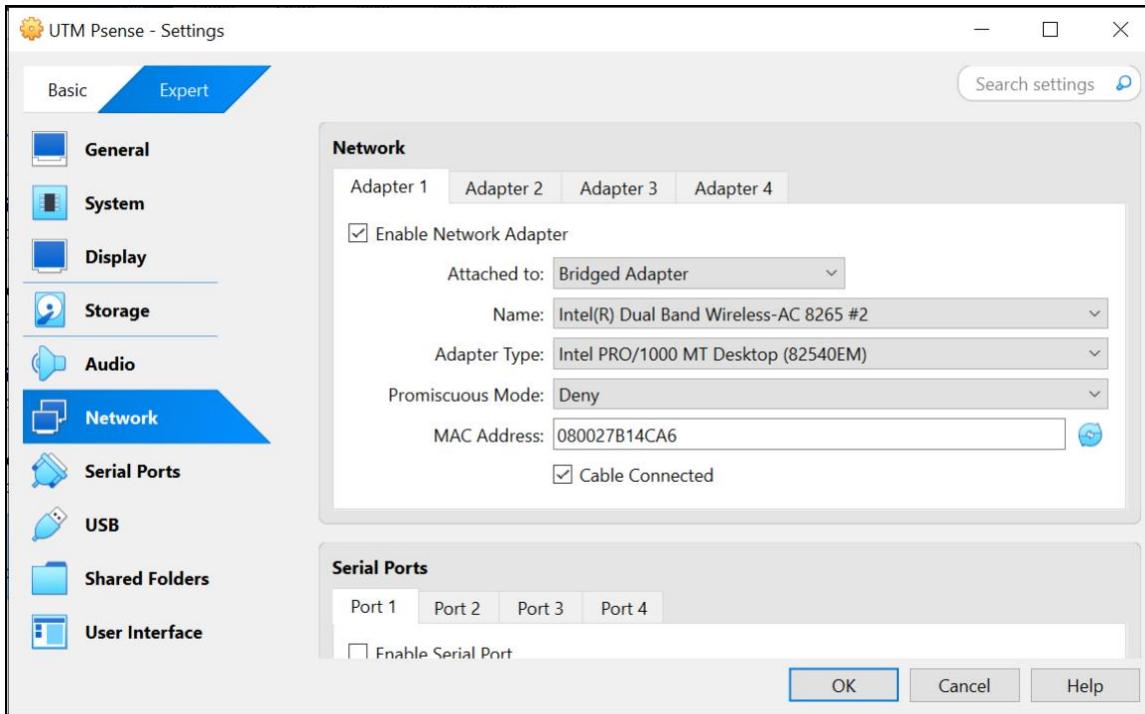


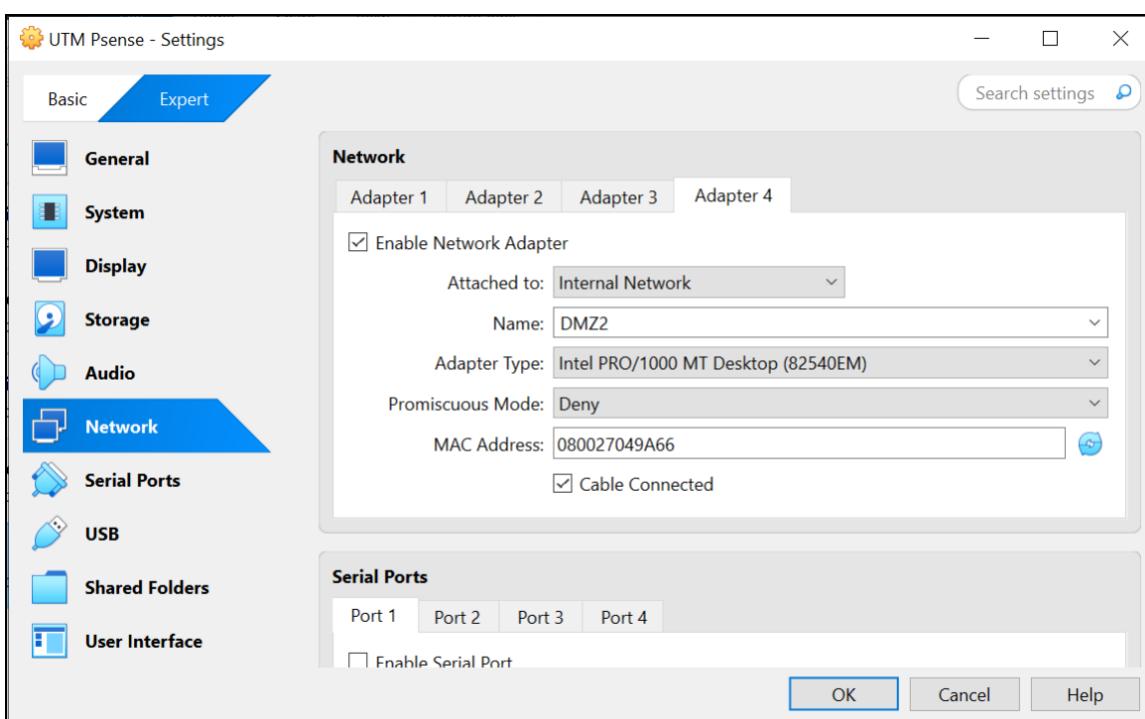
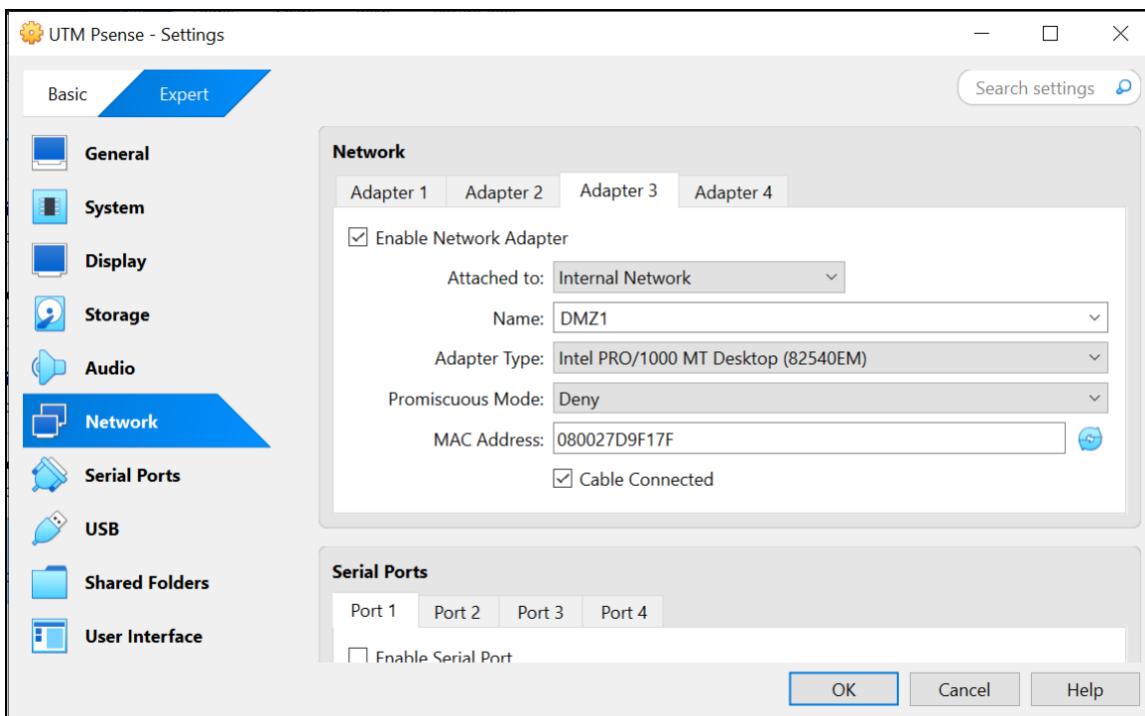


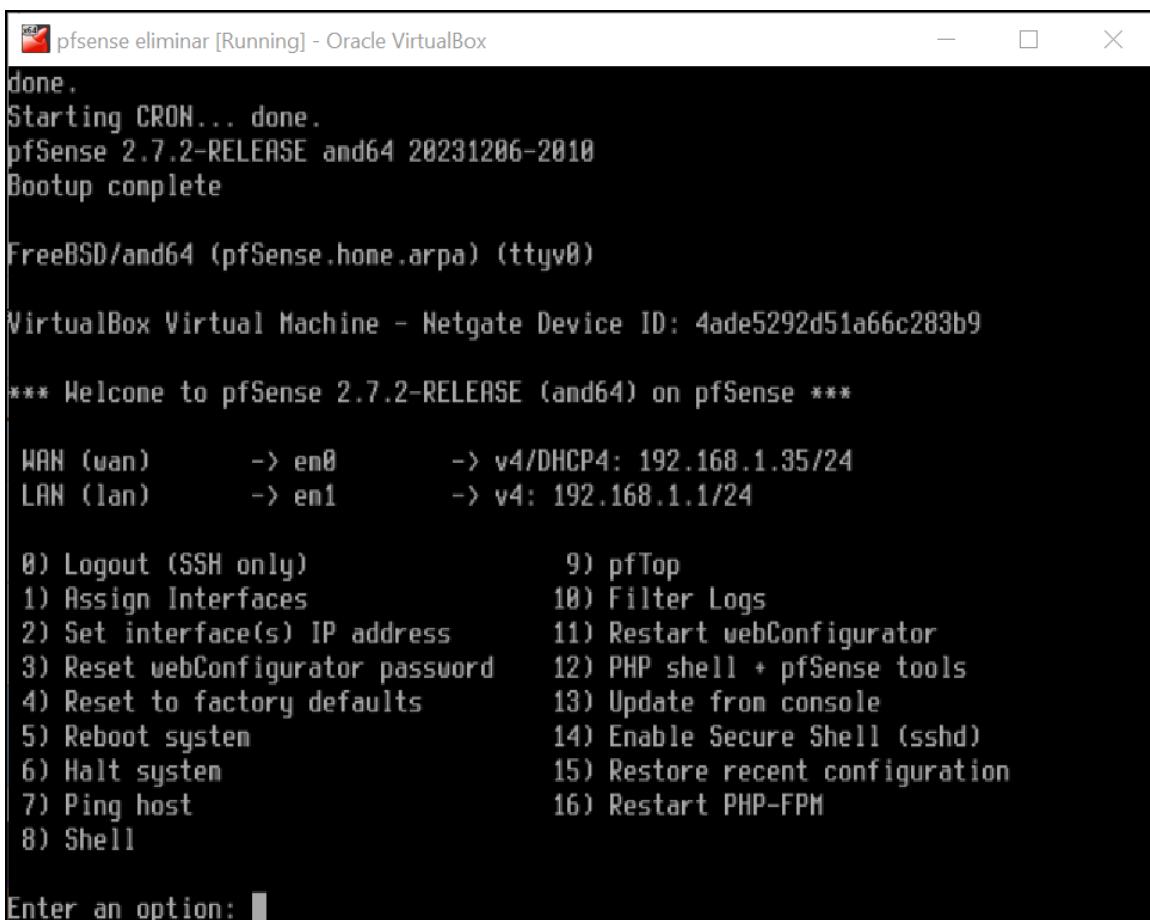
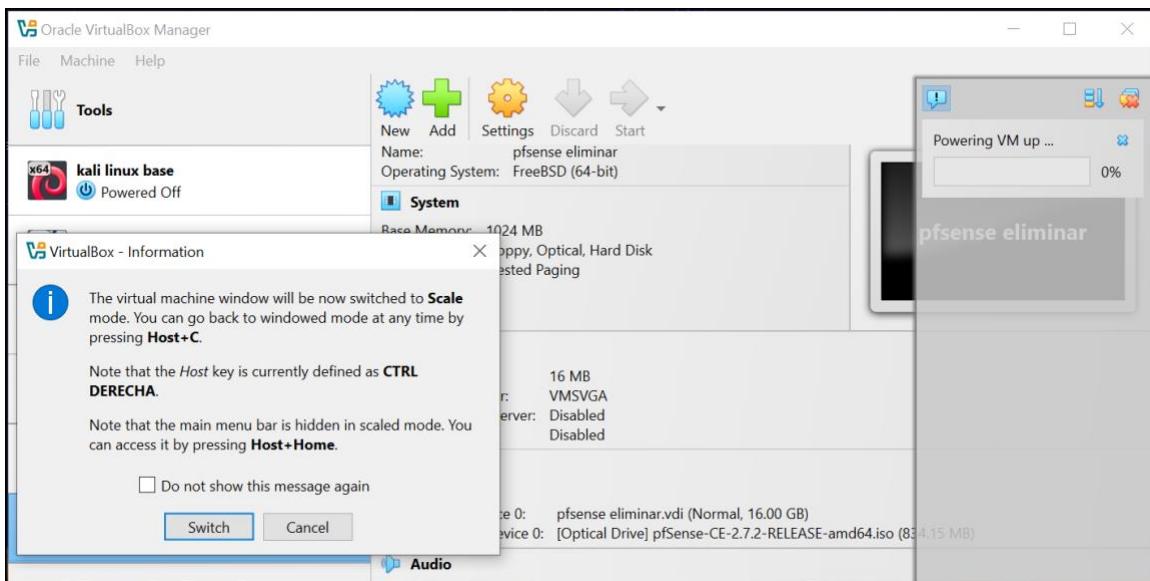








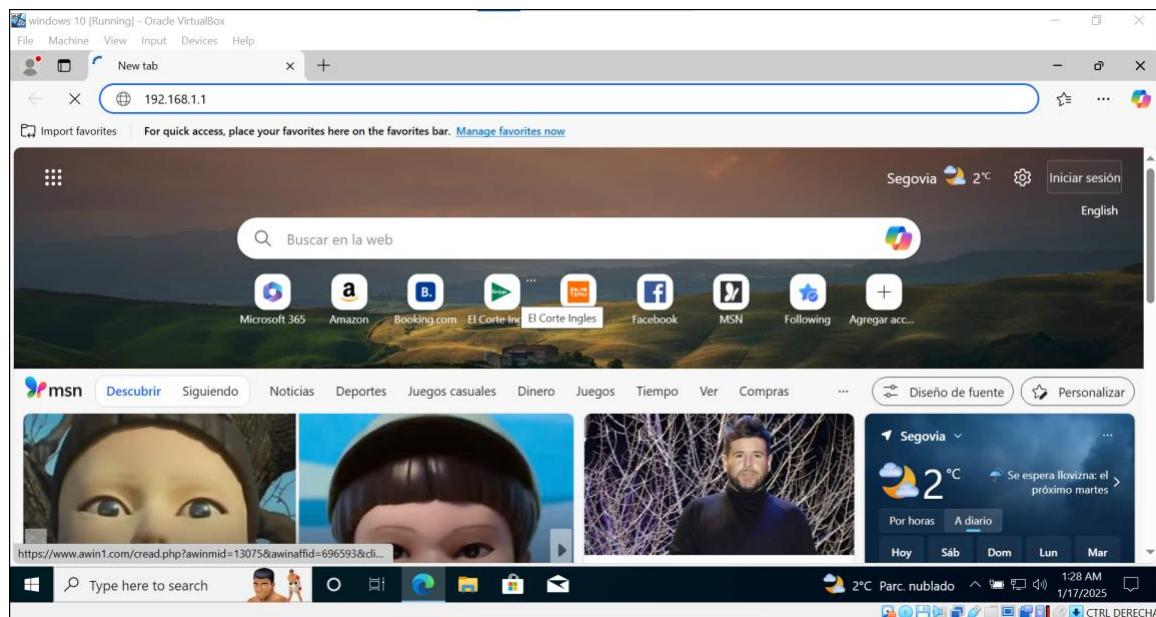
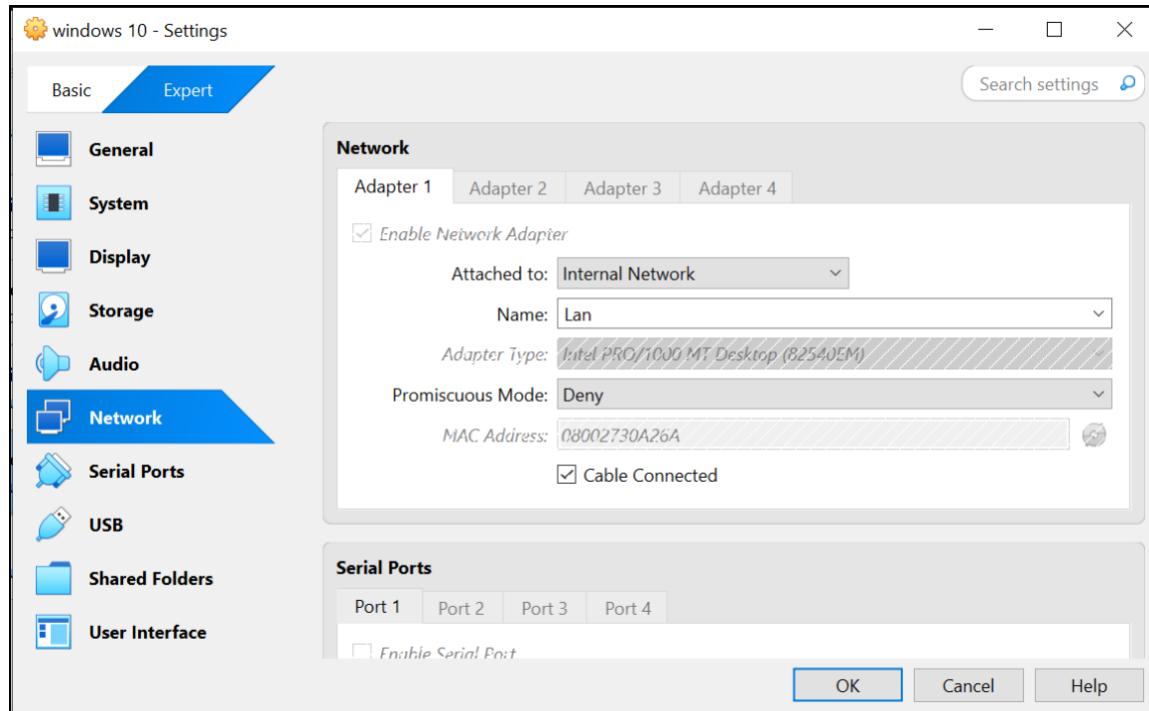


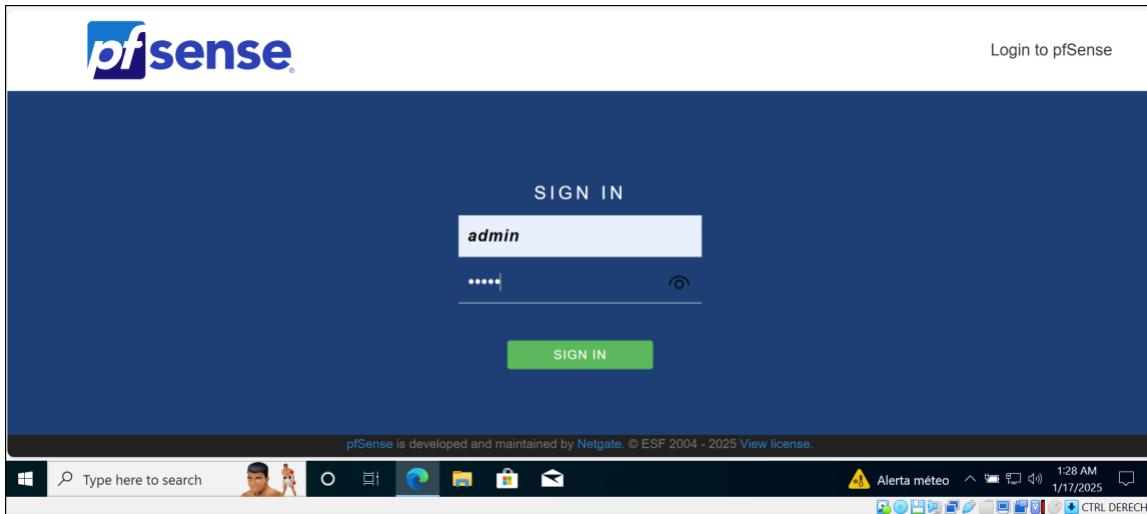


1.2. Configuración

En esta etapa de la práctica, se inició la máquina virtual con Windows y se estableció conexión con **Pfsense** a través del navegador. Durante este proceso, se llevó a cabo la configuración inicial del sistema.

Además, se ha asignado ya la red LAN a esta máquina.





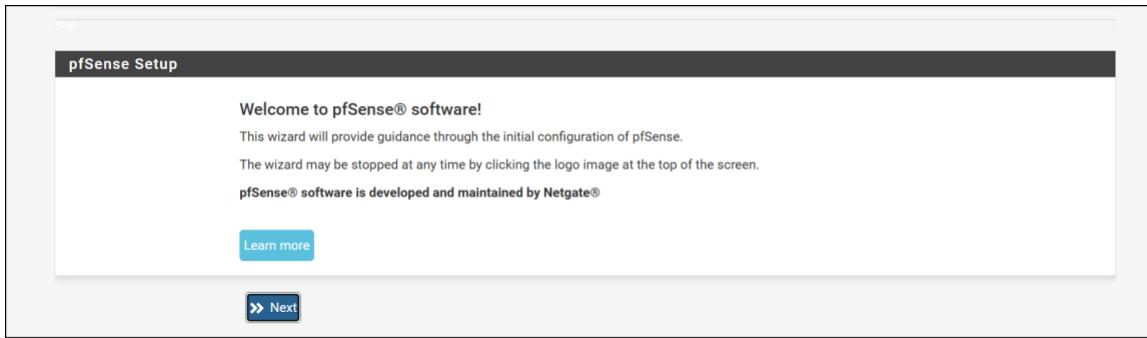
No part of ESF and/or Netgate's information or materials may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of ESF and/or Netgate. The information contained herein is subject to change without notice.

Use, duplication or disclosure by the U.S. Government may be subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance.

The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Enemies List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that Licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

[Accept](#)



On this screen the general pfSense parameters will be set.

Hostname	<input type="text" value="UTM"/>
Name of the firewall host, without domain part.	
Examples: pfsense, firewall, edgefw	
Domain	<input type="text" value="keepcoding.local"/>
Domain name for the firewall.	
Examples: home.arpa, example.com	
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.	
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	<input type="text" value="127.0.0.1"/>
Secondary DNS Server	<input type="text" value="1.1.1.1"/>

Primary DNS Server	<input type="text" value="127.0.0.1"/>
Secondary DNS Server	<input type="text" value="1.1.1.1"/>
Override DNS	<input checked="" type="checkbox"/>
Allow DNS servers to be overridden by DHCP/PPP on WAN	
>> Next	

Time Server Information

Please enter the time, date and time zone.

Time server hostname	<input type="text" value="2.pfsense.pool.ntp.org"/>
Enter the hostname (FQDN) of the time server.	
Timezone	<input type="text" value="Europe/Madrid"/>
>> Next	

Configure WAN Interface

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

SelectedType	<input type="text" value="DHCP"/>
General configuration	
MAC Address	<input type="text"/>
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.	
MTU	<input type="text"/>
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.	
MSS	<input type="text"/>
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If	

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.

