

Practica Blue Team



Profesor: Sergio Vilches

Alumno: Guillermo V. García Muñoz

Práctica de KeepCoding Blue Team

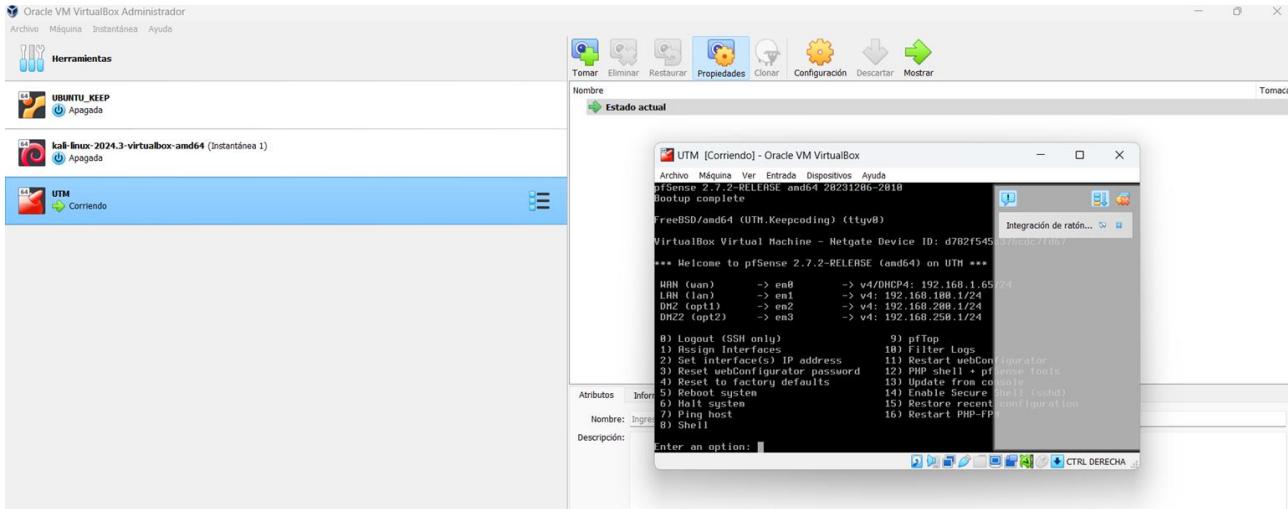
KeepCoding Bootcamp Ciberseguridad | Edición IX

Índice

1. Instalación de Pfsense
2. Configuración de redes
3. Instalación del HoneyPot
4. Instalación de Elastic (Suricata / Windows / Honeypot)

1. Instalación de Pfsense

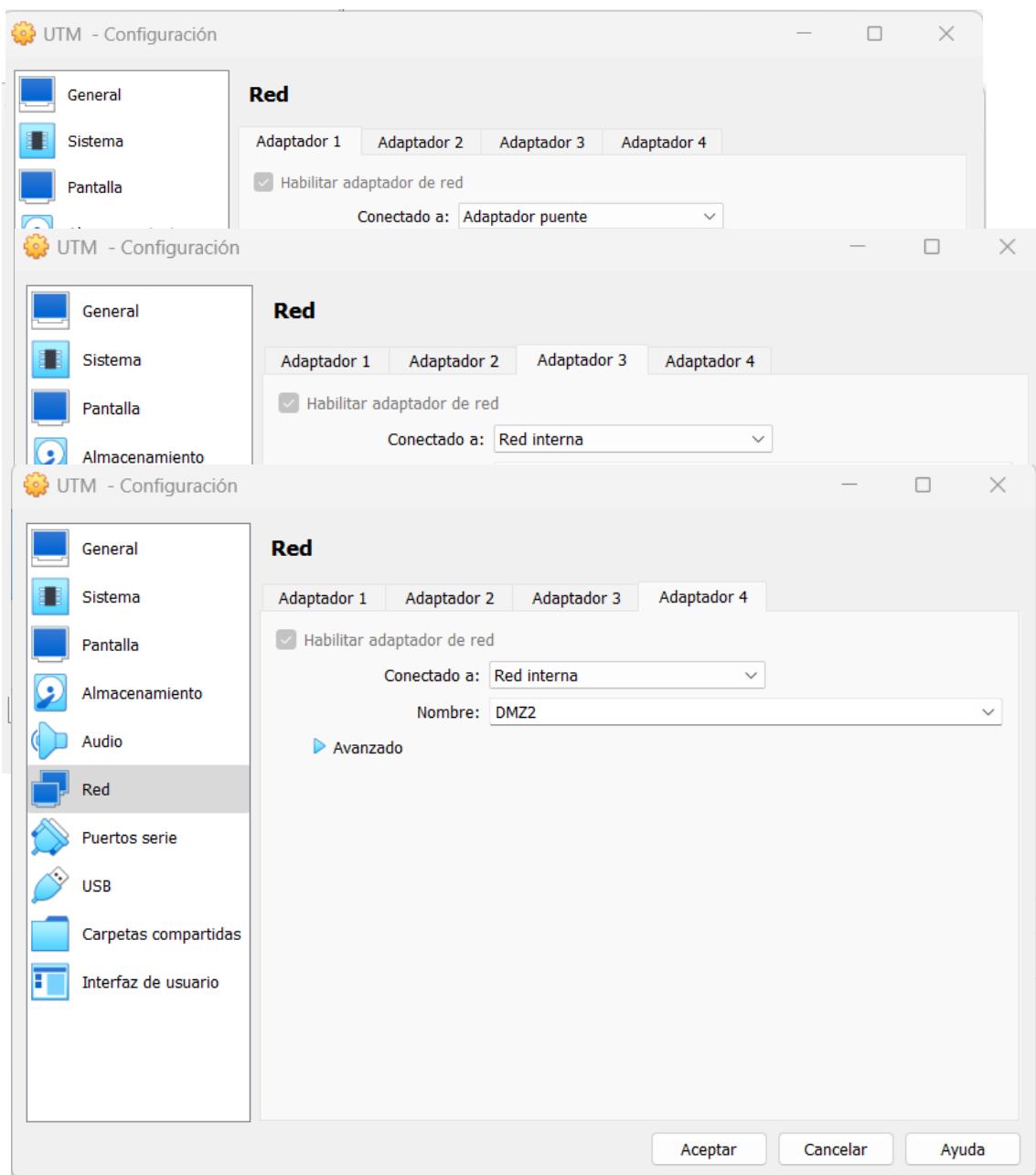
Se instala virtualBox y se crea una máquina nueva, en este caso llamada UTM, que es la que va a ser el Pfsense en el que se van a interconectar nuestro esquema de red con las redes LAN, DMZ y DMZ2.



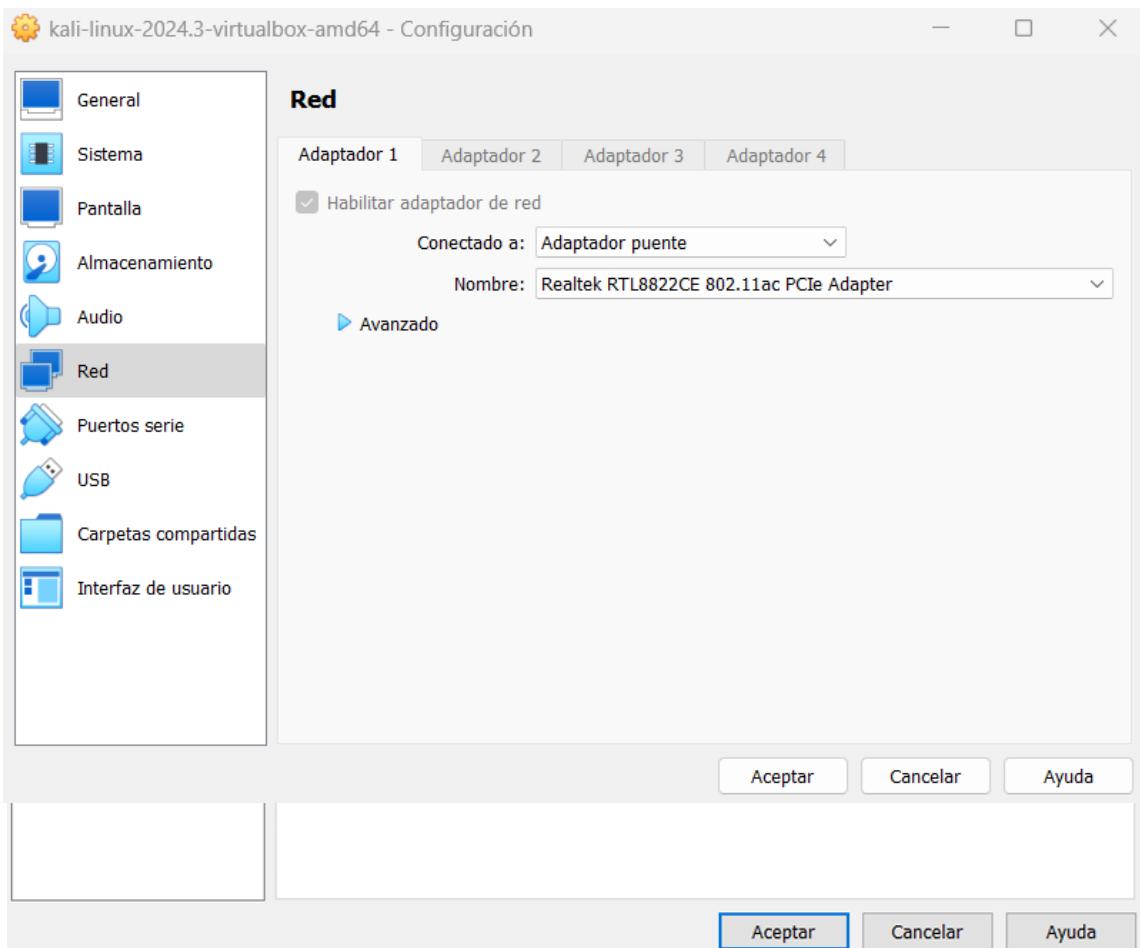
Para ello configuramos las interfaces de red en los adaptadores de red, configurando la red LAN, el DMZ y el DMZ2.

