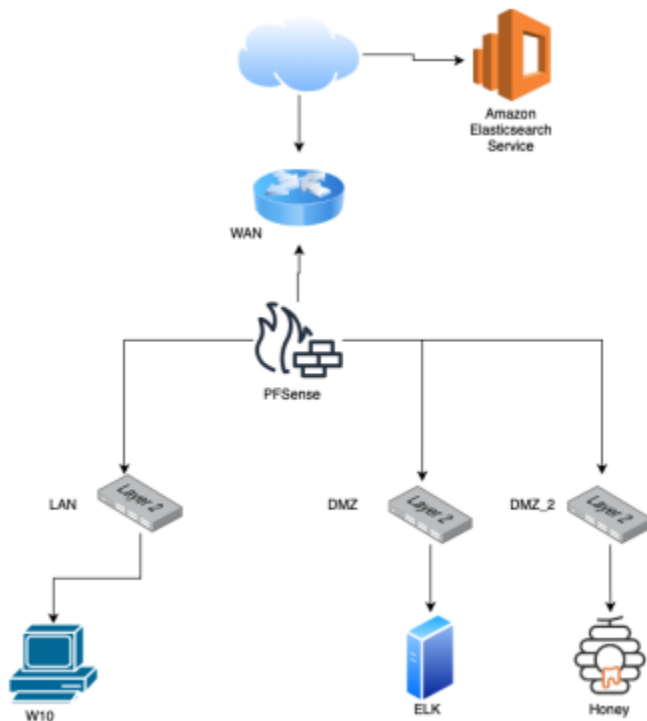


INFORME PRÁCTICA BLUE TEAM

Alexandra Oane

30/10/2022

INFRAESTRUCTURA



REQUISITOS

- Creación de un PfSense en bridge que conecte 3 redes, LAN, DMZ y DMZ_2 estas como red interna.
- Un equipo W10 en LAN, un stack ELK en DMZ y un grupo de honeypots en DMZ_2.
- Queremos transmitir los logs de los honeypots al ELK stack, pero los honeypots no deben tener acceso a las otras redes (solo para transmitir logs) pero los honeypots deben ser accesible desde la red WAN.
- El servidor ELK debe almacenar y poder visualizar los diferentes logs de los honeypots.
- El W10 debe poder conectarse a ELK vía Kibana.

1. CREACIÓN PFSENSE

Pfsense es un sistema operativo basado en FreeBSD diseñado para instalar un firewall que se puede configurar a través de una interfaz web.

Se puede configurar como firewall, que permite y deniega cierto tráfico de red entrante y saliente de las redes de origen y destino o direcciones de host. También permite realizar un filtrado de paquetes a través de protocolos y puertos.

Como servidor VPN, utiliza protocolos de túneles.

La red LAN se refiere a la red interna de la organización conectada a la interfaz LAN. Debe estar protegido contra ataques de internet.

La red DMZ es una zona desmilitarizada, donde se ubica el servidor, al que se puede acceder desde internet como servidor Web y de correo con determinados parámetros.

La red DM2.

La red WAN está conectada a la interfaz WAN de Pfsense, que también se niega a comunicarse desde la red a internet y al revés.

Conexiones permitidas:

Desde Internet → DMZ = se permite la conexión

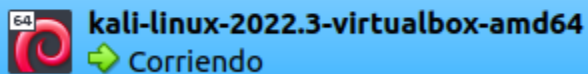
Desde Internet → LAN = se deniega la conexión

Desde DMZ → Internet = se permite la conexión

Desde DMZ → LAN = se deniega la conexión

Desde LAN → DMZ = se permite conexión

Desde LAN → Internet= permite conexión



Se debe configurar la interfaz UTM-Blue-001 para poder abrir Pfsense desde Kali.











Configurar las redes WAN, LAN, DMZ y DMZ2. Además de las redes, las distintas opciones y variaciones que ofrece Pfsense.


```
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 522534f2f389ae597d9b
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.100.1/24
DMZ (opt1)     -> em2      -> v4: 192.168.90.1/24
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: █
```

Interfaces  			
 WAN		1000baseT <full-duplex>	192.168.0.25
 LAN		1000baseT <full-duplex>	192.168.100.1
 DMZ		1000baseT <full-duplex>	192.168.90.1
 DMZ2		1000baseT <full-duplex>	n/a


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




WARNING: The 'admin' account has a default value. Change the password in the User Manager.

