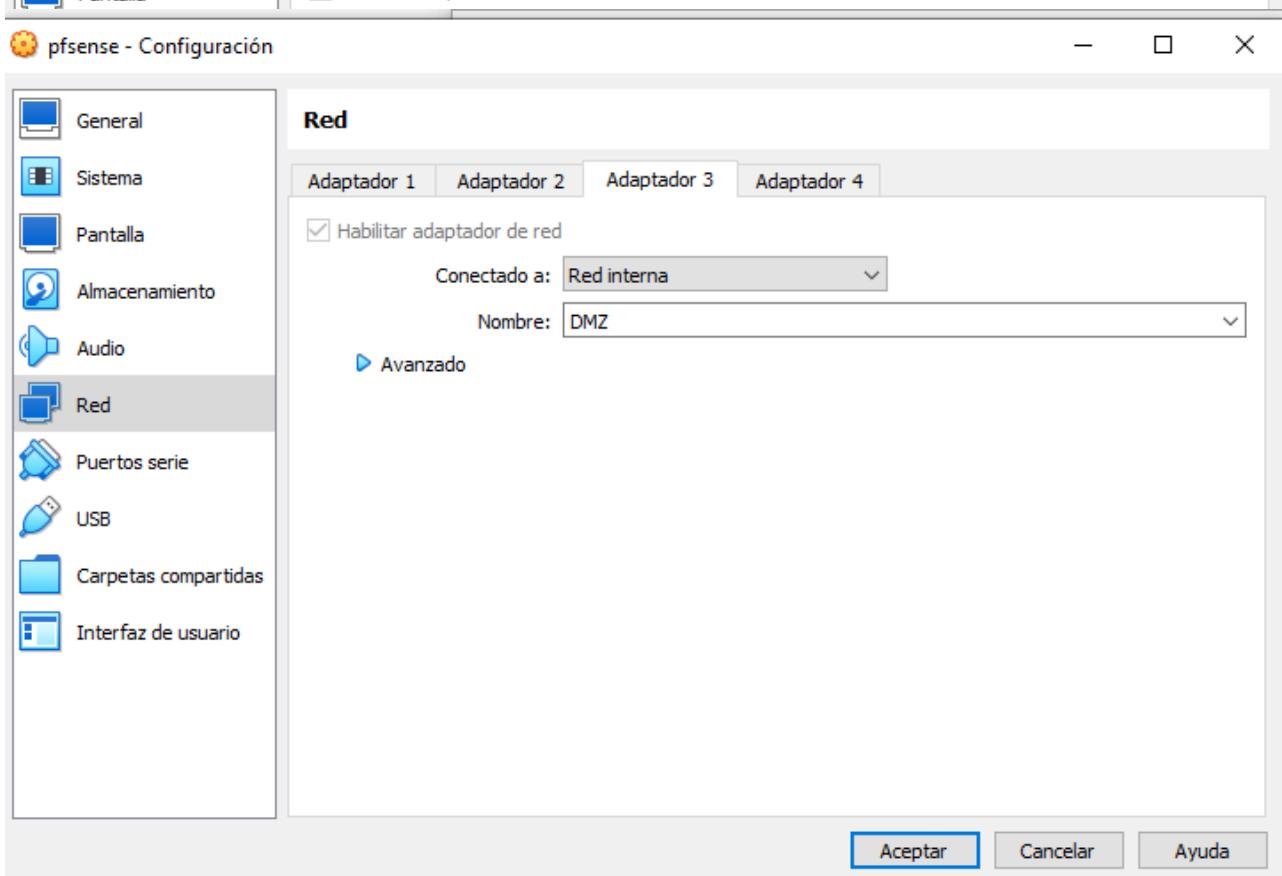
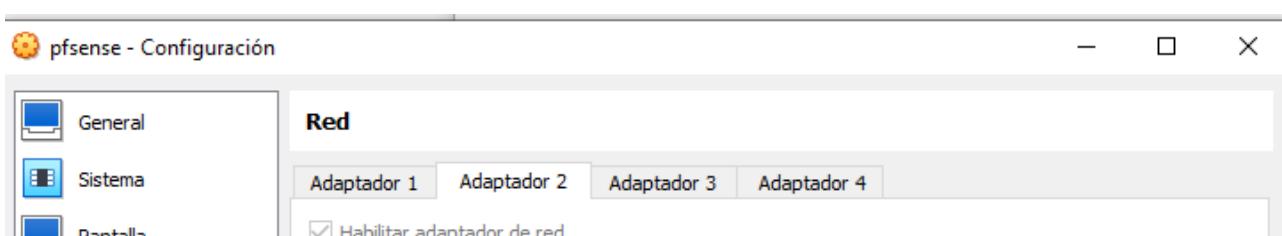
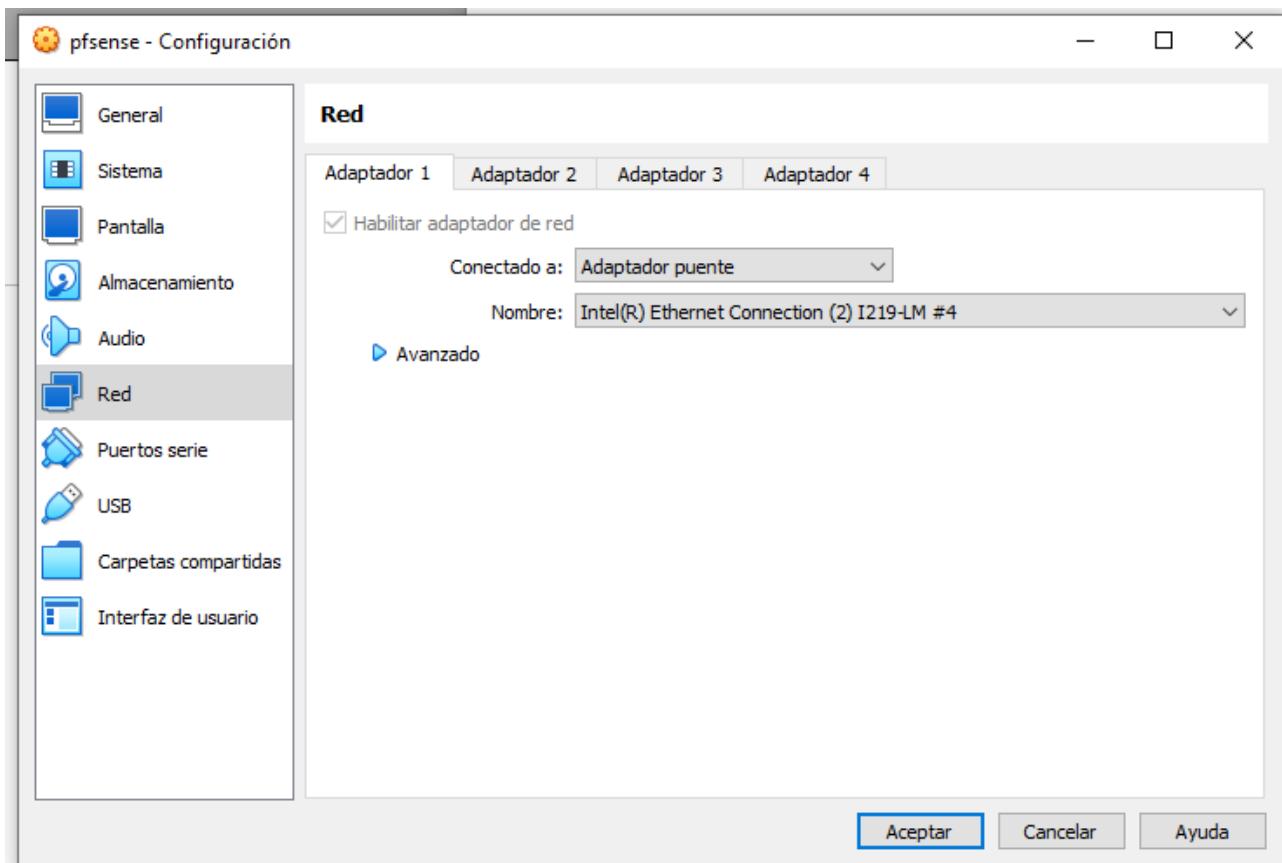
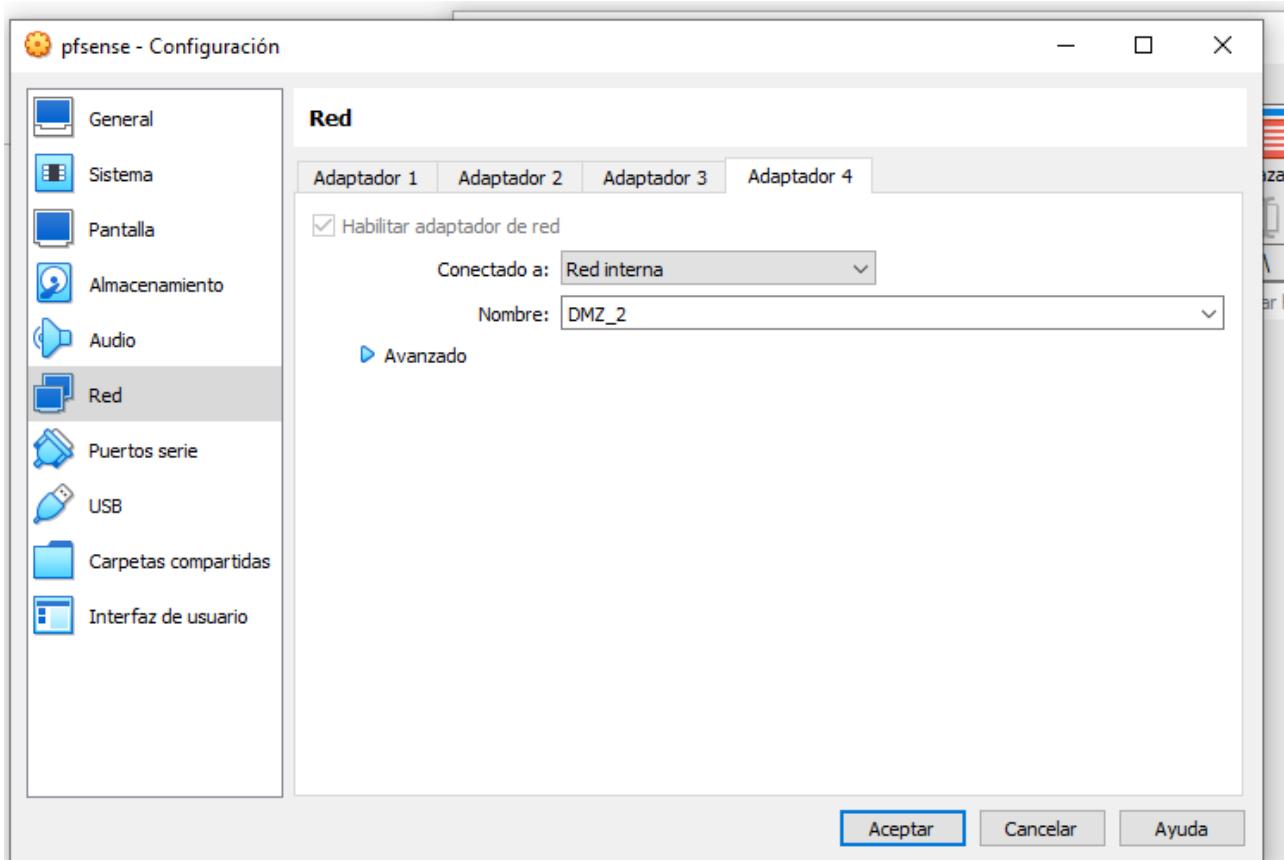