En configuración de máquina, en red, vamos a cambiar los adaptadores:

En el adaptador 1 habilitamos adaptador, lo conectamos a adaptador puente. En adaptador 2 habilitamos, red interna y ponemos LAN. En adaptador 3, habilitamos, red interna y ponemos DMZ. Finalmente en adaptador 4, habilitamos, red interna y ponemos DMZ2.



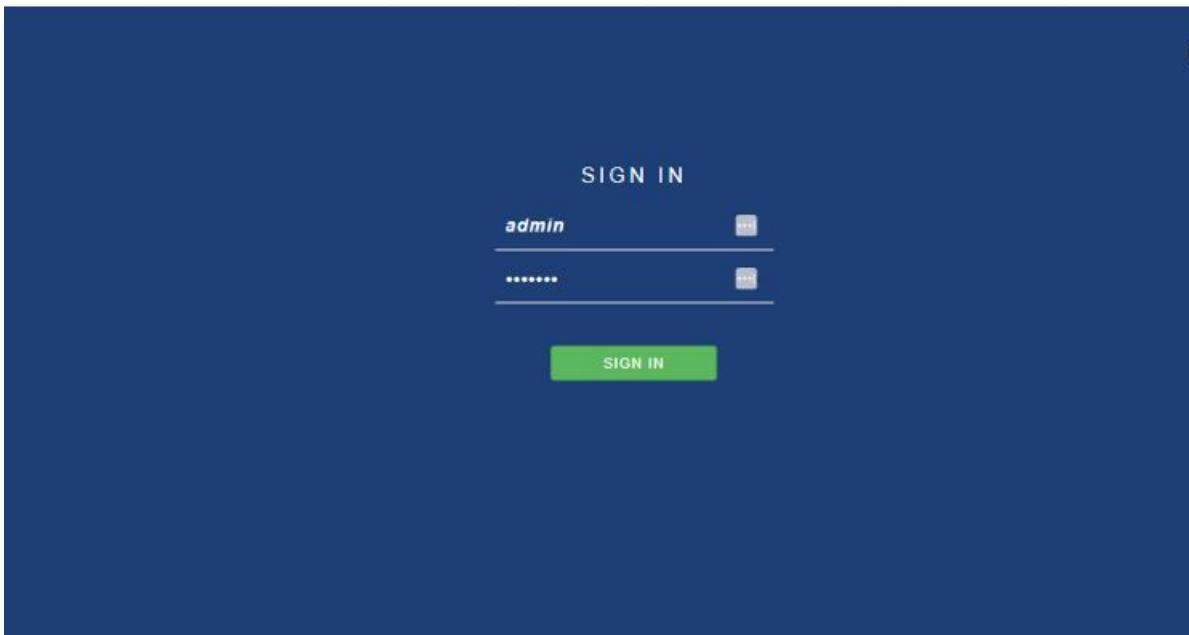
A continuación añadimos la máquina Kali para configurar Pfsense



Añadimos la máquina virtual Kali previamente instalada. La red que nos proporciona nuestro router será la red WAN. A continuación configuraremos la red y accedemos a Pfsense.



Login to pfSense



The image shows the pfSense web-based configuration interface. At the top left is the pfSense logo. To its right is a link labeled "Login to pfSense". The main area is a dark blue rectangle containing a "SIGN IN" form. The form has two input fields: the first is labeled "admin" and the second is a password field filled with "*****". Below the fields is a green "SIGN IN" button. There are also small icons for user and password visibility.

Para configurar Pfsense:

Desde el UTM : 192.168.1.1
Usuario: admin
pass: pfsense

Hostname: UTM
Domain: Keepcoding
DNS server : 127.0.0.1
DNS server: 1.1.1.1

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain 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.

Primary DNS Server

Secondary DNS Server

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

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

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

Timezone

>> Next

Wizard / pfSense Setup / Configure WAN Interface



Step 4 of 9

Configure WAN Interface

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

SelectedType

DHCP

General configuration

MAC Address

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 or leave blank.

MTU

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

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 this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

IP Address

Subnet Mask

32

PPTP configuration

PPTP Username

PPTP Password

Show PPTP password

 Reveal password characters

PPTP Local IP Address

pptplocalsubnet

32

PPTP Remote IP Address

PPTP Dial on demand

 Enable Dial-On-Demand mode

This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

PPTP Idle timeout

If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

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

 Block non-Internet routed networks from entering via WAN

Configuramos la IP de la LAN para poder acceder correctamente, cambiamos el redirecccionamiento a la 192.168.100.1 y Subnet Mask : 24

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

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

LAN IP Address: 192.168.100.1
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

>> Next

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

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: (five dots)

Admin Password AGAIN: (five dots)

>> Next

Configuramos la resolución DNS

En services – DNS resolver, comprobamos que está habilitado, quitamos DNSSEC y habilitamos forwarding mode

General Settings Advanced Settings Access Lists

General DNS Resolver Options

Enable	<input checked="" type="checkbox"/> Enable DNS resolver
Listen Port	53
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.	
Enable SSL/TLS Service	<input type="checkbox"/> Respond to incoming SSL/TLS queries from local clients Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.
SSL/TLS Certificate	GUI default (677ed8db49eb0)
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.	
SSL/TLS Listen Port	853
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.	
Network Interfaces	All WAN LAN DMZ DMZ2
Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.	
Outgoing Network Interfaces	All WAN LAN DMZ DMZ2

Topics. By default all interfaces are used.	
Strict Outgoing Network Interface Binding	<input type="checkbox"/> Do not send recursive queries if none of the selected Outgoing Network Interfaces are available. By default the DNS Resolver sends recursive DNS requests over any available interfaces if none of the selected Outgoing Network Interfaces are available. This option makes the DNS Resolver refuse recursive queries.
<u>System Domain Local Zone Type</u>	Transparent The local-zone type used for the pfSense system domain (System General Setup Domain). Transparent is the default.
DNSSEC	<input type="checkbox"/> Enable DNSSEC Support
Python Module	<input type="checkbox"/> Enable Python Module Enable the Python Module.
DNS Query Forwarding	<input checked="" type="checkbox"/> Enable Forwarding Mode If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under System > General Setup or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).
	<input type="checkbox"/> Use SSL/TLS for outgoing DNS Queries to Forwarding Servers When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.
DHCP Registration	<input type="checkbox"/> Register DHCP leases in the DNS Resolver If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in System > General Setup should also be set to the proper value.
Static DHCP	<input type="checkbox"/> Register DHCP static mappings in the DNS Resolver If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in System > General Setup should also be set to the proper value.
OpenVPN Clients	<input type="checkbox"/> Register connected OpenVPN clients in the DNS Resolver If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in "tun" mode. The domain in System: General Setup should also be set to the proper value.

DHCP Registration Register DHCP leases in the DNS Resolver
If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in [System > General Setup](#) should also be set to the proper value.

Static DHCP Register DHCP static mappings in the DNS Resolver
If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in [System > General Setup](#) should also be set to the proper value.

OpenVPN Clients Register connected OpenVPN clients in the DNS Resolver
If this option is set, then the common name (CN) of connected OpenVPN clients will be registered in the DNS Resolver, so that their name can be resolved. This only works for OpenVPN servers (Remote Access SSL/TLS or User Auth with Username as Common Name option) operating in "tun" mode. The domain in [System: General Setup](#) should also be set to the proper value.

Display Custom Options [Display Custom Options](#)

Save

Host Overrides				
Host	Parent domain of host	IP to return for host	Description	Actions
Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.				

Add

Domain Overrides			
Domain	Lookup Server IP Address	Description	Actions
Enter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, 'invalid' and local domains, and subdomains, can also be entered, such as 'test', 'nas.home.arpa'.			

El siguiente paso, vamos services, DHCP server. En este punto vamos a modificar los rangos dinámicos de la 192.168.100.100 a la 192.168.100.200

En el DNS server vamos a poner la dirección de nuestra WAN que es el 192.168.1.100 y en los secundarios ponemos el 1.1.1.1 y el 8.8.8.8

En Gateway ponemos 192.168.100.1

UTM.Keepcoding - Services

https://192.168.100.1/services_dhcp.php

Kali Linux Kali Tools Damn Vulnerable Nod... UTM.Keepcoding - Sta... Damn Vulnerable Nod... Kali Docs Kali Forums Kali NetHunter

Server Options

WINS Servers	WINS Server 1 WINS Server 2
DNS Servers	192.168.1.100 1.1.1.1 8.8.8.8 DNS Server 4

OMAPI

OMAPI Port	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	OMAPI Key Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.	<input type="checkbox"/> 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	192.168.100.1 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 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 Primary or Secondary. Ensure the advertising skew for the VIP on one firewall is < 20 and the other is > 20.
Static ARP	<input type="checkbox"/> 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 be able to communicate with the firewall on this interface. This behavior is enforced even when DHCP server is disabled.
Time format change	<input type="checkbox"/> Change DHCP display lease time from UTC to local time By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and converted to the time zone selected. This will be used for all DHCP interface lease times.