>> Next

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

>> Next

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

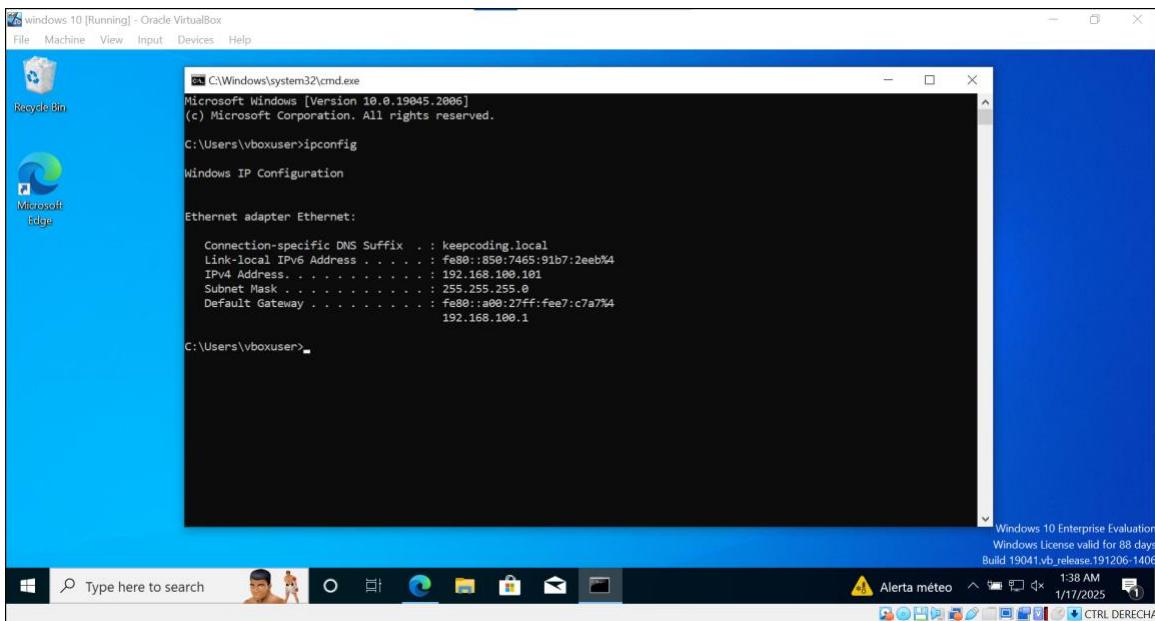
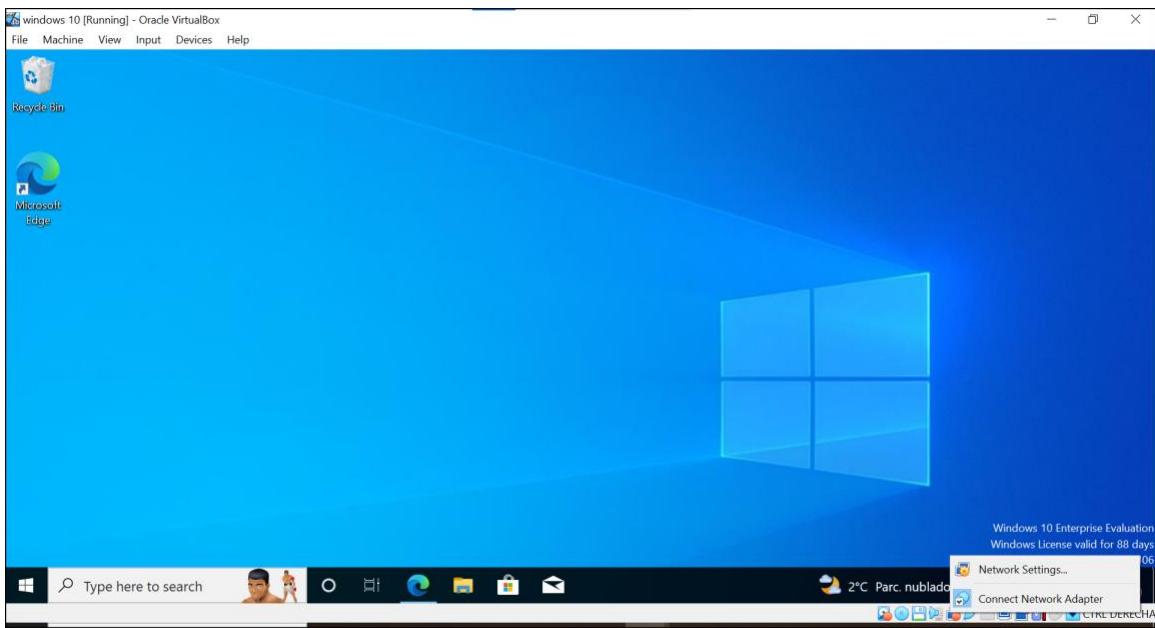
Admin Password AGAIN

>> Next

Reload configuration

Click 'Reload' to reload pfSense with new changes.

>> Reload



```

UTM Psense [Running] - Oracle VirtualBox
php-fpm[397]: /index.php: Successful login for user 'admin' from: 192.168.100.10
1 (Local Database)

FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 92b02f36e4b78d01bdbc

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on UTM ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.34/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24

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

Enter an option: 

```

Windows 10 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

UTM keepcoding.local - Status: D X +

← ⏪ ⏩ ⏴ Not secure | https://192.168.100.1

pfSense COMMUNITY EDITION

Status / Dashboard

System Information

Name	UTM.keepcoding.local
User	admin@192.168.100.101 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 92b02f36e4b78d01bdbc
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 21:10:00 CET 2023 FreeBSD 14.0-CURRENT

The system is on the latest version.
Version information updated at Fri Jan 17 1:24:29 CET 2025 Microsoft Store

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.

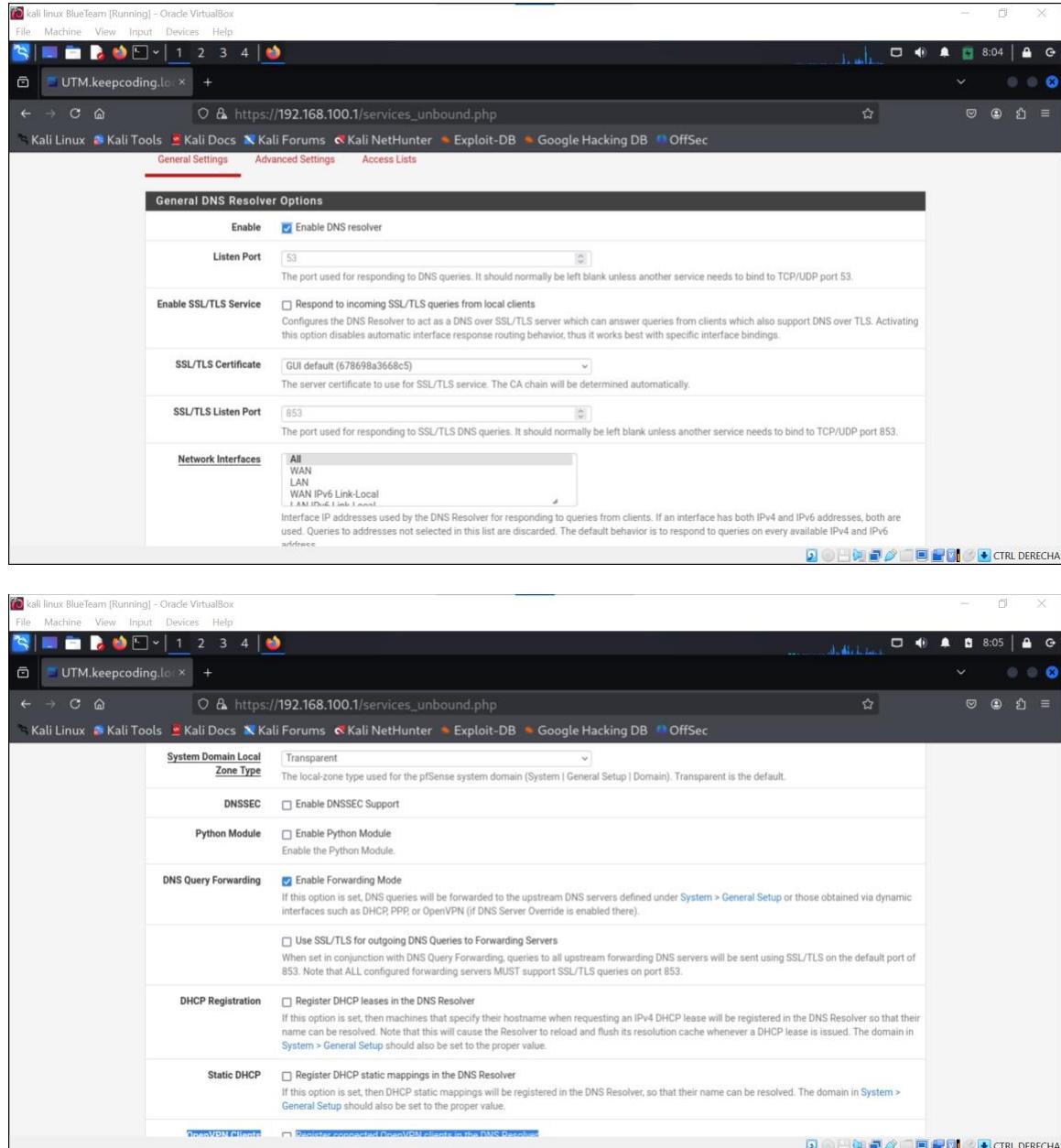
Windows taskbar: Type here to search, Start button, File Explorer, Task View, Edge, File Explorer, Microsoft Store, Mail, Alerta meteo, 1:40 AM, 1/17/2025, CTRL DERECHA

1.3. IPS y DHCP

En este apartado, se procedió a asignar direcciones IP dinámicas a las redes LAN, DMZ y DMZ2, estableciendo rangos específicos de direcciones IP para cada una de ellas, con el objetivo de prevenir conflictos. Para ello, se habilitó el servicio DHCP en dichas redes, permitiendo la asignación automática de direcciones IP a los dispositivos conectados. Además, DHCP simplifica la administración de la red al proporcionar de manera

centralizada otros parámetros esenciales, como la máscara de subred, la puerta de enlace predeterminada y los servidores DNS, asegurando así una configuración correcta y eficiente en todas las conexiones.

1.3.1. DNS



The image shows two screenshots of the pfSense Unbound DNS configuration interface. Both screenshots are taken from a Kali Linux BlueTeam VM running in Oracle VirtualBox, as indicated by the window title.

Screenshot 1: General Settings Tab (Top)

- General DNS Resolver Options:**
 - Enable:** Checked.
 - Listen Port:** Set to 53.
 - Enable SSL/TLS Service:** Unchecked.
 - SSL/TLS Certificate:** Set to "GUI default (678698a3668c5)".
 - SSL/TLS Listen Port:** Set to 853.
 - Network Interfaces:** A dropdown menu showing "All", "WAN", "LAN", "WAN IPv6 Link-Local", and "LAN IPv6 Link-Local".

Screenshot 2: System Domain Local Tab (Bottom)

- System Domain Local Zone Type:** Set to "Transparent".
- DNSSEC:** Unchecked.
- Python Module:** Unchecked.
- DNS Query Forwarding:**
 - Enable Forwarding Mode:** Checked.
 - Use SSL/TLS for outgoing DNS Queries to Forwarding Servers:** Unchecked.
- DHCP Registration:** Unchecked.
- Static DHCP:** Unchecked.
- OpenVPN Clients:** Unchecked.

The screenshot shows a web-based configuration interface for a DNS resolver. The URL is https://192.168.100.1/services_unbound.php. The interface includes sections for:

- DHCP Registration:** Options to register DHCP leases in the DNS Resolver.
- Static DHCP:** Options to register DHCP static mappings in the DNS Resolver.
- OpenVPN Clients:** Options to register connected OpenVPN clients in the DNS Resolver.

At the bottom, there is a "Display Custom Options" button and a "Save" button.

The screenshot shows the pfSense web interface under the "Services / DNS Resolver / General Settings" section. The URL is https://192.168.100.1/services_unbound.php. The interface includes:

- A message: "The DNS resolver configuration has been changed. The changes must be applied for them to take effect." with a "Apply Changes" button.
- A warning: "ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend."
- Three tabs: "General Settings" (selected), "Advanced Settings", and "Access Lists".
- A "General DNS Resolver Options" section with fields for "Enable" (checked), "Listen Port" (set to 53), and "Enable SSL/TLS Service" (unchecked).

1.3.2. DHCP de la red LAN

The screenshot shows the pfSense LAN configuration page. At the top, there is a warning message: "ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend." Below this, the "General DHCP Options" section is displayed. It includes settings for the DHCP Backend (set to ISC DHCP), enabling the DHCP server on the LAN interface, ignoring BOOTP queries, and denying unknown clients (set to "Allow all clients"). There is also an option to ignore denied clients, which is currently disabled. The page has a standard pfSense header with links to System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help.

The screenshot shows the pfSense LAN configuration page with the "Primary Address Pool" and "Server Options" sections. In the "Primary Address Pool" section, the subnet is set to 192.168.100.0/24, and the subnet range is 192.168.100.1 - 192.168.100.254. An address pool range is defined from 192.168.100.100 to 192.168.100.200. A note states that the specified range must not be within the range configured on any other address pool for this interface. In the "Server Options" section, WINS servers are listed as "WINS Server 1" and "WINS Server 2". The page has a standard pfSense header with links to System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help.

kali linux Blueteam [Running] - Oracle VirtualBox

File Machine View Input Devices Help

UTM.keeping.local +

https://192.168.100.1/services_dhcp.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Additional Pools If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Server Options

WINS Servers

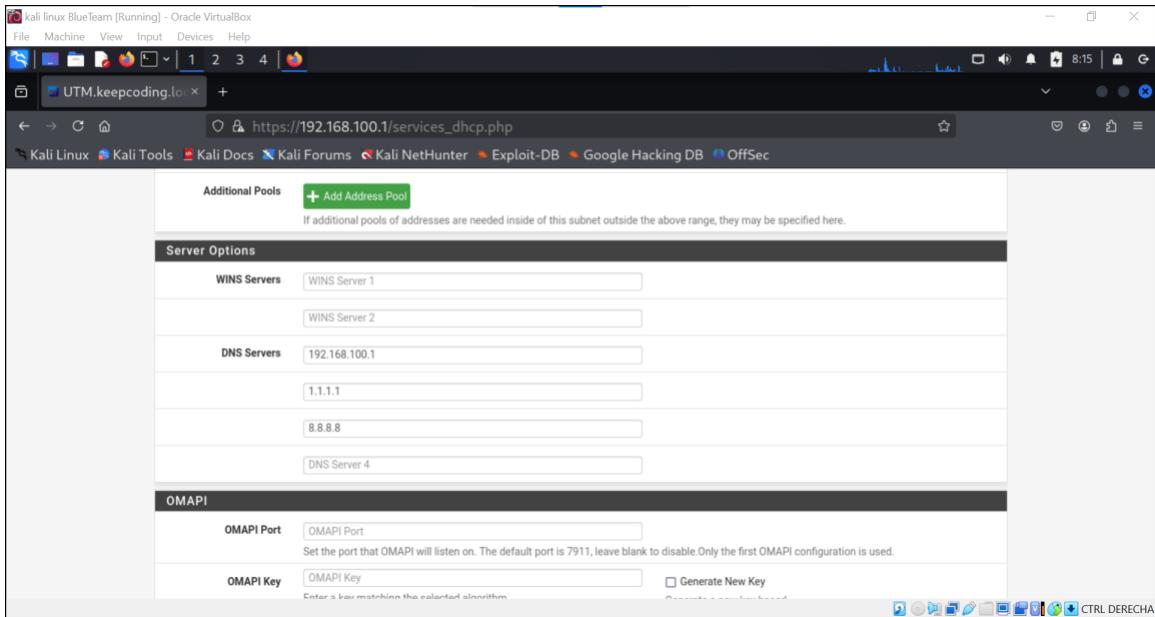
DNS Servers

OMAPI

OMAPI Port Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.

OMAPI Key Generate New Key Enter a key matching the selected algorithm

CTRL DERECHA



kali linux Blueteam [Running] - Oracle VirtualBox

File Machine View Input Devices Help

UTM.keeping.local +

https://192.168.100.1/services_dhcp.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Other DHCP Options

Gateway The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.

Domain Name The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.

Domain Search List The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.

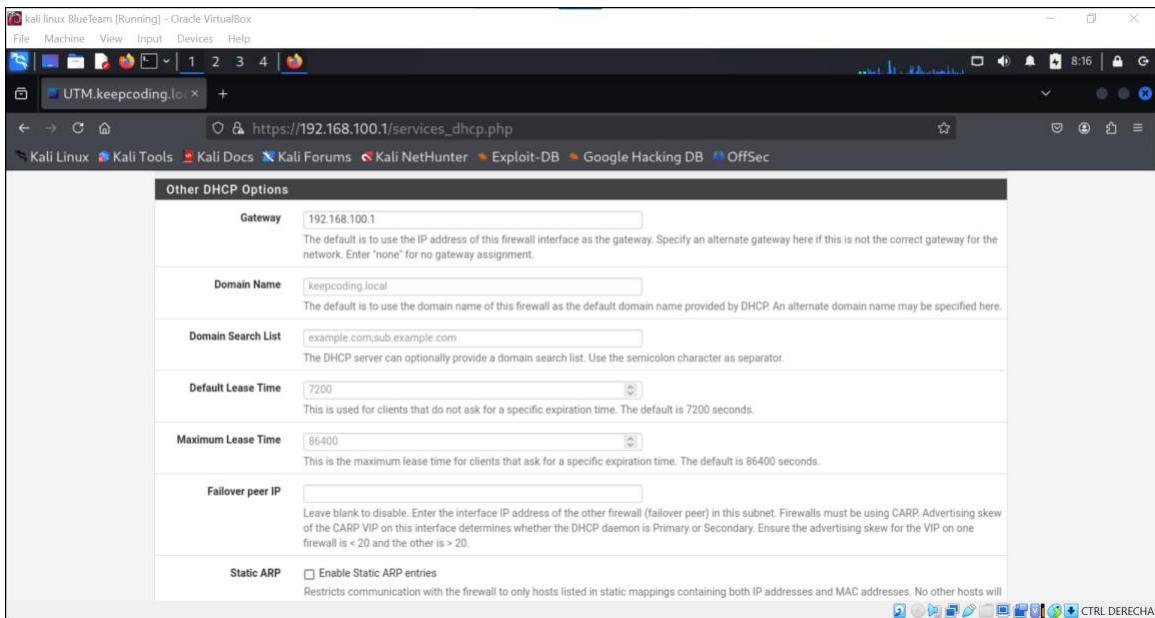
Default Lease Time This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.

Maximum Lease Time This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

Failover peer IP Leave blank to disable. Enter the interface IP address of the other firewall (failover peer) in this subnet. Firewalls must be using CARP. Advertising skew of the CARP VIP on this interface determines whether the DHCP daemon is Primary or Secondary. Ensure the advertising skew for the VIP on one firewall is < 20 and the other is > 20.

Static ARP Enable Static ARP entries Restricts communication with the firewall to only hosts listed in static mappings containing both IP addresses and MAC addresses. No other hosts will

CTRL DERECHA



The screenshot shows the pfSense DHCP configuration interface. At the top, there are several tabs: MAC Address Control, NTP, TFTP, LDAP, Network Booting, and Custom DHCP Options. Below these are buttons for 'display Advanced' and a 'Save' button. A table titled 'DHCP Static Mappings' lists columns for Static ARP, MAC address, IP address, Hostname, and Description. A green '+' button labeled 'Add Static Mapping' is visible. At the bottom, a note states 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.'

The screenshot shows the pfSense DHCP configuration interface under the 'Services / DHCP Server / LAN' section. A message at the top says 'The DHCP Server configuration has changed. The changes must be applied for them to take effect.' with a 'Apply Changes' button. A warning message below states 'ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.' The 'General DHCP Options' section includes fields for 'DHCP Backend' (set to ISC DHCP), 'Enable' (checked), 'Enable DHCP server on LAN interface' (checked), 'BOOTP' (unchecked), and 'Ignore BOOTP queries' (unchecked). A dropdown for 'Deny Unknown Clients' is set to 'Allow all clients'. The pfSense navigation bar at the top includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help.

1.3.2. Añadir red DMZ

A la DMZ le vamos a aplicar una puerta de enlace estática.

kali linux BlueTeam [Running] - Oracle VirtualBox

File Machine View Input Devices Help

UTM.keeping.lo +

https://192.168.100.1/interfaces_assign.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Interfaces / Interface Assignments

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIGs Bridges LAGGs

Interface Network port

WAN	em0 (08:00:27:b1:4c:a6)
LAN	em1 (08:00:27:e7:c7:a7)
Available network ports:	em2 (08:00:27:d9:f1:7f)

Save

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

CTRL DERECHA

This screenshot shows the 'Interface Assignments' page in the pfSense web interface. It lists two assigned ports: 'WAN' (em0) and 'LAN' (em1). Below this, an 'Available network ports:' section shows 'em2'. A note at the bottom states that wireless interfaces must be created on the Wireless tab before they can be assigned.

kali linux BlueTeam [Running] - Oracle VirtualBox

File Machine View Input Devices Help

UTM.keeping.lo +

https://192.168.100.1/interfaces_assign.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Interfaces / Interface Assignments

Interface has been added.

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIGs Bridges LAGGs

Interface Network port

WAN	em0 (08:00:27:b1:4c:a6)
LAN	em1 (08:00:27:e7:c7:a7)
OPT1	em2 (08:00:27:d9:f1:7f)
OPT2	em3 (08:00:27:04:9a:66)

Save

CTRL DERECHA

This screenshot shows the same 'Interface Assignments' page as the previous one, but now it includes four assigned ports: 'WAN' (em0), 'LAN' (em1), 'OPT1' (em2), and 'OPT2' (em3). A success message 'Interface has been added.' is displayed above the table. The note about wireless interfaces still appears at the bottom.

kali linux Blueteam [Running] - Oracle VirtualBox

File Machine View Input Devices Help

UTM.keepingcoding.lo +

https://192.168.100.1/interfaces.php?if=opt1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

pfSense COMMUNITY EDITION

Interfaces / OPT1 (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
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx 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

CTRL DERECHA

kali linux Blueteam [Running] - Oracle VirtualBox

File Machine View Input Devices Help

UTM.keepingcoding.lo +

https://192.168.100.1/interfaces.php?if=opt1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

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".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by clicking here.

Reserved Networks

Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Save

CTRL DERECHA

The screenshot shows the pfSense web interface with the URL <https://192.168.100.1/interfaces.php?if=opt1>. The page title is "Interfaces / DMZ (em2)". A message box at the top right says "The DMZ configuration has been changed. The changes must be applied to take effect. Don't forget to adjust the DHCP Server range if needed after applying." with a "Apply Changes" button. The "General Configuration" section includes fields for "Enable" (checked), "Description" (DMZ), "IPv4 Configuration Type" (Static IPv4), "IPv6 Configuration Type" (None), and "MAC Address" (xxxxxx:xxxx:xxxx). The pfSense navigation bar at the top includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help.

1.3.3 Añadir red DMZ2

A la DMZ2 le vamos a aplicar una puerta de enlace estática.

The screenshot shows the pfSense web interface with the URL <https://192.168.100.1/interfaces.php?if=opt2>. The page title is "Interfaces / OPT2 (em3)". The "General Configuration" section includes fields for "Enable" (checked), "Description" (DMZ2), "IPv4 Configuration Type" (Static IPv4), "IPv6 Configuration Type" (None), and "MAC Address" (xxxxxx:xxxx:xxxx). It also includes "MTU" and "MSS" fields with explanatory text. The pfSense navigation bar at the top includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help.

Static IPv4 Configuration

IPv4 Address: 192.168.250.1

IPv4 Upstream gateway: None

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". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here.

Reserved Networks

Block private networks and loopback addresses Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Save

The DMZ2 configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

Apply Changes

General Configuration

Enable Enable interface

Description: DMZ2
Enter a description (name) for the interface here.

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

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

1.3.4 Comprobar redes añadidas

Lo que vamos a comprobar en Pfsense es si las redes se han añadido correctamente.