MONTAJE DE INFRAESTRUCTURA





arrancamos la Unified Threat Management (UTM)

```
pfSense (UTM funcionando) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

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

VirtualBox Virtual Machine - Netgate Device ID: d16b4b90899ec6066e97

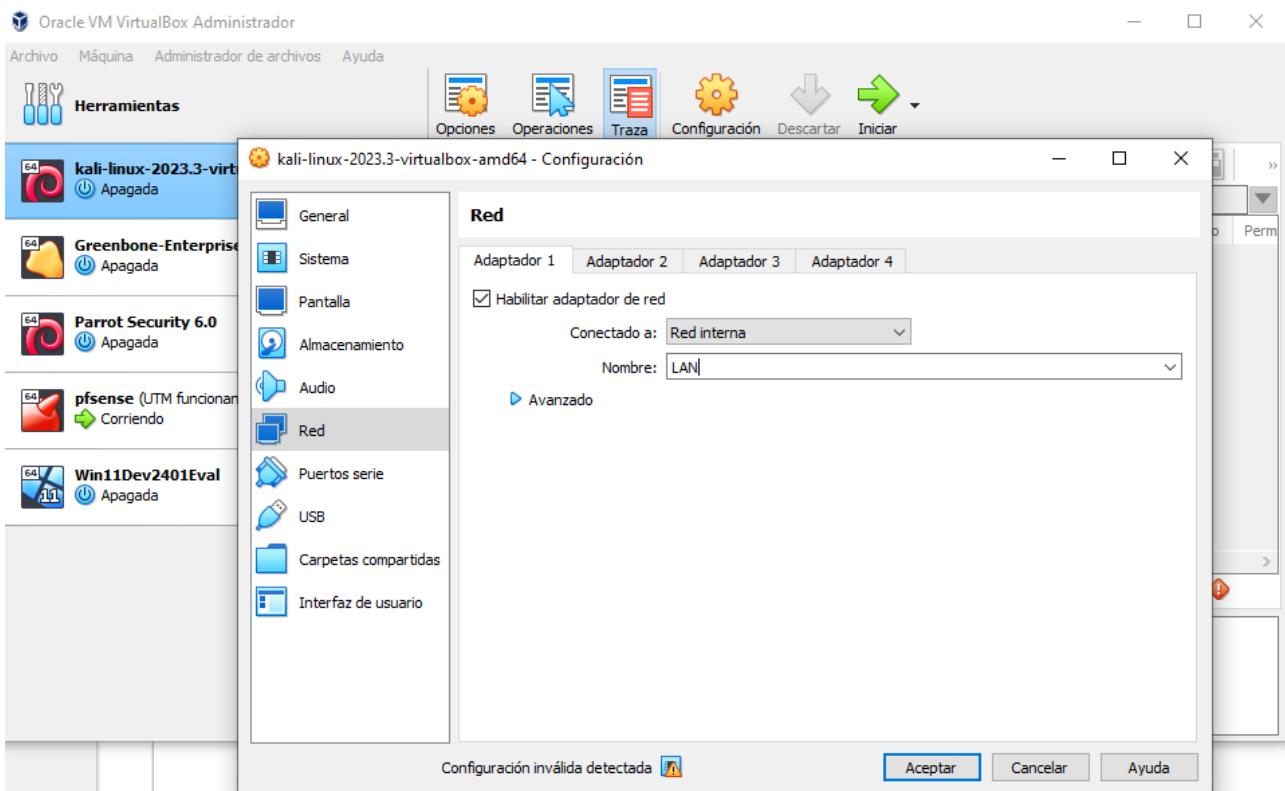
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on UTM ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.16/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24

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: 
```

configuramos la kali en red interna LAN



Arrancamos la kali e introducimos en el navegador la ip del adaptador LAN, en mi caso:

192.168.100.1

A screenshot of a web browser window showing the pfSense login interface. The address bar displays the URL '192.168.100.1'. The page features the pfSense logo at the top left and a 'Login to pfSense' link at the top right. The main content is a dark blue sign-in form with fields for 'admin' (username) and a masked password (password). A green 'SIGN IN' button is located at the bottom of the form. At the very bottom of the page, there is a small footer note: 'pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.'

usuario admin, password pfsense

System Information

Name	UTM.keepinglocal
User	admin@192.168.100.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: d16b4b90899ec6066e97
BIOS	Vendor: innoteck GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE
CPU Type	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 07 Minutes 17 Seconds
Current date/time	Fri Mar 15 0:22:19 CET 2024
DNS server(s)	• 127.0.0.1 • 192.168.0.1

Netgate Services And Support

Retrieving support information

Interfaces

WAN	1000baseT <full-duplex>	192.168.0.18
LAN	1000baseT <full-duplex>	192.168.100.1

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	WAN
IPv4 Configuration Type	DHCP
IPv6 Configuration Type	DHCP6

Advanced Options

Use IPv4 connectivity as parent interface	<input type="checkbox"/> Request a IPv6 prefix/information through the IPv4 connectivity link
Request only an IPv6 prefix	<input type="checkbox"/> Only request an IPv6 prefix, do not request an IPv6 address
DHCPv6 Prefix Delegation size	64
Send IPv6 prefix hint	<input type="checkbox"/> Send an IPv6 prefix hint to indicate the desired prefix size for delegation
Debug	<input type="checkbox"/> Start DHCP6 client in debug mode
Do not wait for a RA	<input type="checkbox"/> Required by some ISPs, especially those not using PPPoE
Do not allow PD/Address release	<input type="checkbox"/> dhcp6c will send a release to the ISP on exit, some ISPs then release the allocated address or prefix. This option prevents that signal ever being sent

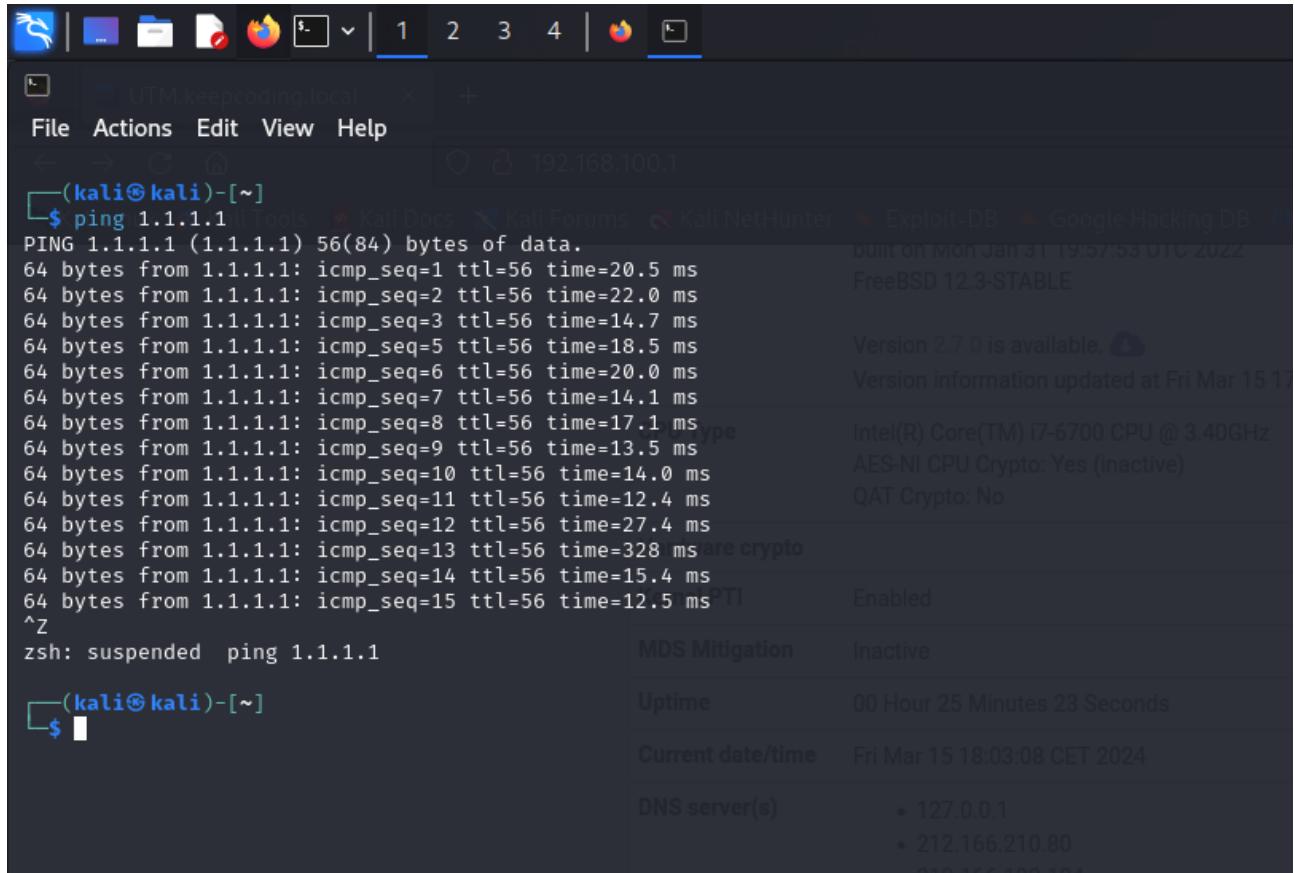
Reserved Networks

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.	
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.	