2. Configuración de redes

Ahora nos vamos a las Interfaces, vamos a asignarle una IP a la puerta de enlace, añadiendo una IP estática 192.168.200.1 / 24 en la DMZ y en la DMZ2 192.168.250.1 / 24

Interfaces Assignments para configurar WAN, LAN, DMZ and DMZ2

Interfaces / Interface Assignments

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

Interface	Network port
WAN	em0 (08:00:27:a6:a8:9c)
LAN	em1 (08:00:27:56:92:fb)
DMZ	em2 (08:00:27:47:5b:05)
DMZ2	em3 (08:00:27:b2:78:ae)

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.

Configuración DMZ

Static IPv4

IPv4 address 192.168.200.1

Establecimiento de la interfaz em2 como DMZ y asignación de un IPv4 estático

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	DMZ 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 or leave blank.
MTU	1500 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	1460 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address	192.168.200.1	/ 24
IPv4 Upstream gateway	None	+ Add a new gateway

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

Speed and Duplex Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address	192.168.200.1	/ 24
IPv4 Upstream gateway	None	+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
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	<input type="checkbox"/> 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	<input type="checkbox"/> 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](#)

Establecimiento de la interfaz em3 como DMZ2 y asignación de un IPv4 estático

The screenshot shows the pfSense web interface for managing network interfaces. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help.

The main page title is "Interfaces / DMZ2 (em3)".

General Configuration:

- Enable:** Checked, with the label "Enable interface".
- Description:** Set to "DMZ2". A placeholder text says "Enter a description (name) for the interface here."
- IPv4 Configuration Type:** Set to "Static IPv4".
- IPv6 Configuration Type:** Set to "None".
- MAC Address:** Set to "XX:XX:XX:XX:XX:XX". A note says "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 or leave blank."
- MTU:** A dropdown menu with a note: "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:** A dropdown menu with a note: "If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect."
- Speed and Duplex:** Set to "Default (no preference, typically autoselect)". A note says "Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced."

Static IPv4 Configuration:

- IPv4 Address:** Set to "192.168.250.1" with a subnet mask of "/24".

Static IPv4 Configuration (Details):

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

- Speed and Duplex:** Set to "Default (no preference, typically autoselect)". A note says "Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced."

Static IPv4 Configuration:

- IPv4 Address:** Set to "192.168.250.1" with a subnet mask of "/24".
- IPv4 Upstream gateway:** Set to "None". A button "+ Add a new gateway" is available.

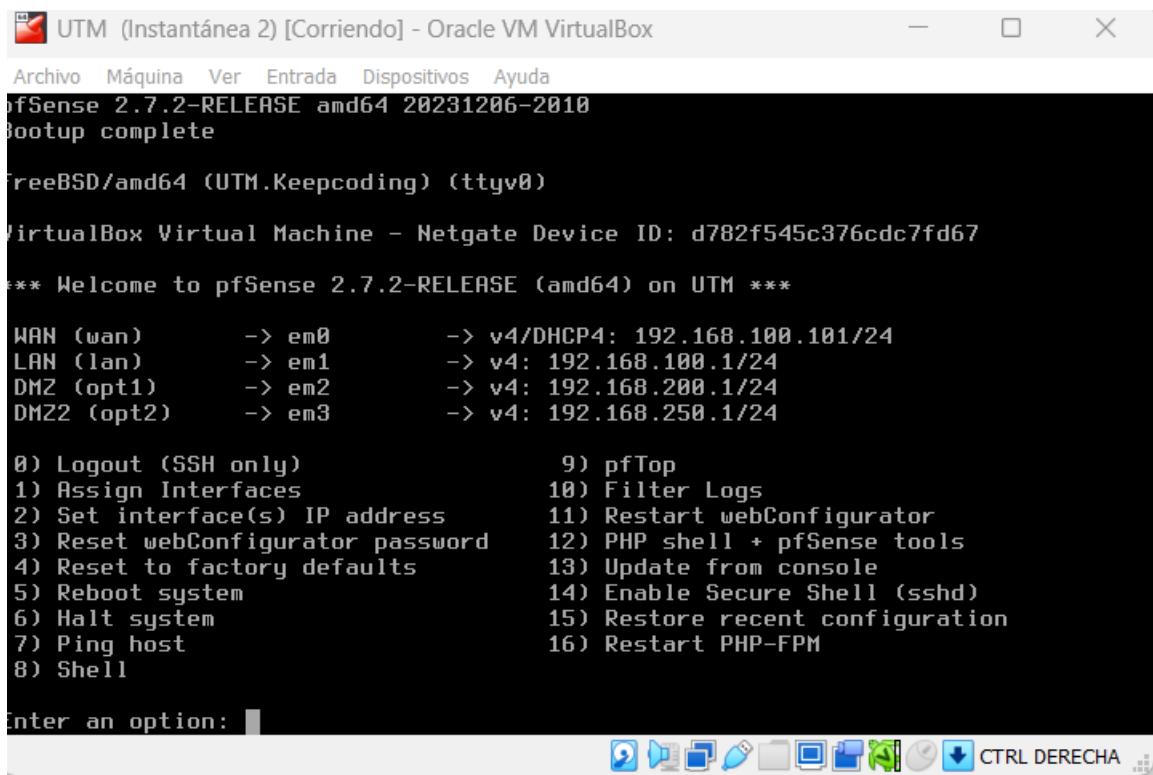
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a **WAN type interface**. Gateways can be managed by [clicking here](#).

Reserved Networks:

- Block private networks and loopback addresses:** An unchecked checkbox. A note says "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:** An unchecked checkbox. A note says "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 button at the bottom left.

Configuración de las IP de WAN, LAN, DMZ and DMZ2



```
UTM (Instantánea 2) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
ifSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (UTM.Keepcoding) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: d782f545c376cdc7fd67

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.100.101/24
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: ■
```

The screenshot shows a terminal window within Oracle VM VirtualBox. The title bar reads "UTM (Instantánea 2) [Corriendo] - Oracle VM VirtualBox". The menu bar includes "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The pfSense boot message "ifSense 2.7.2-RELEASE amd64 20231206-2010" and "Bootup complete" is displayed. The FreeBSD version "FreeBSD/amd64 (UTM.Keepcoding) (ttyv0)" and the VirtualBox device ID "VirtualBox Virtual Machine - Netgate Device ID: d782f545c376cdc7fd67" are shown. The pfSense welcome message "Welcome to pfSense 2.7.2-RELEASE (amd64) on UTM" is followed by a list of 16 numbered options for managing the system. Below the options, there is a prompt "Enter an option: ■". At the bottom of the terminal window, there is a toolbar with various icons and a status bar that says "CTRL DERECHA".

Configuración del servidor DHCP en DMZ, asignación de un rango IP específico y los servidores DNS

Screenshot of the pfSense DHCP Server configuration interface for the DMZ zone.

General DHCP Options

- DHCP Backend:** ISC DHCP
- Enable:** Enable DHCP server on DMZ interface
- BOOTP:** Ignore BOOTP queries
- Deny Unknown Clients:** Allow all clients
 - When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
- Ignore Denied Clients:** Ignore denied clients rather than reject
 - This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
- Ignore Client Identifiers:** Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
 - This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet	192.168.200.0/24
--------	------------------

Primary Address Pool

Subnet	192.168.200.0/24
Subnet Range:	192.168.200.1 - 192.168.200.254
Address Pool Range:	From: 192.168.200.100 To: 192.168.200.150
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
	DNS Server 4

OMAPI

OMAPI Port	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	OMAPI Key
<input type="checkbox"/> Generate New Key	

Other DHCP Options	
Gateway	<input type="text" value="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	<input type="text" value="Keepcoding"/>
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	<input type="text" value="example.com;sub.example.com"/>
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.	
Default Lease Time	<input type="text" value="7200"/>
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.	
Maximum Lease Time	<input type="text" value="86400"/>
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.	
Failover peer IP	<input type="text"/>
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	<input type="checkbox"/> 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 be able to communicate with the firewall on this interface. This behavior is enforced even when DHCP server is disabled.	
Time format change	<input type="checkbox"/> Change DHCP display lease time from UTC to local time
By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and set to the time zone selected. This will be used for all DHCP interfaces lease time.	
Statistics graphs	<input type="checkbox"/> Enable monitoring graphs for DHCP lease statistics
Enable this to add DHCP leases statistics to the Monitoring graphs. Disabled by default.	
Ping check	<input type="checkbox"/> Disable ping check

Act
Ve a

Configuracion del DHCP server en DMZ2, asignacion de un rango de IP y el DNS server

LAN	DMZ	DMZ2
General DHCP Options		
DHCP Backend	ISC DHCP	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on DMZ2 interface	
BOOTP	<input type="checkbox"/> Ignore BOOTP queries	
Deny Unknown Clients	<input type="text" value="Allow all clients"/>	
When set to Allow all clients , any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface , any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface , only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.		
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject	
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.		
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request	
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.		
Primary Address Pool		
Subnet	192.168.250.0/24	
Subnet Range	192.168.250.1 - 192.168.250.254	
Address Pool Range	<input type="text" value="192.168.250.100"/>	<input type="text" value="192.168.250.150"/>
From	To	
The specified range for this pool must not be within the range configured on any other address pool for this interface.		