Interfaces / WAN (em0)

General Configuration

Assignments

- WAN
- LAN
- DMZ
- DMZ2

Interfaces / WAN (em0)   

General Configuration

Enable ☒ Enable interface

Description

WAN

Enter a description (name) for the interface here.

IPv4 Configuration Type

DHCP

IPv6 Configuration Type

DHCP6

MAC Address

xx:xx:xx:xx:xx:xx

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

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.

General Configuration

Enable ☒ Enable interface

Description

LAN

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xx:xx:xx:xx:xx:xx

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

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.

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

192.168.100.1

/ 24

IPv4 Upstream gateway

None

[+ Add a new gateway](#)

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

Reserved Networks

Block private networks and loopback addresses

☐

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

Block bogon networks

☐

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

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:xx:xx:xx:xx:xx

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

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

192.168.90.1

/ 24

IPv4 Upstream gateway

None

[+ Add a new gateway](#)

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

Reserved Networks

Block private networks and loopback addresses

☐

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

Block bogon networks

☐

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

General Configuration

Enable ☒ Enable interface**Description**

Enter a description (name) for the interface here.

IPv4 Configuration Type**IPv6 Configuration Type****MAC Address**This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.**MTU**

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

MSS

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

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.

General Configuration

Enable ☒ Enable interface**Description**

Enter a description (name) for the interface here.

IPv4 Configuration Type**IPv6 Configuration Type****MAC Address**This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.**MTU**

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

MSS

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

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.

Se configuran los servicios del servidor DHCP en la red LAN y DMZ.

Services / DHCP Server / LAN

LAN DMZ

General Options

Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny unknown clients	<div>Allow all clients</div> <p>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 <i>any</i> 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.</p>
Ignore denied clients	<input type="checkbox"/> 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	<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

Subnet	192.168.100.0
Subnet mask	255.255.255.0
Available range	192.168.100.1 - 192.168.100.254
Range	<div>192.168.100.100</div> <div>From</div> <div>192.168.100.200</div> <div>To</div>

Services / DHCP Server / DMZ

LAN
DMZ

General Options

Enable	<input checked="" type="checkbox"/> Enable DHCP server on DMZ interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny unknown clients	<div>Allow all clients</div> <p>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.</p>
Ignore denied clients	<input type="checkbox"/> 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	<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	192.168.90.0
Subnet mask	255.255.255.0
Available range	192.168.90.1 - 192.168.90.254
Range	<div>192.168.90.100</div> <div>192.168.90.200</div> <div>FromTo</div>

Servers

WINS servers	WINS Server 1
	WINS Server 2
DNS servers	192.168.90.1
	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.



Los servidores DNS se configuran para que haya salida a internet.



Other Options

Gateway	192.168.90.1
---------	--------------

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

Se establece en la gateway la IP 192.168.90.1


DHCP Static Mappings for this Interface (total: 1)					
Static ARP	MAC address	IP address	Hostname	Description	
✓	08:00:27:22:46:4f	192.168.90.50	kali_dmz	Kali para DMZ	 

Services / [DHCP Server](#) / [DMZ](#) / [Edit Static Mapping](#)     

Static DHCP Mapping on DMZ

MAC Address

08:00:27:22:46:4f

 Copy My MAC

MAC address (6 hex octets separated by colons)

Client Identifier

IP Address

192.168.90.50

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.

Hostname

kali_dmz

Name of the host, without domain part.

Description

Kali para DMZ

A description may be entered here for administrative reference (not parsed).

ARP Table Static Entry

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

WINS Servers

WINS 1

WINS 2

DNS Servers

192.168.90.1

1.1.1.1

8.8.8.8

DNS 4

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.

Gateway

192.168.90.1

The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network.

Se establecen reglas para las distintas redes.