Save

CONFIGURACIÓN DE LAS INTERFACES

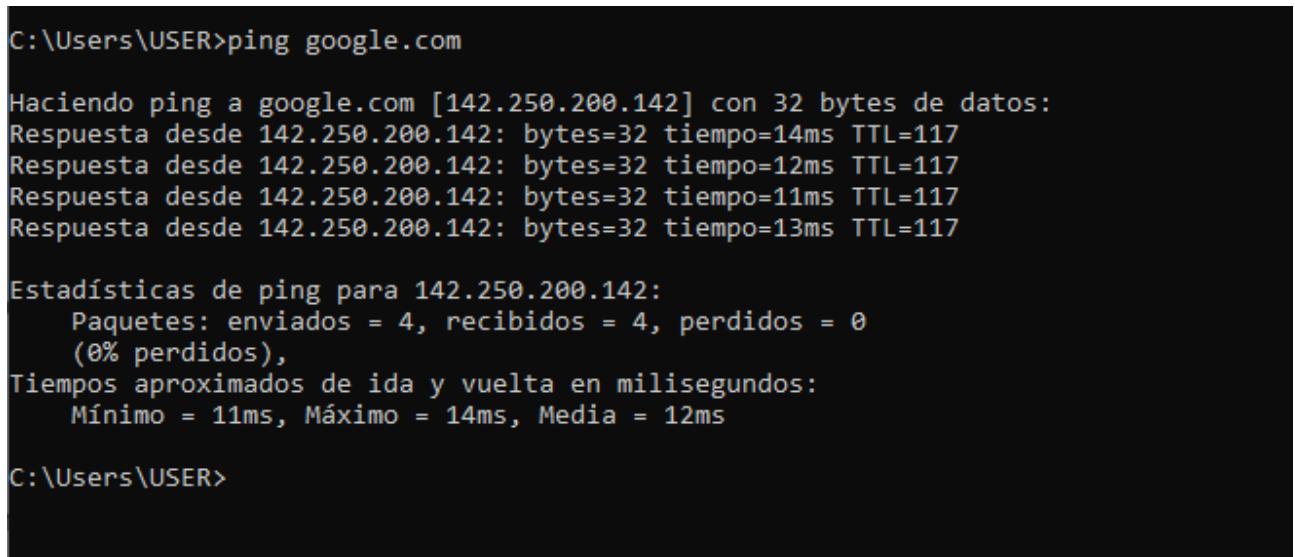
Comprobamos si tenemos accesos a internet en la kali haciendo un ping a 1.1.1.1:



```
(kali㉿kali)-[~]$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=56 time=20.5 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=56 time=22.0 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=56 time=14.7 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=56 time=18.5 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=56 time=20.0 ms
64 bytes from 1.1.1.1: icmp_seq=7 ttl=56 time=14.1 ms
64 bytes from 1.1.1.1: icmp_seq=8 ttl=56 time=17.1 ms
64 bytes from 1.1.1.1: icmp_seq=9 ttl=56 time=13.5 ms
64 bytes from 1.1.1.1: icmp_seq=10 ttl=56 time=14.0 ms
64 bytes from 1.1.1.1: icmp_seq=11 ttl=56 time=12.4 ms
64 bytes from 1.1.1.1: icmp_seq=12 ttl=56 time=27.4 ms
64 bytes from 1.1.1.1: icmp_seq=13 ttl=56 time=328 ms are crypto
64 bytes from 1.1.1.1: icmp_seq=14 ttl=56 time=15.4 ms
64 bytes from 1.1.1.1: icmp_seq=15 ttl=56 time=12.5 ms TI
^Z
zsh: suspended ping 1.1.1.1
```

Uptime: 00 Hour 25 Minutes 23 Seconds
Current date/time: Fri Mar 15 18:03:08 CET 2024
DNS server(s): 127.0.0.1, 212.166.210.80, 212.166.210.101

hacemos ping en nuestro sistema windows a google.com



```
C:\Users\USER>ping google.com

Haciendo ping a google.com [142.250.200.142] con 32 bytes de datos:
Respuesta desde 142.250.200.142: bytes=32 tiempo=14ms TTL=117
Respuesta desde 142.250.200.142: bytes=32 tiempo=12ms TTL=117
Respuesta desde 142.250.200.142: bytes=32 tiempo=11ms TTL=117
Respuesta desde 142.250.200.142: bytes=32 tiempo=13ms TTL=117

Estadísticas de ping para 142.250.200.142:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 11ms, Máximo = 14ms, Media = 12ms

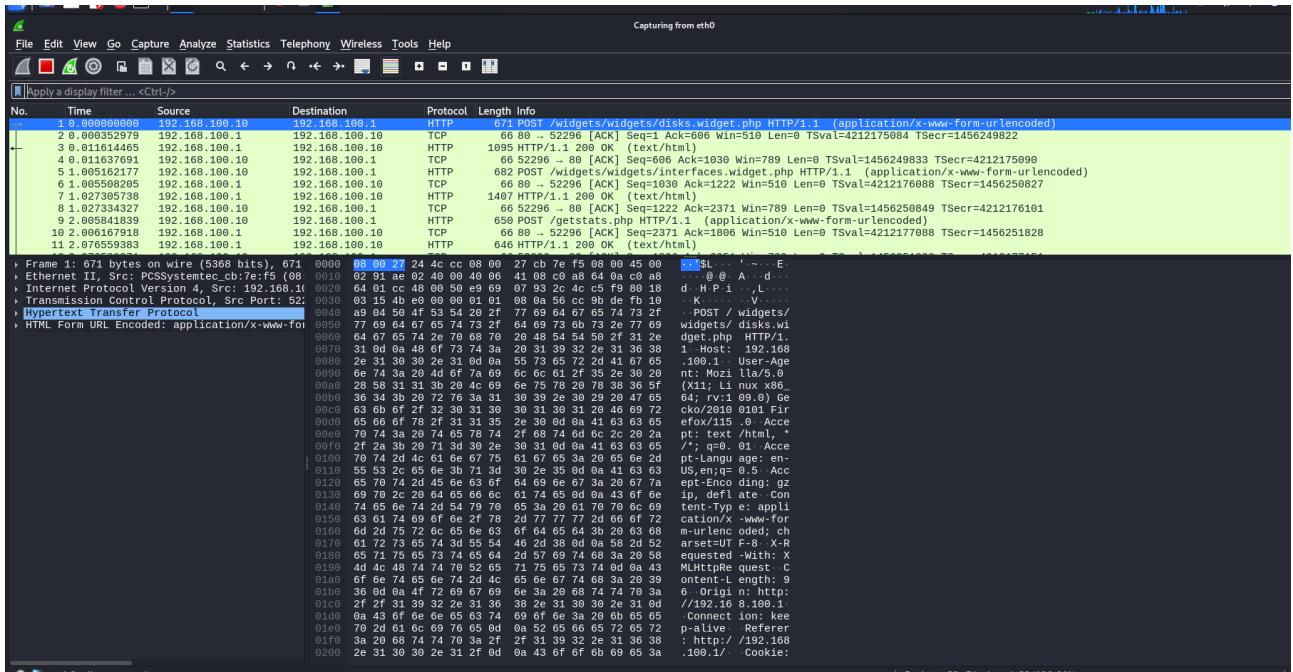
C:\Users\USER>
```

cogemos la ip y la pegamos en kali

```
└─(kali㉿kali)-[~]
$ ping 142.250.200.142
PING 142.250.200.142 (142.250.200.142) 56(84) bytes of data.
64 bytes from 142.250.200.142: icmp_seq=1 ttl=116 time=19.3 ms
64 bytes from 142.250.200.142: icmp_seq=2 ttl=116 time=14.8 ms
64 bytes from 142.250.200.142: icmp_seq=3 ttl=116 time=20.9 ms
64 bytes from 142.250.200.142: icmp_seq=4 ttl=116 time=24.7 ms
64 bytes from 142.250.200.142: icmp_seq=5 ttl=116 time=16.2 ms
64 bytes from 142.250.200.142: icmp_seq=6 ttl=116 time=14.7 ms
64 bytes from 142.250.200.142: icmp_seq=7 ttl=116 time=13.6 ms
^Z
zsh: suspended  ping 142.250.200.142

└─(kali㉿kali)-[~]
$
```

en wireshark podemos ver el tráfico que está pasando por la interface de red eth0:



hacemos click botón derecho en alguna de las tramas, Follow y TCP Stream y vemos todos los paquetes del tráfico:

```

POST /widgets/widgets/disks.widget.php HTTP/1.1
Host: 192.168.100.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html, */*, q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 96
Origin: http://192.168.100.1
Connection: keep-alive
Referer: http://192.168.100.1/
Cookie: PHPSESSID=ba4fb8cfdd7f540d03d2aea1bbc20c0
__crsf_magic=sid:a20c1aae66b5ab314ba9ff0d88872de9bb75bd77,1710521625&ajax=ajax&widgetkey=disks-0HTTP/1.1 200 OK
Server: nginx
Date: Fri, 15 Mar 2024 17:09:08 GMT
Content-Type: text/html; charset=UTF-8
Content-Encoding: gzip
Connection: keep-alive
X-Frame-Options: SAMEORIGIN
Last-Modified: Fri, 15 Mar 2024 17:09:08 GMT
Set-Cookie: PHPSESSID=ba4fb8cfdd7f540d03d2aea1bbc20c0; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Frame-Options: SAMEORIGIN
Content-Encoding: gzip

```

Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface Ethernet II, Src: PCSSystemtec_c [00:0c:29:00:00:04], Dst: 192.168.100.1 [00:0c:29:00:00:01]
`...[REDACTED]`

POST /widgets/widgets/interfaces.widget.php HTTP/1.1
Host: 192.168.100.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html, */*, q=0.01
Accept-Language: en-US,en;q=0.5
108 client pkts, 108 server pkts, 215 turns.

Entire conversation (171 kB) Show data as ASCII Stream 0 Find Next

para ver la información del tráfico.

Configuramos el UTM:

vamos a Services y DNS Resolver

Name	UTM.keeping.local
User	admin@192.168.100.10 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: d164ab90899ec6066e97
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE
CPU Type	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 43 Minutes 15 Seconds

Netgate Services And Support

- Contract type: Community Support
Community Support Only

NETGATE AND pFSENSE COMMUNITY SUPPORT RESOURCES

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

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

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your Netgate Device ID (NDI) from your firewall in order to

deschekamos el DNSSEC que es un protocolo utilizado para firmar la respuesta DNS (asegura que la respuesta no ha sido modificada):

Outgoing Network Interfaces	<input type="checkbox"/> All <input type="checkbox"/> WAN <input type="checkbox"/> LAN <input type="checkbox"/> WAN IPv6 Link-Local <input type="checkbox"/> LAN IPv6 Link-Local
Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. 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.
System Domain Local Zone Type	<input type="button" value="Transparent"/> The local-zone type used for the pfSense system domain (System General Setup Domain). Transparent is the default. Local-Zone type descriptions are available in the unbound.conf(5) manual pages.
DNSSEC	<input type="checkbox"/> Enable DNSSEC Support
Python Module	<input type="checkbox"/> Enable Python Module Enable the Python Module.
DNS Query Forwarding	<input 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.

habilitamos el DNS Query Forwarding para enviar la consulta al servidor secundario el 1.1.1.1, en el caso de que PFSENSE no sea capaz de enviarla:

Interface Binding	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.
System Domain Local Zone Type	<input type="button" value="Transparent"/> The local-zone type used for the pfSense system domain (System General Setup Domain). Transparent is the default. Local-Zone type descriptions are available in the unbound.conf(5) manual pages.
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.

hacemos click en Save para guardar la configuración DNS:

Kali Tools https://www.kali.org/tools/	<small>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).</small> <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.										
Display Custom Options	<input type="button" value="Display Custom Options"/>										
<input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 5px; margin-right: 10px;" type="button" value="Save"/> ←											
Host Overrides <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #0070C0; color: white; text-align: left; padding: 2px;">Host</th> <th style="background-color: #0070C0; color: white; text-align: left; padding: 2px;">Parent domain of host</th> <th style="background-color: #0070C0; color: white; text-align: left; padding: 2px;">IP to return for host</th> <th style="background-color: #0070C0; color: white; text-align: left; padding: 2px;">Description</th> <th style="background-color: #0070C0; color: white; text-align: left; padding: 2px;">Actions</th> </tr> </thead> <tbody> <tr> <td colspan="5" style="padding: 5px;">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', 'ns.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.</td> </tr> </tbody> </table>		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', 'ns.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.				
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', 'ns.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.											

y damos a Apply Changes:

The changes have been applied successfully.