Act
Ve a

Server Options

WINS Servers	WINS Server 1
	WINS Server 2
DNS Servers	192.168.250.1
	1.1.1.1
	8.8.8.8
	DNS Server 4

OMAPI

OMAPI Port	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	OMAPI Key
Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.	
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 interface.	

Vamos a configurar el firewall añadiendo los puertos 80 HTTP y 443 HTTPS

Firewall / Aliases / Edit

Properties

Name	web
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".	
Description	puerto
A description may be entered here for administrative reference (not parsed).	
Type	Port(s)

Port(s)

Hint	Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.		
Port	80	HTTP	
	443	HTTPS	

Save Export to file Add Port

The screenshot shows the pfSense Firewall / Rules / LAN interface. The LAN tab is selected. There are three rules listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 2/2.72 MiB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
<input type="checkbox"/> <input checked="" type="checkbox"/> 2.368K/68.32 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/> <input checked="" type="checkbox"/> 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Buttons at the bottom include: Add, Add, Delete, Toggle, Copy, Save, and Separate.

Vamos a establecer las reglas DMZ respecto al tráfico web en el firewall con la regla recién creada

Regla del tráfico web

The screenshot shows the pfSense Firewall / Rules / Edit interface for creating a new rule. The rule details are as follows:

- Action:** Pass
- Interface:** DMZ
- Protocol:** TCP
- Source:** Any

Below the source section, there is a note: "The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any."

Destination

Destination	<input type="checkbox"/> Invert match	Any	Destination Address	/	<input type="button"/>	
Destination Port Range	(other)	From	Custom	(other)	To	Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.						

Extra Options

Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	Regla Trafico web A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	<input type="button"/> Display Advanced

Rule Information

Tracking ID	1736447449
Created	1/9/25 18:30:49 by admin@192.168.100.100 (Local Database)
Updated	1/9/25 18:36:52 by admin@192.168.100.100 (Local Database)

Save

Establecimiento del DMZ Rules acerca del DNS en el firewall

Regla del tráfico DNS

Firewall / Rules / Edit

Edit Firewall Rule

Action	<input type="button"/> Pass	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.	
Interface	DMZ	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.

Source

Source	<input type="checkbox"/> Invert match	Any	Source Address	/	<input type="button"/>
<input type="button"/> Display Advanced					
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.					

Destination

Destination

Destination	<input type="checkbox"/> Invert match	Any	Destination Address	/	<input type="button" value="..."/>
Destination Port Range	From: DNS (53)	To: Custom	From: DNS (53)	To: Custom	<input type="button" value="..."/>

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	Regla trafico DNS A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	<input type="button" value="Display Advanced"/>

Rule Information

Tracking ID	1736447784
Created	1/9/25 18:36:24 by admin@192.168.100.100 (Local Database)
Updated	1/17/25 18:04:45 by admin@192.168.100.99 (Local Database)

Establecimiento del DMZ Rules acerca del Protocolo ICMP en el firewall

Firewall / Rules / Edit

Edit Firewall Rule

Action	Pass	<input type="button" value="..."/>
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	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.
Interface	DMZ	<input type="button" value="..."/>
Choose the interface from which packets must come to match this rule.		
Address Family	IPv4	<input type="button" value="..."/>
Select the Internet Protocol version this rule applies to.		
Protocol	ICMP	<input type="button" value="..."/>
Choose which IP protocol this rule should match.		

Choose which IP protocol this rule should match.

ICMP Subtypes	Alternate Host Datagram conversion error Echo reply Echo request
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.	
Source	
Source <input type="checkbox"/> Invert match <input type="text" value="Any"/> / <input type="text" value="Source Address"/>	
Destination	
Destination <input type="checkbox"/> Invert match <input type="text" value="Any"/> / <input type="text" value="Destination Address"/>	
Extra Options	
Log	<input type="checkbox"/> Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).	
Description	<input type="text" value="Regla ICMP"/>
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
Advanced Options	Display Advanced
Rule Information	
Tracking ID	1736450309
Created	1/9/25 19:18:29 by admin@192.168.100.100 (Local Database)
Updated	1/17/25 17:35:19 by admin@192.168.100.99 (Local Database)
Save Activ Ve a Co	

DMZ Firewall Rules

Firewall / Rules / DMZ

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

Floating	WAN	LAN	DMZ	DMZ2							
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	*	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP echoreq	*	*	*	*	*	none		Regla ICMP	
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none		Regla trafico DNS	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	web	*	none		Regla Trafico web	
 Add Add Delete Toggle Copy Save Separator											
											

Establecimiento del DMZ2 Rules acerca del trafico Web en el firewall con la nueva regla creada

Firewall / Rules / Edit

Edit Firewall Rule

Action	Pass	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	<input type="checkbox"/> 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	TCP	Choose which IP protocol this rule should match.

Source

Source	<input type="checkbox"/> Invert match	Any	Source Address	/	<input type="button" value=""/>
--------	---------------------------------------	-----	----------------	---	---------------------------------

[Display Advanced](#)

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

Destination

Destination	<input type="checkbox"/> Invert match	Any	Destination Address	/	<input type="button" value=""/>
Destination Port Range	(other)	From	Custom	To	Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	Regla Trafico web
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
Advanced Options	Display Advanced

Rule Information

Tracking ID	1737133097
Created	1/17/25 16:58:17 by admin@192.168.100.99 (Local Database)
Updated	1/17/25 17:07:15 by admin@192.168.100.99 (Local Database)

[Save](#)

Establecimiento en el DMZ2 acerca del DNS en el Firewall

Firewall / Rules / Edit

Edit Firewall Rule

Action 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 Choose the interface from which packets must come to match this rule.

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

Protocol Choose which IP protocol this rule should match.

Source

Source Invert match /

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

Destination

Destination Invert match /

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

Extra Options

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

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

Advanced Options

Rule Information

Tracking ID 1737133950

Created 1/17/25 17:12:30 by admin@192.168.100.99 (Local Database)

Updated 1/17/25 17:12:30 by admin@192.168.100.99 (Local Database)

Establecimiento del DMZ2 rules acerca del protocolo ICMP en el firewall

Firewall / Rules / Edit

Edit Firewall Rule

Action 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 Choose the interface from which packets must come to match this rule.

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

Protocol Choose which IP protocol this rule should match.

ICMP Subtypes Echo reply
 Echo request
 Alternate Host
 Datagram conversion error
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source

Source Invert match /

Destination

Destination Invert match /

Source

Source Invert match /

Destination

Destination Invert match /

Extra Options

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

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

Advanced Options

Rule Information

Tracking ID	1737134392
Created	1/17/25 17:19:52 by admin@192.168.100.99 (Local Database)
Updated	1/17/25 17:35:01 by admin@192.168.100.99 (Local Database)

DMZ2 Firewall Rules

Firewall / Rules / DMZ2

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating WAN LAN DMZ **DMZ2**

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 ICMP	* echoreq	*	*	*	*	none		Regla ICMP	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none		Regla trafico DNS	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	*	*	*	web	*	none		Regla Trafico web	

DHCP Status

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.

Search

Search Term All

Enter a search string or *nix regular expression to filter entries.

Leases							
	IP Address	MAC Address	Hostname	Description	Start	End	Actions
	192.168.100.99	08:00:27:ad:25:87	kali		n/a	n/a	
	192.168.100.101	08:00:27:a6:a8:9c	UTM		2025/03/30 17:17:51	2025/03/30 19:17:51	

Lease Utilization					
Interface	Pool Start	Pool End	Used	Capacity	Utilization
LAN	192.168.100.10	192.168.100.245	1	236	0% of 236

Bloqueo del DMZ2 para el acceso del DMZ

Firewall / Rules / Edit

Edit Firewall Rule

Action: Block

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

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

Interface: DMZ

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

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: Any

Choose which IP protocol this rule should match.