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	vpn.keepcoding.local	   
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	192.168.90.50	80 (HTTP)	*	none	NAT Servidor web	   

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

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

Disabled

☐ Disable this rule

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

Interface

WAN

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Destination

☐ Invert match

THIS Firewall (Self)

Destination Address

Destination Port Range

(other)

9458

(other)

9458

From

Custom

To

Custom

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

Extra Options

Log

☐ Log packets that are handled by this rule


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

Description

vpn.keepcoding.local

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

Advanced Options

 Display Advanced

Rule Information

Tracking ID

1666548716

Created

10/23/22 20:11:56 by admin@192.168.90.50 (Local Database)

Updated

10/23/22 20:12:11 by admin@192.168.90.50 (Local Database)

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.

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

Disabled☐ Disable this rule

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

Associated filter rule

This is associated with a NAT rule.

Editing the interface, protocol, source, or destination of associated filter rules is not permitted.

[View the NAT rule](#)**Interface**

WAN

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source☐ Invert match

any

Source Address /

Display Advanced

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

Destination

Destination☐ Invert match

Single host or alias

192.168.90.50 /

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

To

Custom

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

Extra Options

Log☐ Log packets that are handled by this rule

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

Description

NAT Servidor web

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

Advanced Options

Display Advanced

Rule Information

Tracking ID

1666526798

Created

10/23/22 14:06:38 by NAT Port Forward

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 type="checkbox"/>	✓ 0/0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

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 type="checkbox"/>	✓ 1/571 KiB	IPv4 TCP	*	*	*	web	*	none		Navegaci'on web	
<input type="checkbox"/>	✓ 0/744 B	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none		Navegaci'on web DNS	
Internet											
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP any	*	*	*	*	*	none			




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 type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	*	*	*	none		any	

También se configura OpenVPN en Pfsense con los datos en los campos correspondientes.

VPN / OpenVPN / Servers					
Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export					
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	  

VPN / OpenVPN / Servers / Edit	
Servers Clients Client Specific Overrides Wizards Client Export Shared Key Export	
General Information	
Description	<input type="text" value="VPN-keep"/> <small>A description of this VPN for administrative reference.</small>
Disabled	<input type="checkbox"/> Disable this server <small>Set this option to disable this server without removing it from the list.</small>
Unique VPN ID	Server 1 (ovpns1)
Mode Configuration	
Server mode	<input type="text" value="Remote Access (SSL/TLS + User Auth)"/>
Backend for authentication	<input type="text" value="Local Database"/>
Device mode	<input type="text" value="tun - Layer 3 Tunnel Mode"/>

Endpoint Configuration	
Protocol	<input type="text" value="TCP on IPv4 only"/>
Interface	<input type="text" value="WAN"/> <small>The interface or Virtual IP address where OpenVPN will receive client connections.</small>
Local port	<input type="text" value="9458"/> <small>The port used by OpenVPN to receive client connections.</small>

Cryptographic Settings

TLS Configuration

☒ Use a TLS Key

A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

TLS Key

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
8f540cb9a43186618415f627e1de1dc5
ad2a4783cb06af7ebce07f34f35277ee
```

Paste the TLS key here.

This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.

TLS Key Usage Mode

TLS Authentication

In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.

TLS keydir direction

Use default direction

The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

Peer Certificate Authority

UTM

Peer Certificate Authority

UTM

Peer Certificate Revocation list

No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check

☐ Check client certificates with OCSP

Server certificate

vpn.keepcoding.local (Server: Yes, CA: UTM, In Use)

DH Parameter Length

2048 bit

Diffie-Hellman (DH) parameter set used for key exchange. [i](#)

ECDH Curve

Use Default

The Elliptic Curve to use for key exchange.

The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Tunnel Settings

IPv4 Tunnel Network

192.168.210.0/24

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

Se pueden crear distintos usuarios.

System / User Manager / Users ?					
Users Groups Settings Authentication Servers					
Users					
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input checked="" type="checkbox"/>	alexandra		✓		

Se levanta un contenedor de docker que nos va a permitir tener un servidor SSH.

```
(kali㉿kali)-[~]  
$ sudo docker run -p 29:2222 cowrie/cowrie
```

```
2022-11-01T19:17:23+0000 [-] Generating new ECDSA keypair ...  
2022-11-01T19:17:23+0000 [-] Generating new ed25519 keypair ...  
2022-11-01T19:17:23+0000 [-] Ready to accept SSH connections
```

```
vant@MOOVE2-15:~$ ssh root@172.16.127.129 -p 29  
root@172.16.127.129's password:  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
root@svr04:~# Connection to 172.16.127.129 closed by remote host.  
Connection to 172.16.127.129 closed.
```

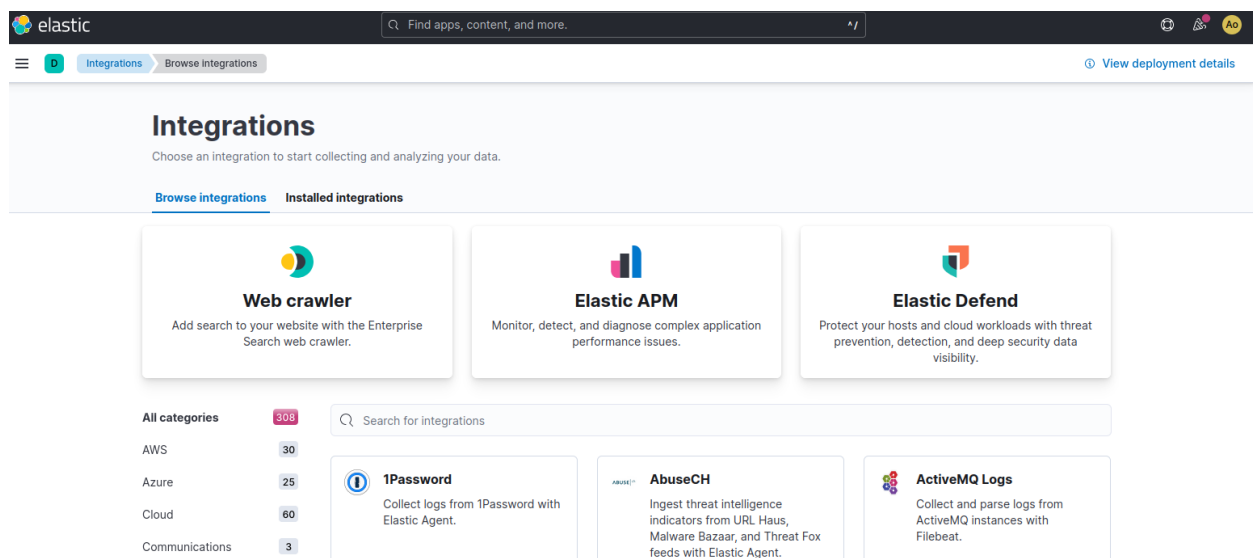
```
2022-11-01T19:38:53+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,172.16.127.1] Terminal Size: 80 24
2022-11-01T19:38:53+0000 [SSHChannel session (0) on SSHService b'ssh-connection' on HoneyPotSSHTransport,1,172.16.127.1] request_env: LANG=es_ES.UTF-8
2022-11-01T19:38:53+0000 [twisted.conch.ssh.session#info] Getting shell
2022-11-01T19:41:53+0000 [-] Timeout reached in HoneyPotSSHTransport
```

```
2022-11-01T19:41:53+0000 [HoneyPotSSHTransport,1,172.16.127.1] avatar root logging out
2022-11-01T19:41:53+0000 [cowrie.ssh.transport.HoneyPotSSHTransport#info] connection lost
2022-11-01T19:41:53+0000 [HoneyPotSSHTransport,1,172.16.127.1] Connection lost after 203 seconds
```

```
(kali㉿kali)-[~]
$ sudo docker run -p 3389:3389 amzedostrich/rdpy
```

El Stack ELK es el conjunto de tres tecnologías de open source. Se complementan para proporcionar un sistema de gestión de logs centralizado y escalable.

Se realiza el registro en Elastic.



La práctica tiene varios puntos que faltan, he tenido algunas dificultades con la instalación de OpenVPN, y siguientes puntos (Elastic, Kibana, Suricata).

Continuaré para tratar de realizarla correctamente.