UTM Psense [Running] - Oracle VirtualBox

```

FreeBSD/amd64 (UTM.keepcoding.local) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 92b02f36e4b78d01bdbe

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on UTM ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.34/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24
DMZ (opt1)     -> em2      -> v4: 192.168.200.1/24
DMZ2 (opt2)    -> em3      -> v4: 192.168.250.1/24

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: 

```

1.3.5 Rango DMZ

kali linux Blue team [Running] - Oracle VirtualBox

The screenshot shows a Kali Linux browser window displaying the pfSense web interface. The URL in the address bar is `https://192.168.100.1/services_dhcp.php?if=opt1`. The page title is "General DHCP Options". Under the "DHCP Backend" section, "ISC DHCP" is selected. The "Enable" checkbox is checked, and "Ignore BOOTP queries" is unchecked. In the "Deny Unknown Clients" section, the dropdown menu is set to "Allow all clients". A note explains that this allows any client to get an IP address within the scope. In the "Ignore Denied Clients" section, the checkbox is unchecked. A note states that this option is incompatible with failover and cannot be enabled when a Failover Peer IP address is configured. In the "Ignore Client Identifiers" section, the checkbox is unchecked. A note indicates that this option is useful for dual booting with different client identifiers. At the bottom, the "Primary Address Pool" section shows a subnet of 192.168.200.0/24.

kali linux Blueteam [Running] - Oracle VirtualBox

File Machine View Input Devices Help

UTM.keeping.local +

https://192.168.100.1/services_dhcp.php?f=opt1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Primary Address Pool

Subnet 192.168.200.0/24

Subnet Range 192.168.200.1 - 192.168.200.254

Address Pool Range 192.168.200.100 To 192.168.200.200
From

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools + Add Address Pool

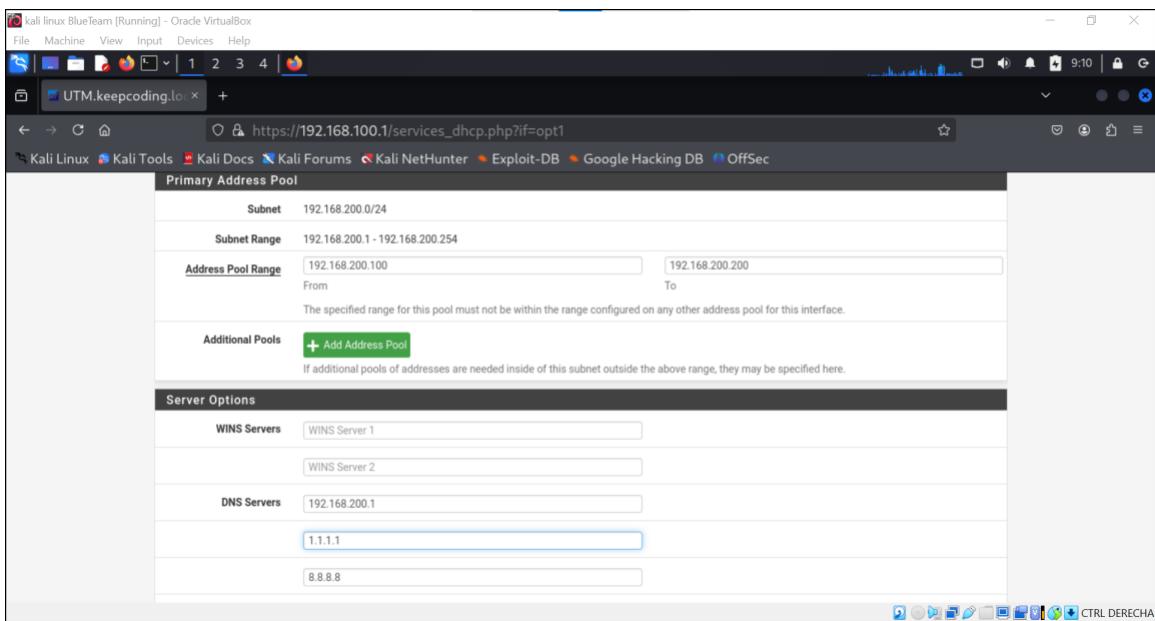
If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Server Options

WINS Servers WINS Server 1
WINS Server 2

DNS Servers 192.168.200.1
1.1.1.1
8.8.8.8

CTRL DERECHA



kali linux Blueteam [Running] - Oracle VirtualBox

File Machine View Input Devices Help

UTM.keeping.local +

https://192.168.100.1/services_dhcp.php?f=opt1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

OMAPI Key (Enter key)
Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.
 Generate New Key
Generate a new key based on the selected algorithm.

Key Algorithm HMAC-SHA256 (current bind9 default)
Set the algorithm that OMAPI key will use.

Other DHCP Options

Gateway 192.168.200.1
The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.

Domain Name keepcoding.local
The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.

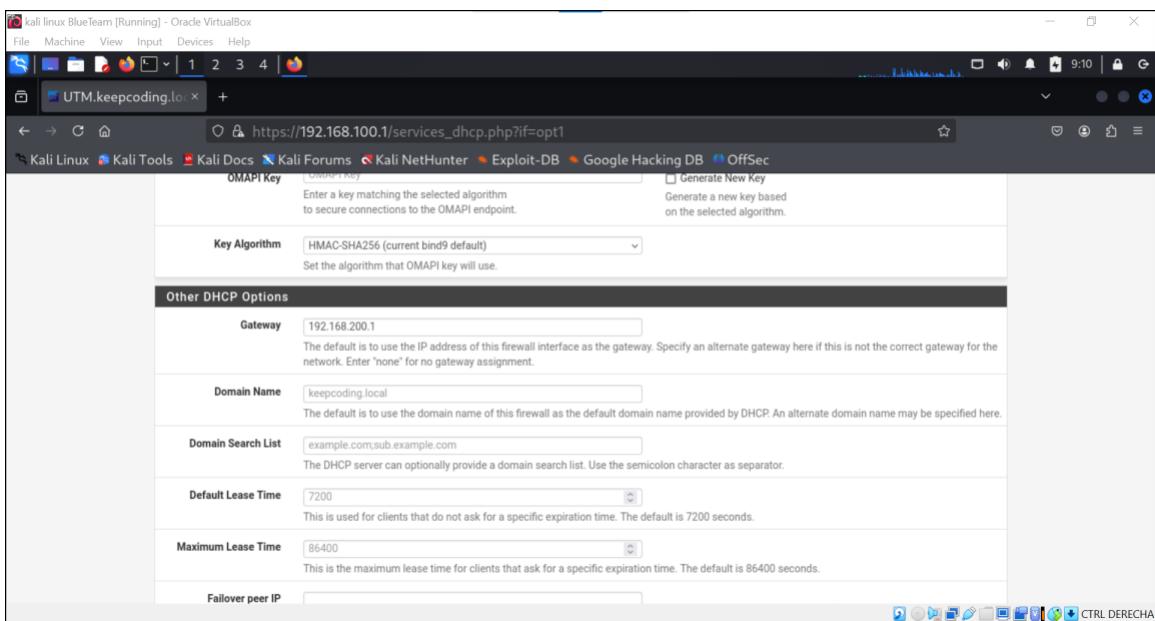
Domain Search List example.com;sub.example.com
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.

Default Lease Time 7200
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.

Maximum Lease Time 86400
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

Failover peer IP

CTRL DERECHA



The screenshot shows the pfSense web interface for the DHCP Server configuration. The URL is https://192.168.100.1/services_dhcp.php?if=opt1. The page title is "Services / DHCP Server / DMZ". A message at the top states: "The DHCP Server configuration has changed. The changes must be applied for them to take effect." A green "Apply Changes" button is visible. Another message below says: "ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend." The "DMZ" tab is selected. Under "General DHCP Options", the "DHCP Backend" is set to "ISC DHCP". The "Enable" checkbox is checked. Under "BOOTP", there is an unchecked checkbox for "Ignore BOOTP queries". The "Deny Unknown Clients" dropdown is set to "Allow all clients".

1.3.6 Rango DMZ2

This screenshot shows the pfSense web interface for the DHCP Server configuration, specifically for the DMZ2 interface. The URL is https://192.168.100.1/services_dhcp.php?if=opt2. The page title is "Services / DHCP Server / DMZ2". A yellow warning box at the top states: "ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend." The "DMZ2" tab is selected. Under "General DHCP Options", the "DHCP Backend" is set to "ISC DHCP". The "Enable" checkbox is checked. Under "BOOTP", there is an unchecked checkbox for "Ignore BOOTP queries". The "Deny Unknown Clients" dropdown is set to "Allow all clients". A detailed note explains that setting "Allow all clients" allows any DHCP client to get an IP address within the scope on this interface. It also mentions static mappings and failover. Other sections like "Ignore Denied Clients" and "Ignore Client Identifiers" are present but not fully expanded.

kali linux Blueteam [Running] - Oracle VirtualBox

File Machine View Input Devices Help

UTM.keeping.lo +

https://192.168.100.1/services_dhcp.php?if=opt2

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Primary Address Pool

Subnet	192.168.250.0/24
Subnet Range	192.168.250.1 - 192.168.250.254
Address Pool Range	192.168.250.100 To 192.168.250.200
From	

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools [+ Add Address Pool](#)

If additional pools of addresses are needed inside of this subnet outside of the above range, they may be specified here.

Server Options

WINS Servers	WINS Server 1
	WINS Server 2
DNS Servers	192.168.250.1
	1.1.1.1
	8.8.8.8

CTRL DERECHA

kali linux Blueteam [Running] - Oracle VirtualBox

File Machine View Input Devices Help

UTM.keeping.lo +

https://192.168.100.1/services_dhcp.php?if=opt2

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

to secure connections to the OMDBP endpoint.

on the selected algorithm.

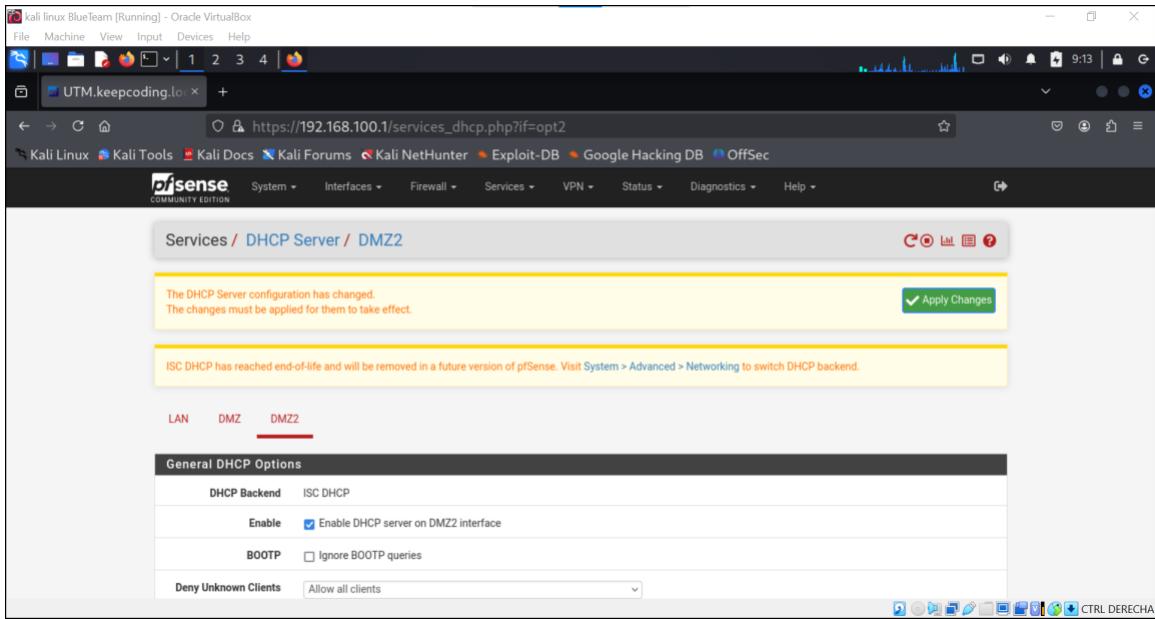
Key Algorithm HMAC-SHA256 (current bind9 default)

Set the algorithm that OMAPI key will use.

Other DHCP Options

Gateway	192.168.250.1	The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.
Domain Name	keeping.local	The default is to use the domain name of this firewall as the default domain name provided by DHCP. An alternate domain name may be specified here.
Domain Search List	example.com;sub.example.com	The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.
Default Lease Time	7200	This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum Lease Time	86400	This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Failover peer IP		Leave blank to disable. Enter the interface IP address of the other firewall (failover peer) in this subnet. Firewalls must be using CARP. Advertising skew of the CARP VIP on this interface determines whether the DHCP daemon is Primarv or Secondarv. Ensure the advertising skew for the VIP is on.

CTRL DERECHA



1.4. Firewall

En esta sección se detallan las reglas principales implementadas en el firewall, junto con la validación del correcto funcionamiento del servicio DNS y la definición de políticas específicas para la gestión de las comunicaciones entre las diferentes redes configuradas.

Se establece que la red DMZ estará completamente aislada de las redes internas LAN y DMZ2, sin posibilidad de comunicación en ningún sentido. No obstante, se permitirá acceso bidireccional entre la red DMZ y la red externa WAN, cumpliendo con los requisitos de segmentación y control. Asimismo, se asigna esta red al Honeypot, como parte de la estrategia de detección y análisis de posibles amenazas externas.

Esta configuración refuerza los principios de seguridad perimetral y minimiza los riesgos asociados a accesos no autorizados desde redes externas hacia la infraestructura interna.

1.4.1 Alias a puertos

Vamos a otorgar el alias "Web" a los puertos 80 (HTTP) y 443 (HTTPS), ya que ambos están comúnmente asociados a la transmisión de datos a través de páginas web. El puerto 80 (HTTP) se utiliza para establecer conexiones no cifradas, lo que significa que los datos transmitidos entre el cliente y el servidor pueden ser interceptados y leídos fácilmente por terceros. Por otro lado, el puerto 443 (HTTPS) opera con un nivel de seguridad superior, ya que emplea protocolos de cifrado como TLS (Transport Layer Security), lo que garantiza la confidencialidad e integridad de los datos transmitidos.

The screenshot shows the pfSense web interface under the 'Firewall / Aliases / Edit' section. A new alias named 'Web' is being created. The 'Name' field is set to 'Web'. The 'Description' field contains 'Puertos para trafico web'. The 'Type' dropdown is set to 'Port(s)'. Under the 'Port(s)' section, two ports are listed: port 80 is mapped to 'HTTP' and port 443 is mapped to 'HTTPS'. There are 'Save' and '+ Add Port' buttons at the bottom.

1.4.2. Reglas Firewall DMZ

The screenshot shows the pfSense web interface under the 'Firewall / Rules / DMZ' section. The 'DMZ' tab is selected. A table titled 'Rules (Drag to Change Order)' shows a single row: 'No rules are currently defined for this interface'. Below the table are buttons for 'Add', 'Delete', 'Toggle', 'Copy', 'Save', and 'Separator'. The footer of the interface includes the Netgate copyright information.

Primero vamos a bloquear la comunicación entre DMZ y DMZ2.

The screenshot shows the 'Edit Firewall Rule' interface in pfSense. The 'Action' dropdown is set to 'Block'. The 'Disabled' checkbox is unchecked. The 'Interface' is set to 'DMZ'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'Any'. A note at the top right says: '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.'

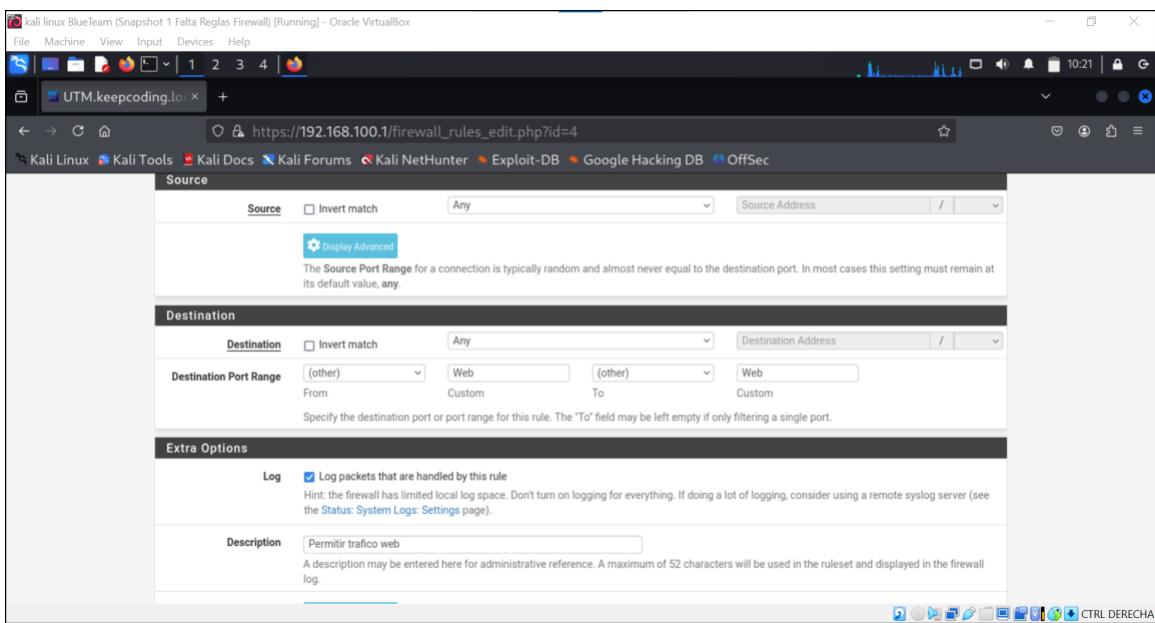
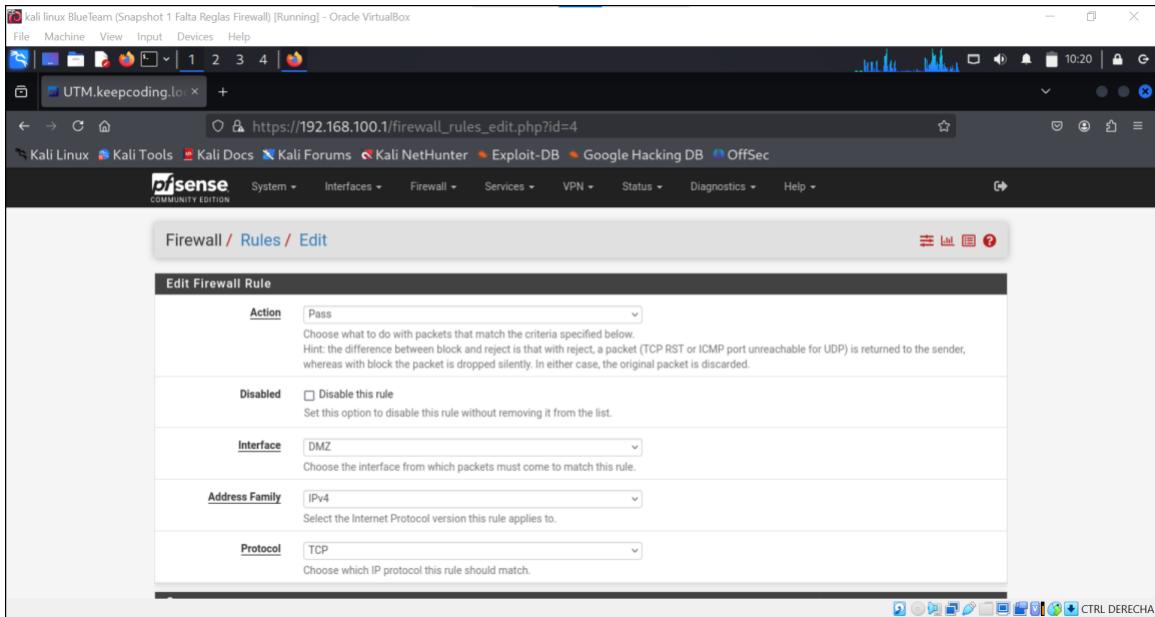
This screenshot shows the same 'Edit Firewall Rule' interface but with more detailed settings visible. The 'Protocol' dropdown is expanded to show 'Any'. Below it, the 'Source' and 'Destination' sections are shown. Under 'Source', 'Protocol' is 'Any', 'Invert match' is checked, and 'Source Address' is 'DMZ subnets'. Under 'Destination', 'Protocol' is 'Any', 'Invert match' is checked, and 'Destination Address' is 'DMZ2 subnets'. The 'Extra Options' section includes a checked 'Log' checkbox with a note about logging space. The 'Description' field contains 'Block DMZ2'. The 'Advanced Options' button is highlighted.

A continuación, bloquearemos también la comunicación entre la red DMZ y LAN.

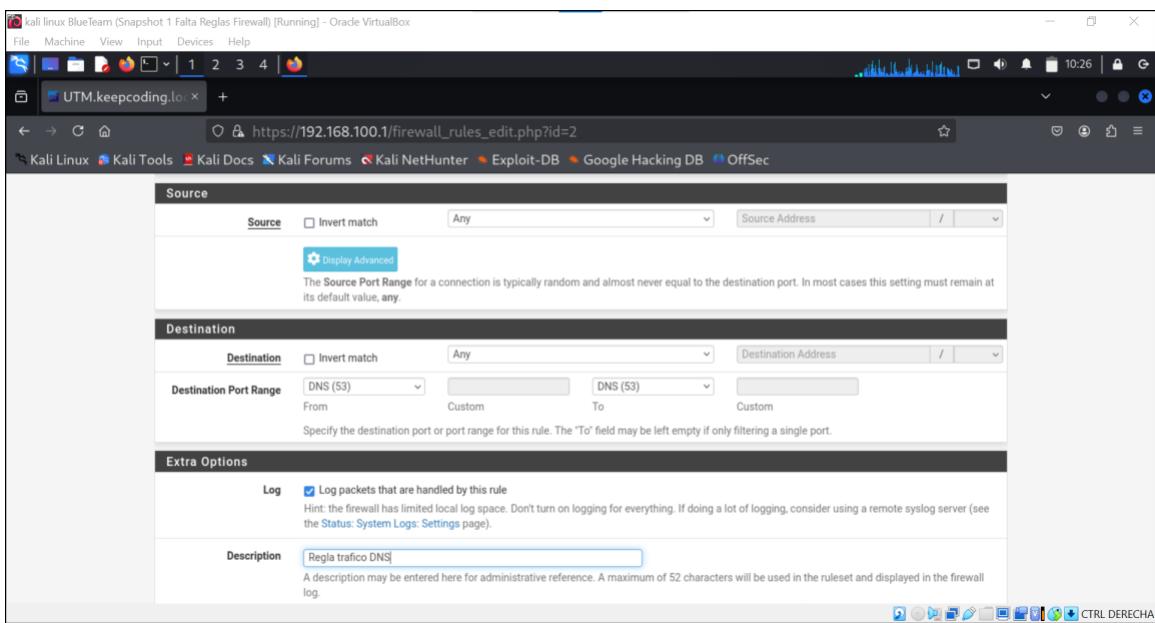
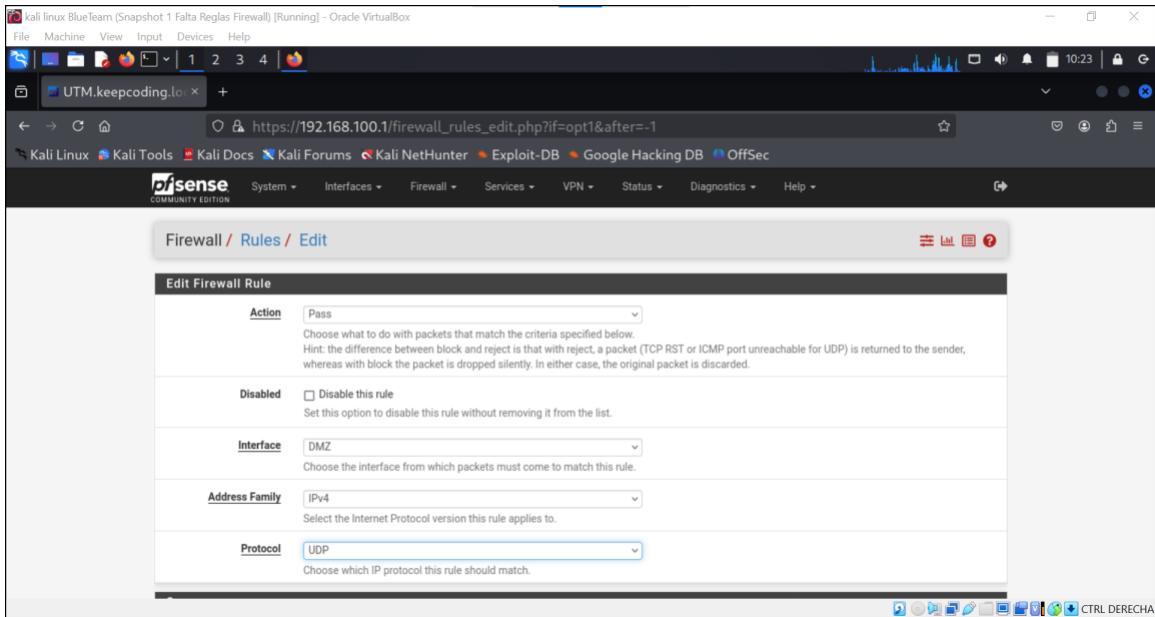
The screenshot shows the 'Edit Firewall Rule' interface in pfSense. The 'Action' dropdown is set to 'Block'. The 'Disabled' checkbox is unchecked. The 'Interface' is set to 'DMZ'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'Any'. The page includes a note about the difference between 'Block' and 'Reject' actions.

