



Trabajo BlueTeam

De

Daniel Shved

OBJETIVOS:

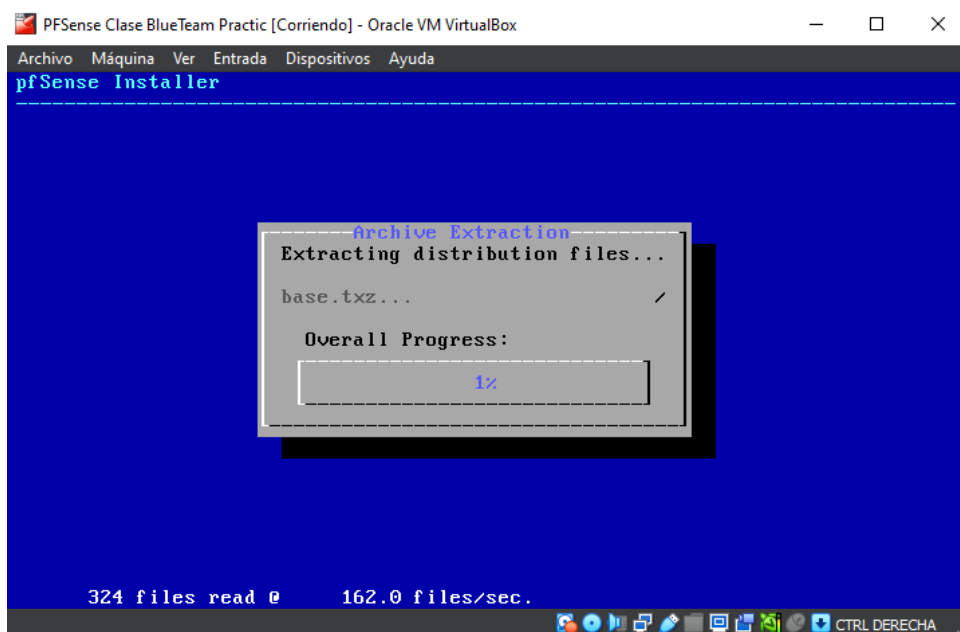
Montar una red de con wan, lan y dmz. En lan poner un Windows 10 con el cliente de elk y openvpn. En dmz poner el servidor de elk y openvpn. Entre ambos esta la dicha vpn. Lan y Dmz cuelgan del utm pfsense.

HERRAMIENTAS USADAS:

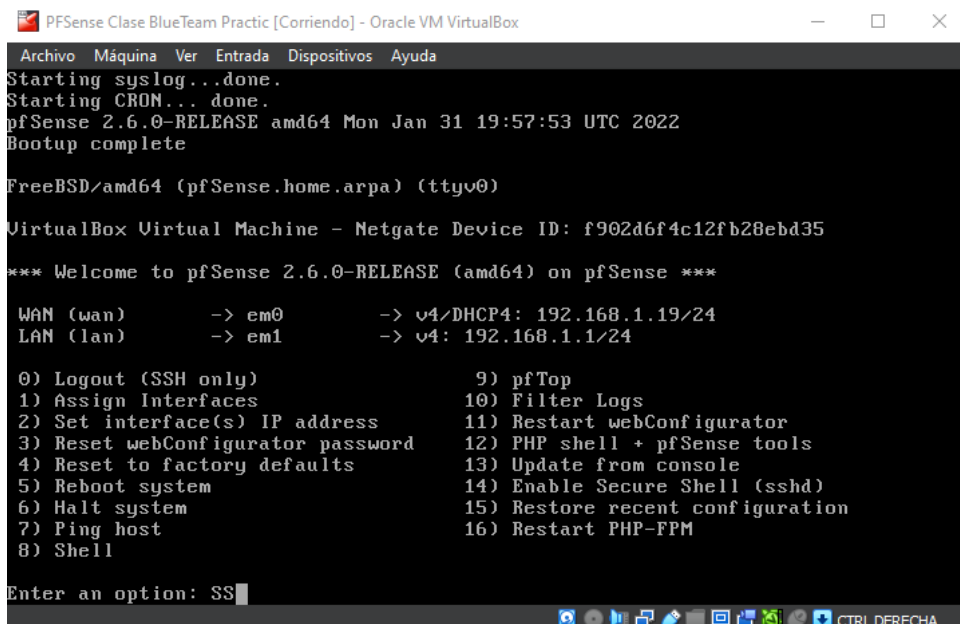
- VirtualBox: Tecnologia de virtualización de sistemas operativos.
- Pfsense: “Un Firewall que ha ido al gimnasio”. Es un firewall y un router con una gran cantidad de paquetes y personaliacion.
- OpenVpn: Herramienta de conectividad basada en SSL y en una red privada virtual.
- ELK: Sistema de integración de logs.