Source

Source: Invert match, DMZ subnets, Source Address /

Destination

Destination: Invert match, DMZ2 subnets, Destination Address /

Extra Options

Log: Log packets that are handled by this rule

Advanced

Bloqueo de LAN para el acceso al DMZ

Firewall / Rules / Edit

Edit Firewall Rule

Action	Block
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	DMZ
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	Any
Choose which IP protocol this rule should match.	
Source	
Source	<input type="checkbox"/> Invert match
DMZ subnets	
Source Address /	
Destination	
Destination	<input type="checkbox"/> Invert match
LAN subnets	
Destination Address /	
Extra Options	
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule

DMZ Rules

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / DMZ

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

Floating	WAN	LAN	DMZ	DMZ2							
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	X	0/0 B	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		X A P C S D
<input type="checkbox"/>	X	0/0 B	IPv4 *	DMZ subnets	*	DMZ2 subnets	*	*	none		X A P C S D
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	*	*	*	none		X A P C S D
<input type="checkbox"/>	✓	0/0 B	IPv4 ICMP echoreq	*	*	*	*	*	none	Regla ICMP	X A P C S D
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none	Regla trafico DNS	X A P C S D
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	web	*	none		Regla Trafico web	X A P C S D

▲ Add ▼ Add Delete Toggle Copy Save + Separator

Bloqueo del DMZ2 al DMZ

Firewall / Rules / Edit

Edit Firewall Rule

Action	Block		
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.			
Disabled	<input type="checkbox"/> 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	Any		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	DMZ2 subnets	Source Address
Destination			
Destination	<input type="checkbox"/> Invert match	DMZ subnets	Destination Address
Extra Options			
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see Ve a Configuración)		

DMZ2 Rules

Firewall / Rules / DMZ2

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating	WAN	LAN	DMZ	DMZ2						
Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 ICMP echoreq	*	*	*	*	none		Regla ICMP	
<input type="checkbox"/>	0/0 B	IPv4 UDP	*	*	53 (DNS)	*	none		Regla trafico DNS	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	web	*	none		Regla Trafico web	
<input type="checkbox"/>	0/0 B	IPv4 *	DMZ2 subnets	*	DMZ subnets	*	none		Regla bloqueo DMZ a DMZ2	

Add Add Delete Toggle Copy Save Separator

WAN Honeypot ssh

The screenshot shows the pfSense Firewall Rules configuration for the WAN interface. A success message at the top indicates that changes have been applied successfully and the firewall rules are reloading. The table lists two rules:

Index	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	✓	IPv4 TCP	*	*	192.168.200.99	22 (SSH)	*	none	NAT		
0/0 B	✓	IPv4 TCP	*	*	192.168.100.99	80 (HTTP)	*	none	NAT Servidor Apache		

Below the table are several action buttons: Add, Add, Delete, Toggle, Copy, Save, and Separator.

NAT Honeypot ssh

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Actions	Description	NAT Ports	NAT IP	Dest. Ports	Dest. Address	Source Ports	Source Address	Protocol	Interface	Check
		222	192.168.100.99	222	WAN address	*	*	TCP	WAN	

Legend
 Pass
 Linked rule

3. Instalación del Honeypot:

Vamos a comenzar ejecutando en nuestra máquina el comando:

```
docker run -p 222:2222 cowrie/cowrie
```

Implementamos un Honeypot por ssh:

El siguiente paso es conectar nuestro servidor con nuestra máquina Kali:

Para ello ponemos la Kali en el adaptador 1 en adaptador puente, abrimos una consola en nuestro Windows y ejecutamos el comando `ssh -p 222 root@192.168.1.68` para conectarnos con nuestra máquina Kali. Tenemos que poner nuestra dirección IP en el comando.

```

kali㉿kali: ~
File Actions Edit View Help
starting service b'ssh-connection'
2025-01-19T10:24:58+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got channel b'session' request
2025-01-19T10:24:58+0000 [cowrie.ssh.session.HoneyPotSSHSessi...]
channel open
2025-01-19T10:24:58+0000 [cowrie.ssh.connection.CowrieSSHConnection#debug] got global b'no-more-sessions@openssh.com' request
2025-01-19T10:24:59+0000 [twisted.conch.ssh.session#info] Handling pty request: b'xterm-256color' (30, 120, 640, 480)
2025-01-19T10:24:59+0000 [SSHChannel session () on SSHService b'ssh-connecti...]
on HoneyPotSSHTransport,0,192.168.1.47] Terminal Size: 120 30
2025-01-19T10:24:59+0000 [twisted.conch.ssh.session#info] Getting shell
2025-01-19T10:27:08+0000 [HoneyPotSSHTransport,0,192.168.1.47] CMD: ls
2025-01-19T10:27:11+0000 [HoneyPotSSHTransport,0,192.168.1.47] CMD: ls
2025-01-19T10:27:11+0000 [HoneyPotSSHTransport,0,192.168.1.47] Command found: ls
2025-01-19T10:27:59+0000 [-] Timeout reached in HoneyPotSSHTransport
2025-01-19T10:27:59+0000 [HoneyPotSSHTransport,0,192.168.1.47] Closing TTY Log: var/lib/cowrie/tty/2d2872d8464223ad05fdbfadd0172fdc37f42137ce3c884439be8701bf140235 after 180.0 seconds
2025-01-19T10:27:59+0000 [HoneyPotSSHTransport,0,192.168.1.47] avatar root logging out
2025-01-19T10:27:59+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-01-19T10:27:59+0000 [HoneyPotSSHTransport,0,192.168.1.47] Connection lost after 202.3 seconds

```

A través de los comandos en nuestra Kali:

docker run -p 333:3389 amazedostrich/rdp
 docker exec -it -u 0 [c8b24ded835a](#) /bin/bash (Tenemos que añadir nuestro identificador)

Nos conectamos a través de nuestra consola y nuestro escritorio remoto para poder ver los logs generados en rdp:

```

File Actions Edit View Help
31 minutes 2223/tcp, 0.0.0.0:222→2222/tcp, :::22→2222/tcp ! priceless_wilson
bash-4.4# cd /var/log/rdpy/
bash-4.4# ls
rdpy.log
bash-4.4# tail -f rdpy.log
[*] INFO: (800, 600) → /home/rdpy/3
[*] INFO:
[*] INFO: 2025-01-27T10:37:12.440339Z,Connection from 192.168.1.59:49712
[*] INFO:
[*] INFO: 2025-01-27T10:37:18.673714Z,Connection from 192.168.1.59:49714
[*] INFO: [*] select file (1920, 1080) → /home/rdpy/1
[*] INFO:
[*] INFO: 2025-01-27T10:37:18.730024Z,domain:,username:,password:,hostname:DESKTOP-NJFFQM4
[*] INFO:
[*] INFO: 2025-01-27T10:37:18.757040Z,domain:,username:,password:,hostname:DESKTOP-NJFFQM4
[*] INFO:
[*] INFO: 2025-01-27T10:52:20.510134Z,Connection from 192.168.1.59:50064
[*] INFO:
[*] INFO: 2025-01-27T10:52:22.070955Z,Connection from 192.168.1.59:50065
[*] INFO: [*] select file (1920, 1080) → /home/rdpy/1
[*] INFO:
[*] INFO: 2025-01-27T10:52:22.127260Z,domain:,username:Prueba,password:,hostname:DESKTOP-NJFFQM4
[*] INFO:
[*] INFO: 2025-01-27T10:52:22.151822Z,domain:,username:Prueba,password:,hostname:DESKTOP-NJFFQM4

```

Pasamos a instalar suricata con los comandos :

sudo apt update
 sudo apt install suricata
 suricata -c /etc/suricata/suricata.yaml -i eth0

```
(kali㉿kali)-[~]
$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
└: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
└: detect: No rule files match the pattern /var/lib/suricata/rules/suricata.rules
└: detect: 1 rule files specified, but no rules were loaded!
└: threads: Threads created → W: 2 FM: 1 FR: 1   Engine started.
```

Añadimos las siguientes reglas que guardamos en suricata:

Vamos a seguir la siguiente línea de comandos entre otros para añadirlas;

```
sudo -s para darle privilegios
cd /etc/suricata
ls
cd rules
less files.rules
touch suricata.rules
ls
nano suricata.rules
```

Las dos reglas que añadimos son:

```
alert tcp any any -> any any (msg:"trafico detectado"; sid:1;)
```

```
alert tcp any any -> any any (msg:"PDF Archivo descargado"; flow:established,to_client;
fileext:"pdf"; sid:3; classtype:file-download;)
```

```
alert tcp any any -> 192.168.1.65 22 (msg:"Trafico SSH detectado"; sid:2; classtype:attempted-admin;)
```

```
root@kali:/etc/suricata/rules
File Actions Edit View Help
GNU nano 8.2          suricata.rules
alert tcp any any -> any any (msg:"trafico detectado"; sid:1;)
alert tcp any any -> 192.168.1.65 22 (msg:"Trafico SSH detectado"; sid:2; class
[ Read 6 lines ]
^D Help      ^O Write Out  ^F Where Is  ^X Cut      ^T Execute  ^C Location
^X Exit     ^R Read File  ^A Replace   ^U Paste    ^J Justify  ^V Go To Line
```

Una vez que aplicamos las reglas conseguimos conectarnos para ver los logs:

The left terminal window shows the configuration of the Suricata rules directory:

```

root@kali: /etc/suricata
File Actions Edit View Help
[root@kali ~]# 
[root@kali ~]# (root@kali)-[~/etc/suricata/rules]
[root@kali ~]# 
[root@kali ~]# (root@kali)-[~/etc/suricata/rules]
[root@kali ~]# app-layer-events.rules files.rules kerberos-events.rules quic-events.rules stream-events.rules
[root@kali ~]# decoder-events.rules ftp-events.rules modbus-events.rules rfb-events.rules suricata.rules
[root@kali ~]# dhcp-events.rules http2-events.rules mqtt-events.rules smb-events.rules suricata.ruleses
[root@kali ~]# dnsp3-events.rules http-events.rules nfts-events.rules smtp-events.rules suricata.yaml
[root@kali ~]# dns-events.rules ipsec-events.rules ntp-events.rules ssh-events.rules tls-events.rules
[root@kali ~]# (root@kali)-[~/etc/suricata/rules]
[root@kali ~]# nano suricata.yaml
[root@kali ~]# cd rules
cd: no such file or directory: rules
[root@kali ~]# (root@kali)-[~/etc/suricata/rules]
[root@kali ~]# cd ..
[root@kali ~]# nano suricata.yaml
[root@kali ~]# suricata -c /etc/suricata/suricata.yaml -i eth0
Info: conf-yaml-loader: Configuration node 'default-rule-path' redefined.
: suricata: This is Suricata version 7.0.8 RELEASE running in SYSTEM mode
: threads: Threads created -> W: 2 FM: 1 FR: 1 Engine started.