The screenshot shows the 'Edit Firewall Rule' interface in pfSense, expanded to show more details. The 'Protocol' is still 'Any'. Under 'Source', 'Source' is set to 'DMZ subnets' and 'Destination' is set to 'LAN subnets'. In the 'Extra Options' section, the 'Log' checkbox is checked. The 'Description' is 'Block LAN'. The 'Advanced Options' button is visible.

Después, vamos a permitir el tráfico web a la red de DMZ. Para ello se ha utilizado el protocolo UTP, que garantiza la importación de los paquetes enteros. Es el típico que se utiliza para conexiones HTTPS.



Ahora vamos a habilitar las reglas de DNS en la red de DMZ. Para ello se va a utilizar el protocolo UDP, que no garantiza importar los paquetes completos en diferencia al protocolo UTP.



Ahora vamos a habilitar el ping utilizando el protocolo ICMP, que es un protocolo de red perteneciente a la familia de protocolos TCP/IP que se utiliza para enviar mensajes de diagnóstico y control en las comunicaciones entre dispositivos de una red. Su principal objetivo es reportar errores, proporcionar información sobre problemas de conectividad y verificar el estado de la red.

The screenshot shows the 'Edit Firewall Rule' interface for a rule with the action set to 'Pass'. The 'Protocol' is selected as 'ICMP'. Under 'ICMP Subtypes', 'any' is selected, along with 'Alternate Host', 'Datagram conversion error', and 'Echo reply'. Other options like 'ICMPv6' and 'ICMPv4' are also listed.

The screenshot shows the 'Edit Firewall Rule' interface with a more detailed configuration. It includes sections for 'Source' (Source: Any, Destination: Any), 'Destination' (Destination: Any), 'Extra Options' (Log: checked, Log packets that are handled by this rule), and 'Description' (Protocol Ping ICMP). The 'Advanced Options' section has a 'display Advanced' button. A 'Save' button is at the bottom.

Y aquí tenemos todas las reglas de firewall que hemos asignado a DMZ.

The screenshot shows the pfSense Firewall Rules / DMZ interface. A message at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, there are tabs for Floating, WAN, LAN, DMZ (which is selected), and DMZ2. The main area displays a table of rules:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	X B	IPv4 *	DMZ subnets	*	DMZ2 subnets	*	*	none		Block DMZ2	
<input type="checkbox"/>	X B	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		Block LAN	
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	Web	*	none			Permitir trafico web	
<input checked="" type="checkbox"/>	0/0 B	IPv4 UDP	*	*	53 (DNS)	*	none			Regla trafico DNS	
<input checked="" type="checkbox"/>	0/0 B	IPv4 ICMP	*	*	*	*	*	none		Prot.	

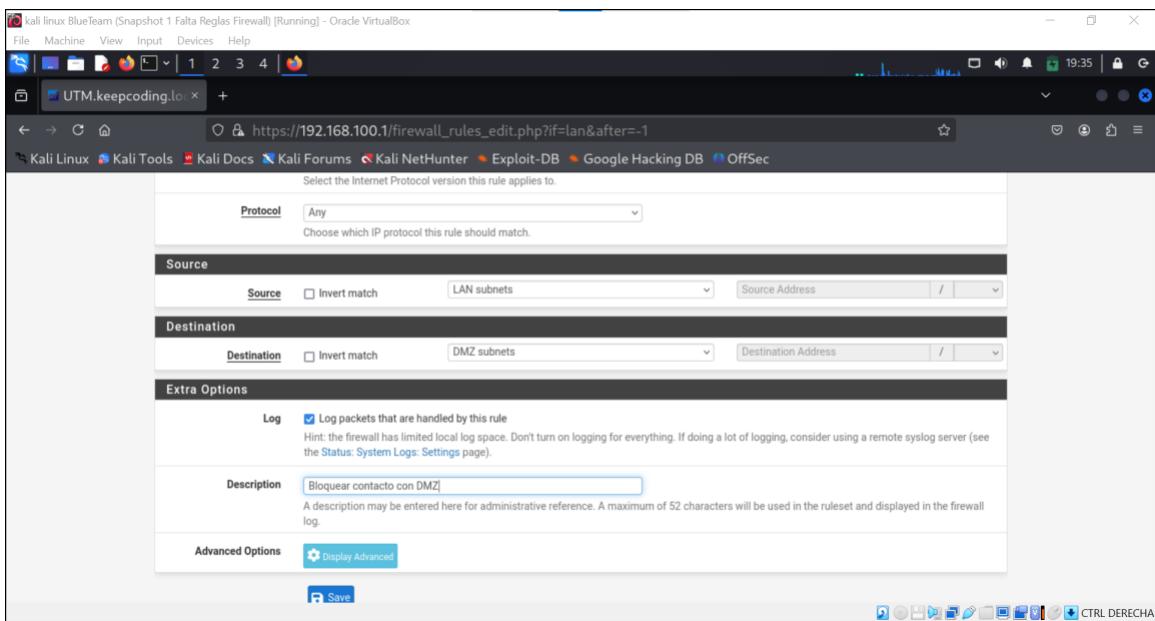
A tooltip "Toggle selected rules" is visible over the last column of the table. At the bottom, there are several icons for managing rules and a "CTRL DERECHA" key indicator.

1.4.3. Reglas Firewall LAN

Aquí solo vamos a añadir solamente una regla, porque las demás ya estaban creadas automáticamente.

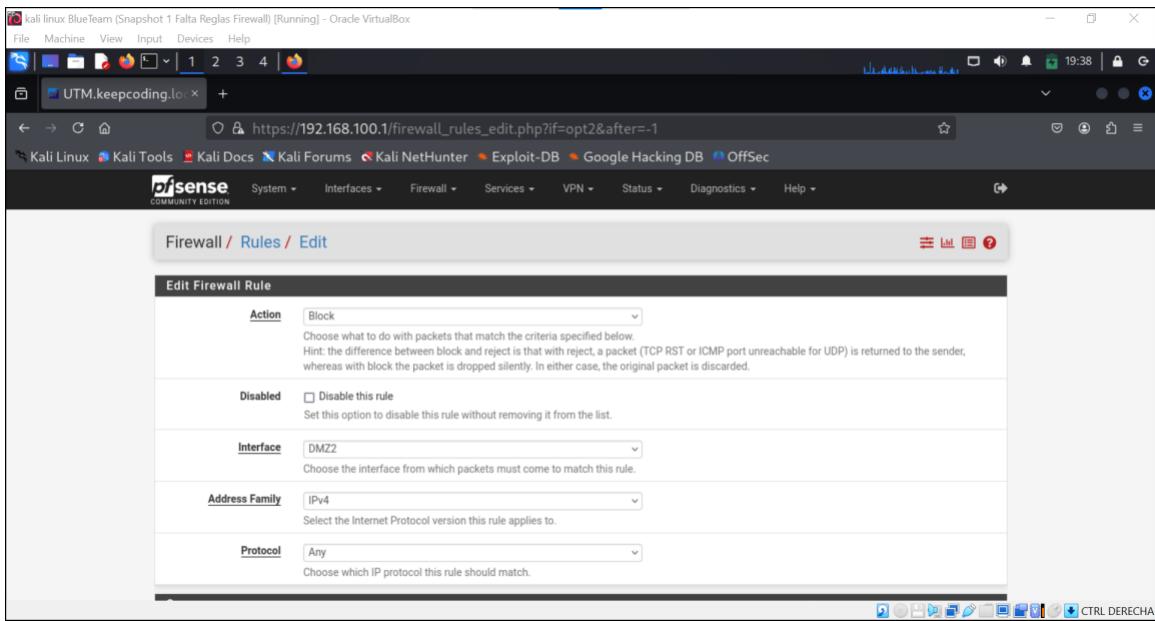
Vamos a bloquear la conexión con la red DMZ.

The screenshot shows the pfSense Edit Firewall Rule configuration dialog. The "Action" dropdown is set to "Block". The "Disabled" section contains a checkbox "Disable this rule" which is unchecked. The "Interface" dropdown is set to "LAN". The "Address Family" dropdown is set to "IPv4". The "Protocol" dropdown is set to "Any". A note below the "Protocol" field says: "Choose which IP protocol this rule should match." The pfSense navigation bar and browser header are visible at the top.



1.4.4. Reglas firewall DMZ2

Vamos a bloquear la comunicación con la red DMZ



The screenshot shows a web-based interface for managing firewall rules. The URL is https://192.168.100.1/firewall_rules_edit.php?f=opt2&after=-1. The form fields are as follows:

- Protocol:** Any
- Source:** Source: DMZ2 subnets, Destination: DMZ subnets
- Extra Options:** Log (checked), Description: Bloqueo contacto con DMZ
- Advanced Options:** display Advanced

Ahora vamos a permitir los paquetes web a las red DMZ2.

The screenshot shows a web-based interface for managing firewall rules on pfSense. The URL is https://192.168.200.1/firewall_rules_edit.php?f=opt2. The form fields are as follows:

- Action:** Pass
- Disabled:** Disable this rule
- Interface:** DMZ2
- Address Family:** IPv4
- Protocol:** TCP

The screenshot shows a web-based interface for managing firewall rules. The URL is https://192.168.200.1/firewall_rules_edit.php?f=opt2. The interface is divided into sections: Source, Destination, Extra Options, and a toolbar at the bottom.

- Source:** Set to "Any".
- Destination:** Set to "Web".
- Extra Options:**
 - Log:** Checked.
 - Description:** "Permitir paquetes WEB".

At the bottom right of the interface, there is a toolbar with various icons and the text "CTRL DERECHA".

Ahora vamos a crear la regla DNS.

The screenshot shows a web-based interface for managing firewall rules, specifically for pfSense. The URL is https://192.168.200.1/firewall_rules_edit.php?id=10. The interface is titled "Edit Firewall Rule".

Action: Pass (selected).
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: DMZ2
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: UDP
Choose which IP protocol this rule should match.

At the bottom right of the interface, there is a toolbar with various icons and the text "CTRL DERECHA".

The screenshot shows a web-based interface for editing a firewall rule. The URL is https://192.168.200.1/firewall_rules_edit.php?d=10. The rule configuration is as follows:

- Source:** Destination Port Range: DNS (53) -> DNS (53)
- Destination:** Destination Port Range: DNS (53) -> DNS (53)
- Extra Options:**
 - Log:** Log packets that are handled by this rule
 - Description:** Activo protocolo dns

Protocolo ping.

The screenshot shows a web-based interface for editing a firewall rule. The URL is https://192.168.200.1/firewall_rules_edit.php?f=opt2. The rule configuration is as follows:

- Action:** Pass
- Disabled:** Disable this rule
- Interface:** DMZ2
- Address Family:** IPv4
- Protocol:** ICMP
- ICMP Subtypes:** any, Alternate Host, Datagram conversion error, Echo reply

The screenshot shows the pfSense firewall rules configuration page. A new rule is being created with the following details:

- Source:** Source is set to "Any".
- Destination:** Destination is set to "Any".
- Extra Options:**
 - Log:** The checkbox "Log packets that are handled by this rule" is checked.
 - Description:** The description is "Protocolo Ping ICMP".
 - Advanced Options:** A "display Advanced" button is visible.
- Buttons:** A "Save" button is at the bottom.

1.4.5. Reglas firewall WAN

En este apartado hemos definido 3 reglas:

La primera es la que permite la conexión con red dentro de casa con la red DMZ.

La tercera es que nos podemos conectar mediante SSH a la red DMZ por el puerto 222.

The screenshot shows the pfSense Firewall / Rules / WAN interface. Three rules have been defined:

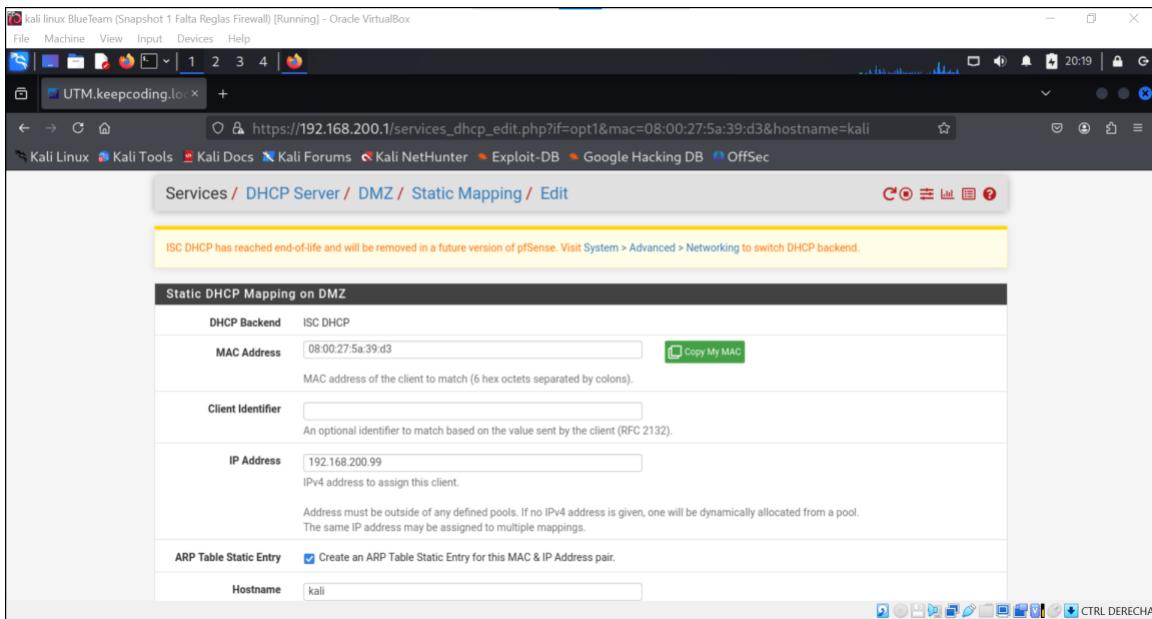
Index	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
1	0/0 B	IPv4 *	WAN subnets	*	DMZ subnets	*	*	none		Permitir conexión WAN a DMZ	
2	0/13 K/B	IPv4 TCP	*	*	192.168.100.99	80 (HTTP)	*	none		NAT Apache WAN	
3	0/0 B	IPv4 TCP	*	*	DMZ address	222	*	none		Puerto 222 para DMZ NAT SSH	

A message at the top indicates: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress."

1.5. Definir IPs estáticas

En este punto vamos a definir las IPs estáticas para las redes internas LAN, DMZ y DMZ2. El objetivo de esto es poder comprobar las conexiones entre ellas para verificar las reglas del firewall.

1.5.1 DMZ



The screenshot shows a Firefox browser window on a Kali Linux system. The URL is https://192.168.200.1/services_dhcp_edit.php?if=opt1&mac=08:00:27:5a:39:d3&hostname=kali. The page title is "Services / DHCP Server / DMZ / Static Mapping / Edit". A yellow warning box at the top states: "ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend." The main form is titled "Static DHCP Mapping on DMZ". It contains the following fields:

- DHCP Backend:** ISC DHCP
- MAC Address:** 08:00:27:5a:39:d3
- Client Identifier:** (empty input field)
- IP Address:** 192.168.200.99
- IPv4 address to assign this client.
Address must be outside of any defined pools. If no IPv4 address is given, one will be dynamically allocated from a pool.
The same IP address may be assigned to multiple mappings.
- ARP Table Static Entry:** Create an ARP Table Static Entry for this MAC & IP Address pair.
- Hostname:** kali

Screenshot 1: Kali Linux Terminal Output

```

kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
Home Trash File Actions Edit View Help
link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
    valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5a:39:d3 brd ff:ff:ff:ff:ff:ff
        inet 192.168.200.99/24 brd 192.168.200.255 scope global dynamic noprefixroute eth0
            valid_lft 7198sec preferred_lft 7198sec
            inet6 fe80::910f:4a21:3bcc:f90b/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
        inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
            valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ 

```

Screenshot 2: pfSense DHCP Leases Status

IP Address	MAC Address	Hostname	Description	Start	End	Actions
192.168.200.100	08:00:27:5a:39:d3	kali		2025/01/19 01:16:43	2025/01/19 03:16:43	Edit Delete

Interface	Pool Start	Pool End	Used	Capacity	Utilization
DMZ	192.168.200.100	192.168.200.200	1	101	0% of 101

[Show All Configured Leases](#) [Clear All DHCP Leases](#)

1.5.2 DMZ2

The screenshot shows the pfSense web interface under the 'Status / DHCP Leases' section. It displays two leases assigned to the 'DMZ2' interface. The first lease is for IP address 192.168.200.99 with MAC address 08:00:27:5a:39:d3, hostname 'kali', and start/end times 'n/a'. The second lease is for IP address 192.168.250.100 with MAC address 08:00:27:5a:39:d3, hostname 'kali', and start/end times 2025/01/19 01:24:06 / 2025/01/19 03:24:06. The 'Lease Utilization' table shows the pool range from 192.168.250.100 to 192.168.250.200, with one used lease and a capacity of 101.

The screenshot shows the pfSense web interface under the 'Services / DHCP Server / DMZ2 / Static Mapping / Edit' section. It is configuring a static DHCP mapping for the 'DMZ2' interface. The 'IP Address' field is set to 192.168.250.99, corresponding to the MAC address 08:00:27:5a:39:d3 and hostname 'kali'. A checkbox 'Create an ARP Table Static Entry for this MAC & IP Address pair.' is checked. The 'Client Identifier' field is empty.

```

kali linux BlueTeam (Snapshot 1 Falta Reglas Firewall) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4 | CTRL DERECHA

Home Trash File Actions Edit View Help
link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
    valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5a:39:d3 brd ff:ff:ff:ff:ff:ff
        inet 192.168.250.99 brd 192.168.250.255 scope global dynamic noprefixroute eth0
            valid_lft 7197sec preferred_lft 7197sec
            inet6 fe80::910f:4a21:3bcc:f90b/64 scope link noprefixroute
                valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
        inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
            valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
└─$ 

```

1.5.3 LAN

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

dhcse COMMUNITY EDITION

Status / DHCP Leases

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

	IP Address	MAC Address	Hostname	Description	Start	End	Actions
192.168.250.99	08:00:27:5a:39:d3	kali		n/a	n/a		
192.168.200.99	08:00:27:5a:39:d3	kali		n/a	n/a		
192.168.100.99	08:00:27:5a:39:d3	kali		n/a	n/a		
192.168.100.100	08:00:27:5a:39:d3	kali		2025/01/19 01:30:27	2025/01/19 03:30:27		

Lease Utilization

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

Static DHCP Mapping on LAN

DHCP Backend: ISC DHCP

MAC Address: 08:00:27:5a:39:d3

Client Identifier:

IP Address: 192.168.100.99

ARP Table Static Entry Create an ARP Table Static Entry for this MAC & IP Address pair.

Hostname: kali

```
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5a:39:d3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.99/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
        valid_lft 7198sec preferred_lft 7198sec
        inet6 fe80::910f:4a21:3bcc:f90b/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:fe:17:93:fd brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
```

2. Honeypots

Un honeypot es una herramienta que simula un equipo virtual, cuya función es enmascararse y adaptarse con la mayor exactitud a una página web ya existente para atraer a atacantes y estudiar su “modus operandi”. Por lo tanto, los puertos a esta máquina se suelen dejar fácilmente accesibles para que el atacante pueda acceder con una facilidad relativa; por el simple hecho de que si es demasiado simple acceder entonces sería fácil de llegar a la conclusión de que se trata de un honeypot.

También hay que recoger todos los logs en un documento de texto para después enviárselos a la plataforma web Elastic. Esto se ha logrado utilizando el comando “tail -f rdp.log | tee >> /var/log/log_honeypots”. Y después habría que sincronizar este archivo con otro que se encontraría en el escritorio. Todo esto nos va a permitir secopilar y analizar los logs en “tiempo real”.

Por lo tanto, para crear y configurar esta herramienta primero debemos a acceder a nuestra máquina virtual Kali y nos conectaremos a la red DMZ.