MONTAMOS PFSense EN VIRTUAL BOX:

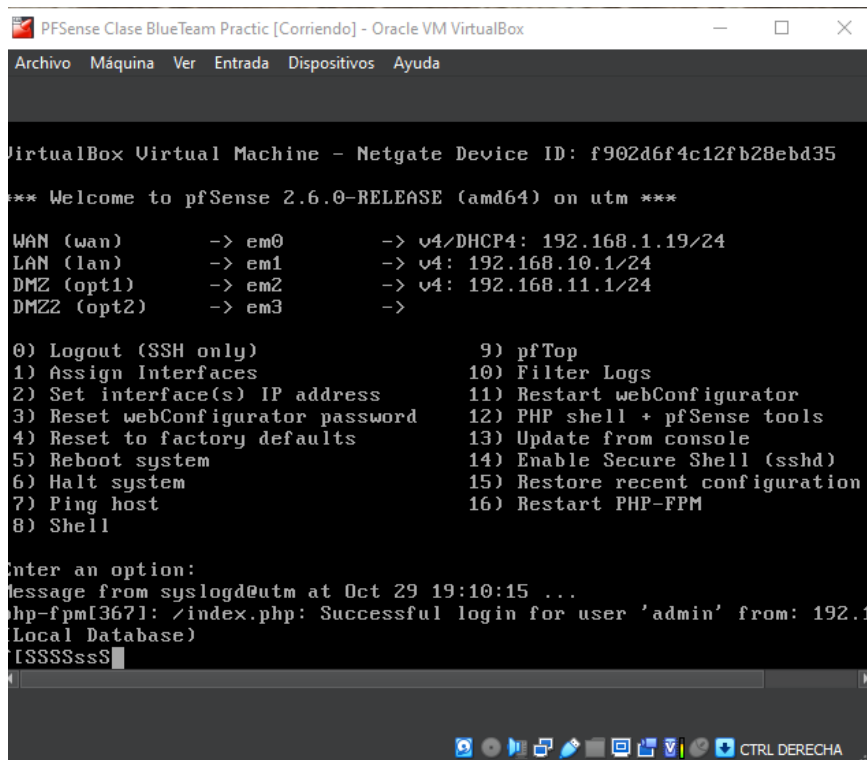
Instalamos PfSense en su mayoría por defecto.



Tras la instalación queda así:



Asignamos las diferentes interfaces que vamos a usar, en nuestro caso Lan va a ser 192.168.10.1/24 y Dmz 192.168.11.1/24.



```
VirtualBox Virtual Machine - Netgate Device ID: f902d6f4c12fb28ebd35
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on utm ***

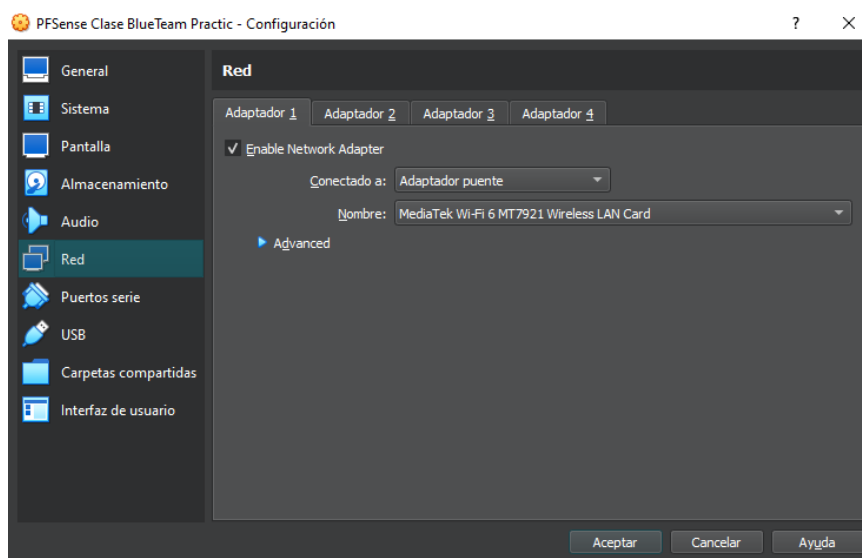
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.19/24
LAN (lan)      -> em1      -> v4: 192.168.10.1/24
DMZ (opt1)     -> em2      -> v4: 192.168.11.1/24
DMZ2 (opt2)    -> em3      ->

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

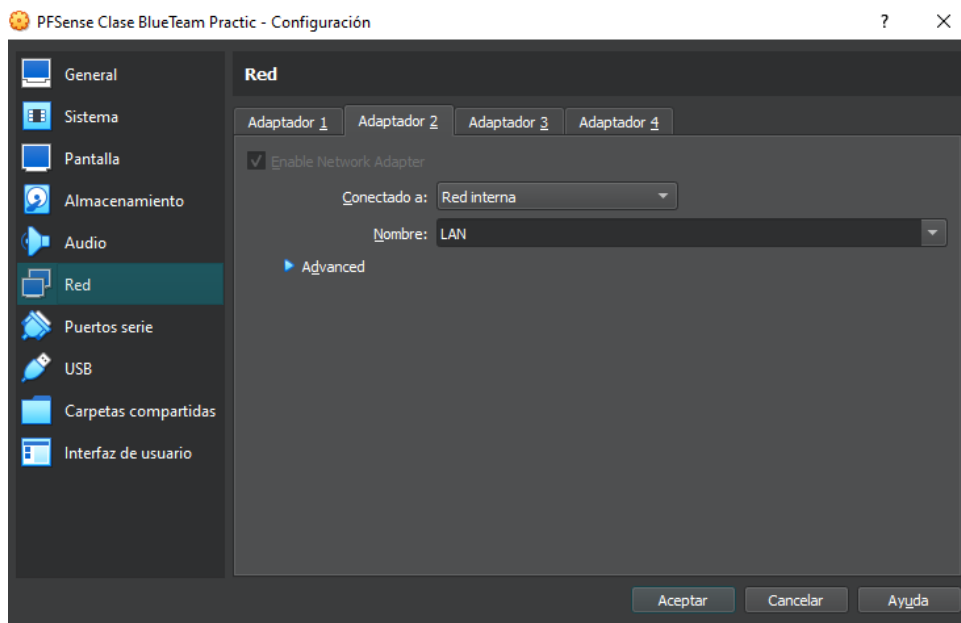
Enter an option:
Message from syslogd@utm at Oct 29 19:10:15 ...
php-fpm[3671]: /index.php: Successful login for user 'admin' from: 192.1
(Local Database)
[SSSSssS]
```