```

The right terminal window shows the Suricata log output:

```

kali@kali: /var/log/suricata
File Actions Edit View Help
[kali@kali ~]# 
[kali@kali ~]# tail -f fast.log
tail:f: command not found
[kali@kali ~]# (kali@kali)-[~/var/log/suricata]
[kali@kali ~]# $ tail -f fast.log
01/19/2025-15:35:39.526813 [*] [1:2200076:2] SURICATA ICMPv4 invalid checksum [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {ICMP} 192.168.1.68>192.168.1.1:0
01/19/2025-15:35:39.526816 [*] [1:2200073:2] SURICATA IPv4 invalid checksum [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {ICMP} 192.168.1.68>192.168.1.1:0
01/19/2025-15:36:46.116649 [*] [1:2200073:2] SURICATA IPv4 invalid checksum [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {ICMP} 192.168.1.68>192.168.1.1:0
01/27/2025-09:57:04.242509 [*] [1:1:1:8] trafico detectado [*] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.68:44360 -> 34.117.188.166:443
01/27/2025-09:57:04.261873 [*] [1:1:1:8] trafico detectado [*] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.68:4432 -> 192.168.1.68:4252
01/27/2025-09:57:04.628442 [*] [1:1:1:8] trafico detectado [*] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.68:44360 -> 34.117.188.166:4443
01/27/2025-09:57:04.735111 [*] [1:1:1:8] trafico detectado [*] [Classification: (null)] [Priority: 3] {TCP} 34.117.188.166:443 -> 192.168.1.68:44366
01/27/2025-09:57:04.735111 [*] [1:1:1:8] trafico detectado [*] [Classification: (null)] [Priority: 3] {TCP} 34.117.188.166:443 -> 192.168.1.68:44366
01/27/2025-09:57:04.735111 [*] [1:1:1:8] trafico detectado [*] [Classification: (null)] [Priority: 3] {TCP} 34.117.188.166:443 -> 192.168.1.68:44366
01/27/2025-09:57:05.126324 [*] [1:1:1:8] trafico detectado [*] [Classification: (null)] [Priority: 3] {TCP} 142.250.200.67:88 -> 192.168.1.68:33078
01/27/2025-09:57:05.260301 [*] [1:1:1:8] trafico detectado [*] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.68:39966 -> 184.31.8.44:80
01/27/2025-09:57:05.280365 [*] [1:1:1:8] trafico detectado [*] [Classification: (null)] [Priority: 3] {TCP} 184.31.8.44:80 -> 192.168.1.68:39966
01/27/2025-09:57:06.611204 [*] [1:1:1:8] trafico detectado [*] [Classification: (null)] [Priority: 3] {TCP} 192.168.1.68:39966 -> 184.31.8.44:80

```

4. Instalación de Elastic (Suricata / Windows / Honeypot)

Nos identificamos en la web de elastic con un mail, bien propio o bien temporal.

Los pasos a seguir desde la web son: Assets / Fleet / Agent Policies/ Create agent Policy / añadimos un nombre (Suricata/Linux) / pinchamos en las políticas / añadimos una integración / en búsqueda : suricata y añadimos la integración.

Debemos pegar el comando generado en nuestra Kali para la instalación.

Nos vamos a una consola en nuestra máquina Kali, hacemos Ping para comprobar que hay conexión y copiamos en comando de elastic para instalarlo.

```

kali@kali: ~/elastic-agent-8.17.1-linux-x86_64
File Actions Edit View Help
[sudo] password for kali:
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service.
Do you want to continue? [Y/n]:y
[=] Service Started [11s] Elastic Agent successfully installed, starting enrollment.
[=] Waiting For Enroll... [12s] {"log.level": "info", "@timestamp": "2025-01-27T15:31:07.975-0500", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff", "file.name": "cmd/enroll_cmd.go", "file.line": "520"}, "message": "Starting enrollment to URL: https://fac28c00d7bb43lf823113b9487c0a38.fleet.europe-west1.gcp.cloud.es.io:443/", "ecs.version": "1.6.0"}
[=] Waiting For Enroll... [15s] {"log.level": "info", "@timestamp": "2025-01-27T15:31:07.975-0500", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff", "file.name": "cmd/enroll_cmd.go", "file.line": "520"}, "message": "Starting enrollment to URL: https://fac28c00d7bb43lf823113b9487c0a38.fleet.europe-west1.gcp.cloud.es.io:443/", "ecs.version": "1.6.0"}
[=] Waiting For Enroll... [15s] {"log.level": "info", "@timestamp": "2025-01-27T15:31:10.691-0500", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff", "file.name": "cmd/enroll_cmd.go", "file.line": "483"}, "message": "Restarting agent daemon, attempt 0", "ecs.version": "1.6.0"}
[=] Waiting For Enroll... [15s] {"log.level": "info", "@timestamp": "2025-01-27T15:31:10.727-0500", "log.origin": {"function": "github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).Execute", "file.name": "cmd/enroll_cmd.go", "file.line": "301"}, "message": "Successfully triggered restart on running Elastic Agent.", "ecs.version": "1.6.0"}
[=] Done [15s]
Elastic Agent has been successfully installed.

```

Volvemos a elastic, y podemos comprobar en Assets / Fleet que ya nos saldría nuestro agente añadido suricata/linux.

[Back to integrations](#)

Suricata

Elastic Agent

Version 2.23.0

- Overview
- Integration policies
- Assets
- 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

Compatibility

This module has been developed against Suricata v4.0.4, but is expected to work with other versions of Suricata.

EVE

An example event for `eve` looks as following:

Suricata / Linux		Revision 3	Integrations 2	Agents 1 agent	Last updated on Mar 18, 2025	Actions
View all agent policies						Edit
Integrations	Settings					
<input type="text"/> Search...						Namespace
						Add integration
Integration policy	Integration	Namespace	Output	Actions		
suricata-1	Suricata v2.23.0	default	Default output			
system-1	System v1.67.3	default	Default output			

Fleet

Centralized management for Elastic Agents.

- Agents
- Agent policies
- Enrollment tokens
- Uninstall tokens
- Data streams
- Settings

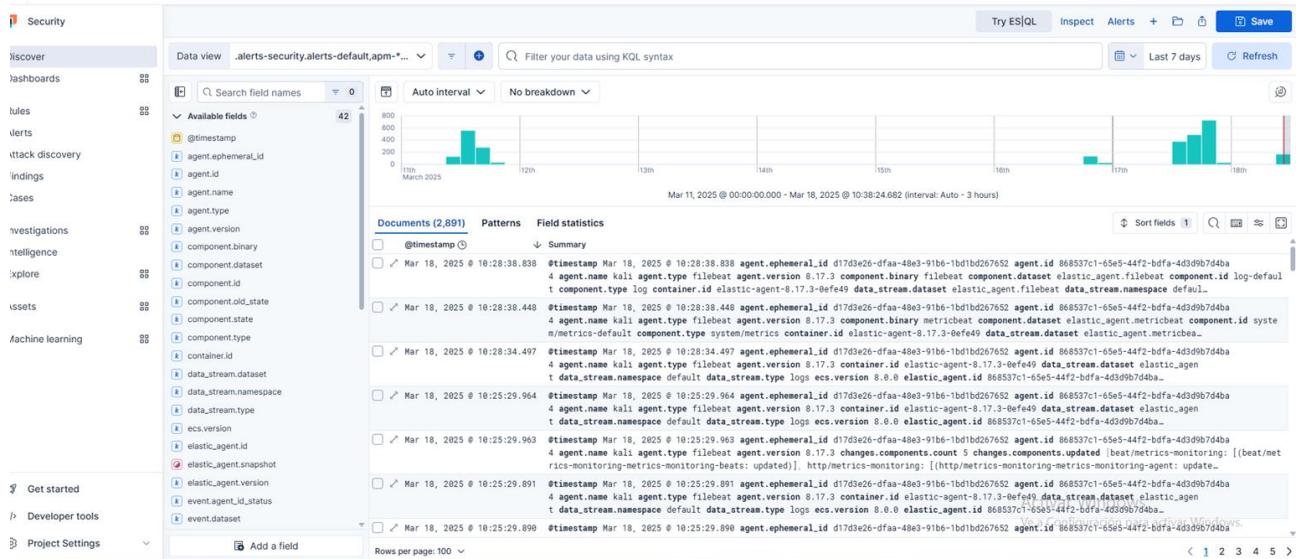
[Ingest Overview Metrics](#) [Agent Info Metrics](#) [Agent activity](#) [Add agent](#)

Filter your data using KQL syntax

Showng 1 agent [Clear filters](#) Status: 1 Healthy, 0 Unhealthy, 0 Orphaned, 0 Updating, 0 Offline, 0 Inactive, 0 Unenrolled, 0 Uninstalled [Upgrade available](#)