Cuando estemos dentro, activaremos la terminal y seguiremos los siguientes pasos:

1. Pondremos el siguiente comando:

```
docker run -p 222:2222 cowrie/cowrie #| El puerto 22 es el que corre el ssh.
```

2. Después en nuestra maquina Kali tenemos que hacer ip -a para saber nuestra ip.
3. Ejecutamos el siguiente comando en nuestro Windows, donde la ip es nuestra ip estatica:

```
ssh -p 222 root@192.168.200.99
```

4. Y desde ese momento ya tenemos el control sobre la máquina virtual.

The screenshot shows a Windows Command Prompt window with the following text output:

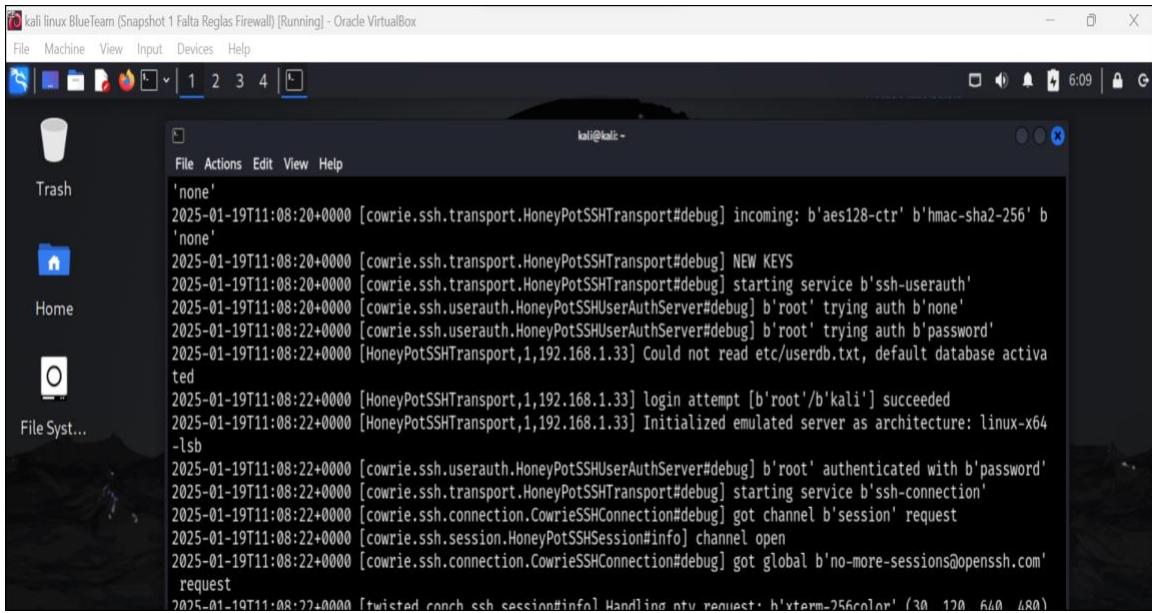
```
C:\WINDOWS\system32\cmd.exe - ssh -p 222 root@192.168.1.38
Microsoft Windows [Version 10.0.22631.4751]
(c) Microsoft Corporation. All rights reserved.

C:\Users\PC>ssh -p 222 root@192.168.200.99
ssh: connect to host 192.168.200.99 port 222: Connection timed out

C:\Users\PC>ssh -p 222 root@192.168.1.38
The authenticity of host '[192.168.1.38]:222 ([192.168.1.38]:222)' can't be established.
ED25519 key fingerprint is SHA256:m6YookPwrwyJEjy3KHxUqwE82w4gzMR4FLqSEZDUG/s.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.1.38]:222' (ED25519) to the list of known hosts.
root@192.168.1.38's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@svr04:~# dir
root@svr04:~# pwd
/root
```



A screenshot of a Kali Linux terminal window titled "kali@kali: ~". The window shows a terminal session with the following log output:

```
'none'  
2025-01-19T11:08:20+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] incoming: b'aes128-ctr' b'hmac-sha2-256' b  
'none'  
2025-01-19T11:08:20+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] NEW KEYS  
2025-01-19T11:08:20+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-userauth'  
2025-01-19T11:08:20+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'none'  
2025-01-19T11:08:22+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' trying auth b'password'  
2025-01-19T11:08:22+0000 [HoneyPotSSHTransport,1,192.168.1.33] Could not read etc/userdb.txt, default database activated  
2025-01-19T11:08:22+0000 [HoneyPotSSHTransport,1,192.168.1.33] login attempt [b'root'/b'kali'] succeeded  
2025-01-19T11:08:22+0000 [HoneyPotSSHTransport,1,192.168.1.33] Initialized emulated server as architecture: linux-x64  
-lsb  
2025-01-19T11:08:22+0000 [cowrie.ssh.userauth.HoneyPotSSHUserAuthServer#debug] b'root' authenticated with b'password'  
2025-01-19T11:08:22+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#debug] starting service b'ssh-connection'  
2025-01-19T11:08:22+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request  
2025-01-19T11:08:22+0000 [cowrie.ssh.session.HoneyPotSSHSession#info] channel open  
2025-01-19T11:08:22+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com'  
request  
2025-01-19T11:08:22+0000 [twisted.conch.ssh.session#info] Handling ntu request: b'vtterm-256color' (30 128 640 480)
```

3. Suricata

Suricata es una herramienta avanzada de detección y prevención de intrusiones que permite monitorear redes para identificar actividades sospechosas. Vamos a documentar su instalación, configuración y personalización mediante reglas diseñadas para detectar eventos específicos, como tráfico de red, intentos de conexión SSH y descargas de archivos PDF. La instalación se realiza actualizando los paquetes del sistema e instalando Suricata, seguida de una ejecución inicial para verificar su funcionamiento.

Además, se describieron procedimientos para analizar y guardar los logs generados, esenciales para el análisis posterior y la respuesta a incidentes. Los logs se almacenan en el directorio /var/log/suricata, y se pueden respaldar mediante compresión y transferencia a un servidor remoto para asegurar su disponibilidad. En conjunto, estas configuraciones convierten a Suricata en una herramienta poderosa para fortalecer la seguridad de la red, proporcionando visibilidad y capacidad de respuesta frente a posibles amenazas. Los logs posteriormente se guardarán en la plataforma web Elastic.

```
root@kali: /etc/suricata/rules
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.3 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48.7 kB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [258 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [192 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [868 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [23.3 kB]
Fetched 70.5 MB in 9s (7,570 kB/s)
163 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali㉿kali)-[~]
$ sudo apt install suricata
The following packages were automatically installed and are no longer required:
  libbfin1      libegl-dev      libgles-dev      libglvnd-dev      libpaper1      openjdk-23-jre
  libc++1-19    libfmt9        libgles1        libjxl0.9       libsuperlu6    openjdk-23-jre-headless
  libc++abi1-19 libgl1-mesa-dev libglvnd-core-dev libcrypto7t64 libunwind-19 python3-appdirs
Use 'sudo apt autoremove' to remove them.
```

```
root@kali: /etc/suricata/rules
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
Command 'udo' not found, but can be installed with:
sudo apt install udo
Do you want to install it? (N/y)
sudo apt install udo
The following packages were automatically installed and are no longer required:
  libbfin1      libegl-dev      libgles-dev      libglvnd-dev      libpaper1      openjdk-23-jre
  libc++1-19    libfmt9        libgles1        libjxl0.9       libsuperlu6    openjdk-23-jre-headless
  libc++abi1-19 libgl1-mesa-dev libglvnd-core-dev libcrypto7t64 libunwind-19 python3-appdirs
Use 'sudo apt autoremove' to remove them.

Installing:
  udo

Summary:
```

```
root@kali: /etc/suricata/rules
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ sudo -s
(root㉿kali)-[/home/kali]
# cd /etc/suricata
(root㉿kali)-[/etc/suricata]
# ls
classification.config reference.config rules suricata.yaml threshold.config
(root㉿kali)-[/etc/suricata]
# cd rules
(root㉿kali)-[/etc/suricata/rules]
# ls
app-layer-events.rules files.rules    kerberos-events.rules quic-events.rules stream-events.rules
decoder-events.rules   ftp-events.rules  modbus-events.rules  rfb-events.rules  tls-events.rules
dhcp-events.rules     http2-events.rules mqtt-events.rules  smb-events.rules
dnsp3-events.rules    http-events.rules nfs-events.rules   smtp-events.rules
dns-events.rules      ipsec-events.rules ntp-events.rules  ssh-events.rules
```

Primera regla de suricata.

```
root@kali: /etc/suricata/rules
File Actions Edit View Help
# less files.rules
(root㉿kali)-[/etc/suricata/rules]
# touch suricata.rules
(root㉿kali)-[/etc/suricata/rules]
# ls
app-layer-events.rules files.rules    kerberos-events.rules quic-events.rules stream-events.rules
decoder-events.rules   ftp-events.rules  modbus-events.rules  rfb-events.rules  suricata.rules
dhcp-events.rules     http2-events.rules mqtt-events.rules  smb-events.rules
dnsp3-events.rules    http-events.rules nfs-events.rules   smtp-events.rules
dns-events.rules      ipsec-events.rules ntp-events.rules  ssh-events.rules
(root㉿kali)-[/etc/suricata/rules]
# nano suricata.rules
(root㉿kali)-[/etc/suricata/rules]
# cat suricata.rules
alert tcp any any → any any (msg:trafico detectado; sid:1:)
```

```
# nano suricata.rules
(root@kali:[/etc/suricata])
# cat suricata.rules
alert tcp any any → any any (msg:trafico detectado; sid:1;)

(root@kali:[/etc/suricata])
# less suricata.rules
zsh: suspended less suricata.rules
[root@kali:/etc/suricata]
# less suricata.rules
zsh: suspended less suricata.rules
[root@kali:/etc/suricata]
# cd ..
```

```
GNU nano 8.2          suricata.yaml +
# See Napatech NTPL documentation other hashmodes and details on their use.
#
# This parameter has no effect if auto-config is disabled.
#
hashmode: hashStuplesorted

##
## Configure Suricata to load Suricata-Update managed rules.
##

#default-rule-path: /var/lib/suricata/rules
default-rule-path: /etc/suricata/rules

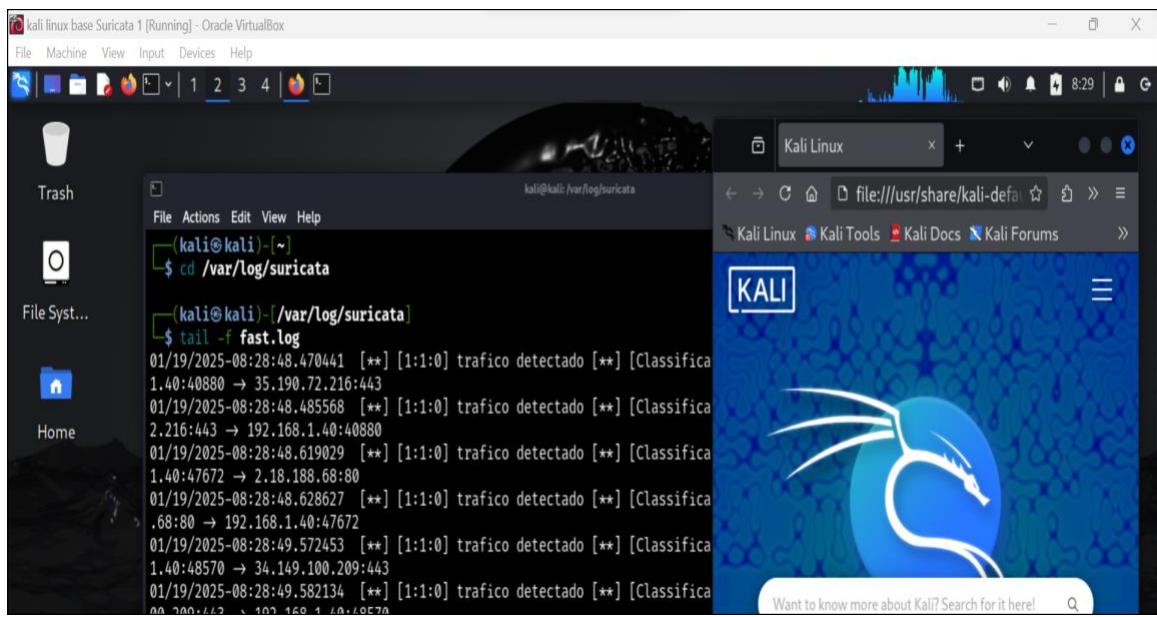
rule-files:
  - suricata.rules
##
```

kali linux BlueTeam Suricata [Running] - Oracle VirtualBox

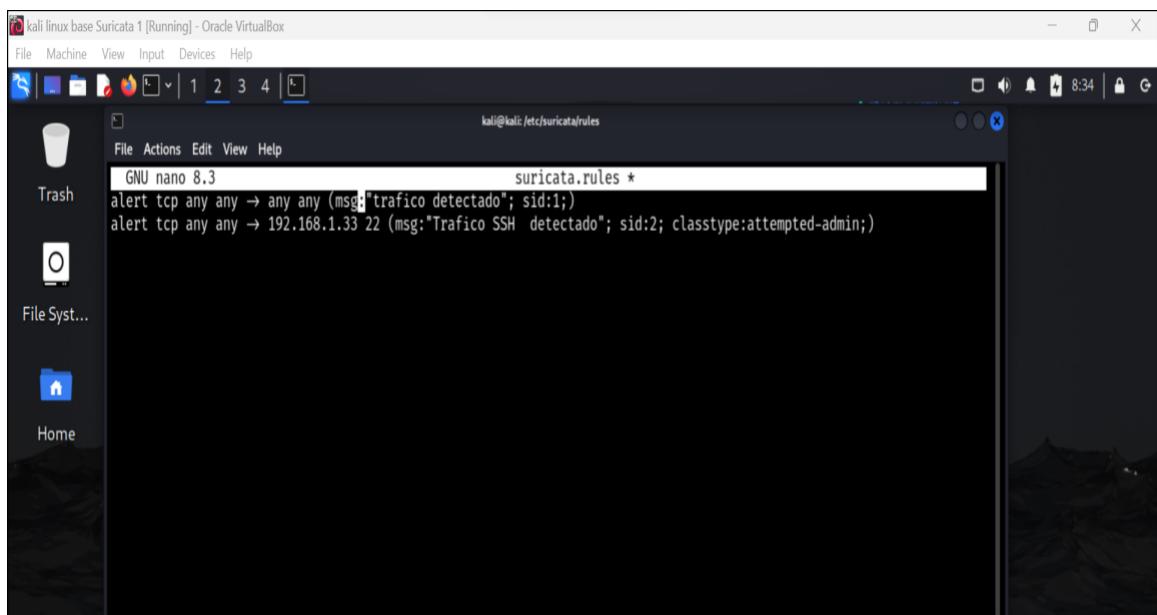
```
File Machine View Input Devices Help
Trash
File Syst...
Home
root@kali:/etc/suricata
File Actions Edit View Help
[root@kali ~]# cd ..
[root@kali ~]# ls
classification.config reference.config rules suricata.yaml threshold.config
[root@kali ~]# nano suricata.yaml
[root@kali ~]# nano suricata.yaml
[root@kali ~]# nano suricata.yaml
[root@kali ~]# sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
```

kali linux base Suricata 1 [Running] - Oracle VirtualBox

```
File Machine View Input Devices Help
Trash
File Syst...
Home
root@kali:/etc/suricata
File Actions Edit View Help
[root@kali ~]# less suricata.rules
zsh: suspended less suricata.rules
[root@kali ~]# cat suricata.rules
alert tcp any any → any any (msg:"trafico detectado"; sid:1;)
[root@kali ~]# cd ..
[root@kali ~]# ls
classification.config reference.config rules suricata.yaml threshold.config
[root@kali ~]# nano suricata.yaml
```



Segunda regla de suricata.



kali linux base Suricata 1 [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Trash

File Syst...

Home

File Actions Edit View Help

kali@kali: /var/log/suricata

```
.80:443 → 192.168.1.40:44396
01/19/2025-08:29:33.944178 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 34.36.54
.80:443 → 192.168.1.40:44380
01/19/2025-08:29:34.003756 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.40:35444 → 142.250.184.163:80
01/19/2025-08:29:34.003671 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.40:35428 → 142.250.184.163:80
01/19/2025-08:29:34.004212 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.40:35460 → 142.250.184.163:80
01/19/2025-08:29:34.014005 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 142.250.184.163:80 → 192.168.1.40:35444
01/19/2025-08:29:34.013998 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 142.250.184.163:80 → 192.168.1.40:35460
01/19/2025-08:29:34.014004 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 142.250.184.163:80 → 192.168.1.40:35428
01/19/2025-08:49:43.562965 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 192.168.1.33:58984 → 192.168.1.40:22
01/19/2025-08:49:43.562965 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.33:58984 → 192.168.1.40:22
01/19/2025-08:49:43.562965 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.33:58984 → 192.168.1.40:22
```

C:\WINDOWS\system32\cmd.exe

```
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Wireless LAN adapter Conexión de área local* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Conexión de área local* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi 2:

Connection-specific DNS Suffix . : home
Link-local IPv6 Address . . . . . : fe80::384:f84b:311f:a4be%14
IPv4 Address. . . . . : 192.168.1.33
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Conexión de red Bluetooth:
```

A screenshot of a terminal window titled "kali linux base Suricata 1 [Running] - Oracle VirtualBox". The window shows a file browser sidebar on the left with icons for Trash, File Syst..., and Home. The main terminal area has a dark background and displays the following command and its output:

```
kali@kali:~/var/log/suricata
$ tail -f fast.log
^C
[(kali㉿kali)-~/var/log/suricata]
$ tail -f fast.log
01/19/2025-08:29:33.944178 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 34.36.54.80:443 → 192.168.1.40:44380
01/19/2025-08:29:34.003756 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.40:35444 → 142.250.184.163:80
01/19/2025-08:29:34.003671 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.40:35428 → 142.250.184.163:80
01/19/2025-08:29:34.004212 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.40:35460 → 142.250.184.163:80
01/19/2025-08:29:34.014005 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 142.250.184.163:80 → 192.168.1.40:35444
01/19/2025-08:29:34.013998 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 142.250.184.163:80 → 192.168.1.40:35460
01/19/2025-08:29:34.014004 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 142.250.184.163:80 → 192.168.1.40:35428
01/19/2025-08:49:43.562965 [**] [1:2:0] Trafico SSH detectado [**] [Classification: Attempted Administrator Privile...
```

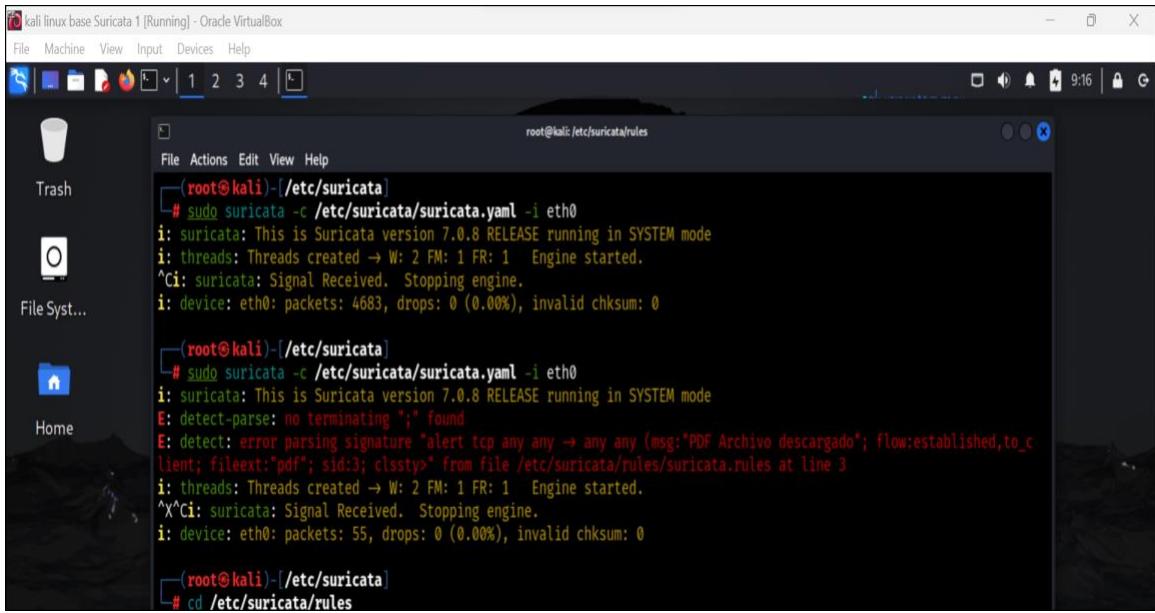
Tercera regla de suricata.

A screenshot of a terminal window titled "kali linux base Suricata 1 [Running] - Oracle VirtualBox". The window shows a file browser sidebar on the left with icons for Trash, File Syst..., and Home. The main terminal area has a dark background and displays the following command and its output:

```
root@kali:/etc/suricata/rules
# sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
i: threads: Threads created → W: 2 FM: 1 FR: 1 Engine started.
^C: suricata: Signal Received. Stopping engine.
i: device: eth0: packets: 4683, drops: 0 (0.00%), invalid checksum: 0

[(root㉿kali)-~/etc/suricata]
# sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
E: detect-parse: no terminating ";" found
E: detect: error parsing signature "alert tcp any any → any any (msg:"PDF Archivo descargado"; flow:established,to_client; fileext:"pdf"; sid:3; clssty:" from file /etc/suricata/rules/suricata.rules at line 3
i: threads: Threads created → W: 2 FM: 1 FR: 1 Engine started.
^X: suricata: Signal Received. Stopping engine.
i: device: eth0: packets: 55, drops: 0 (0.00%), invalid checksum: 0

[(root㉿kali)-~/etc/suricata]
# cd /etc/suricata/rules
```

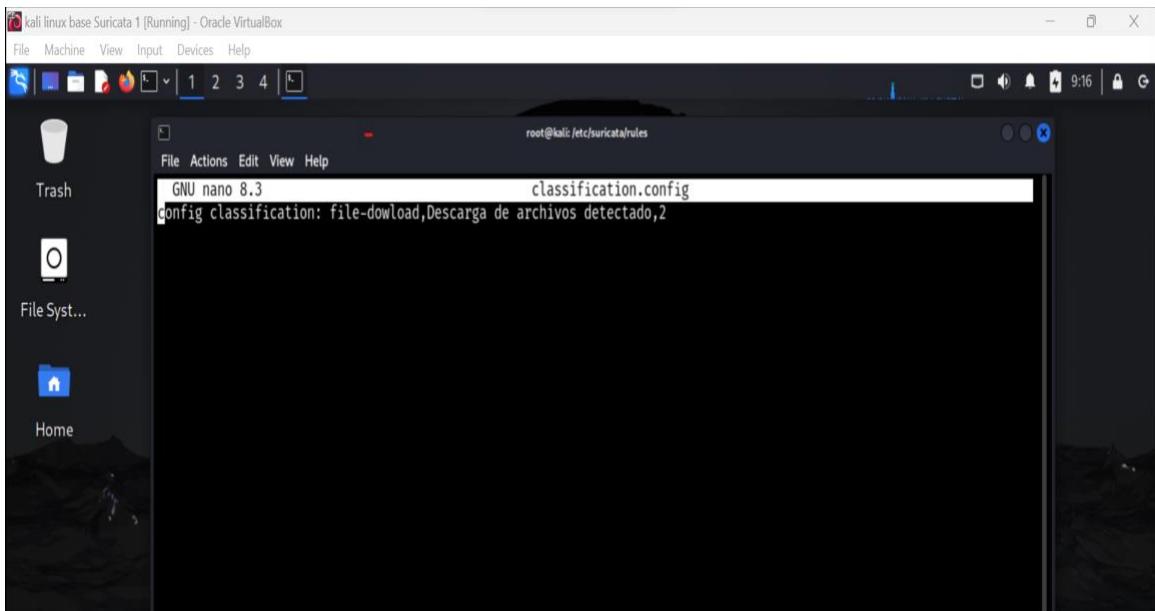


kali linux base Suricata 1 [Running] - Oracle VirtualBox

```
File Machine View Input Devices Help
Trash File Syst... Home
File Actions Edit View Help
root@kali:/etc/suricata/rules
[root@kali ~]# ./suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
i: threads: Threads created → W: 2 FM: 1 FR: 1 Engine started.
^C: suricata: Signal Received. Stopping engine.
i: device: eth0: packets: 4683, drops: 0 (0.00%), invalid checksum: 0

[root@kali ~]# ./suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
E: detect-parse: no terminating ";" found
E: detect: error parsing signature "alert tcp any any → any any (msg:"PDF Archivo descargado"; flow:established,to_client; fileext:"pdf"; sid:3; clssty:" from file /etc/suricata/rules/suricata.rules at line 3
i: threads: Threads created → W: 2 FM: 1 FR: 1 Engine started.
^X: suricata: Signal Received. Stopping engine.
i: device: eth0: packets: 55, drops: 0 (0.00%), invalid checksum: 0

[root@kali ~]# cd /etc/suricata/rules
```



kali linux base Suricata 1 [Running] - Oracle VirtualBox

```
File Machine View Input Devices Help
Trash File Syst... Home
File Actions Edit View Help
root@kali:/etc/suricata/rules
[root@kali ~]# nano classification.config
classification.config
config classification: file-download,Descarga de archivos detectado,2
```

A screenshot of a Kali Linux desktop environment within Oracle VirtualBox. The desktop has a dark theme with icons for Trash, Home, and File System. A terminal window is open in the foreground, showing the command 'nano /etc/suricata/rules'. The file contains several Suricata alert definitions:

```
GNU nano 8.3
root@kali:/etc/suricata/rules
alert tcp any any → any any (msg:"trafico detectado"; sid:1;)
alert tcp any any → 192.168.1.40 22 (msg:"Trafico SSH detectado"; sid:2; classtype:attempted-admin;)
alert tcp any any → any any (msg:"PDF Archivo descargado"; flow:established,to_client; fileext:"pdf"; sid:3; classtype:attempted-admin;)
```

A screenshot of a Kali Linux desktop environment within Oracle VirtualBox. The desktop has a dark theme with icons for Trash, Home, and File System. A terminal window is open in the foreground, showing the command 'nano classification.config'. The terminal output shows an error message from Suricata:

```
^X^C: suricata: Signal Received. Stopping engine.
i: device: eth0: packets: 55, drops: 0 (0.00%), invalid checksum: 0

(root@kali)-[/etc/suricata]
└─# cd /etc/suricata/rules
  └─# nano classification.config

(root@kali)-[/etc/suricata/rules]
└─# nano classification.config

[root@kali]-[/etc/suricata/rules]
└─# cd /suricata/ruels
cd: no such file or directory: /suricata/ruels

[root@kali]-[/etc/suricata/rules]
└─# cd /suricata/rules
cd: no such file or directory: /suricata/rules
```

```
kali@kali:~/etc/suricata$ cd ..
(kali㉿kali)-[~/etc/suricata]
$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
i: threads: Threads created → W: 2 FM: 1 FR: 1 Engine started.
^X^C i: suricata: Signal Received. Stopping engine.
i: device: eth0: packets: 30, drops: 0 (0.00%), invalid checksum: 0

(kali㉿kali)-[~/etc/suricata]
$ cd rules
(kali㉿kali)-[~/etc/suricata/rules]
$ sudo nano suricata.rules

(kali㉿kali)-[~/etc/suricata/rules]
$ cd ..
(kali㉿kali)-[~/etc/suricata]
$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
```

Microsoft Word - C:\Users\Kali\Documents\Capítulo 5 - Protocolo HTTP.docx

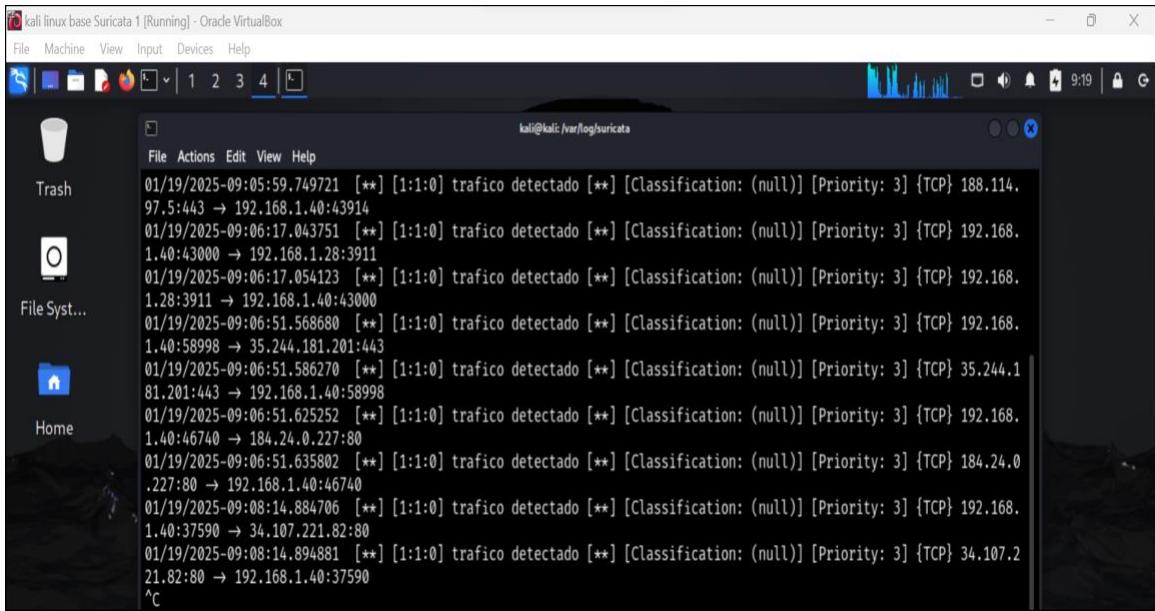
https://biblus.us.es/bibing/proyectos/abreproj/11214/fichero/TOMO+I%252F05+Capitulo+5+Protocolo+HTTP.pdf

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

1 of 8 Automatic Zoom

Capítulo 5: Protocolo HTTP

En este proyecto, se establece que los clientes, a través de la aplicación instalada en sus terminales, accedan al servicio que le proporciona la transacción económica, de alguna forma. Puesto que tanto el servicio como el terminal móvil admiten conexiones HTTP, vamos a usar este protocolo para realizar la comunicación. Por ello se va a



A screenshot of a terminal window titled "kali linux base Suricata 1 [Running] - Oracle VirtualBox". The window shows a list of log entries from the file "/var/log/suricata". The logs are timestamped and detail network traffic detection. The terminal interface includes a menu bar with File, Actions, Edit, View, Help, and a toolbar with icons for trash, file operations, and search.

```
File Actions Edit View Help
kali@kali: /var/log/suricata
01/19/2025-09:05:59.749721 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 188.114.97.5:443 → 192.168.1.40:43914
01/19/2025-09:06:17.043751 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.40:43000 → 192.168.1.28:3911
01/19/2025-09:06:17.054123 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.28:3911 → 192.168.1.40:43000
01/19/2025-09:06:51.568680 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.40:58998 → 35.244.181.201:443
01/19/2025-09:06:51.586270 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 35.244.1.81.201:443 → 192.168.1.40:58998
01/19/2025-09:06:51.625252 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.40:46740 → 184.24.0.227:80
01/19/2025-09:06:51.635802 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 184.24.0.227:80 → 192.168.1.40:46740
01/19/2025-09:08:14.884706 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.40:37590 → 34.107.221.82:80
01/19/2025-09:08:14.894881 [**] [1:1:0] trafico detectado [**] [Classification: (null)] [Priority: 3] {TCP} 34.107.21.82:80 → 192.168.1.40:37590
^c
```

4. Elastic

Por último, vamos a almacenar los logs en la web Elastic.

Para ello primero nos debemos de meter en la plataforma, en el apartado de Fleet, que lo que representa son las políticas del SIEM, que son un conjunto de reglas que se van aplicar a nuestros sistemas. Por ejemplo, para que un sistema operativo como kali tenga la misma configuración en toda la empresa. O podemos configurarlo por departamento, etc.

En conclusión, sirve para otorgar reglas de funcionamiento y acción.

En el primer caso que vamos a crear unas reglas para Suricata. Cuando vayamos a crear la primera política aparecerá una casilla automáticamente clicada "Collect system logs and metrics" que por defecto nos va a recoger los logs generados.

Cuando lleguemos a la parte de pegar el link que nos proporciona elastic, lo copiamos, abrimos nuestra máquina kali, y lo pegamos y ejecutamos.

4.1. Suricata

The screenshot shows the Kibana interface for the 'Assets' section. The left sidebar has a 'Security' tab selected, with options like Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore. The main panel is titled 'ASSETS' and contains sections for 'Fleet', 'Endpoints', and 'Cloud'. Each section has a brief description and a link to 'Cloud [BETA]'. At the bottom, there are links for 'Policies', 'Trusted applications', 'Event filters', 'Host isolation exceptions', 'Blocklist', and 'Response actions history'.

The screenshot shows the Elastic Fleet interface. The left sidebar has a 'Security' tab selected, with options like Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore. A message at the top says: 'We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.' The main panel is titled 'Fleet' and has a sub-header 'Centralized management for Elastic Agents.' Below it are tabs for 'Agents', 'Agent policies', 'Enrollment tokens', 'Uninstall tokens', 'Data streams', and 'Settings'. A 'Send feedback' button is visible. At the bottom, there is a search bar with 'Filter your data using KQL syntax', status filters ('Status 0', 'Tags 0', 'Agent policy 0'), and a 'Upgrade available' button. Below the search bar, it says 'Showing 0 agents' and 'Clear filters'.

The screenshot shows the 'Agent policies' section of the Fleet interface. The left sidebar includes options like Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore. The main area displays a message about added privileges for viewing and editing agent policies. Below this is a 'Fleet' header and a sub-header 'Centralized management for Elastic Agents.' A navigation bar at the top of the main content area includes 'Agents', 'Agent policies' (which is underlined), 'Enrollment tokens', 'Uninstall tokens', 'Data streams', and 'Settings'. A search bar with placeholder text 'Filter your data using KQL syntax' is followed by a 'Reload' button and a 'Create agent policy' button. A table header with columns 'Name', 'Last updated on', 'Unprivileged / Privileged', 'Integrations', and 'Actions' is shown, with a note 'No agent policies' below it.

The screenshot shows the 'Create agent policy' dialog box overlaid on the Fleet interface. The dialog has a title 'Create agent policy' and a descriptive text about agent policies. It contains a 'Name' input field with 'Suricata/Linux' typed into it, and a checked checkbox for 'Collect system logs and metrics'. There is also a link 'Advanced options' at the bottom right of the dialog.

Agent policies - Fleet - Elastic

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Assets / Fleet / Agent policies

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore

We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.

Fleet

Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens Uninstall tokens Data streams Settings

Filter your data using KQL syntax Reload Create agent policy

Name	Last updated on	Unprivileged / Privileged	Integrations	Actions
Suricata/Linux rev. 1	Jan 19, 2025	0 / 0 (0)	1	...

Suricata/Linux - Agent policies

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/a9fd3...

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Assets / Fleet / Agent policies Suricata/Linux

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore

Suricata/Linux

Revision 1 Integrations 1 Agents Add agent Last updated on Jan 19, 2025 Actions

Integrations Settings

Search... Namespace Add integration

Integration policy	Integration	Namespace	Output	Actions
system-1	System v1.63.2	default	Default output	...

Browse integrations - Integrations

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/integrations/browse... Give feedback

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Integrations / Browse integrations

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore

Integrations

Choose an integration to start collecting and analyzing your data.

Browse integrations **Installed integrations**

All categories 390

AWS 41 **Suricata** Azure 29 Cloud

Suricata Collect logs from

Can't find an Integration?
Create a custom one to fit your requirements [Create new integration](#)

Suricata - Integrations - Elastic

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/integrations/detail/suricata... Give feedback

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Integrations / Suricata

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore

Back to integrations

Suricata

Elastic Agent

Version 2.21.4 [Add Suricata](#)

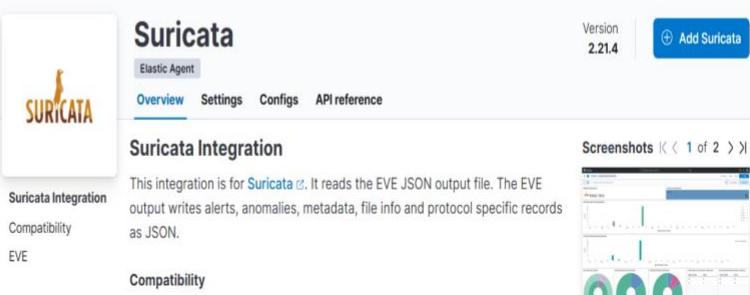
Overview **Settings** **Configs** **API reference**

Suricata Integration

This integration is for [Suricata](#). It reads the EVE JSON output file. The EVE output writes alerts, anomalies, metadata, file info and protocol specific records as JSON.

Suricata Integration Compatibility: EVE

Screenshots < 1 of 2 >



Ready to add your first integration?

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our [downloads page](#). This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our [installation docs](#).

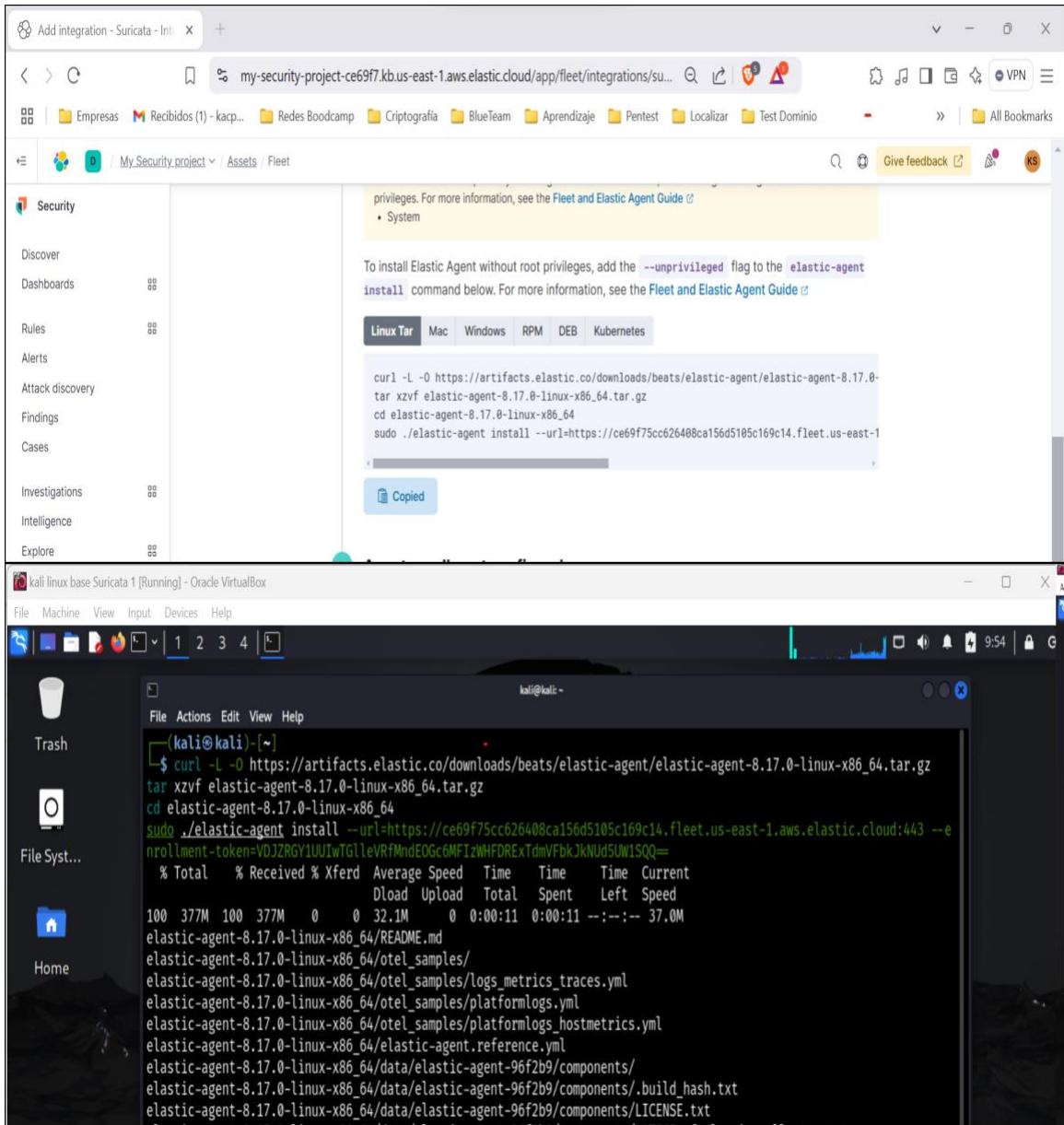
⚠ Root privileges required

This agent policy contains the following integrations that require Elastic Agents to have root privileges. To ensure that all data required by the integrations can be collected, enroll the agents using an account with root privileges. For more information, see the [Fleet and Elastic Agent Guide](#).

- System

To install Elastic Agent without root privileges, add the `--unprivileged` flag to the `elastic-agent install` command below. For more information, see the [Fleet and Elastic Agent Guide](#).

Linux Tar Mac Windows RPM DEB Kubernetes



The screenshot shows the 'Add integration - Suricata - Integrations' page in the Elastic Cloud interface. The left sidebar includes 'Discover', 'Dashboards', 'Rules', 'Alerts', 'Attack discovery', 'Findings', 'Cases', 'Investigations', 'Intelligence', and 'Explore'. The main content area displays instructions for installing the Elastic Agent without root privileges, providing a command-line example for Linux:

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.17.0-linux-x86_64.tar.gz  
tar xzvf elastic-agent-8.17.0-linux-x86_64  
cd elastic-agent-8.17.0-linux-x86_64  
sudo ./elastic-agent install --url=https://ce69f75cc626408ca156d5105c14.fleet.us-east-1
```

A 'Copied' message is visible at the bottom of the code block.

The screenshot shows the 'Agents - Fleet - Elastic' page in the Elastic Cloud interface. The left sidebar includes 'Discover', 'Dashboards', 'Rules', 'Alerts', 'Attack discovery', 'Findings', 'Cases', 'Investigations', 'Intelligence', and 'Explore'. The main content area features a 'Fleet' section with a sub-header 'Centralized management for Elastic Agents.' and tabs for 'Agents', 'Agent policies', 'Enrollment tokens', 'Uninstall tokens', 'Data streams', and 'Settings'. Below these tabs are two buttons: 'Ingest Overview Metrics' and 'Agent Info Metrics'. A search bar with the placeholder 'Filter your data using KQL syntax' is present. At the bottom, there are filters for 'Status' (Healthy 1, Unhealthy 0, Updating 0, Offline 0, Inactive 0, Unenrolled 0), 'Tags', 'Agent policy', and an 'Upgrade available' button. A note at the top right says 'We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.'

Agent policies - Fleet - Elastic

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Assets / Fleet / Agent policies

Send feedback

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore

Fleet

Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens Uninstall tokens Data streams Settings

Filter your data using KQL syntax

Create agent policy

Name	Last updated on	Unprivileged / Privileged	Integrations	Actions
Suricata/Linux rev. 1	Jan 19, 2025	0 / 1 (1)	1	...

Suricata/Linux - Agent policies

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/a9fd3...

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Assets / Fleet / Agent policies / Suricata/Linux

Send feedback

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore

View all agent policies

Suricata/Linux

Revision 1 Integrations 1 Agents 1 agent Last updated on Jan 19, 2025 Actions

Integrations Settings

Search...

Add integration

Integration policy	Integration	Namespace	Output	Actions
system-1	System v1.83.2	default	Default output	...

Screenshot of the 'Browse integrations' page in the Elastic Cloud interface.

The left sidebar shows navigation links: Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore.

The main area displays the 'Integrations' section with the title 'Integrations'. It says 'Choose an integration to start collecting and analyzing your data.' and provides tabs for 'Browse integrations' (selected) and 'Installed integrations'.

A search bar at the top right contains the text 'suricata'. Below it, there are two categories: 'AWS' with 41 integrations and 'Azure' with 29 integrations. A card for 'Suricata' is shown, with the subtext 'Collect logs from'.

A callout box in the top right corner says 'Can't find an Integration? Create a custom one to fit your requirements' with a 'Create new integration' button.

Screenshot of the 'Suricata - Integrations - Elastic' page in the Elastic Cloud interface.

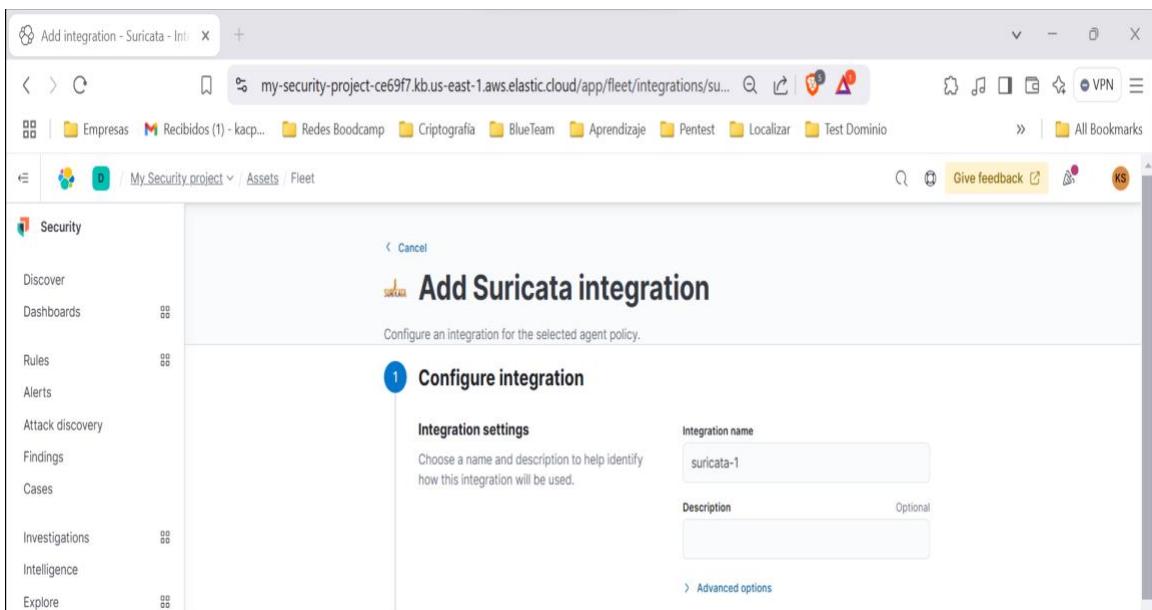
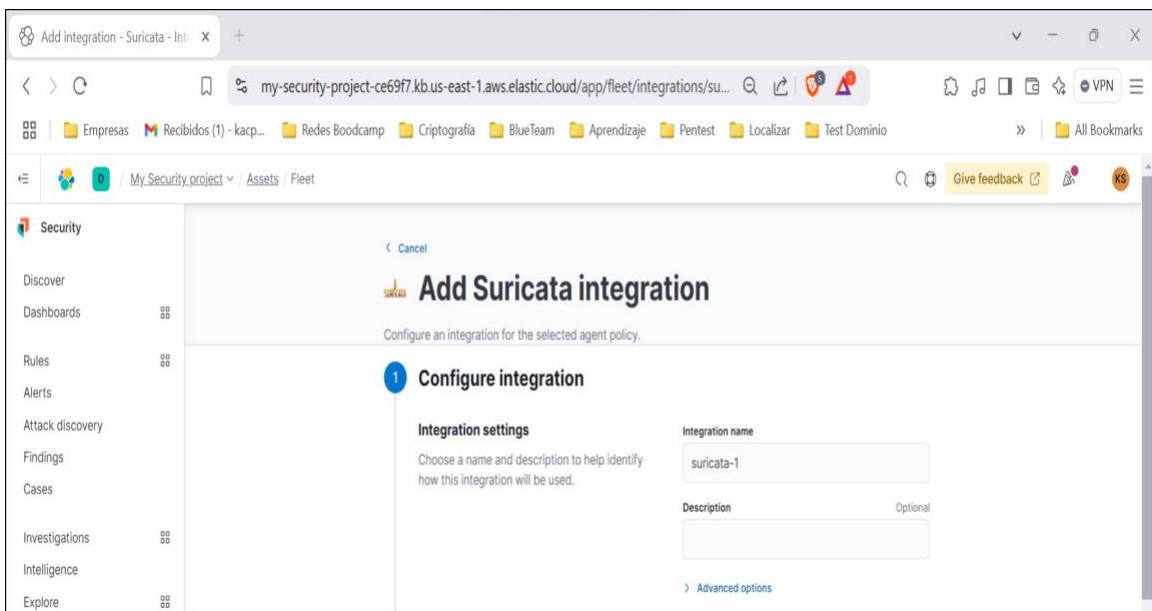
The left sidebar shows the same navigation links as the previous screenshot.

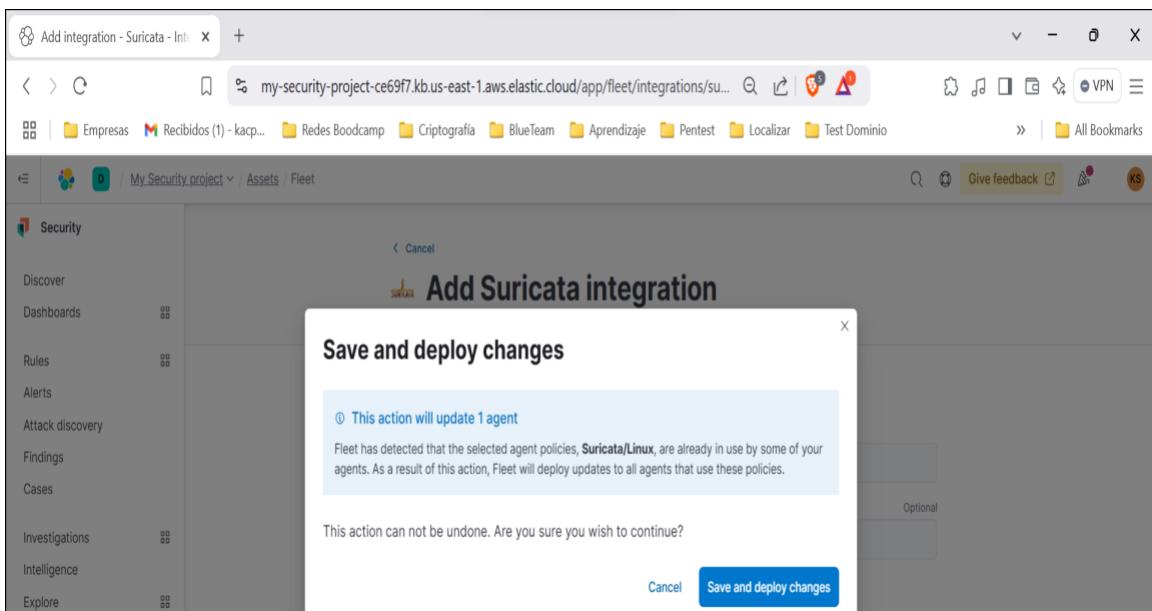
The main area displays the 'Suricata' integration details. It includes a logo, the version '2.21.4', and a 'Add Suricata' button.

Below this, the 'Suricata Integration' section is described: 'This integration is for [Suricata](#). It reads the EVE JSON output file. The EVE output writes alerts, anomalies, metadata, file info and protocol specific records as JSON.'

The 'Compatibility' section notes: 'This module has been developed against Suricata v4.0.4, but is expected to work with other versions of Suricata.'

A 'Screenshots' section shows two small preview images of the integration's interface.





The screenshot shows a browser window with the URL `my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/a9fd3...`. The main page has a sidebar with 'Security' selected and various navigation links. A table titled 'Suricata/Linux' is displayed under the 'Integrations' tab. The table has columns for 'Integration policy', 'Integration', 'Namespace', 'Output', and 'Actions'. It lists two entries: 'suricata-1' (Suricata v2.21.4, default namespace, Default output) and 'system-1' (System v1.63.2, default namespace, Default output). There is also a 'Settings' tab, a search bar, and a 'Send feedback' button at the top right of the table area.

Integration policy	Integration	Namespace	Output	Actions
suricata-1	Suricata v2.21.4	default	Default output	...
system-1	System v1.63.2	default	Default output	...

The screenshot shows the Elastic Fleet interface. On the left, a sidebar lists various security-related sections: Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore. The main area is titled 'Fleet' and contains tabs for Agents, Agent policies, Enrollment tokens, Uninstall tokens, Data streams, and Settings. Under the Agents tab, there are links for Ingest Overview Metrics and Agent Info Metrics. A search bar at the top right allows filtering by Status (Healthy), Tags, Agent policy, and Upgrade available. Below the search bar, a summary table shows one agent: 'Status' (Healthy), 'Host' (kali), 'Agent policy' (Suricata/Linux), 'CPU' (1.70 %), 'Memory' (215 MB), 'Last acti...' (16 seconds), 'Version' (8.17.0), and 'Actions'. The status is highlighted in green.

The screenshot shows the Elastic Discover interface. The sidebar includes Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore. The main area features a histogram with the x-axis representing time from January 19, 2025, to January 19, 2025, and the y-axis representing event counts from 0 to 200. The histogram shows a significant peak around 15:57. Below the histogram, a table displays 'Documents (229)'. The first document listed is: '@timestamp @ 2025-01-19T15:37:22.952Z @timestamp Jan 19, 2025 @ 16:04:02.966 agent.ephemeral_id 8c8b48bc-6bc3-4c10-8cec-623ab0acf2eb agent.id 172142d-afdf-4bc7-a0c4-97f5336b9bde agent.name kali agent.type filebeat agent.version 8.17.0'. There are also tabs for Patterns and Field statistics.

Ejemplo:

```
{  
  "@timestamp": [  
    "2025-01-19T15:37:22.952Z"  
  ],  
  "agent.ephemeral_id": [  
    "06a43a1d-699c-40c9-9b07-3dee85e78bcd"  
  ]}
```

],
"agent.id": [
 "7172142d-afd9-48c7-a0c4-97f5336b9bde"
],
"agent.name": [
 "kali"
],
"agent.type": [
 "filebeat"
],
"agent.version": [
 "8.17.0"
],
"component.id": [
 "log-default"
],
"component.state": [
 "HEALTHY"
],
"container.id": [
 "elastic-agent-8.17.0-96f2b9"
],
"data_stream.dataset": [
 "elastic_agent"
],
"data_stream.namespace": [

```
"default"

],
"data_stream.type": [
"logs"
],
"ecs.version": [
"8.0.0"
],
"elastic_agent.id": [
"7172142d-afd9-48c7-a0c4-97f5336b9bde"
],
"elastic_agent.snapshot": [
false
],
"elastic_agent.version": [
"8.17.0"
],
"event.agent_id_status": [
"verified"
],
"event.dataset": [
"elastic_agent"
],
"event.ingested": [
"2025-01-19T15:37:38.000Z"
],
]`
```

```
"host.architecture": [  
    "x86_64"  
,  
    "host.containerized": [  
        false  
,  
        "host.hostname": [  
            "kali"  
,  
            "host.id": [  
                "55e5305955694ed3b6c7506b1268fad8"  
,  
                "host.ip": [  
                    "192.168.1.40",  
                    "fe80::a414:97ff:512:c48b",  
                    "172.17.0.1"  
,  
                    "host.mac": [  
                        "02-42-86-07-EA-9E",  
                        "08-00-27-DF-0F-2D"  
,  
                        "host.name": [  
                            "kali"  
,  
                            "host.os.codename": [  
                                "kali-rolling"
```

```
],
"host.os.family": [
    "debian"
],
"host.os.kernel": [
    "6.11.2-amd64"
],
"host.os.name": [
    "Kali GNU/Linux"
],
"host.os.name.text": [
    "Kali GNU/Linux"
],
"host.os.platform": [
    "kali"
],
"host.os.type": [
    "linux"
],
"host.os.version": [
    "2024.4"
],
"input.type": [
    "filestream"
],
"log.file.device_id": [
```

"2049"

],

"log.file.inode": [

"1836133"

],

"log.file.path": [

"/opt/Elastic/Agent/data/elastic-agent-8.17.0-96f2b9/logs/elastic-agent-20250119-2.ndjson"

],

"log.level": [

"info"

],

"log.offset": [

78081

],

"log.origin.file.line": [

663

],

"log.origin.file.name": [

"coordinator/coordinator.go"

],

"log.origin.function": [

"github.com/elastic/elastic-
agent/internal/pkg/agent/application/coordinator.(*Coordinator).watchRuntimeCompone
nts"

],

"log.source": [

```
"elastic-agent"
],
"message": [
    "Unit      state      changed      log-default-logfile-suricata-4219fd77-11b9-4bf6-9a49-0e43da5419e1 (STARTING->HEALTHY): Healthy"
],
"unit.id": [
    "log-default-logfile-suricata-4219fd77-11b9-4bf6-9a49-0e43da5419e1"
],
"unit.old_state": [
    "STARTING"
],
"unit.state": [
    "HEALTHY"
],
"unit.type": [
    "input"
],
"_id": "AZR_NrR0sttFzmZkTyyt",
"_index": ".ds-logs-elasticsearch-default-2025.01.19-000001",
"_score": null
}
```

4.2. HoneyPot

The screenshot shows the Kibana interface for the 'Assets' section. The left sidebar has a 'Security' icon and lists various navigation options: Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore. The main content area is titled 'Assets' and contains three sections: 'Fleet', 'Endpoints', and 'Cloud'. The 'Fleet' section includes 'Centralized management for Elastic Agents', 'Agents', 'Policies', and 'Enrollment tokens'. The 'Endpoints' section includes 'Hosts running Elastic Defend.', 'Policies', and 'Event filters'. The 'Cloud' section includes 'Cloud hosts running Elastic Defend.'.

The screenshot shows the Kibana interface for the 'Agents - Fleet' section. The left sidebar has a 'Security' icon and lists various navigation options: Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore. A message at the top states: 'We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.' The main content area is titled 'Fleet' and includes tabs for 'Agents', 'Agent policies', 'Enrollment tokens', 'Uninstall tokens', 'Data streams', and 'Settings'. Below these tabs, there are sections for 'Ingest Overview Metrics' and 'Agent Info Metrics'. A search bar at the bottom allows filtering data using KQL syntax. At the very bottom, it shows 'Showing 1 agent' with status indicators: Healthy (1), Unhealthy (0), Updating (0), Offline (0), Inactive (0), and Unenrolled (0). There are also buttons for 'Clear filters', 'Status', 'Tags', 'Agent policy', and 'Upgrade available'.

The screenshot shows the 'Agent policies' section of the Fleet interface. On the left, a sidebar lists various security-related options like Discover, Dashboards, Rules, and Findings. The main area is titled 'Fleet' and describes it as 'Centralized management for Elastic Agents'. Below this, there are tabs for Agents, Agent policies (which is selected), Enrollment tokens, Uninstall tokens, Data streams, and Settings. A search bar at the top allows filtering by KQL syntax. A prominent blue button labeled '+ Create agent policy' is visible. A table below shows existing agent policies, with one entry for 'Suricata/Linux'.

This screenshot shows the 'Create agent policy' dialog box overlaid on the Fleet interface. The dialog has a title 'Create agent policy' and a descriptive text explaining that agent policies manage settings across groups of agents. It includes a 'Name' input field where 'HoneyPot' is typed, and a checked checkbox for 'Collect system logs and metrics'. There is also a link to 'Advanced options'.

HoneyPot - Agent policies - File x +

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/b402c...

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Assets / Fleet / Agent policies HoneyPot Give feedback Send feedback

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore

View all agent policies

HoneyPot

Integrations Settings

Revision 1 Integrations 1 Agents Add agent Last updated on Jan 19, 2025 Actions

Search... Namespace Add integration

Integration policy	Integration	Namespace	Output	Actions
system-2	System v1.63.2	default	Default output	...

Browse integrations - Integrations - File x +

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/integrations/browse...

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografia BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Integrations / Browse integrations Give feedback

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore

All categories 390

AWS 41

Azure 29

Cloud 89

Containers 15

Custom 30

Database 29

Elastic Stack 12

Elasticsearch, CSV 6

Connection details

Custom Azure Blob Storage Input Collect log data from configured Azure Blob Storage Container with Elastic Agent.	Custom GCS (Google Cloud Storage) Input Collect JSON data from configured GCS Bucket with Elastic Agent.	Custom Google Pub/Sub Logs Collect Logs from Google Pub/Sub topics
Custom HTTP Endpoint Logs Collect JSON data from listening HTTP port with Elastic Agent.	Custom Journald logs Collect logs from journald with Elastic Agent.	Custom Kafka Logs Collect data from kafka topic with Elastic Agent.

Custom Logs - Integrations - my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/integrations/detail/...

Empresas Recibidos (1) - kacp... Redes Boodcamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Integrations / Custom Logs

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore

Custom Logs

Elastic Agent

Version 2.3.3 Add Custom Logs

Overview Settings Configs

Custom Logs Package

The Custom Logs package is used to ingest arbitrary log files and parse their contents using Ingest Pipelines. Follow the steps below to set up and use this package.

Get started ECS Field Mapping

Details

Version 2.3.3 Category Custom, Custom Logs Subscription - Developed by Elastic

This screenshot shows the 'Custom Logs' integration page within the Elastic Cloud interface. On the left, there's a sidebar with various security-related options like Discover, Dashboards, and Rules. The main area is titled 'Custom Logs' and features a large icon of a document with three horizontal lines. Below the icon, it says 'Elastic Agent' and 'Version 2.3.3'. There are tabs for Overview, Settings, and Configs, with 'Overview' selected. A section titled 'Custom Logs Package' describes its purpose for ingesting log files and parsing them using Ingest Pipelines. It includes links to 'Get started' and 'ECS Field Mapping'. To the right, there's a 'Details' panel showing the version, category (Custom, Custom Logs), subscription status, and developer information (Elastic). At the bottom right of the main area is a blue button labeled '+ Add Custom Logs'.

Add integration - Custom Log - my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/lo...

Empresas Recibidos (1) - kacp... Redes Boodcamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Assets / Fleet

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore

Add Custom Logs integration

Configure an integration for the selected agent policy.

1 Configure integration

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name: log-1

Description: /home/kali/Desktop

Optional

Advanced options

This screenshot shows the 'Add Custom Logs integration' configuration dialog. On the left, there's a sidebar with security-related options like Discover, Dashboards, and Rules. The main area is titled 'Add Custom Logs integration' and has a sub-section 'Configure integration'. It asks to 'Configure an integration for the selected agent policy.' Below this, there's a step 1 'Configure integration' section. It has a 'Integration settings' sub-section with a note about choosing a name and description. It shows an 'Integration name' field containing 'log-1' and a 'Description' field containing '/home/kali/Desktop'. There's also an 'Optional' label next to the description field. At the bottom of this section is a link 'Advanced options'. The top of the dialog has a 'Cancel' button and a 'Next Step' button.

Add integration - Custom Log

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/lo...

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Assets / Fleet

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name: log-1

Description: Optional

Advanced options

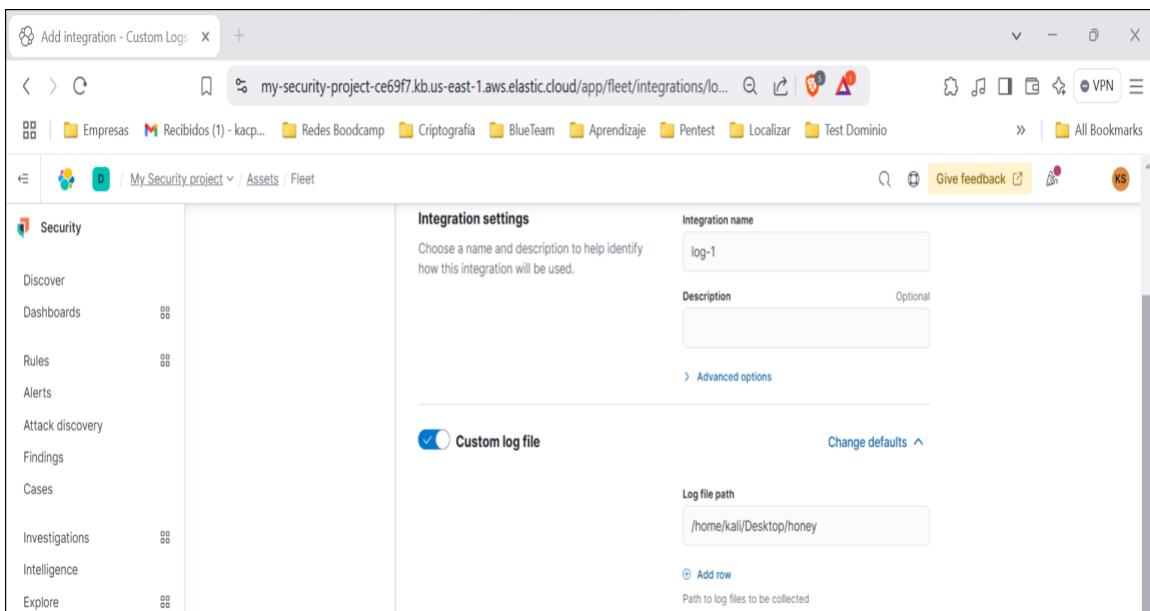
Custom log file (checked)

Change defaults

Log file path: /home/kali/Desktop/honey

Add row

Path to log files to be collected



HoneyPot - Agent policies - Fle

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies/b402c...

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Assets / Fleet / Agent policies / HoneyPot

Security

Discover

Dashboards

Rules

Alerts

Attack discovery

Findings

Cases

Investigations

Intelligence

Explore

HoneyPot

Integrations Settings

Search...

Integration policy: log-1

system-2

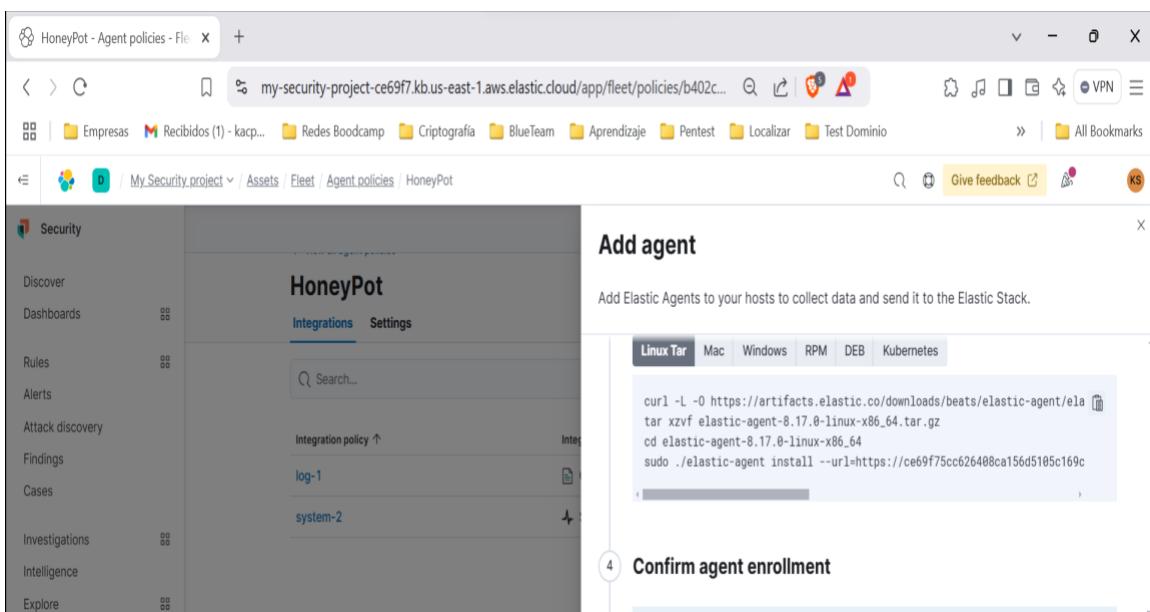
Add agent

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

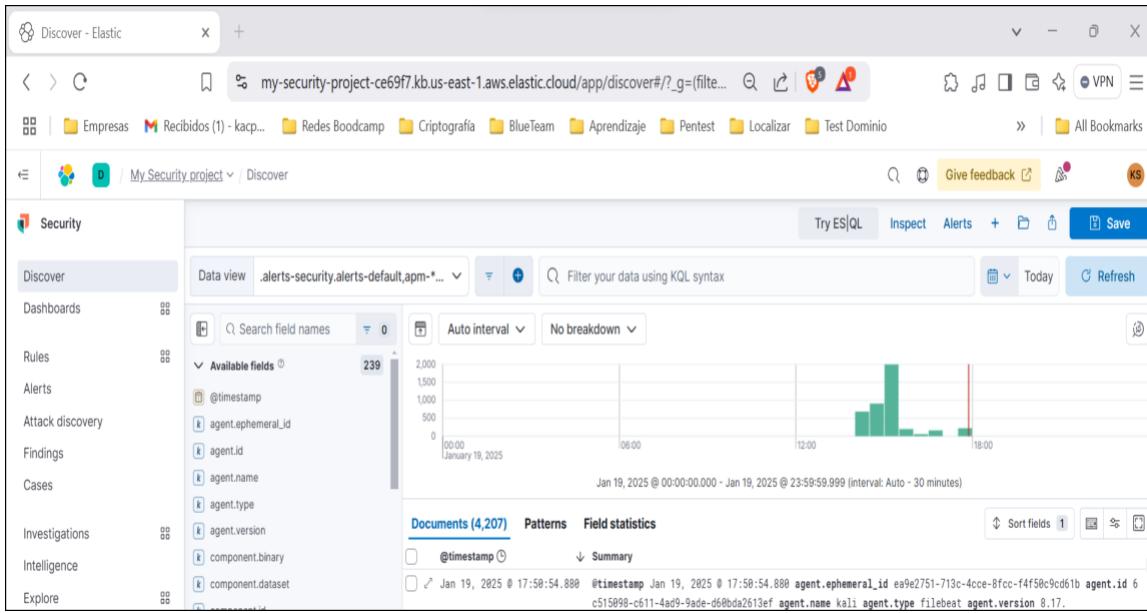
Linux Tar Mac Windows RPM DEB Kubernetes

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/ela...
tar xzvf elastic-agent-8.17.0-linux-x86_64.tar.gz
cd elastic-agent-8.17.0-linux-x86_64
sudo ./elastic-agent install --url=https://ce69f75cc626408ca156d5105c169c
```

4 Confirm agent enrollment



The screenshot shows the 'Agent policies' page within the HoneyPot project. The left sidebar includes options like Security, Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore. The main content area displays the 'HoneyPot' dashboard with sections for Integrations (selected) and Settings. A search bar is present. Below these are two entries: 'log-1' and 'system-2'. To the right, a modal window titled 'Add agent' is open, showing the message 'Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.' Below this, a success message 'Agent enrollment confirmed' is displayed with the note '1 agent has been enrolled.' and a 'View enrolled agents' button.



Ejemplo:

```
{
  "@timestamp": [
    "2025-01-19T16:50:43.343Z"
  ],
  "agent.ephemeral_id": [
    "3c02ab2e-e741-4b27-b23a-692c003e04a4"
  ],
  "agent.id": [
    "6c515098-c611-4ad9-9ade-d60bda2613ef"
  ],
  "agent.name": [
    "kali"
  ],
  "agent.type": [
    "filebeat"
  ]
}
```

```
],
"agent.version": [
    "8.17.0"
],
"data_stream.dataset": [
    "generic"
],
"data_stream.namespace": [
    "default"
],
"data_stream.type": [
    "logs"
],
"ecs.version": [
    "8.0.0"
],
"elastic_agent.id": [
    "6c515098-c611-4ad9-9ade-d60bda2613ef"
],
"elastic_agent.snapshot": [
    false
],
"elastic_agent.version": [
    "8.17.0"
],
"event.agent_id_status": [
```

```
    "verified":  
    ],  
    "event.dataset": [  
        "generic"  
    ],  
    "event.ingested": [  
        "2025-01-19T16:50:54.000Z"  
    ],  
    "host.architecture": [  
        "x86_64"  
    ],  
    "host.containerized": [  
        false  
    ],  
    "host.hostname": [  
        "kali"  
    ],  
    "host.id": [  
        "55e5305955694ed3b6c7506b1268fad8"  
    ],  
    "host.ip": [  
        "192.168.1.38",  
        "fe80::910f:4a21:3bcc:f90b",  
        "172.17.0.1",  
        "fe80::42:e0ff:fe05:163f",  
        "fe80::20a5:2eff:fe7f:36",  
        "fe80::172.17.0.1%1"  
    ]  
}
```

"fe80::7489:baff:feb1:47ed"

],

"host.mac": [

"02-42-E0-05-16-3F",

"08-00-27-5A-39-D3",

"22-A5-2E-7F-00-36",

"76-89-BA-B1-47-ED"

],

"host.name": [

"kali"

],

"host.os.codename": [

"kali-rolling"

],

"host.os.family": [

"debian"

],

"host.os.kernel": [

"6.11.2-amd64"

],

"host.os.name": [

"Kali GNU/Linux"

],

"host.os.name.text": [

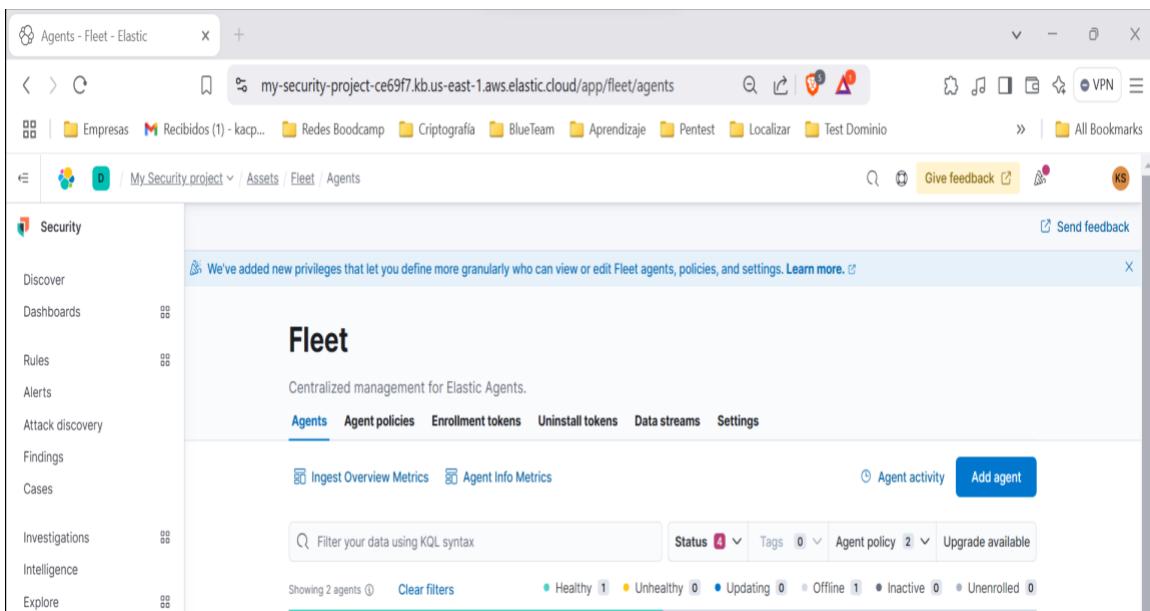
"Kali GNU/Linux"

],

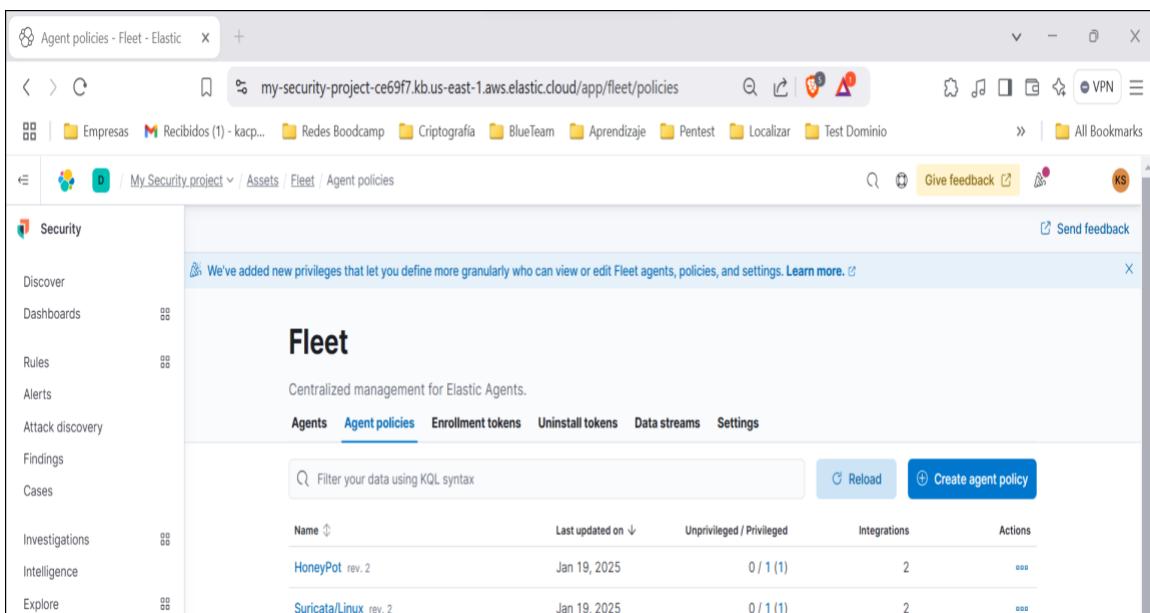
```
"host.os.platform": [  
    "kali"  
],  
"host.os.type": [  
    "linux"  
],  
"host.os.version": [  
    "2024.4"  
],  
"input.type": [  
    "log"  
],  
"log.file.path": [  
    "/home/kali/Desktop/honey"  
],  
"log.file.path.text": [  
    "/home/kali/Desktop/honey"  
],  
"log.offset": [  
    718  
],  
"message": [  
    "2025-01-19T16:21:57.442331Z, domain:, username:, password:, hostname: KK"  
],  
    "_id": "AZR_ebR0sttFzmZ8Ty3r",  
    "_index": ".ds-logs-generic-default-2025.01.19-000001",
```

```
        "_score": null  
    }  
  
}
```

4.3. Windows



The screenshot shows the Elastic Fleet interface for managing agents. The left sidebar includes options like Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore. The main content area is titled 'Fleet' and describes centralized management for Elastic Agents. It features tabs for Agents, Agent policies, Enrollment tokens, Uninstall tokens, Data streams, and Settings. The Agents tab is selected, showing an 'Ingest Overview Metrics' section with 'Agent activity' and 'Add agent' buttons. Below this is a search bar and a status filter section. A message at the top right says, 'We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.'



The screenshot shows the Elastic Fleet interface for managing agent policies. The left sidebar includes options like Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore. The main content area is titled 'Fleet' and describes centralized management for Elastic Agents. It features tabs for Agents, Agent policies, Enrollment tokens, Uninstall tokens, Data streams, and Settings. The Agent policies tab is selected, showing a 'Create agent policy' button and a table of existing policies. The table columns include Name, Last updated on, Unprivileged / Privileged, Integrations, and Actions. Two policies are listed: 'HoneyPot rev. 2' and 'Suricata/Linux rev. 2'. The 'HoneyPot' policy was last updated on Jan 19, 2025, has 0/1 (1) integrations, and 2 actions. The 'Suricata/Linux' policy was last updated on Jan 19, 2025, has 0/1 (1) integrations, and 2 actions.

Name	Last updated on	Unprivileged / Privileged	Integrations	Actions
HoneyPot rev. 2	Jan 19, 2025	0 / 1 (1)	2	...
Suricata/Linux rev. 2	Jan 19, 2025	0 / 1 (1)	2	...

Agent policies - Fleet - Elastic

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies?create

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Assets / Fleet / Agent policies

Security

Discover

Dashboards

Rules

Alerts

Attack discovery

Findings

Cases

Investigations

Intelligence

Explore

Fleet

Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens Uninstall tokens

Filter your data using KQL syntax

Name: Windows

Collect system logs and metrics

Advanced options

We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.

Create agent policy

Agent policies are used to manage settings across a group of agents. You can add integrations to your agent policy to specify what data your agents collect. When you edit an agent policy, you can use Fleet to deploy updates to a specified group of agents.

Agent policies - Fleet - Elastic

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/policies

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Assets / Fleet / Agent policies

Send feedback

Security

Discover

Dashboards

Rules

Alerts

Attack discovery

Findings

Cases

Investigations

Intelligence

Explore

Fleet

Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens Uninstall tokens Data streams Settings

Filter your data using KQL syntax

Reload Create agent policy

Name	Last updated on	Unprivileged / Privileged	Integrations	Actions
Windows rev. 1	Jan 19, 2025	0 / 0 (0)	1	...
HoneyPot rev. 2	Jan 19, 2025	0 / 1 (1)	2	...

We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.

Browse integrations - Integrations

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/integrations/browse...

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Integrations / Browse integrations

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore

Integrations

Choose an integration to start collecting and analyzing your data.

Browse integrations Installed integrations

All categories 390 windows

AWS 41 Azure 29

Custom Windows Event Logs Lateral Movement Detection Windows Collect logs and metrics

Can't find an Integration? Create a custom one to fit your requirements

Create new integration

Connection details

This screenshot shows the 'Browse integrations' section of a security platform. On the left, there's a sidebar with navigation links for Security, Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore. The main area is titled 'Integrations' and displays a list of available integrations categorized by source (All categories, AWS, Azure) and type (Custom Windows Event Logs, Lateral Movement Detection, Windows). A search bar at the top right is set to 'windows'. A callout box suggests creating a custom integration if none are found.

Add integration - Windows - Integrations

my-security-project-ce69f7.kb.us-east-1.aws.elastic.cloud/app/fleet/integrations/windows...

Empresas Recibidos (1) - kacp... Redes Boocamp Criptografía BlueTeam Aprendizaje Pentes Localizar Test Dominio All Bookmarks

My.Security.project / Assets / Fleet

Security

Discover Dashboards Rules Alerts Attack discovery Findings Cases Investigations Intelligence Explore

Add Windows integration

Configure an integration for the selected agent policy.

1 Configure integration

Integration settings

Integration name: windows-1

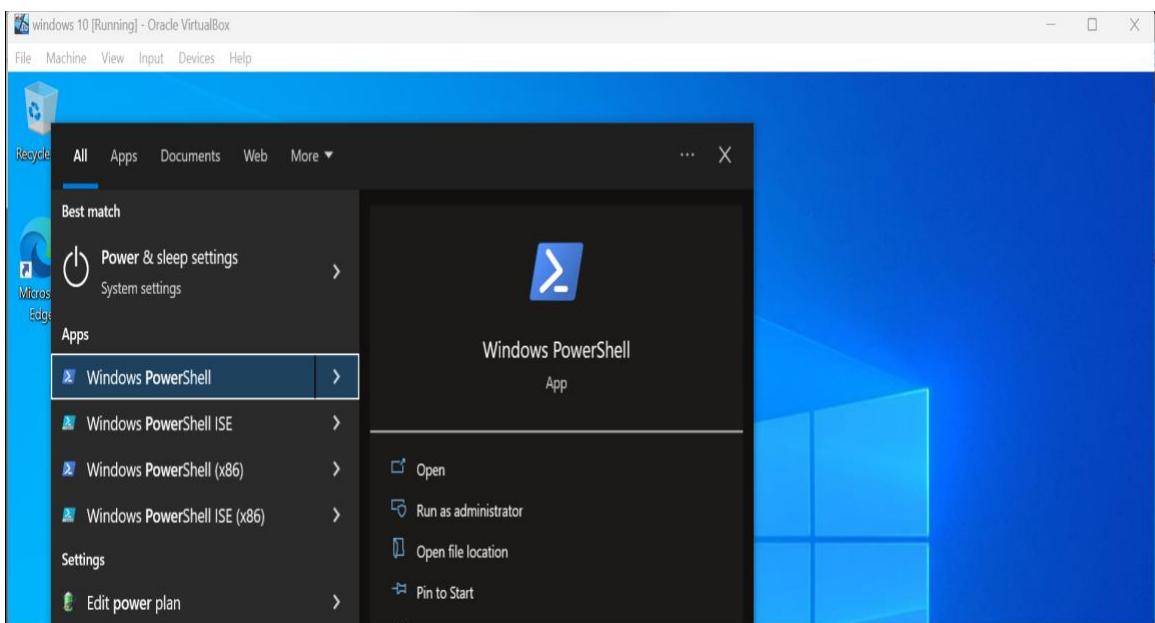
Description: Optional

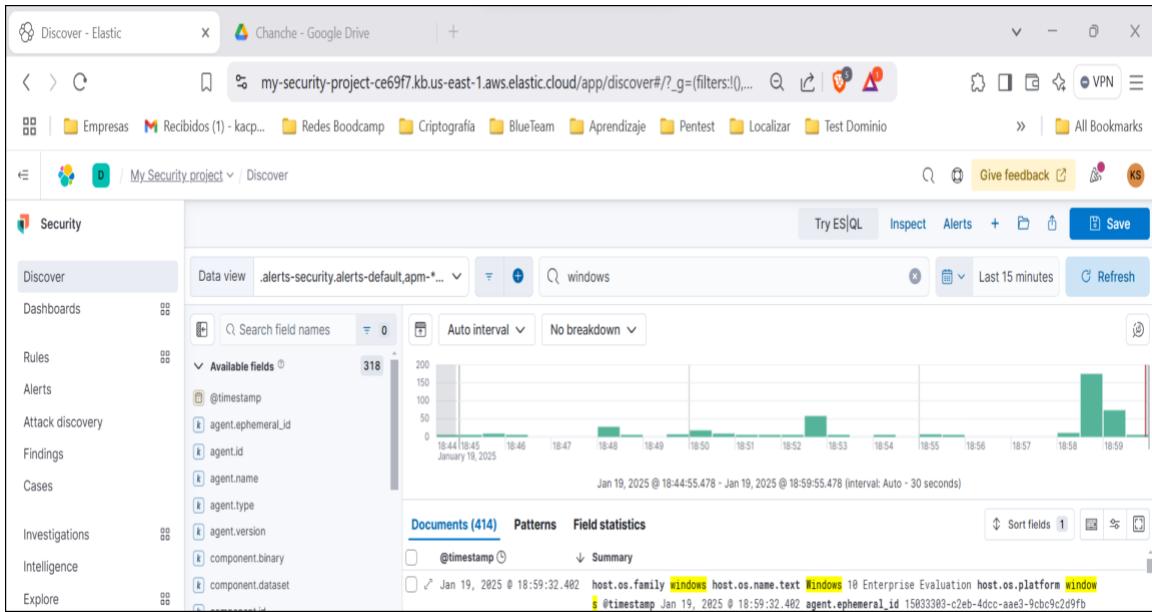
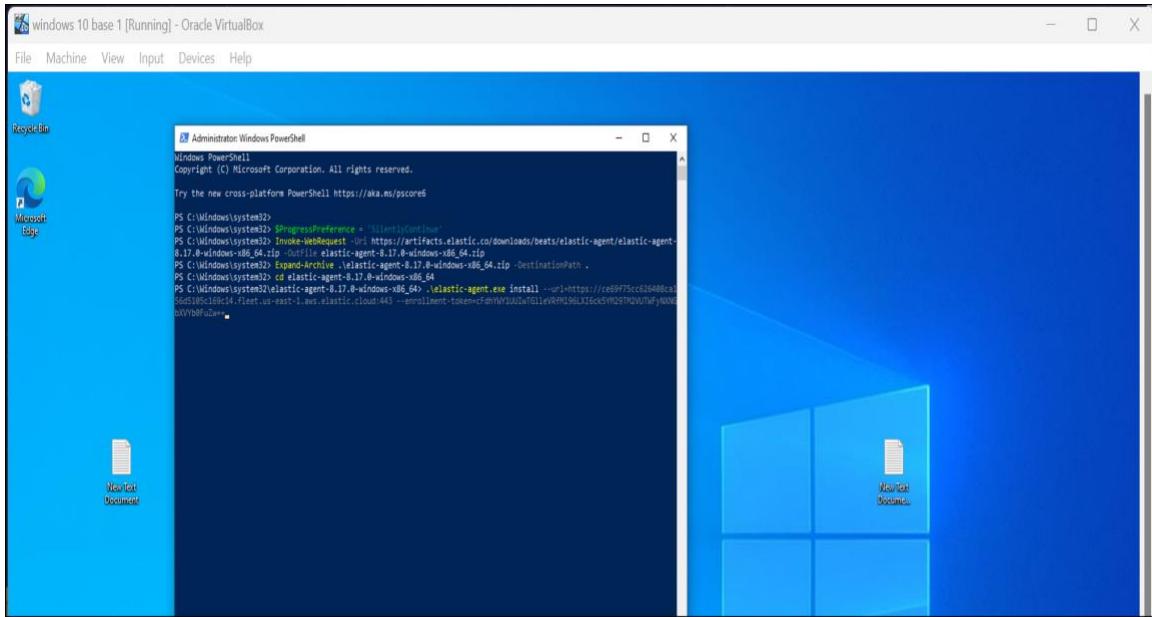
Advanced options

This screenshot shows the 'Add Windows integration' dialog. It has a header 'Add Windows integration' and a sub-header 'Configure an integration for the selected agent policy.' Below this, there's a step indicator '1 Configure integration'. The 'Integration settings' section contains fields for 'Integration name' (set to 'windows-1') and 'Description' (with a note 'Optional'). At the bottom right of the dialog, there's a link 'Advanced options'.

The screenshot shows the Fleet interface for managing agent policies. On the left, there's a sidebar with various navigation options like Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, and Explore. The main area is titled 'Windows' and shows two integration policies: 'system-3' and 'windows-1'. A modal window titled 'Add agent' is open, prompting the user to add Elastic Agents to hosts to collect data and send it to the Elastic Stack. It includes instructions for installing the agent without root privileges using the --unprivileged flag. Below the instructions, there are tabs for Linux Tar, Mac, Windows, RPM, DEB, and Kubernetes, with 'Windows' selected. A code snippet for installing the agent on Windows is provided:

```
$ProgressPreference = 'SilentlyContinue'  
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elast  
Expand-Archive .\elastic-agent-8.17.0-windows-x86_64.zip -DestinationPath  
cd elastic-agent-8.17.0-windows-x86_64  
.\\elastic-agent.exe install --url=https://ce69f75cc626408ca156d5105c169c1
```





Ejemplo:

```
{
  "@timestamp": [
    "2025-01-19T17:59:32.402Z"
  ],
  "agent.ephemeral_id": [
    "15033303-c2eb-4dcc-aae3-9cbc9c2d9fb"
  ]
}
```

],
"agent.id": [
 "0a37e4d3-4dd5-498b-9eeb-1fcba2615353"
],
"agent.name": [
 "windows10"
],
"agent.type": [
 "filebeat"
],
"agent.version": [
 "8.17.0"
],
"component.binary": [
 "metricbeat"
],
"component.dataset": [
 "elastic_agent.metricbeat"
],
"component.id": [
 "system/metrics-default"
],
"component.type": [
 "system/metrics"
],
"data_stream.dataset": [

```
"elastic_agent.metricbeat"
],
"data_stream.namespace": [
  "default"
],
"data_stream.type": [
  "logs"
],
"ecs.version": [
  "8.0.0"
],
"elastic_agent.id": [
  "0a37e4d3-4dd5-498b-9eeb-1fcba2615353"
],
"elastic_agent.snapshot": [
  false
],
"elastic_agent.version": [
  "8.17.0"
],
"event.agent_id_status": [
  "verified"
],
"event.dataset": [
  "elastic_agent.metricbeat"
],
```



```
"windows"
],
"host.os.kernel": [
    "10.0.19041.2006 (WinBuild.160101.0800)"
],
"host.os.name": [
    "Windows 10 Enterprise Evaluation"
],
"host.os.name.text": [
    "Windows 10 Enterprise Evaluation"
],
"host.os.platform": [
    "windows"
],
"host.os.type": [
    "windows"
],
"host.os.version": [
    "10.0"
],
"input.type": [
    "filestream"
],
"log.file.idxhi": [
    "262144"
],
```

```
"log.file.idxlo": [  
    "114720"  
],  
"log.file.path": [  
    "C:\\Program Files\\\\Elastic\\\\Agent\\\\data\\\\elastic-agent-8.17.0-96f2b9\\\\logs\\\\elastic-  
agent-20250119-1.ndjson"  
],  
"log.file.vol": [  
    "1324036786"  
],  
"log.level": [  
    "error"  
],  
"log.offset": [  
    200651  
],  
"log.origin.file.line": [  
    324  
],  
"log.origin.file.name": [  
    "module(wrapper.go"  
],  
"log.origin.function": [  
    "github.com/elastic/beats/v7/metricbeat/mb/module.(*metricSetWrapper).handleFetchEr  
ror"  
],
```

```
"log.source": [  
    "system/metrics-default"  
],  
  
"message": [  
    "Error fetching data for metricset system.process: Not enough privileges to fetch  
information: Not enough privileges to fetch information: GetInfoForPid: could not get all  
information for PID 0: error fetching name: OpenProcess failed for pid=0: The parameter is  
incorrect.\nerror fetching status: OpenProcess failed for pid=0: The parameter is  
incorrect.\nGetInfoForPid: could not get all information for PID 4: error fetching name:  
GetProcessImageFileName failed for pid=4: GetProcessImageFileName failed: invalid  
argument\nnon fatal error fetching PID some info for 92, metrics are valid, but partial:  
FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch  
information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info  
for 340, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching  
process args: Not enough privileges to fetch information: OpenProcess failed: Access is  
denied.\nnon fatal error fetching PID some info for 428, metrics are valid, but partial:  
FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch  
information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info  
for 500, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching  
process args: Not enough privileges to fetch information: OpenProcess failed: Access is  
denied.\nnon fatal error fetching PID some info for 512, metrics are valid, but partial:  
FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch  
information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info  
for 608, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching  
process args: Not enough privileges to fetch information: OpenProcess failed: Access is  
denied.\nnon fatal error fetching PID some info for 1780, metrics are valid, but partial:  
FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch  
information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info  
for 2884, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching  
process args: Not enough privileges to fetch information: OpenProcess failed: Access is  
denied.\nnon fatal error fetching PID some info for 3588, metrics are valid, but partial:  
FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch  
information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info  
for 5644, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching  
process args: Not enough privileges to fetch information: OpenProcess failed: Access is  
denied.\nnon fatal error fetching PID some info for 5828, metrics are valid, but partial:  
FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch  
information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info  
for 5840, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching  
process args: Not enough privileges to fetch information: OpenProcess failed: Access is  
denied.\nnon fatal error fetching PID some info for 6952, metrics are valid, but partial:
```

```
FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 5360, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied.\nnon fatal error fetching PID some info for 3832, metrics are valid, but partial: FillMetricsRequiringMoreAccess: error fetching process args: Not enough privileges to fetch information: OpenProcess failed: Access is denied."
],
"service.name": [
"metricbeat"
],
"_id": "AZR_uLR0sttFzmZzVV9g",
"_index": ".ds-logs-elastic_agent.metricbeat-default-2025.01.19-000001",
"_score": null
}
```

5. Propuesta de mejora

Podemos mejorar la siguiente infraestructura al reforzar la segmentación de las redes utilizando VLANs y aplicando reglas estrictas en el firewall PfSense, como limitando solamente el tránsito de los logs hacia Elastic, y encriptando todo tipo de información sensible con ChaCha20-Poly1305.

Tambien habría que separar y eliminar la interacción bilateral entre las redes internas DMZ2 y LAN, tal como ya se hizo con la red DMZ con el honeypot para que solo sea accesible desde la WAN. Además, se habilitaría un sistema de detección y prevención de intrusos (IDS/IPS) como Suricata en el firewall, así como listas blancas para controlar el tráfico permitido y listas negras dinámicas para bloquear direcciones IP maliciosas conocidas.

Además, los logs generados deben segregarse y analizarse mediante herramientas especializadas, configurando alertas en tiempo real para detectar actividad sospechosa como intentos de explotación o conexiones no autorizadas.

Por último, habría que implementar un sistema de copias de seguridad automáticas y periódicas de todos los datos críticos, asegurándose de que las copias sean almacenadas en una ubicación segura y aislada de la red principal.