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.	

comprobamos en el navegador que tenemos acceso a marca.com

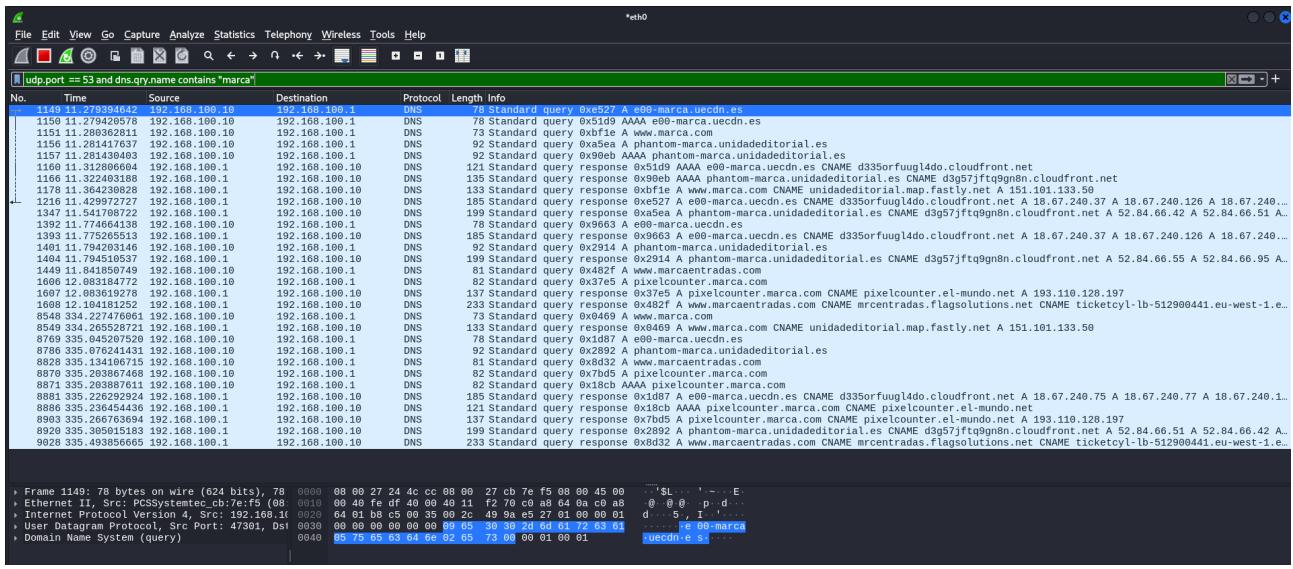
With your consent, we and our partners use cookies or similar technologies to store, access, and process personal data like your visit on this website. You can withdraw your consent or object to data processing based on legitimate interest at any time by clicking on "Learn more" or in our Cookie Policy on this website.

We and our partners process data for the following purposes Actively scan device characteristics for identification, Analizar su idoneidad para ofrecerle soluciones basadas en su red de telecomunicaciones, Create profiles for personalised advertising, Create profiles to personalise content, Develop and improve services, Enriching the profile with third-party information, Measure advertising performance, Measure content performance, Sharing your browsing analysis and interest groups with third parties, Storage and access to geolocation information for targeted advertising purposes, Storage and access to geolocation information to carry out marketing studies, Store and/or access information on a device, Understand audiences

y vemos el tráfico en wireshark con el filtro `tcp.port == 53 or udp.port == 53:`

No.	Time	Source	Destination	Protocol	Length	Info
6755	31.768267747	192.168.100.10	192.168.100.1	DNS	85	Standard query 0x0fc6 AAAA ade.googlesyndication.com
6756	31.781877552	192.168.100.1	192.168.100.10	DNS	142	Standard query response 0xfc6 AAAA ade.googlesyndication.com 60A ns1.google.com
6757	31.781877552	192.168.100.10	192.168.100.10	DNS	142	Standard query response 0xfc6 AAAA ade.googlesyndication.com 60A ns1.google.com
6986	53.431096757	192.168.100.10	192.168.100.1	DNS	74	Standard query 0xfdb5 A px.moatads.com
6987	53.431029269	192.168.100.10	192.168.100.1	DNS	74	Standard query 0x03b4 AAAA px.moatads.com
6988	53.494183169	192.168.100.1	192.168.100.10	DNS	212	Standard query response 0x03b4 AAAA px.moatads.com CNAME wildcard.moatads.com.edgekey.net CNAME e13136.g.akamaiedge.net SOA n0g.akamaihdn.com 142.250.184.2
6989	53.515931864	192.168.100.1	192.168.100.10	DNS	170	Standard query response 0xf4b5 A px.moatads.com CNAME wildcard.moatads.com.edgekey.net CNAME e13136.g.akamaiedge.net A 23.213.45.1...
7911	141.765990892	192.168.100.10	192.168.100.1	DNS	85	Standard query 0x03b4 AAAA ade.googlesyndication.com
7912	141.765990888	192.168.100.10	192.168.100.1	DNS	85	Standard query 0xc78e AAAA ade.googlesyndication.com
7915	141.783760971	192.168.100.1	192.168.100.10	DNS	101	Standard query response 0xd1b8 A ade.googlesyndication.com A 142.250.178.162
7922	141.855173945	192.168.100.1	192.168.100.10	DNS	142	Standard query response 0xc70e AAAA ade.googlesyndication.com SOA ns1.google.com

o con el filtro `udp.port == 53 and qry.name contains "marca"`



vemos todo el tráfico que interceptamos con pfsense hacia marca.com.

Configuramos el rang de ips en DHCP Server, desde la 192.168.100.100 hasta la 192.168.100.200 para conseguir la sured que hemos definido en el esquema, también configuramos un DNS secundario 1.1.1.1 y terciario 8.8.8.8 (google):

Ignore client identifiers		<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.	
Subnet	192.168.100.0	Subnet mask	255.255.255.0
Available range	192.168.100.1 - 192.168.100.254		
Range	192.168.100.100	From	192.168.100.200
Additional Pools			
Add	+ Add pool		
If additional pools of addresses are needed inside of this subnet outside of the above Range, they may be specified here.			
Pool Start	Pool End	Description	Actions
Servers			
WINS servers	WINS Server 1		
	WINS Server 2		
DNS servers	192.168.100.1		
	1.1.1.1		
	8.8.8.8		
Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.			

así tendría configurada la red LAN

Configuración de DMZ y DMZ2:

Vamos a Interfaces – Assignments y añadimos, nos saldrán OPT1 y OPT2:

192.168.100.1/interfaces_assign.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/ HackTricks

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall Services VPN Status Diagnostics Help

Assignments

WAN LAN OPT1 OPT2

Interface has been added.

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

Interface	Network port
WAN	em0 (08:00:27:0d:10:27)
LAN	em1 (08:00:27:24:4c:cc)
OPT1	em2 (08:00:27:86:26:83)
OPT2	em3 (08:00:27:26:f7:bd)

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.

192.168.100.1/interfaces.php?f=opt1

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/ HackTricks

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

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

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

Static IPv4 Configuration

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

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

The screenshot shows the pfSense web interface at <http://192.168.100.1/interfaces.php?if=opt1>. The top navigation bar includes links for Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Maltego, Tails, Metasploitable2 - Linux, 10 Minute Mail - Free ..., https://dehashed.com/, and HackT. The main menu has options for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A red banner at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title "Interfaces / DMZ (em2)" is shown. A yellow box contains the message: "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." A green "Apply Changes" button is visible. Under the "General Configuration" section, the "Enable" checkbox is checked.

Configuramos la DMZ2:

The screenshot shows the pfSense web interface at <http://192.168.100.1/interfaces.php?if=opt2>. The top navigation bar and main menu are identical to the previous screenshot. The title "Interfaces / OPT2 (em3)" is displayed. The "General Configuration" section includes fields for "Description" (set to "DMZ2"), "IPv4 Configuration Type" (set to "Static IPv4"), "IPv6 Configuration Type" (set to "None"), "MAC Address" (set to "XX:XX:XX:XX:XX:XX"), "MTU" (set to blank), "MSS" (set to blank), and "Speed and Duplex" (set to "Default (no preference, typically autoselect)"). The "Static IPv4 Configuration" section includes "IPv4 Address" (set to "192.168.250.1") and "IPv4 Upstream gateway" (set to "None"). A green "Add a new gateway" button is present. A note at the bottom of the page states: "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"."

The screenshot shows the pfSense web interface at 192.168.100.1/interfaces.php?if=opt2. The top navigation bar includes links for Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, Maltego, Tails, Metasploitable2 - Linux, 10 Minute Mail - Free ..., https://dehashed.com/, and a search bar. The main menu has options like System, Interfaces (selected), Firewall, Services, VPN, Status, Diagnostics, and Help.

In the 'Interfaces' section, the 'DMZ2' tab is selected. A warning message states: "WARNING: The 'admin' account has the same password as the root account. This is a security risk. Please change the password in the User Manager." Below this, there are tabs for WAN, LAN, DMZ, and DMZ2. A green banner at the bottom indicates: "The changes have been applied successfully."