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
<input checked="" type="checkbox"/> Healthy	kali	Suricata / Linux rev. 1	3.74 %	181 MB	18 seconds ago	8.17.3	

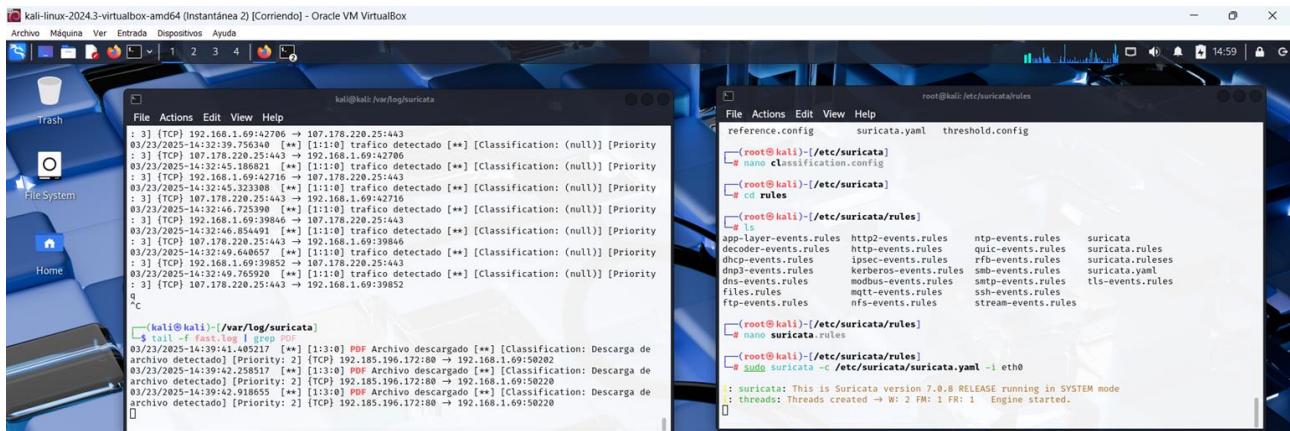
Finalmente en Discover podemos visualizar los logs:



Hemos creado la regla :

```
alert tcp any any -> any any (msg:"PDF Archivo descargado"; flow:established,to_client;
fileext:"pdf"; sid:3; classtype:file-download;)
```

Mas abajo podemos ver los logs "PDF Archivo descargado" generados por Suricata en nuestra máquina Kali.



Se adjunta el log generado por Suricata en elastic y descargado desde el elastic:

```
{ "@timestamp": [ "2025-03-23T18:39:47.917Z" ], "agent.ephemeral_id": [ "99d20f18-fd14-4ff0-a7ac-622072c8c521" ], "agent.id": [ "868537c1-65e5-44f2-bdfa-4d3d9b7d4ba4" ], "agent.name": [ "kali" ], "agent.type": [ "filebeat" ], "agent.version": [ "8.17.3" ], "data_stream.dataset": [ "suricata.eve" ], "data_stream.namespace": [ "default" ], "data_stream.type": [ "logs" ], "destination.address": [ "192.168.1.69" ], "destination.domain": [ "manosnegras.com" ], "destination.ip": [ "192.168.1.69" ], "destination.port": [ 50220 ], "ecs.version": [ "8.17.0" ], "elastic_agent.id": [ "868537c1-65e5-44f2-bdfa-4d3d9b7d4ba4" ], "elastic_agent.snapshot": [ false ], "elastic_agent.version": [ "8.17.3" ], "event.agent_id_status": [ "verified" ], "event.category": [ "network" ], "event.created": [ "2025-03-23T18:39:48.425Z" ], "event.dataset": [ "suricata.eve" ], "event.ingested": [ "2025-03-23T18:39:58.000Z" ], "event.kind": [ "event" ], "event.module": [ "suricata" ], "file.path": [ "/unir2018/wp-content/uploads/2017/11/Tema2.pdf" ], "file.path.text": [ "/unir2018/wp-content/uploads/2017/11/Tema2.pdf" ], "file.size": [ 65536 ], "http.request.method": [ "GET" ], "http.request.referrer": [ "https://www.google.com/" ], "http.response.body.bytes": [ 65536 ], "http.response.status_code": [ 206 ], "input.type": [ "log" ], "log.file.path": [ "/var/log/suricata/eve.json" ], "log.offset": [ 8321020 ], "network.community_id": [ "1:ANFZ+smBtvKNXhm19NF0y49DIWM=" ], "network.protocol": [ "http" ], "network.transport": [ "tcp" ], "observer.hostname": [ "kali" ], "observer.ip": [ "192.168.1.69", "fe80::b4b0:9a6a:b0aa:5394", "172.17.0.1", "fe80::42:e7ff:fee4:5dae" ], "observer.mac": [ "02-42-E7-E4-5D-AE", "08-00-27-AD-25-87" ], "observer.product": [ "Suricata" ], "observer.type": [ "ids" ], "observer.vendor": [ "OISF" ], "related.hosts": [ "manosnegras.com" ], "related.ip": [ "192.185.196.172", "192.168.1.69" ], "source.address": [ "192.185.196.172" ], "source.as.number": [ 19871 ], "source.as.organization.name": [ "NETWORK-SOLUTIONS-HOSTING" ], "source.as.organization.name.text": [ "NETWORK-SOLUTIONS-HOSTING" ], "source.geo.continent_name": [ "North America" ], "source.geo.country_iso_code": [ "US" ], "source.geo.country_name": [ "United States" ], "source.geo.location": [ { "coordinates": [ -97.8220000024885, 37.75099997408688 ], "type": "Point" } ], "source.ip": [ "192.185.196.172" ], "source.port": [ 80 ], "suricata.eve.event_type": [ "fileinfo" ], "suricata.eve.fileinfo.end": [ "1970-01-01T00:48:03.583Z" ], "suricata.eve.fileinfo.gaps": [ false ], "suricata.eve.fileinfo.start": [ "1970-01-01T00:46:58.048Z" ], "suricata.eve.fileinfo.state": [ "CLOSED" ], "suricata.eve.fileinfo.stored": [ false ], "suricata.eve.fileinfo.tx_id": [ 1 ], "suricata.eve.flow_id": [ "1433806486926790" ], "suricata.eve.http.content_range.end": [ "1970-01-01T00:48:03.583Z" ], "suricata.eve.http.content_range.raw": [ "bytes 2818048-2883583/2916403" ], "suricata.eve.http.content_range.size": [ 2916403 ], "suricata.eve.http.content_range.start": [ "1970-01-01T00:46:58.048Z" ], "suricata.eve.http.http_content_type": [ "application/pdf" ], "suricata.eve.http.protocol": [ "HTTP/1.1" ], "suricata.eve.in_iface": [ "eth0" ], "suricata.eve.pkt_src": [ "wire/pcap" ], "tags": [ "forwarded", "suricata-eve" ], "url.domain": [ "manosnegras.com" ], "url.original": [ "/unir2018/wp-content/uploads/2017/11/Tema2.pdf" ], "url.original.text": [ "/unir2018/wp-content/uploads/2017/11/Tema2.pdf" ], "url.path": [ "/unir2018/wp-content/uploads/2017/11/Tema2.pdf" ], "user_agent.device.name": [ "Other" ], "user_agent.name": [ "Firefox" ], "user_agent.original": [ "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" ], "user_agent.original.text": [ "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0" ], "user_agent.os.name": [ "Linux" ], "user_agent.os.name.text": [ "Linux" ], "user_agent.version": [ "128.0" ], "_id": "AZXETRA31VbRquz2bzVB", "_index": ".ds-logs-suricata.eve-default-2025.03.23-000001", "_score": null }
```

Para ver los logs del Windows nos vamos a la política de suricata/linux creada y le añadimos otra integración para recopilar los logs del Windows:

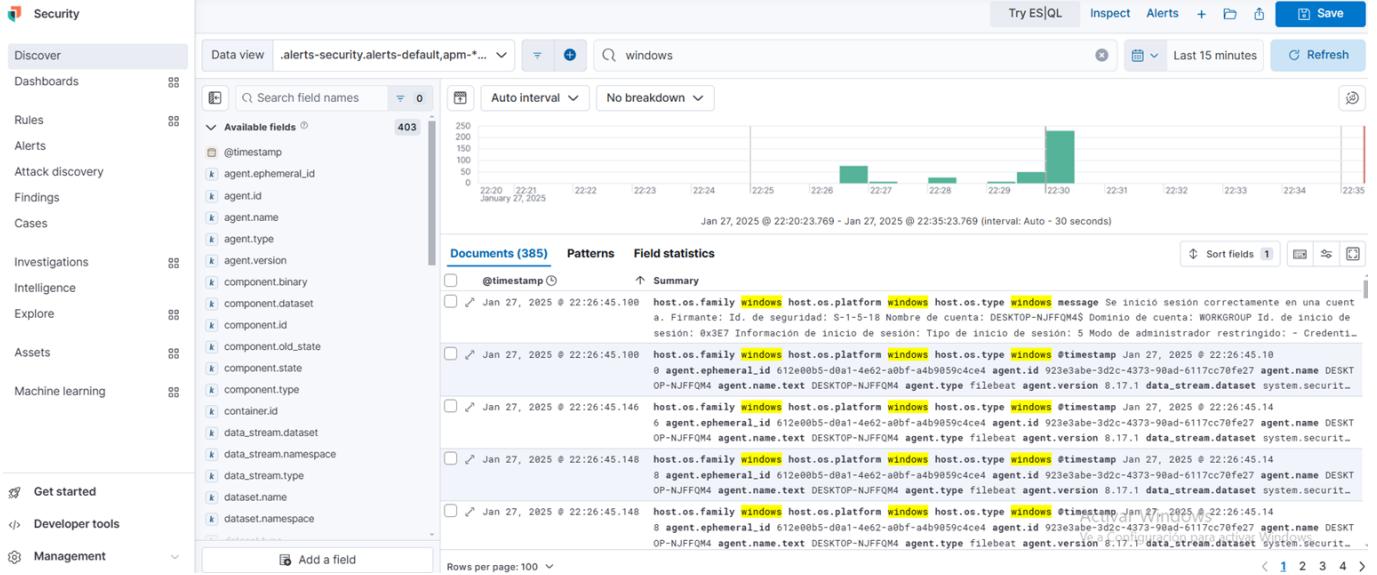
(Previamente hemos instalado en VirtualBox nuestra máquina de Windows, de modo que es independiente y logueada en elastic).