EN VIRTUAL BOX DISTRIBUIMOS LAS REDES DE LA SIGUIENTE MANERA:

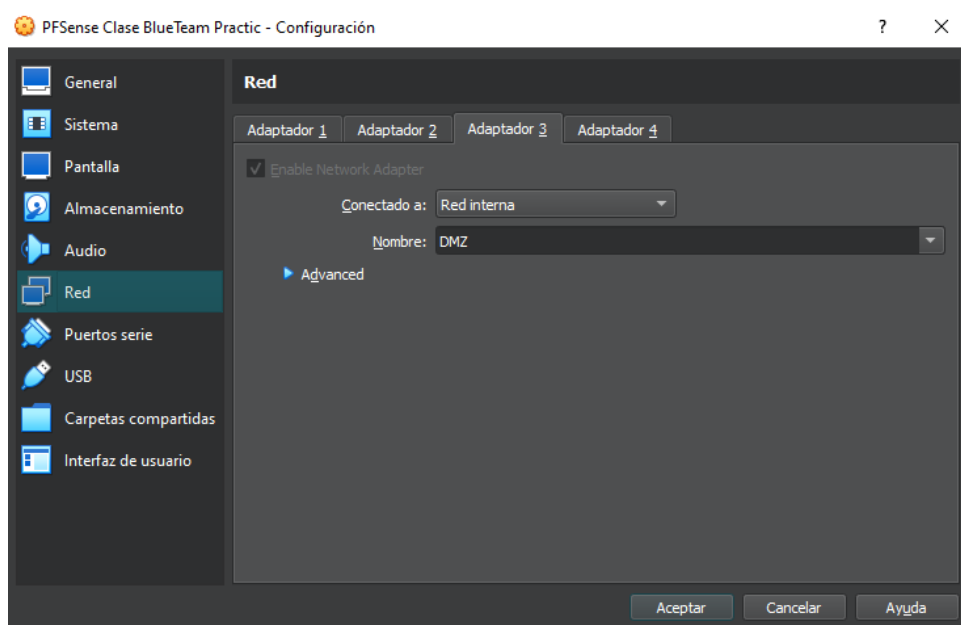
Pfsense lo ponemos en adaptador puente, para que este gericamente arriba en la red.



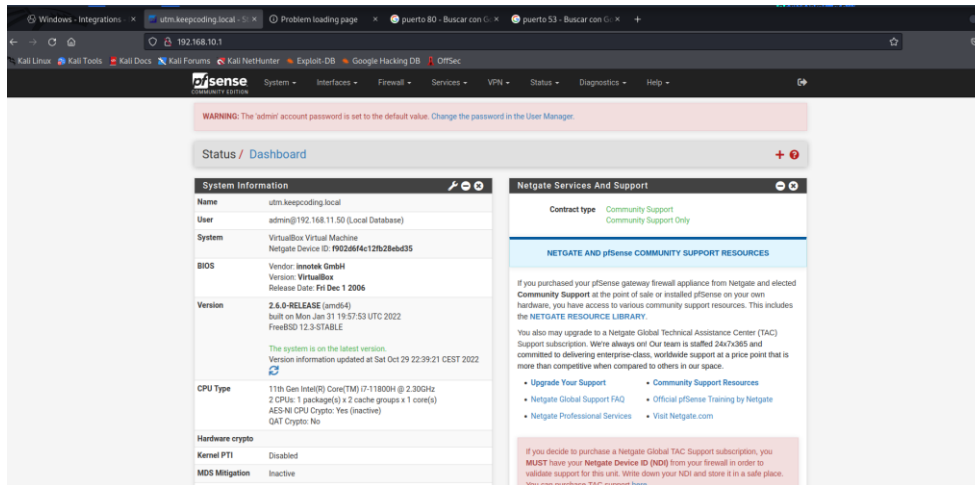
LAN en red interna para que cuelgue de esta:



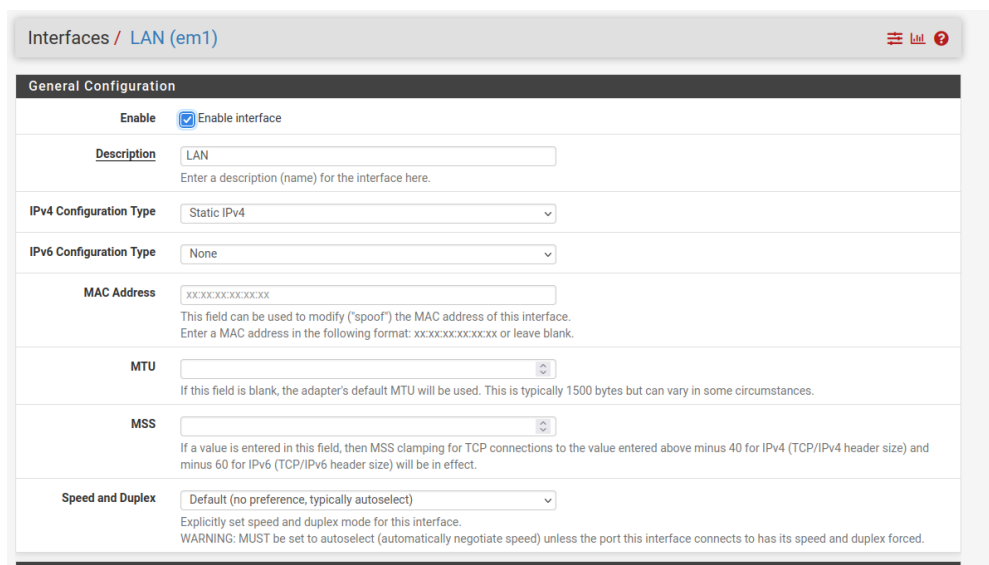
Dmz también en red interna para que cuelgue de pfsense:



En el Kali virtual que va a estar en Dmz, entramos en la configuración de pfsense en <http://192.168.10.1/>:



Habilitamos interfaz LAN



Habilitamos interfaz DMZ:

Interfaces / DMZ (em2)

General Configuration

Enable

☒ Enable interface

Description

DMZ

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xxxxxxxxxxxx

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

MTU

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

MSS

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

Speed and Duplex

Default (no preference, typically autoselect)

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

Static IPv4 Configuration

IPv4 Address

192.168.11.1

/ 24

Desmarcamos para permitir el trafico de ips privadas, que son las que vamos a usar (192.168.x.x)

Reserved Networks

Block private networks and loopback addresses

☐

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

Block bogon networks

☐

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

Habilitamos y configuramos el servidor DHCP de LAN: Establecemos que el rango para distribuir ips es de 192.168.10.100 a 192.168.10.200.

LAN DMZ

General Options

Enable

☒ Enable DHCP server on LAN interface

BOOTP

☐ Ignore BOOTP queries

Deny unknown clients

Allow all clients

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

Ignore denied clients

☐ Denied clients will be ignored rather than rejected.

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

Ignore client identifiers

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

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

Subnet

192.168.10.0

Subnet mask

255.255.255.0

Available range

192.168.10.1 - 192.168.10.254

Range

192.168.10.100

192.168.10.200

From To

Additional Pools

Hacemos lo mismo con DMZ:

LAN

DMZ

General Options

Enable

☒ Enable DHCP server on DMZ interface

BOOTP

☐ Ignore BOOTP queries

Deny unknown clients

Allow all clients

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

Ignore denied clients

☐ Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers

☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet

192.168.11.0

Subnet mask

255.255.255.0

Available range

192.168.11.1 - 192.168.11.254

Range

192.168.11.100

192.168.11.200

Establecemos los DNS, primer que pregunte a si mismo, a su red. Luego a Cloudflare y a Google.

WINS Server 2

DNS servers

192.168.11.1

1.1.1.1

8.8.8.8

DNS Server 4

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

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

☐ Generate New Key

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

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 Options

Gateway

192.168.11.1

Asignamos ip estatica identificada a la mac.

Static DHCP Mapping on DMZ

MAC Address	<input type="text" value="08:00:27:22:46:4f"/>	Copy My MAC
MAC address (6 hex octets separated by colons)		
Client Identifier	<input type="text"/>	
IP Address	<input type="text" value="192.168.11.50"/> <small>If an IPv4 address is entered, the address must be outside of the pool. If no IPv4 address is given, one will be dynamically allocated from the pool. The same IP address may be assigned to multiple mappings.</small>	
Hostname	<input type="text" value="kali_dmz"/> <small>Name of the host, without domain part.</small>	
Description	<input type="text" value="Kali para DMZ"/> <small>A description may be entered here for administrative reference (not parsed).</small>	
ARP Table Static Entry	<input checked="" type="checkbox"/> Create an ARP Table Static Entry for this MAC & IP Address pair.	
WINS Servers	<input type="text" value="WINS 1"/> <input type="text" value="WINS 2"/>	
DNS Servers	<input type="text" value="192.168.11.1"/> <input type="text" value="1.1.1.1"/> <input type="text" value="8.8.8.8"/> <input type="text" value="DNS 4"/> <small>Note: 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 General page.</small>	
Gateway	<input type="text" value="192.168.11.1"/>	

De la misma manera el dns, que pregunte primero a si mismo luego fuera:

Servers

WINS servers	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
DNS servers	<input type="text" value="192.168.11.1"/>
	<input type="text" value="1.1.1.1"/>
	<input type="text" value="8.8.8.8"/>
	<input type="text" value="DNS Server 4"/>

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

CONFIGURACION DE FIREWALL:

No lo hice en este orden pero para tener el informe mas ordenado explico directamente toda la configuración del firewall:

Cualquier cosa que entre desde fuera tiene que pasar por el puerto 9458

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / WAN

Floating WAN LAN DMZ DMZ2 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP	*	*	This Firewall	9458	*	none		Add Add Delete Save Separator

LAN: Entradas puerto 80 abierto para web. Salidas todas permitidas.

Firewall / Rules / LAN

Floating WAN LAN DMZ DMZ2 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	5 / 392.65 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

DMZ: habilitamos los web 80 443 y los de resolución de dns 53 para web.

Firewall / Rules / DMZ

Floating WAN LAN DMZ DMZ2 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	19 / 11.05 MiB	IPv4 TCP	*	*	*	web	*	none		Navegacion web	
<input checked="" type="checkbox"/>	0 / 61 KiB	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		Navegacion web DNS	

Add Add Delete Save Separator

VPN: Dejamos pasar todo para que nos llegue la información para mas adelante montar el elk y el openVPN

Firewall / Rules / OpenVPN

Floating WAN LAN DMZ DMZ2 OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4 / 388.63 MiB	IPv4 *	*	*	*	*	*	none		any	

Add Add Delete Save Separator

MONTAMOS OPENVPN

Descargamos el paquete de openvpn para pfsense:

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / [Package Manager](#) / [Package Installer](#) ?

Please wait while the installation of **pfSense-pkg-openvpn-client-export** completes.
This may take several minutes. Do not leave or refresh the page!

Installed Packages Available Packages **Package Installer**

Package Installation

The following 4 package(s) will be affected (0/0 checked):

New packages to be INSTALLED:

- openvpn-client-export: 2.5.2 [pfSense]
- p7zip: 16.02_3 [pfSense]
- pfSense-pkg-openvpn-client-export: 1.6_4 [pfSense]
- zip: 3.0_1 [pfSense]

Number of packages to be installed: 4

The process will require 25 MiB more space.
17 MiB to be downloaded.

```
[1/4] Fetching pfSense-pkg-openvpn-client-export-1.6_4.pkg: ... done
[2/4] Fetching openvpn-client-export-2.5.2.pkg: ..... done
[3/4] Fetching zip-3.0_1.pkg: ..... done
[4/4] Fetching p7zip-16.02_3.pkg: .....]
```

Creamos la entidad certificadora y el certificado.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / [Certificate Manager](#) / [Certificates](#) ?

Created internal certificate vpn.keepcoding.local

CAs **Certificates** Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (63598cac9c395) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-63598cac9c395 Valid From: Wed, 26 Oct 2022 21:38:20 +0200 Valid Until: Tue, 28 Nov 2023 20:38:20 +0100		
vpn.keepcoding.local Server Certificate CA: No Server: Yes	UTM	ST=Madrid, O=Keecoding, L=Madrid, CN=vpn.keepcoding.local, C=ES Valid From: Sat, 29 Oct 2022 19:25:51 +0200 Valid Until: Tue, 26 Oct 2023 19:25:51 +0200		

[+ Add/Sign](#)

Configuramos la vpn con las ips de lan y dmz:

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	TCP4 / 9458 (TUN)	192.168.210.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	VPN-keep	

+ Add

Creamos Usuario y contraseña.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

System / User Manager / Users

Users Groups Settings Authentication Servers

Users				
	Username	Full name	Status	Groups
<input type="checkbox"/>	admin	System Administrator	✓	admins
<input type="checkbox"/>	kali	vpn.keepcoding.local	✓	

+ Add Delete

Como dijimos antes en firewall dejamos pasar todo en la vpn.

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / OpenVPN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

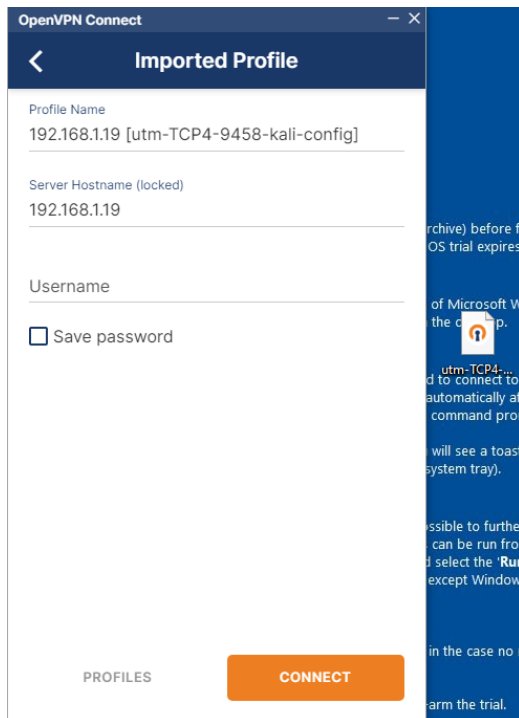
✓ Apply Changes

Floating WAN LAN DMZ DMZ2 OpenVPN

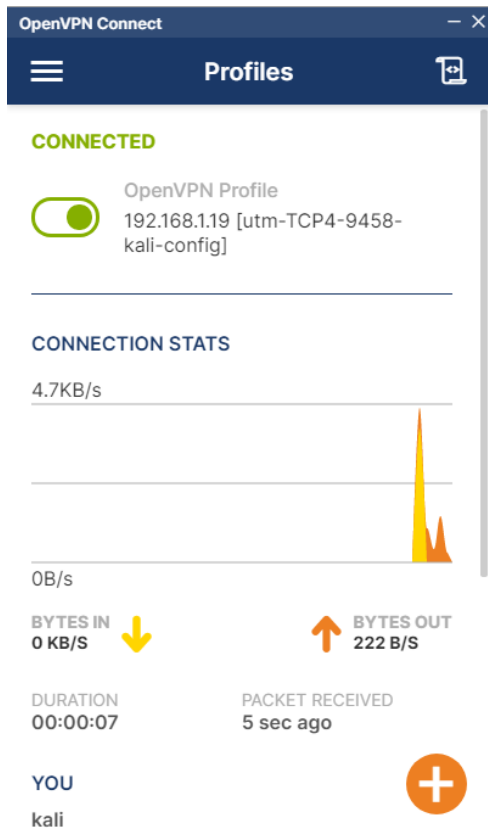
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 0 B	IPv4 *	*	*	*	*	*	none	any	

Add Add Delete Save Separator

Instalamos cliente open vpn en el pc virtual de Windows en la red de LAN.
Usamos el archivo de configuración que nos genero pfsense.



Conexión establecidas:



MONTAMOS ELK CON DOCKER

Despues de descargar la imagen de elk, lo montamos con docker-compose up

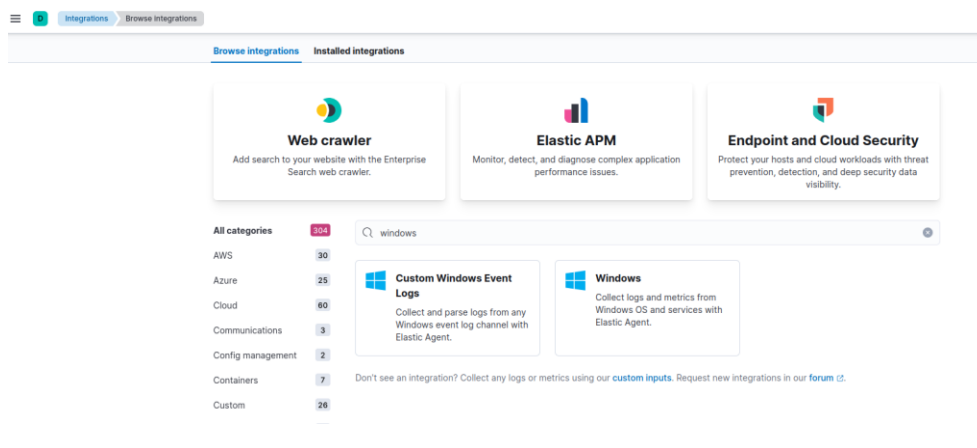
```
File Actions Edit View Help

(kali@kali)-[~]
$ docker ps
Got permission denied while trying to connect to the Docker daemon socket at
unix:///var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.24/con
tainers/json": dial unix /var/run/docker.sock: connect: permission denied

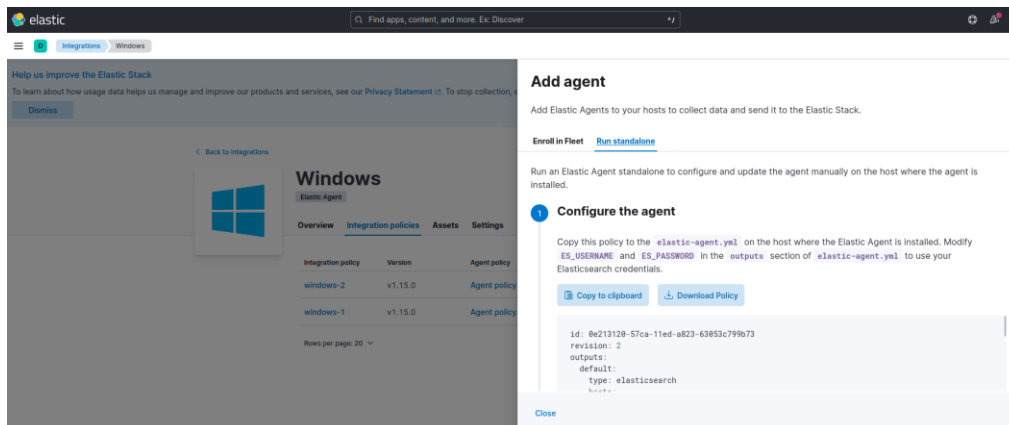
(kali@kali)-[~]
$ sudo docker ps
[sudo] password for kali:
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS          NAMES
(kali@kali)-[~]
$ sudo su
(root@kali)-[/home/kali]
# pwd
/home/kali
(root@kali)-[/home/kali]
# cd BlueTeam
(root@kali)-[/home/kali/BlueTeam]
# cd docker-elk
(root@kali)-[/home/kali/BlueTeam/docker-elk]
# docker-compose up -d
Starting docker-elk_elasticsearch_1
Starting docker-elk_elasticsearch_1
... done
Starting docker-elk_setup_1
...
Starting docker-elk_logstash_1
Starting docker-elk_setup_1
... done docker-elk_kibana_1
...
Starting docker-elk_logstash_1
... done

(root@kali)-[/home/kali/BlueTeam/docker-elk]
#
```

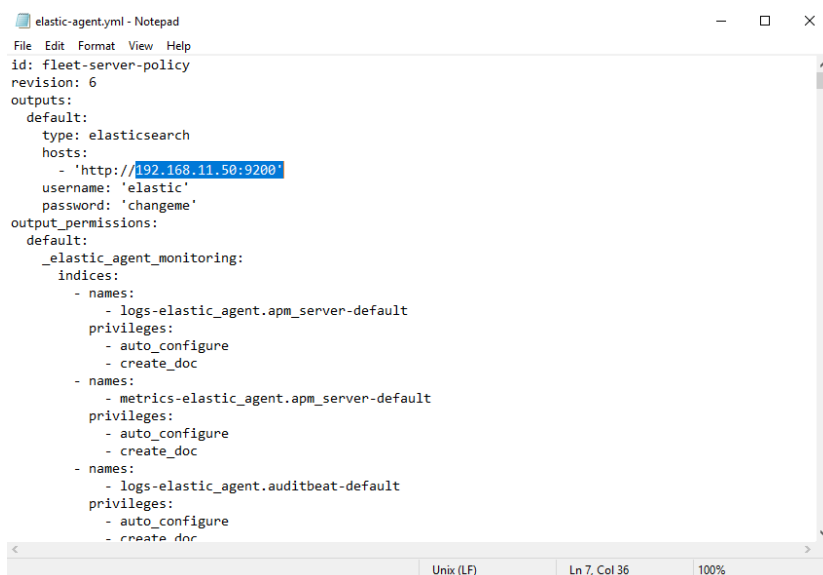
Entramos en la interfaz de elk buscamos la integración de Windows y la instalamos con la configuración por defecto.



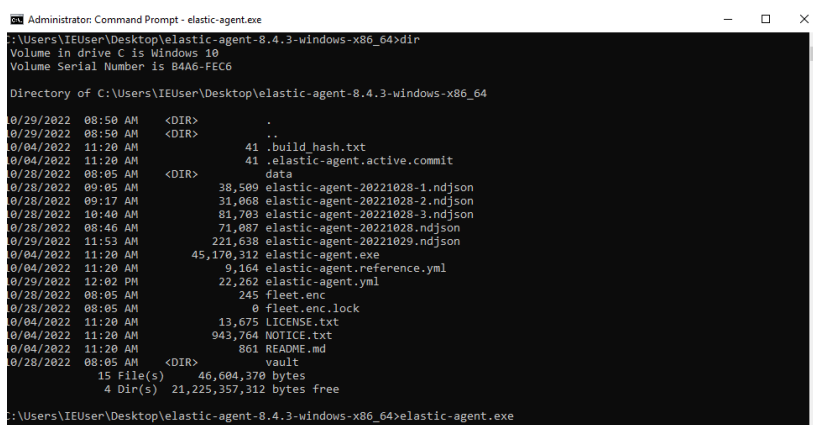
En run stand alone copiamos a clipboard. Tenemos que poner nuestra ip y el usuario y contraseña por defecto que es elastic y changeme.



Despues de descargar el cliente de ELK en Windows pegamos el clipboard y cambiamos ip usuario y contraseña. Aquí con los cambios ya hechos.

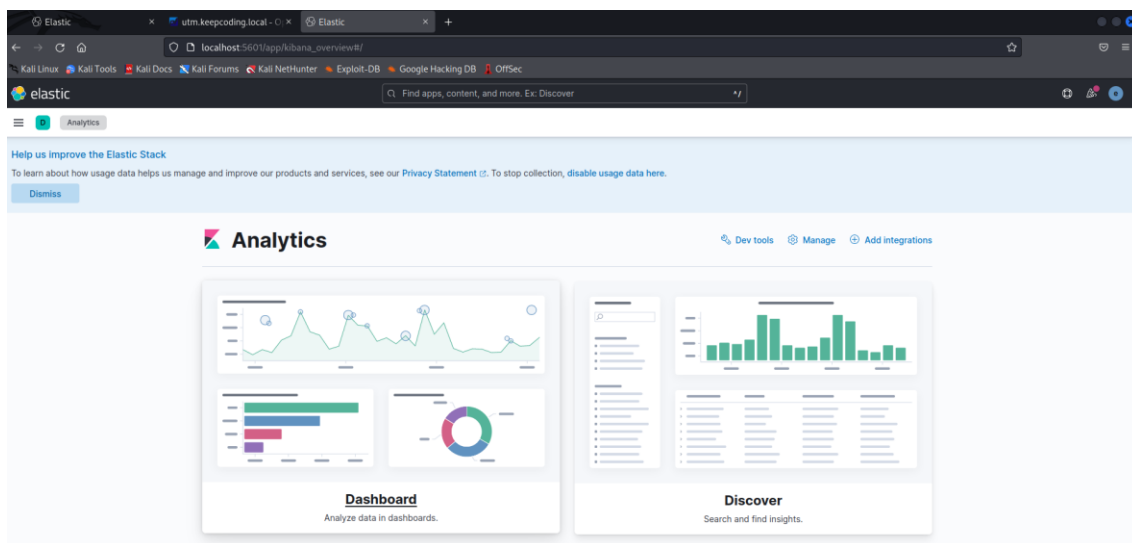


Ejecutamos el cliente de ELK desde cmd en modo administrador:

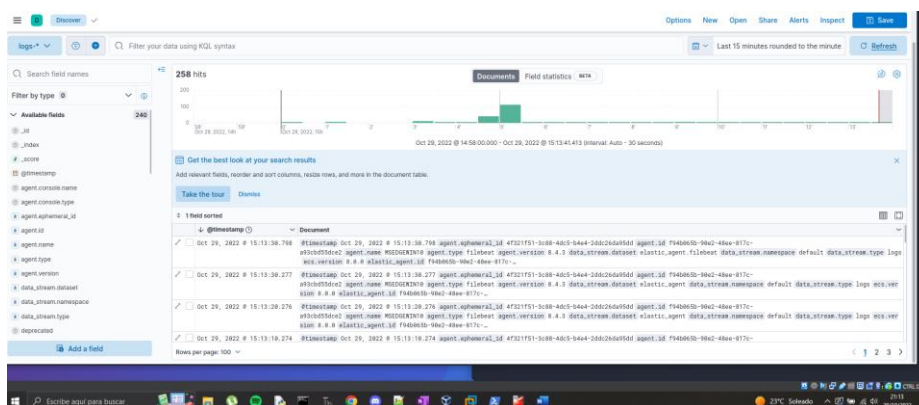


MONITORIZACION:

Tenemos acceso a toda la información que nos brinda el ELK en el Windows de LAN, que nos manda al Kali de DMZ:



La hora no coincide por la razón que sea:



Pero al actualizar toda la información se actualiza al minuto. Damos la red y el informe por finalizado.