The 'General Configuration' form for the DMZ2 interface includes fields for:

- Enable: checked
- Description: DMZ2
- IPv4 Configuration Type: Static IPv4
- IPv6 Configuration Type: None
- MAC Address: XXXXX:XXXX:XXXX

vamos a pfSense y comprobamos todas las redes configuradas:

The terminal window shows the pfSense 2.6.0 RELEASE (amd64) environment. It displays the following network interface configurations:

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

VirtualBox Virtual Machine - Netgate Device ID: d16b4b90899ec6066e97

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on UTM ***

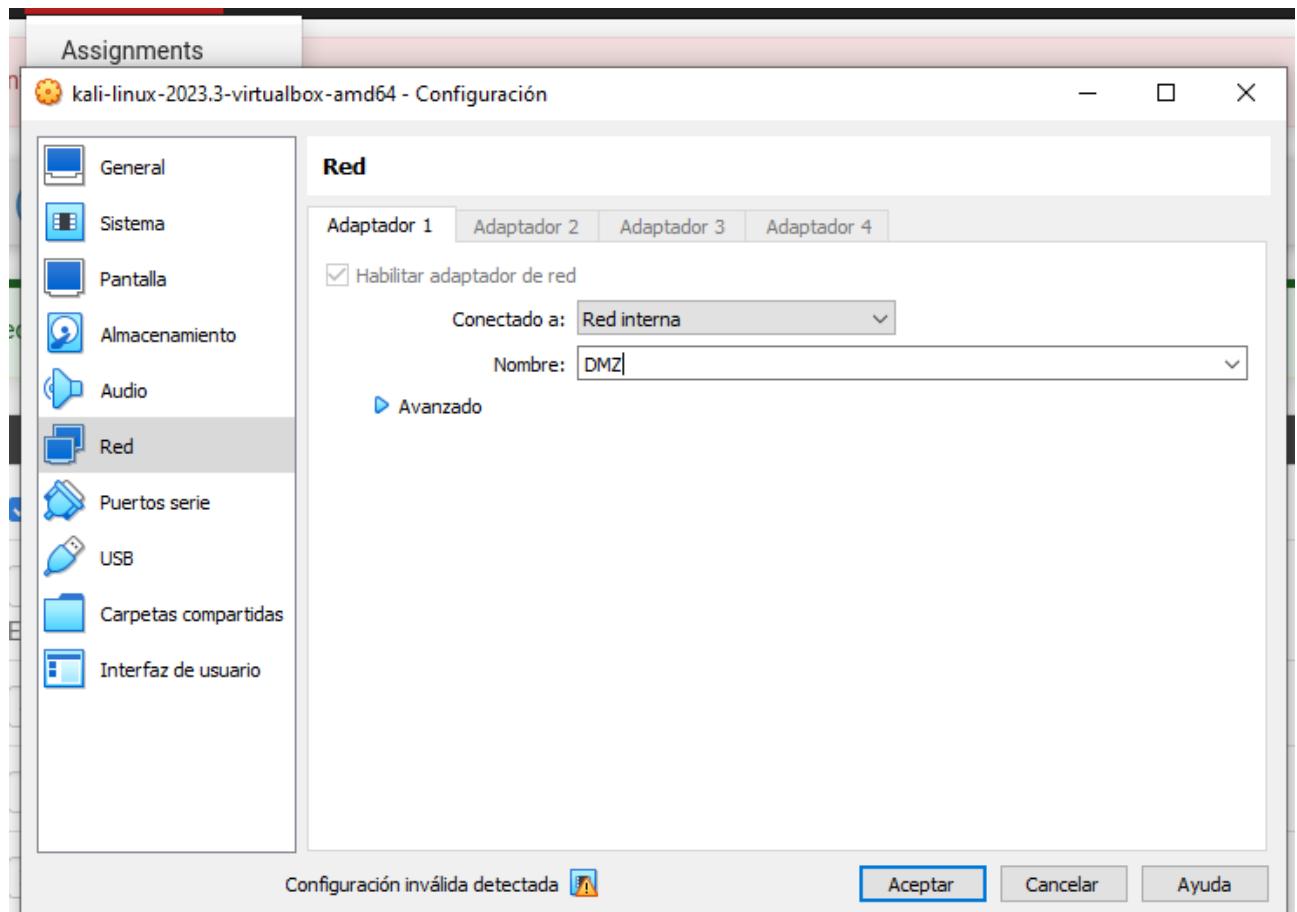
WAN (wan)      -> em0          -> v4/DHCP4: 192.168.0.18/24
LAN (lan)      -> em1          -> v4: 192.168.100.1/24
DMZ (opt1)     -> em2          -> v4: 192.168.200.1/24
DMZ2 (opt2)    -> em3          -> v4: 192.168.250.1/24
```

A command-line menu is displayed with the following options:

```
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
```

The prompt "Enter an option: " is visible at the bottom, along with a set of icons for file operations (copy, paste, etc.) and a "CTRL DERECHA" key indicator.

vamos a la kali y cambiamos la red LAN a DMZ



desconectamos el adaptador de red de la kali, lo volvemos a conectar y comprobamos en cmd, que ha cambiado la ip:

```
(kali㉿kali)-[~]
$ ip a
Key Algorithm HMAC-SHA256 (current bind9 default)
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:cb:7e:f5 brd ff:ff:ff:ff:ff:ff
        inet 192.168.200.100/24 brd 192.168.200.255 scope global dynamic noprefixroute eth0
            valid_lft 7101sec preferred_lft 7101sec
        inet6 fe80::cdf2:29d0:7fca:5c9c/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 02:42:05:32:65:47 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
Domain name: Domain search list: The DHCP Server can dynamically provide domain names to clients.
Domain search list: The DHCP Server can dynamically provide domain names to clients.

(kali㉿kali)-[~]
```

Para configurar las reglas, primero configuramos alias y puertos para el firewall

Properties

Name	webs	The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	PuertosWebs	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	Delete
	443	HTTPS	Delete

Save + Add Port

Creamos la reglas

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	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	TCP	Choose which IP protocol this rule should match.

Source

Source	<input type="checkbox"/> Invert match	any	Source Address	/
--------	---------------------------------------	-----	----------------	---

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

Destination

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)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	*	webs	*	none		salida trafico web	Edit Delete Save + Separator

Add Add Delete Save + Separator

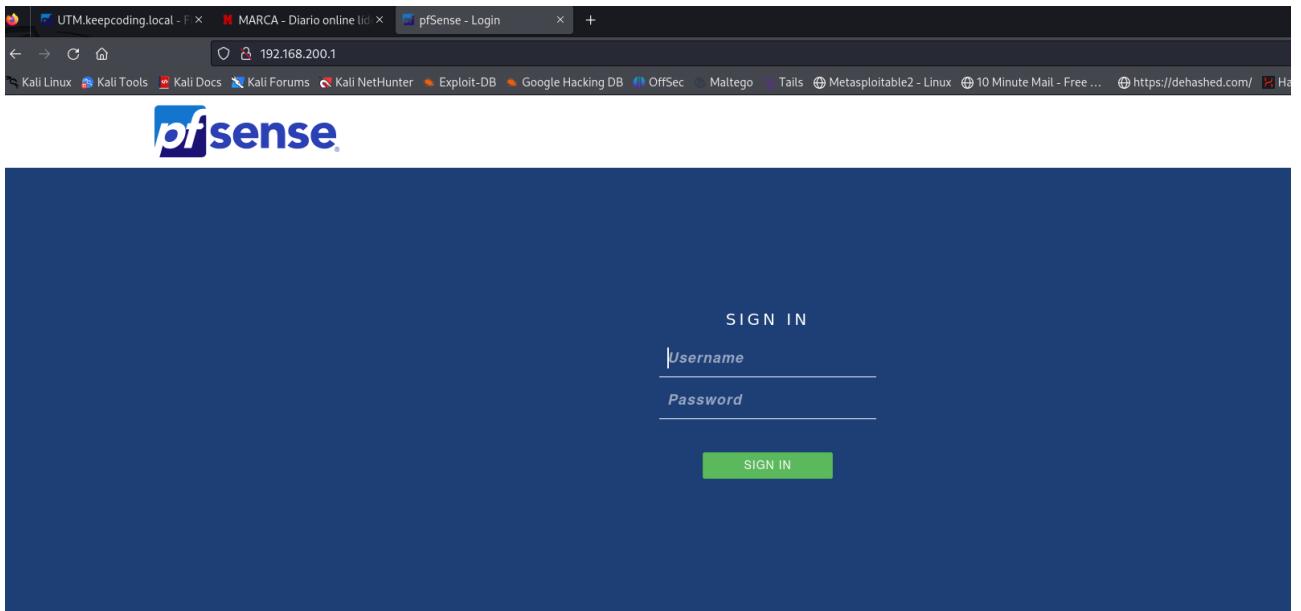
The screenshot shows the 'Edit Firewall Rule' page. The 'Action' dropdown is set to 'Pass'. Under 'Disabled', there is a checkbox for 'Disable this rule'. The 'Interface' is set to 'DMZ'. 'Address Family' is 'IPv4' and 'Protocol' is 'UDP'. The 'Source' section shows 'any' selected under 'Source' with an 'Invert match' checkbox. The 'Destination' section shows 'any' selected under 'Destination' with an 'Invert match' checkbox. Under 'Destination Port Range', 'From' is 'DNS (53)' and 'To' is 'DNS (53)', both set to 'Custom'.

The screenshot shows the 'Firewall / Rules / DMZ' page. 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 is a table of rules:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none		permítir tráfico DNS	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	*	*	*	webs	*	none		salida tráfico web	

At the bottom are buttons for 'Add', 'Save', and 'Separator'.

cambiamos a LAN en la kali, y comprobamos que tenemos acceso a internet:



comprobamos las reglas configuradas:

A screenshot of the pfSense firewall rules configuration interface. The title bar shows the URL 192.168.200.1/firewall_rules.php?if=opt2. The main area displays a table of rules under the "DMZ2" tab. The table has columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are three rules listed: one for ICMP (any to any), one for UDP (any to 53 DNS), and one for TCP (any to webs). A message at the top indicates that changes have been applied successfully and the firewall is reloading. A status bar at the bottom shows "Monitor the filter reload progress.".

mapeamos una IP estática:

The screenshot shows the pfSense web interface under 'Services / DHCP Server / LAN / Edit Static Mapping'. The form is titled 'Static DHCP Mapping on LAN'. It contains the following fields:

- MAC Address:** 08:00:27:cb:7e:f5
- Client Identifier:** (empty)
- IP Address:** 192.168.100.99
- Hostname:** kali
- Description:** Establecimiento estático de IP
- ARP Table Static Entry:** Create an ARP Table Static Entry for this MAC & IP Address pair.
- WINS Servers:** WINS 1 (selected), WINS 2 (disabled)
- DNS Servers:** DNS 1 (selected), DNS 2 (disabled), DNS 3 (disabled), DNS 4 (disabled)

comprobamos el cambio de ip

```
vista_tic@vista_tic-VirtualBox:~$ ifconfig
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cb:7e:f5 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 7196sec preferred_lft 7196sec
      inet6 fe80::cdf2:29d0:7fca:5c9c/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 02:42:05:32:65:47 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
Subnet          192.168.100.0
Subnet mask     255.255.255.0
vista_tic@vista_tic-VirtualBox:~$
```

levantamos el servidor APACHE:

```
(kali㉿kali)-[~]
$ service apache2 start
Failed to start apache2.service: Connection timed out
See system logs and 'systemctl status apache2.service' for details.

(kali㉿kali)-[~]
$ sudo service apache2 start
[sudo] password for kali:

(kali㉿kali)-[~]
$
```

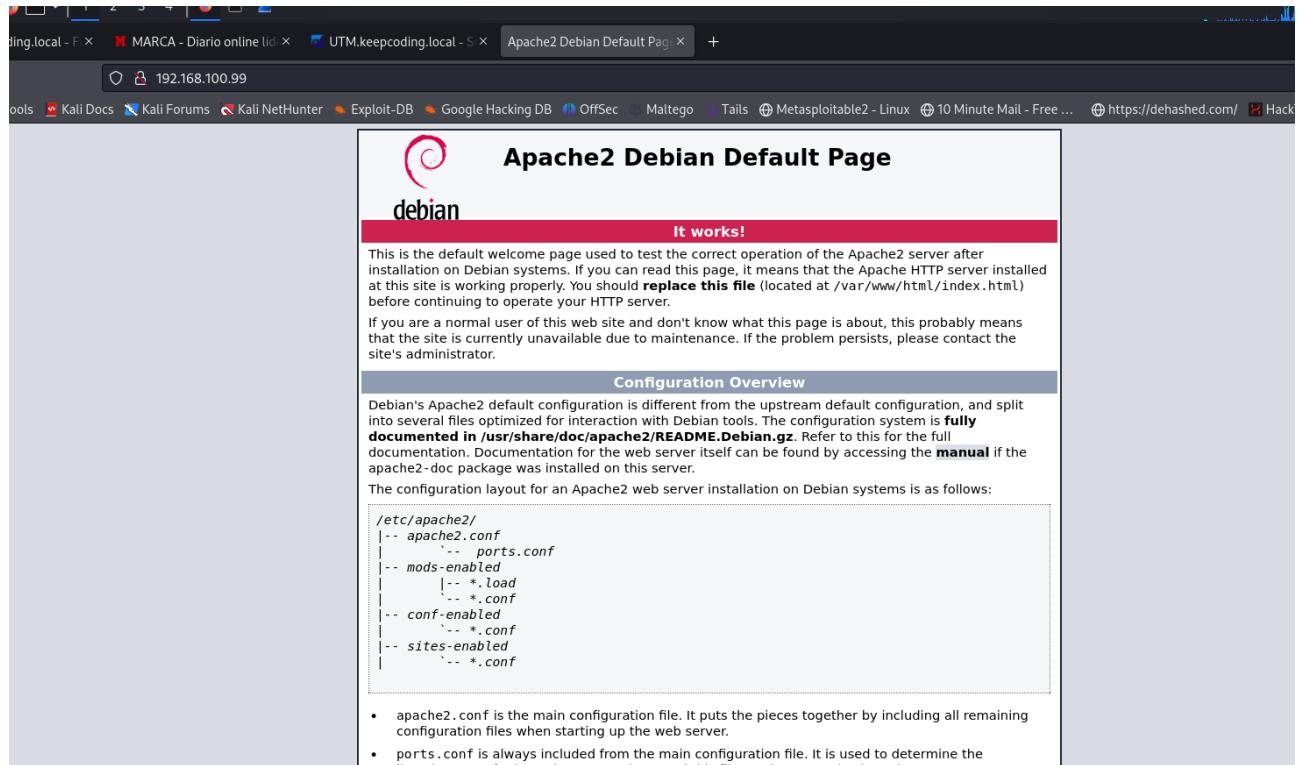
y comprobamos que está levantado el servidor:

```
(kali㉿kali)-[~]
$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sat 2024-03-16 09:49:14 EDT; 1min 17s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Process: 99091 ExecStart=/usr/sbin/apache2 start (code=exited, status=0/SUCCESS)
 Main PID: 99107 (apache2)
   Tasks: 6 (limit: 13937)
  Memory: 19.7M (peak: 20.2M)
    CPU: 70ms
   CGroup: /system.slice/apache2.service
           ├─99107 /usr/sbin/apache2 -k start
           ├─99110 /usr/sbin/apache2 -k start
           ├─99111 /usr/sbin/apache2 -k start
           ├─99112 /usr/sbin/apache2 -k start
           ├─99113 /usr/sbin/apache2 -k start
           └─99114 /usr/sbin/apache2 -k start

Mar 16 09:49:14 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Mar 16 09:49:14 kali apache2[99106]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1. Set the 'ServerName' directive globally to suppress this message
Mar 16 09:49:14 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

(kali㉿kali)-[~]
```

y comprobamos que se levanta en la ip 192.168.100.99



Crearemos una regla para que todo el tráfico que nos llegue a nuestro puerto 80, es decir la red WAN, nos redirija a nuestra red LAN:

192.168.200.1/firewall_nat_edit.php?after=-1

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/ H

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled	<input type="checkbox"/> Disable this rule			
No RDR (NOT)	<input type="checkbox"/> Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.			
Interface	WAN			
Choose which interface this rule applies to. In most cases "WAN" is specified.				
Address Family	IPv4			
Select the Internet Protocol version this rule applies to.				
Protocol	TCP			
Choose which protocol this rule should match. In most cases "TCP" is specified.				
Source	Display Advanced			
Destination	<input type="checkbox"/> Invert match.	WAN address	Type	Address/mask
Destination port range	Other	80	Other	80
From port Custom To port Custom				
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.				
Redirect target IP	Single host	192.168.100.99		
Type		Address		
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::*) to local scope (::1)				
Redirect target port	Other	80	Custom	
Port				

192.168.200.1/firewall_nat.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Maltego Tails Metasploitable2 - Linux 10 Minute Mail - Free ... https://dehashed.com/ H

disense COMMUNITY EDITION

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

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / NAT / Port Forward

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

Port Forward 1:1 Outbound NPt

Rules	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.100.99	80 (HTTP)	Regla apache server	Edit Delete

Legend

- ▶ Pass
- ☒ Linked rule

Add **Save** **Separator**

ahora sí accedemos desde nuestra máquina a la ip del servidor apache

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should [replace this file](#) (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   '-- *.Load
|   '-- *.conf
|-- conf-enabled
|   '-- *.conf
|-- sites-enabled
|   '-- *.conf

```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite` and `a2dissite`.

Creamos ahora la VPN, nos vamos a System / Package Manager / Available Packages

Name	Version	Description	Action
acme	0.7.5	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.	+ Install

instalamos el openvpn-client-export

Name	Version	Description	Action
Open-VM-Tools	10.1.0_5.1	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.	+ Install
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.	+ Install
pfBlockerNG	3.2.0_6	Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. GeoIP database by MaxMind Inc. (GeoLite2 Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced Integration for Proofpoint ET IORisk IP Reputation Threat Sources.	+ Install

me da error al intentar instalar la vpn

The screenshot shows a browser window with the URL `192.168.200.1/pkg_mgr_install.php`. The page is titled "System / Package Manager / Package Installer". A red error message box states: "pfSense-pkg-openvpn-client-export installation failed!". Below the message, there are tabs for "Installed Packages", "Available Packages", and "Package Installer", with "Package Installer" being the active tab. A warning message in a blue box says: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." At the bottom of the page, another warning message in a blue box says: "WARNING: Current pkg repository has a new PHP major version. pfSense should be upgraded before installing any new package." The pfSense logo is visible at the top of the page.

Lanzamos en nuestra kali el honeypot Cowrie con el comando:

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

The screenshot shows a terminal window on a Kali Linux desktop. The title bar says "kali-linux-2023.3-virtualbox-amd64 [Corriendo] - Oracle VM VirtualBox". The terminal prompt is "(kali㉿kali)-[~]" and the command entered is "\$ docker run -p 2222:2222 cowrie/cowrie". The output of the command is displayed in the terminal, showing logs from the Cowrie honeypot. The logs include messages about twisted and cryptography deprecation warnings, Python version information, and the start of the Cowrie SSH factory on port 2222. A warning message at the bottom of the terminal window says: "WARNING: Current pkg repository has a new PHP major version. pfSense should be upgraded before installing any new package." The terminal window has a dark theme with a light-colored scroll bar.

se quedará listo para aceptar conexiones.

Con el siguiente comando corremos el amazedostrich:

```
docker run -p 333:3389 amazedostrich/rdpy
```

Hago un docker ps para ver las imágenes docker en ejecución:

```
(kali㉿kali)-[~]
└─$ docker ps
CONTAINER ID   IMAGE           COMMAND                  CREATED        STATUS          PORTS
d1fab0c055ad   amazedostrich/rdpy   "/bin/sh -c '/usr/bi..."  14 minutes ago   Up 14 minutes   0.0.0.0:333→3389/tcp
, ::333→3389/tcp
crazy_vaughan
9b9cb5e1f707   cowrie/cowrie      "/cowrie/cowrie-env/..."  41 minutes ago   Up 41 minutes   0.0.0.0:2222→2222/tcp
p, ::2222→2222/tcp, 2223/tcp
eager_elgamal

(kali㉿kali)-[~]
└─$
```

con este comando nos abrirá una terminal dentro del docker:

```
(kali㉿kali)-[~]
└─$ docker ps
CONTAINER ID   IMAGE           COMMAND                  CREATED
 NAMES
d1fab0c055ad   amazedostrich/rdpy   "/bin/sh -c '/usr/bi..."  21 minutes ago
crazy_vaughan
9b9cb5e1f707   cowrie/cowrie      "/cowrie/cowrie-env/..."  49 minutes ago
eager_elgamal

(kali㉿kali)-[~]
└─$ docker exec -it -u 0 d1fab0c055ad /bin/bash
bash-4.4#
```

con este comando iremos a los logs del honeypot

```
bash-4.4# ls
bin  dev  etc  home  lib  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
bash-4.4# cd rdp
bash: cd: rdp: No such file or directory
bash-4.4# cd /var/log
bash-4.4# ls
rdpy
bash-4.4# cd rdp
bash-4.4# ls
rdpy.log
bash-4.4#
```

con el comando tail -f rdp.log vemos los logs del honeypot

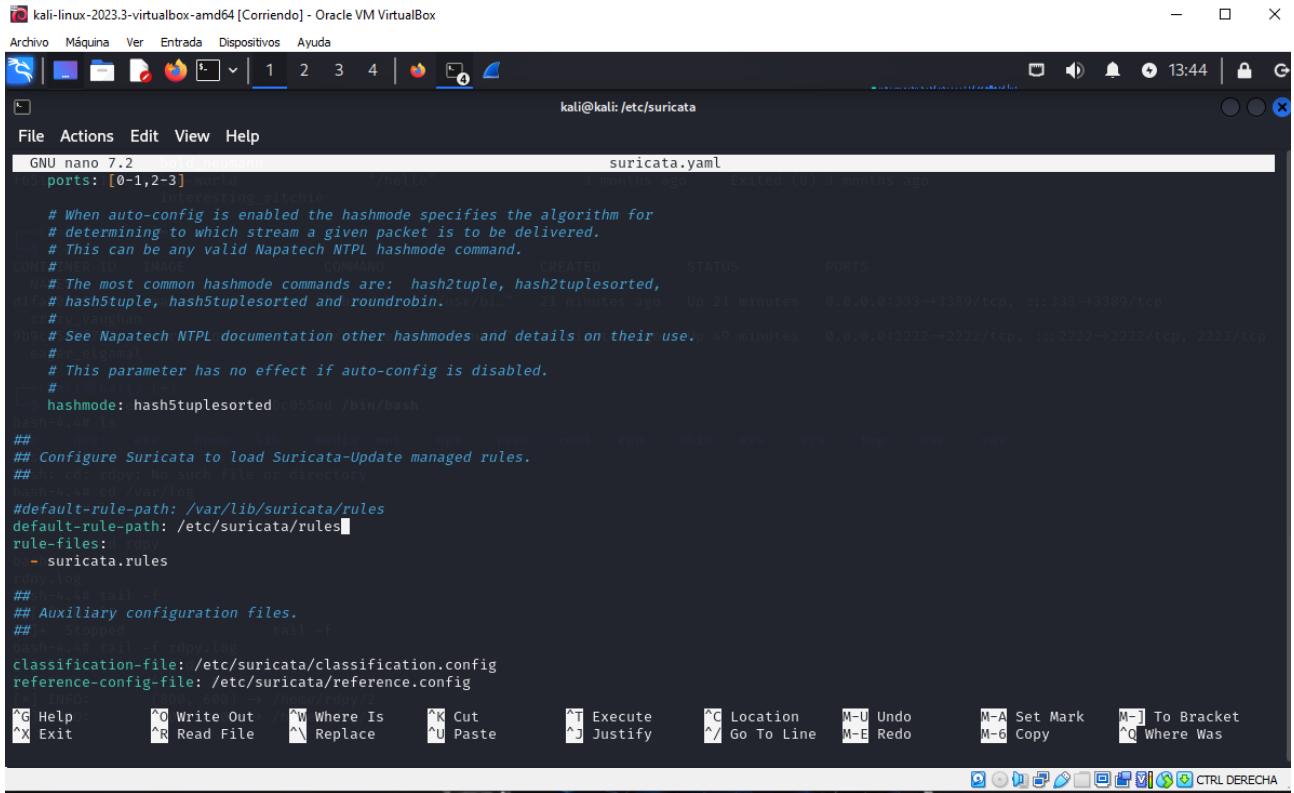
```
[1]: stopped          tail -f
bash-4.4# tail -f rdp.log
[*] INFO:      Build size map
[*] INFO:      (1024, 800) → /home/rdpy/1
[*] INFO:      (800, 600) → /home/rdpy/2
[*] INFO:      (800, 600) → /home/rdpy/3
[1]
```

Reglas de SURICATA:

```
(kali㉿kali)-[~]
$ cd /etc/suricata
/home lib media net opt proc root run skin srv sys tmp user var
drwxr-xr-x 2 root root 4096 Mar 12 14:28 suricata
(kali㉿kali)-[/etc/suricata] directory
$ ls -l
classification.config reference.config rules suricata.yaml threshold.config
drwxr-xr-x 2 root root 4096 Mar 12 14:28 rules
(kali㉿kali)-[/etc/suricata]
$ cd rules
drwxr-xr-x 2 root root 4096 Mar 12 14:28 rules
(kali㉿kali)-[/etc/suricata/rules]
$ ls -lH
app-layer-events.rules dns-events.rules http-events.rules mqtt-events.rules rfb-events.rules stream-events.rules
decoder-events.rules files.rules ipsec-events.rules nfs-events.rules smb-events.rules tls-events.rules
dhcp-events.rules ftp-events.rules kerberos-events.rules ntp-events.rules smtp-events.rules
dnp3-events.rules http2-events.rules modbus-events.rules quic-events.rules ssh-events.rules
drwxr-xr-x 2 root root 4096 Mar 12 14:28 rules
└── INFO[1]: (800, 600) → /home/kali/copy/2
(kali㉿kali)-[/etc/suricata/rules] copy/2
$
```

Creamos la regla para suricata

en el archivo suricata.yaml, cambiamos lo siguiente:



```
GNU nano 7.2                               suricata.yaml
---[REDACTED]--- 3 months ago   Exited (0) 3 months ago
ports: [0-1,2-3]                                /hello"      3 months ago
# When auto-config is enabled the hashmode specifies the algorithm for
# determining to which stream a given packet is to be delivered.
# This can be any valid Napatech NTPL hashmode command.
CONTAINER_ID IMAGE          COMMAND      CREATED     STATUS      PORTS
# The most common hashmode commands are: hash2tuple, hash2tuplesorted,
# hash5tuple, hash5tuplesorted and roundrobin. $ ./01... 21 minutes ago   Up 21 minutes  0.0.0.0:333→3389/tcp, :::333→3389/tcp
# See Napatech NTPL documentation other hashmodes and details on their use. 49 minutes   0.0.0.0:2222→2222/tcp, :::2222→2222/tcp, 2223/tcp
# This parameter has no effect if auto-config is disabled.
# hashmode: hash2tuple
hashmode: hash5tuplesorted@0555ad /bin/bash
hash-0:# ls
## /etc/suricata/  home  lib  media  opt  proc  root  run sbin  sys  tmp  usr  var
## Configure Suricata to load Suricata-Update managed rules.
## cat rdp.log
## tail -f rdp.log
## Auxiliary configuration files.
## Stopped tail -f rdp.log
classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
INFO: (800, 600) → /home/rdpy/2
^G Help      ^O Write Out    ^W Where Is    ^X Cut        ^T Execute      ^C Location    M-U Undo      M-A Set Mark    M-] To Bracket
^X Exit      ^R Read File    ^A Replace     ^U Paste       ^J Justify      ^Y Go To Line   M-E Redo      M-6 Copy      ^Q Where Was

```

para que nos coja por defecto el archivo suricata.rules que hemos creado

ejecutamos Suricata:



```
bash-4.4# tail -f rdp.log
[(kali㉿kali)-[/etc/suricata]]
$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
i: threads: Threads created → W: 2 / FM: y13 FR: 1   Engine started.
```

vemos los logs:

```

kali@kali:~/var/log/suricata
File Actions Edit View Help
(kali㉿kali)-[~/var/log/suricata] ~
$ tail -f fast.log
^Z
zsh: suspended tail -f fast.log
zsh: suspended tail -f fast.log
(kali㉿kali)-[~/var/log/suricata] ~
$ tail -f fast.log
^Z
zsh: suspended tail -f fast.log
zsh: suspended tail -f fast.log
(kali㉿kali)-[~/var/log/suricata] ~
$ tail -f fast.log
03/16/2024-13:57:47.618458 [**] [1:1:0] Trafico detectado [**] [Classification: (null)] [Priority: 1] {TCP} 192.168.0.16:33092 → 34.107.221.82:8
0
03/16/2024-13:57:47.622124 [**] [1:1:0] Trafico detectado [**] [Classification: (null)] [Priority: 1] {TCP} 192.168.0.16:53332 → 34.107.243.93:4
43
03/16/2024-13:57:47.630315 [**] [1:1:0] Trafico detectado [**] [Classification: (null)] [Priority: 1] {TCP} 34.107.221.82:80 → 192.168.0.16:330
2
03/16/2024-13:57:47.637423 [**] [1:1:0] Trafico detectado [**] [Classification: (null)] [Priority: 1] {TCP} 34.107.243.93:443 → 192.168.0.16:533
32
03/16/2024-13:57:47.714429 [**] [1:1:0] Trafico detectado [**] [Classification: (null)] [Priority: 1] {TCP} 192.168.0.16:53342 → 34.107.243.93:4
43
03/16/2024-13:57:47.729483 [**] [1:1:0] Trafico detectado [**] [Classification: (null)] [Priority: 1] {TCP} 34.107.243.93:443 → 192.168.0.16:533
42
2024-03-16T16:06:37+0000 [twisted.scripts._twistd_unix.UnixAppLogger.info]: twistd 23.10.0 (/cowrie/cowrie-env/bin/python3 3.11.2) starting up.
2024-03-16T16:06:37+0000 [twisted.scripts._twistd_unix.UnixAppLogger.info]: reactor class: twisted.internet.epollreactor.EPollReactor.
2024-03-16T16:06:37+0000 [cowrie.ssh.factory.CowrieSSHFactory] Starting factory <cowrie.ssh.factory.CowrieSSHFactory object at 0x7fc700b0c350>
2024-03-16T16:06:37+0000 [...] Generating new RSA keypair...
2024-03-16T16:06:37+0000 [-] Generating new ECDSA keypair...
2024-03-16T16:06:37+0000 [-] Generating new ed25519 keypair...

```

se me peta windows 11 y no puedo hacer nada con él

ELASTIC CLOUD

Deployment	Status	Version	Cloud provider & region	Actions
Mik	Healthy	8.12.2	GCP - Iowa (us-central1)	Open Manage

vamos a Management – Integrations

Screenshot of the Elastic Home page (<https://77229e0d983f4c70acd0169abcc47226.us-central1.gcp.cloud.es.io:9243/app/home#/>)

The left sidebar shows navigation categories: Home, User Experience, Universal Profiling, Security (selected), Dashboards, Rules, Alerts, Findings, Cases, Timelines, Intelligence, Explore, Manage, Management (selected), Dev Tools, Integrations (circled in red), Fleet, Osquery, Stack Monitoring, Stack Management, and a prominent blue "Add integrations" button.

The main content area features a "Welcome home" header and four cards: Search, Observability, Security, and Analytics. Below this is a section titled "Get started by adding integrations" with buttons for "Setup guides", "Add integrations" (highlighted in blue), "Try sample data", and "Upload a file".

The "Management" section includes links for "Manage permissions", "Monitor the stack", "Back up and restore", and "Manage index lifecycles".

y luego a Elastic Defend

Screenshot of the Integrations browser (<https://77229e0d983f4c70acd0169abcc47226.us-central1.gcp.cloud.es.io:9243/app/integrations/browse>)

The left sidebar shows "Integrations" selected and "Browse integrations" highlighted. The main content area displays a grid of integration cards. A red circle highlights the "Elastic Defend" card, which is described as "Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility." To the right of the card is a "Select Elastic Defend" panel with a "Continue" button. Other visible cards include APM, 1Password, AbuseCH, and ActiveMQ.

Elastic Defend

Version 8.12.0 | Agent policies 0 | Add Elastic Defend

Elastic Defend Integration

Elastic Defend provides organizations with prevention, detection, and response capabilities with deep visibility for EPP, EDR, SIEM, and Security Analytics use cases across Windows, macOS, and Linux operating systems running on both traditional endpoints and public cloud environments. Use Elastic Defend to:

- Prevent complex attacks - Prevent malware (Windows, macOS, Linux) and ransomware (Windows) from executing, and stop advanced threats with malicious behavior (Windows, macOS, Linux), memory threat (Windows, macOS, Linux), and credential hardening (Windows) protections. All powered by [Elastic Labs](#) and our global community.
- Alert in high fidelity - Bolster team efficacy by detecting threats centrally and minimizing false positives via extensive corroboration.
- Detect threats in high fidelity - Elastic Defend facilitates deep visibility by instrumenting the process, file, and network data in your environments with minimal data collection overhead.
- Triage and respond rapidly - Quickly analyze detailed data from across your hosts. Examine host-based activity with interactive visualizations. Invoke remote response actions across distributed endpoints. Extend investigation capabilities even further with the Osquery integration, fully integrated into Elastic Security workflows.
- Secure your cloud workloads - Stop threats targeting cloud workloads and cloud-native

Requirements

Permissions root privileges

Details

Version	8.12.0
Category	EDR/XDR, Security
Elasticsearch assets	Index templates 2 Transforms 2 Ingest pipelines 1 5
Features	logs, metrics
Subscription	basic
Developed by	Elastic
License	LICENSE.txt
Changelog	View Changelog

instalamos el agente en la kali, copiando el script:

Set up Elastic Defend integration

Install Elastic Agent Add the integration Confirm incoming data

These steps configure and enroll the Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent. As an alternative to Fleet, advanced users can run agents in [standalone mode](#).

1 Install Elastic Agent on your host

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](#).

Linux Tar Mac Windows RPM DEB Kubernetes

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.12.2-linux-x86_64.tar.gz
cd elastic-agent-8.12.2-linux-x86_64
sudo ./elastic-agent install --url=https://f4454082062a4600b181747ba704bef4.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=UTg4ZUdvNEJD...
```

2 Confirm agent enrollment

```
(kali㉿kali)[~]
$ curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.12.2-linux-x86_64.tar.gz
cd elastic-agent-8.12.2-linux-x86_64
sudo ./elastic-agent install --url=https://f4454082062a4600b181747ba704bef4.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=UTg4ZUdvNEJD...
```

```

kali@kali: ~ - Wireshark - Analyze - Statistics - Telephony - Wireless - Tools - Help
File Actions Edit View Analyze Statistics Telephony Wireless Tools Help
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/tomcat.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/traefik.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/uwsgi.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/vsphere.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/windows.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/zeek.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/zookeeper.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/zoom.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/modules.d/zscaler.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/monitors.d/
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/monitors.d/sample.http.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/monitors.d/sample.icmp.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/monitors.d/sample.tcp.yml.disabled
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquery-extension.ext
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat.reference.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osqueryd
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat.reference.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-collector
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-collector.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-symbolizer
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-symbolizer.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-host-agent
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-host-agent.spec.yml
elastic-agent-8.12.2-linux-x86_64/.elastic-agent.active.commit
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]:
```

instalado el agente:

```

kali@kali: ~/elastic-agent-8.12.2-linux-x86_64 - Wireshark - Analyze - Statistics - Telephony - Wireless - Tools - Help
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat.reference.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osquerybeat.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/osqueryd
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat.reference.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/packetbeat.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-collector
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-collector.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-symbolizer
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-elastic-symbolizer.spec.yml
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-host-agent
elastic-agent-8.12.2-linux-x86_64/data/elastic-agent-de80b0/components/pf-host-agent.spec.yml
elastic-agent-8.12.2-linux-x86_64/.elastic-agent.active.commit
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 [34s] Elastic Agent successfully installed, starting enrollment.
[ =] Waiting For Enroll... [35s] {"log.level": "info", "@timestamp": "2024-03-17T07:52:22.521-0400", "log.origin": {"file.name": "cmd/enroll_cmd.go", "file.line": 496}, "message": "Starting enrollment to URL: https://f44540820624600b181747ba70abef4.fleet.us-central1.gcp.cloud.es.io:443/", "ecs.version": "1.6.0"}
[ =] Waiting For Enroll... [37s] {"log.level": "info", "@timestamp": "2024-03-17T07:52:25.065-0400", "log.origin": {"file.name": "cmd/enroll_cmd.go", "file.line": 461}, "message": "Restarting agent daemon, attempt 0", "ecs.version": "1.6.0"}
{"log.level": "info", "@timestamp": "2024-03-17T07:52:25.067-0400", "log.origin": {"file.name": "cmd/enroll_cmd.go", "file.line": 285}, "message": "Successfully triggered restart on running Elastic Agent.", "ecs.version": "1.6.0"}
Successfully enrolled the Elastic Agent.
[ =] Done [37s] User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Elastic Agent has been successfully installed.
```

damos en Add the itegration

These steps configure and enroll the Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent. As an alternative to Fleet, advanced users can run agents in [standalone mode](#).

✓ Install Elastic Agent on your host

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 arch64, 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](#).

[Linux Tar](#) [Mac](#) [Windows](#) [RPM](#) [DEB](#) [Kubernetes](#)

```
curl -L -o https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.12.2-linux-x86_64.tar.gz  
tar xzvf elastic-agent-8.12.2-linux-x86_64.tar.gz  
cd elastic-agent-8.12.2-linux-x86_64  
sudo ./elastic-agent install --url=https://f4454082062a4600b181747ba704bef4.fleet.us-cent
```

 Copied

✓ Agent enrollment confirmed

✓ 1 agent has been enrolled.

Set up Elastic Defend integration

Install Elastic Agent

Add the integration

Confirm incoming data

We'll save your integration with our recommended defaults.



✓ Windows, macOS, and Linux event collection

You can edit these settings later in the Elastic Defend integration policy. [Learn more](#)

Go back

Confirm incoming data

aquí vemos los logs que vienen de kali:

The screenshot shows the 'Set up Elastic Defend integration' page. It has three steps: 'Install Elastic Agent', 'Add the integration', and 'Confirm incoming data'. The third step is completed, indicated by a green checkmark and the message 'Incoming data received from 1 enrolled agent.' Below this, there is a preview of incoming data from a Kali Linux agent. The logs show the agent starting up and upgrading its watcher process. At the bottom right of the preview area are two buttons: 'Add another integration' and 'View assets'.

```
Mar 17, 2024 @ 12:52:27.183 container.id: "elastic-agent-de80b0" agent.name: "kali" agent.type: "filebeat" agent.version: "8.12.2" log.file.inode: "3066218" log.file.path: "/opt/Elastic-Agent/data/elastic-agent-de80b0/logs/elastic-agent-watcher-20240317.ndjson" log.file.device_id: "2049" log.offset: 0 elastic_agent.version: "8.12.2" elastic_agent.snapshot: false process.pid: 7347 message: "Upgrade Watcher started" input.type: "filestream" log.origin.file.line: 67 log.origin.file.name: "cmd/watch.go" ecs.version: "8.0.0" data_stream.type: "logs" data_stream.dataset: "elastic.agent" Mar 17, 2024 @ 12:52:22.029 container.id: "elastic-agent-de80b0" agent.name: "kali" agent.type: "filebeat" agent.version: "8.12.2" log.file.inode: "3066198" log.file.path: "/opt/Elastic-Agent/data/elastic-agent-de80b0/logs/elastic-agent-watcher-20240317.ndjson" log.file.device_id: "2049" log.offset: 0 log.source: "elastic-agent" elastic_agent.version: "8.12.2" elastic_agent.snapshot: false process.pid: 7166 message: "Elastic Agent started" input.type: "filestream" log.origin.file.line: 157 log.origin.file.name: "cmd/run.go" ecs.version: "8.0.0" data_stream.type: "log" Mar 17, 2024 @ 12:52:27.183 container.id: "elastic-agent-de80b0" agent.name: "kali" agent.type: "filebeat" agent.version: "8.12.2" log.file.inode: "3066218" log.file.path: "/opt/Elastic-Agent/data/elastic-agent-de80b0/logs/elastic-agent-watcher-20240317.ndjson" log.file.device_id: "2049" log.offset: 220 elastic_agent.version: "8.12.2" elastic_agent.snapshot: false message: "update marker not present at '/opt/Elastic-Agent/data'" input.type: "filestream" log.origin.file.line: 75
```

damos click a ver assets (ver activos)

nos vamos a Fleet para ver las políticas, que son las reglas para recoger los logs:

The screenshot shows the 'Fleet' management interface. It displays a list of agents, with two currently visible: 'kali' and '57d606d90412'. Both agents are marked as 'Healthy'. The 'Status' column shows the number of healthy, unhealthy, updating, and offline agents. There are buttons for 'Agent activity', 'Add Fleet Server', and 'Add agent'. A search bar at the top allows filtering by KQL syntax. The bottom of the screen shows pagination controls.

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	kali	My first agent policy rev. 2	0.27 %	26 MB	17 seconds ago	8.12.2	...
Healthy	57d606d90412	Elastic Cloud agent policy rev. 5	N/A	N/A	24 seconds ago	8.12.2	...

podemos integrar Suricata para recoger los logs de Suricata.

The screenshot shows the 'Suricata' integration page in the Elastic Stack interface. At the top, there's a navigation bar with the Elastic logo, a search bar, and links for 'Live Chat' and 'Setup guide: step'. Below the navigation is a breadcrumb trail: 'Integrations > Suricata'. The main content area has a title 'Suricata' with a logo, a version '2.21.0' indicator, and a 'Add Suricata' button. A 'Suricata Integration' section contains tabs for 'Overview', 'Settings', 'Configs', and 'API reference'. The 'Overview' tab is selected, showing a brief description of the integration for Suricata, its compatibility with v4.0.4, and an example event JSON. To the right, there are 'Screenshots' and 'Details' sections.

This screenshot shows the 'Add Suricata integration' configuration dialog. It includes a 'Cancel' button, a title 'Add Suricata integration', and a 'Configure an integration for the selected agent policy' message. It lists two agent policies: 'Agent policy' and 'Agent policy 2'. A 'Configure integration' step is shown with a sub-dialog titled 'Suricata integration added'. This sub-dialog instructs the user to add an Elastic Agent to their hosts. It features a 'Collect Suricata eve logs (input: logfile)' checkbox (which is checked), a 'Paths' field containing '/var/log/suricata/eve.json', and a 'Preserve original event' option. Buttons for 'Add Elastic Agent later' and 'Add Elastic Agent to your hosts' are present. The background of the main dialog shows the configuration options for the integration.

The screenshot shows the 'Suricata' integration management page. At the top, it displays the integration name, version '2.21.0', agent policies (2), and a 'Add Suricata' button. Below this is a table with columns: Integration policy, Version, Agent policy, Last updated by, Last updated, Agents, and Actions. One row is visible for 'suricata-1' with version 'v2.21.0', agent policy 'Agent policy...', last updated '3 hours ago', and an 'Add agent' button. Navigation controls for rows per page (20) and pages (1) are at the bottom.

Aquí vemos la integración que tiene nuestra máquina kali con suricata, para poder tener logs de suricata.

En discover vemos los logs, pero no veo los de suricata ni los de windows 11 :(

podemos crear los conjuntos de datos que queremos ver

The screenshot shows the 'Create data view' interface in the Elasticsearch UI. On the left, a sidebar lists various fields like @timestamp, agent.build.original, and client.ip. The main area displays a histogram of hits over time, with a count of 23,847 hits. The 'Index pattern' field contains 'example-*'. The 'Timestamp field' dropdown is set to '@timestamp'. The right side shows a list of available index patterns, all labeled as 'Data stream'. A message at the top states, 'Your index pattern can match 15 sources.' Buttons at the bottom include 'Close', 'Use without saving', and 'Save data view to Kibana'.

This screenshot shows the same 'Create data view' interface but with an error. The 'Index pattern' field now contains 'logs-suricata-*'. An error message at the top right says, 'The index pattern you entered doesn't match any data streams, indices, or index aliases. You can match 17 sources.' The 'Matching sources' tab is selected, listing 17 different data streams and indices. The rest of the interface is identical to the first screenshot.

FIN DE PRÁCTICA