The screenshot shows the Suricata interface with the 'Windows' integration selected. The top bar displays 'Revision 2', 'Integrations 2', 'Agents 1 agent', and 'Last updated on Jan 27, 2025'. Below this, there's a search bar and a table listing two integrations: 'system-2' (System v1.64.0) and 'windows-1' (Windows v2.3.6). A button for 'Add integration' is visible. The left sidebar includes options like Discover, Dashboards, Rules, Alerts, Attack discovery, Findings, Cases, Investigations, Intelligence, Explore, Assets, and Machine learning.

Una vez hemos instalada la política copiamos el comando y lo pegamos en la consola powershell para instalarlo

This screenshot shows the 'Add agent' window for the Windows integration. It contains a command line for installing the Elastic Agent: \$ProgressPreference = 'SilentlyContinue'; Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent-8.17.1-windows-x86_64.zip -DestinationPath .\elastic-agent-8.17.1-windows-x86_64.\elastic-agent.exe install --url=https://fac28c0bd7bb431f823113b9487c. The 'Windows' tab is selected. Below the command, a green box indicates 'Agent enrollment confirmed' with the message '1 agent has been enrolled.' and a link to 'View enrolled agents'.

En el apartado de Discover podemos ver los logs de Windows:



Finalmente vamos a instalar el Honeypot en el elastic como una integración en suricata-Linux ya que estamos usando la misma máquina kali, y lo haremos con la integración de Customlog:

Fleet

Centralized management for Elastic Agents.

Agents **Agent policies** **Enrollment tokens** **Uninstall tokens** **Data streams** **Settings**

Ingest Overview Metrics **Agent Info Metrics**

Agent activity **Add agent**

Filter your data using KQL syntax

Status: 3 Tags: 1 Agent policy: 1 Upgrade available

Showing 1 agent (1) Clear filters

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	kali	Honeypot rev. 2	2.71 %	190 MB	21 seconds ago	8.17.4	Upgrade available

Rows per page: 20

Aquí podemos ver los logs del Honeypot:

Discover / My_Security_project Discover

Try ES|QL Inspect Alerts + Save

Filter your data using KQL syntax

Search field names

Last 15 minutes Refresh

Copy value

Sort fields

Copy

Timestamp Apr 16, 2025 @ 12:35:50.969 agent.ephemeral_id be100837-a1e5-4f62-ba90-2e53e9c03f9
b agent.id 8d90d3f6-6633-4e0f-b849-537daf8601c1 agent.name kali agent.type filebea
t agent.version 8.17.4 data_stream.dataset generic data_stream.namespace default

Timestamp Apr 16, 2025 @ 12:35:50.969 agent.ephemeral_id be100837-a1e5-4f62-ba90-2e53e9c03f9
b agent.id 8d90d3f6-6633-4e0f-b849-537daf8601c1 agent.name kali agent.type filebea
t agent.version 8.17.4 data_stream.dataset generic data_stream.namespace default

Timestamp Apr 16, 2025 @ 12:35:47.961 agent.ephemeral_id be100837-a1e5-4f62-ba90-2e53e9c03f9
b agent.id 8d90d3f6-6633-4e0f-b849-537daf8601c1 agent.name kali agent.type filebea
t agent.version 8.17.4 data_stream.dataset generic data_stream.namespace default

Timestamp Apr 16, 2025 @ 12:35:47.961 agent.ephemeral_id be100837-a1e5-4f62-ba90-2e53e9c03f9
b agent.id 8d90d3f6-6633-4e0f-b849-537daf8601c1 agent.name kali.agent.type filebeaWindows

```

kali@kali: ~
File Actions Edit View Help
2025-04-16T09:48:37+0000 [twisted.conch.ssh.session#info] Getting shell
2025-04-16T09:49:27+0000 [HoneyPotSSHTransport,1,192.168.1.59] CMD: ls
2025-04-16T09:49:27+0000 [HoneyPotSSHTransport,1,192.168.1.59] Command found: ls
2025-04-16T09:51:37+0000 [-] Timeout reached in HoneyPotSSHTransport
2025-04-16T09:51:37+0000 [HoneyPotSSHTransport,1,192.168.1.59] Closing TTY Log: var/lib/cowrie/tty
/1d887ce0f8672e4914d9000e801cd74ecd805dd9366c0bc42dc16adc0197dc2f after 179.9 seconds
2025-04-16T09:51:37+0000 [HoneyPotSSHTransport,1,192.168.1.59] avatar root logging out
2025-04-16T09:51:37+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2025-04-16T09:51:37+0000 [HoneyPotSSHTransport,1,192.168.1.59] Connection lost after 217.3 seconds
^C2025-04-16T10:02:09+0000 [twisted.internet.base#info] Received SIGINT, shutting down.
2025-04-16T10:02:09+0000 [-] (TCP Port 2222 Closed)
2025-04-16T10:02:09+0000 [cowrie.ssh.factory.CowrieSSHFactory#info] Stopping factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7ef0d0453250>
2025-04-16T10:02:09+0000 [twisted.internet.base#info] Main loop terminated.
2025-04-16T10:02:09+0000 [twisted.scripts._twistd_unix.UnixAppLogger#info] Server Shut Down.

(kali㉿kali)-[~]
$ docker run -p 222:2222 cowrie/cowrie > cowrie.log
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:105: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-cbc": (algorithms.TripleDES, 24, modes.CBC),
/cowrie/cowrie-env/lib/python3.11/site-packages/twisted/conch/ssh/transport.py:112: CryptographyDeprecationWarning: TripleDES has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.TripleDES and will be removed from cryptography.hazmat.primitives.ciphers.algorithms in 48.0.0.
  b"3des-ctr": (algorithms.TripleDES, 24, modes.CTR),

```

```

{
  "@timestamp": [ "2025-04-16T10:45:35.794Z" ],
  "agent.ephemeral_id": [ "be100837-a1e5-4f62-ba90-2e53e9c03f9b" ],
  "agent.id": [ "8d90d3f6-6633-4e0f-b849-537daf8601c1" ],
  "agent.name": [ "kali" ],
  "agent.type": [ "filebeat" ],
  "agent.version": [ "8.17.4" ],
  "data_stream.dataset": [ "generic" ],
  "data_stream.namespace": [ "default" ],
  "data_stream.type": [ "logs" ],
  "ecs.version": [ "8.0.0" ],
  "elastic_agent.id": [ "8d90d3f6-6633-4e0f-b849-537daf8601c1" ],
  "elastic_agent.snapshot": [ false ],
  "elastic_agent.version": [ "8.17.4" ],
  "event.agent_id_status": [ "verified" ],
  "event.dataset": [ "generic" ],
  "event.ingested": [ "2025-04-16T10:45:48.000Z" ],
  "host.architecture": [ "x86_64" ],
  "host.containerized": [ false ],
  "host.hostname": [ "kali" ],
  "host.id": [ "30e662c5c81d4191bd2444a79c97d2e0" ],
  "host.ip": [ "192.168.1.69" ],
  "fe80::b4b0:9a6a:b0aa:5394", "172.17.0.1",
  "fe80::42:35ff:fe34:b0b8",
  "fe80::9c1e:58ff:fe0a:7e3d" ],
  "host.mac": [ "02-42-35-34-B0-B8", "08-00-27-AD-25-87", "9E-1E-58-0A-7E-3D" ],
  "host.name": [ "kali" ],
  "host.os.codename": [ "kali-rolling" ],
  "host.os.family": [ "debian" ],
  "host.os.kernel": [ "6.12.13-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": [ "2025.1" ],
  "input.type": [ "log" ],
  "log.file.path": [ "/home/kali/cowrie.log" ],
  "log.file.path.text": [ "/home/kali/cowrie.log" ],
  "log.offset": [ 16062 ],
  "message": [ "2025-04-16T10:45:33+0000 [HoneyPotSSHTransport,4,192.168.1.59] Command found: cd opt" ],
  "_id": "AZY-NO_7dOcSX215YFyY",
  "_index": ".ds-logs-generic-default-2025.04.16-000001",
  "_score": null
}

```

generado: