P5: OPENVPN

1. Descripción

Creación de un túnel OpenVPN en modo road-warrior para la transferencia de información de forma encriptada.

2. Entorno de prácticas

En estas prácticas se empleará el software de virtualización VIRTUALBOX para simular los equipos GNU/Linux sobre los que se realizarán las pruebas.

3. Imágenes a utilizar

Se proporcionan scripts de instalación tanto para GNU/Linux como para Windows. Windows es bastante inestable con algunas configuraciones de la Máquina Virtual que se usarán durante la realización de las prácticas. Por ello, se recomienda encarecidamente usar Linux como sistema base.

- Script GNU/Linux: ejercicio-ficheros.sh (desde línea de comandos)

```
01 alumno@pc: $ sh ejercicio-dmz-openvpn.sh
```

- MS Windows: ejercicio-ficheros.ps1 (desde cmd)

```
01 Powershell.exe -executionpolicy bypass -file
02 ejercicio-dmz-openvpn.ps1
```

Notas:

- Se pedirá un identificador (sin espacios) para poder reutilizar las versiones personalizadas de las imágenes creadas.
- En ambos scripts la variable $DIR_BASE específica donde se descargarán las imágenes y se crearán las MVs.
- Por defecto en GNU/Linux será en $HOME/CDA2425 y en Windows en C:/CDA2425.
- Puede modificarse antes de lanzar los scripts para hacer la instalación de las imágenes en otro directorio más conveniente (disco externo, etc)
- Si se hace desde el script anterior, se pueden arrancar las instancias VIRTUALBOX desde el interfaz gráfico de VirtualBOX o desde la línea de comandos con VBoxManage startvm <nombre MV>_<id>

4. Credenciales de acceso

La distribución Linux incluida en la MV tiene dados de alta dos usuarios con las siguientes credenciales y permisos:

login	password	permisos
root	purple	root
usuario	purple	permite sudo

5. Entorno de prácticas

Una vez ejecutado el script se habrán definido las tres redes y los 4 equipos virtualizados donde se realizarán los ejercicios:

- Red interna (10.10.10.0 ↔ 10.10.10.255):
  - Máquina dentro (enp0s3)
  - Interfaz enp0s3 de firewall3
- Red DMZ (10.20.20.0 ↔ 10.20.20.255)
  - Máquina dmz (enp0s3)
  - Interfaz enp0s8 de firewall3
- Red externa (193.147.87.0 ↔ 193.147.87.255)
  - Máquina fuera (enp0s3)
  - Interfaz enp0s9 de firewall3

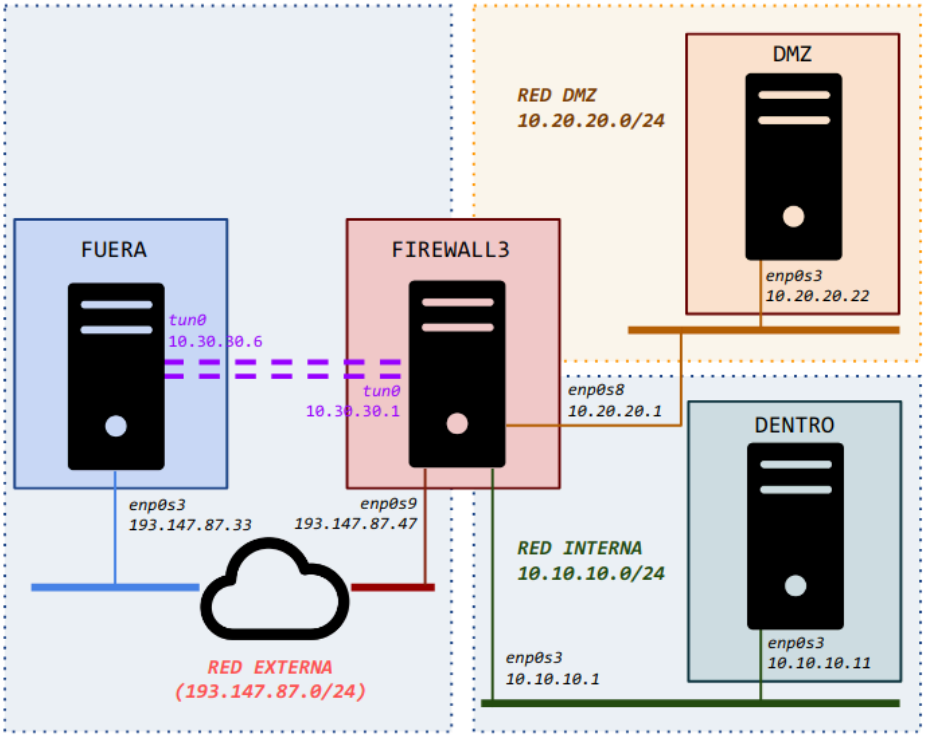

Fig 1. Configuración inicial del entorno de prácticas.

6. Ejercicio

Tarea 1 : Uso de enlaces cifrados con OpenVPN

Pasos previos:

- Habilitar el acceso como usuario root en el servidor SSH de la máquina firewall3 [10.10.10.1, 10.20.20.1, 193.147.87.47] y reiniciar el servicio

```
01 firewall3:~$ sudo nano /etc/ssh/sshd_config
02 ...
03 PermitRootLogin yes
04 ...
05 firewall3:~$ sudo systemctl restart sshd
```

- Establecer tráfico a través de la máquina firewall3 [10.10.10.1, 10.20.20.1, 193.147.87.47]
  - Establecer la configuración por defecto de NETFILTER/iptables (política ACCEPT)

```
01 firewall3:~$ sudo iptables -F
```

```
02 firewall3:~$ sudo iptables -t nat -F
03 firewall3:~$ sudo iptables -P INPUT ACCEPT
04 firewall3:~$ sudo iptables -P OUTPUT ACCEPT
05 firewall3:~$ sudo iptables -P FORWARD ACCEPT
```

- Habilitar la redirección de tráfico.

```
01 firewall3:~$ sudo echo 1 > /proc/sys/net/ipv4/ip_forward
```

- Escaneo desde la máquina fuera para verificar los servicios accesibles inicialmente **[Ejercicio 1]**

```
01 fuera:~# nmap -T4 10.10.10.11
02 fuera:~# nmap -T4 10.20.20.22
03 fuera:~# nmap -T4 193.147.87.47
```

Creación de un enlace VPN

- Creación de la CA y de los certificados de servidor y clientes.
  - Crear la autoridad certificadora" (CA) en el firewall
    - Editar los parámetros de la CA y los metadatos de los certificados a generar

```
01 firewall3:~$ cd /usr/share/easy-rsa
02 firewall3:/usr/share/easy-rsa$ sudo cp vars.example vars
03 firewall3:/usr/share/easy-rsa$ sudo nano vars
04 ...
05 set_var EASYRSA_REQ_COUNTRY    "ES"
06 set_var EASYRSA_REQ_PROVINCE   "Ourense"
07 set_var EASYRSA_REQ_CITY       "Ourense"
08 set_var EASYRSA_REQ_ORG        "ESEI"
09 set_var EASYRSA_REQ_EMAIL      "cda@cda.net"
10 set_var EASYRSA_REQ_OU         "CDA"
11 ...
```

    - Inicializar la CA

```
01 firewall3:~# cd /etc/openvpn/
02 firewall3:/etc/openvpn$ sudo /usr/share/easy-rsa/easyrsa
03 init-pki
```

    - Generar el par de claves de la CA (cuando pida el valor Common Name, indicar CA prueba)

```
01 firewall3:/etc/openvpn$ sudo /usr/share/easy-rsa/easyrsa
02 build-ca nopass
```

- Crear el certificado del equipo "servidor" OpenVPN.

```
01 firewall3:/etc/openvpn$ sudo /usr/share/easy-rsa/easyrsa
02 build-server-full firewall3.cda.net nopass
```

- Crear el certificado del equipo "cliente" OpenVPN.

```
01 firewall3:/etc/openvpn$ sudo /usr/share/easy-rsa/easyrsa
02 build-client-full fuera nopass
```

- Crear los parámetros del algoritmo de intercambio de claves Diffie-Hellman necesarios para la negociación de claves secretas durante el establecimiento de la conexión TLS/SSL

```
01 firewall3:/etc/openvpn$ sudo /usr/share/easy-rsa/easyrsa gen-dh
```

- Configuración y creación del enlace OpenVPN.
  - Configuración del servidor: en la máquina firewall3, directorio /etc/openvpn/server.
    - Crear una clave secreta para la autenticación HMAC (hash-based message authentication code) de los paquetes TLS/SSL

```
01 firewall3:~$ cd /etc/openvpn
02 firewall3:/etc/openvpn$ cd server/
03
04 firewall3:/etc/openvpn/server$ sudo openvpn --genkey secret
05 ta.key
```

    - Crear el fichero de configuración del servidor (se usará como base el ejemplo disponible en /usr/share/doc/openvpn/examples/sample-config-files/)

```
01 firewall3:/etc/openvpn/server$ sudo cp
02 /usr/share/doc/openvpn/examples/sample-config-files/server.conf .
```

    - Editar los parámetros concretos para nuestros túneles VPN (con "→" se señalan los cambios a efectuar):

```
01 firewall3:/etc/openvpn/server$ sudo nano server.conf
```

```
port 1194      ## puerto por defecto del servidor OpenVPN
proto udp      ## protocolo por defecto del servidor OpenVPN
dev tun        ## tipo de dispositivo de red virtual
               ## (= tarjeta de red "software") a través del
```

```
                ## cual se accederá al túnel cifrado establecido
...
→ ca /etc/openvpn/pki/ca.crt     ## parámetros de cifrado
→ cert /etc/openvpn/pki/issued/firewall3.cda.net.crt
→ key /etc/openvpn/pki/private/firewall3.cda.net.key
...
→ dh /etc/openvpn/pki/dh.pem
...
→ server 10.30.30.0 255.255.255.0     ## rango de direcciones a
...                                   ## asignar a los clientes
...                                   ## OpenVPN que se vayan
...                                   ## conectando
...
→ push "route 10.10.10.0 255.255.255.0" ## configuración de las
→ push "route 10.20.20.0 255.255.255.0" ## rutas a establecer en
                                        ## los clientes para las
                                        ## conexiones cifradas
                                        ## que se vayan creando
                                        ## en nuestro caso son
                                        ## las rutas hacia las 2
                                        ## redes (interna y dmz)
                                        ## gestionadas por
                                        ## firewall3
...
→ tls-auth /etc/openvpn/server/ta.key 0
...
```

- Configuración de los clientes: en la máquina fuera (193.147.87.33), directorio /etc/openvpn/client
  - Copiar las claves/certificados necesarios al directorio /etc/openvpn/client

```
01 fuera:~$ cd /etc/openvpn
02 fuera:/etc/openvpn$ cd client
03 fuera:/etc/openvpn/client$ sudo scp
04 root@firewall3.cda.net:/etc/openvpn/pki/{ca.crt,issued/fuera.crt,p
05 rivate/fuera.key} .
```

  - Copiar (mediante copia segura sobre SSH con scp) la clave secreta de autenticación de paquetes HMAC

```
01 fuera:/etc/openvpn/client$ sudo scp
02 root@firewall3.cda.net:/etc/openvpn/server/ta.key .
```

  - Crear el fichero de configuración del cliente

```
01 fuera:/etc/openvpn/client#$ sudo cp
02 /usr/share/doc/openvpn/examples/sample-config-files/client.conf .
03
```

- Editar el fichero de configuración del cliente (con "→" se señalan los cambios a efectuar)

```
01  fuera:/etc/openvpn/client$ sudo nano client.conf
```

```
    client     ## indica que es la configuración para un cliente
    dev tun    ## tipo de dispositivo de red virtual (= tarjeta de
               ## red "software") a través del cual se accederá al
               ## túnel cifrado establecido con el servidor

→   remote firewall3.cda.net 1194  ## dirección IP y puerto de
                                   ## escucha del servidor OpenVPN
                                   ## con el que se establecerá el
                                   ## túnel cifrado
    ...
→   ca /etc/openvpn/client/ca.crt ## parámetros de cifrado
→   cert /etc/openvpn/client/fuera.crt
→   key /etc/openvpn/client/fuera.key
    ...
→   tls-auth /etc/openvpn/client/ta.key 1
```

- Crear el túnel OpenVPN
  - Iniciar OpenVPN en servidor (firewall3)

```
01 firewall3:/etc/openvpn/server$ sudo systemctl restart
02 openvpn-server@server
```

  - Iniciar OpenVPN en cliente (fuera)

```
01 fuera:/etc/openvpn/client$ sudo systemctl restart
02 openvpn-client@client
```

- Comprobar el túnel creado **[Ejercicio 2]**

```
01 fuera:~$ nmap -T4 10.10.10.11  [escaneo de dentro]
02 fuera:~$ nmap -T4 10.20.20.22  [escaneo de dmz]
```

Integración del enlace OpenVPN con Shorewall:

- Preparación de Shorewall
  - Copiar los ficheros de configuración en el directorio de configuración de Shorewall (`/etc/shorewall/`)

```
01 firewall3:~#  cd /etc/shorewall
02 firewall3:/etc/shorewall# cp
03 /usr/share/doc/shorewall/examples/three-interfaces/* .
```

- Configurar las zonas

```
01 firewall3:/etc/shorewall# nano zones
```

```
#############################################################
#ZONE    TYPE    OPTIONS         IN                      OUT
#                                OPTIONS                 OPTIONS
fw      firewall
net     ipv4
loc     ipv4
dmz     ipv4
```

- Configurar los interfaces (`/etc/shorewall/interfaces`)

```
01 firewall3:/etc/shorewall# nano interfaces
```

```
#############################################################
?FORMAT 2
#############################################################
#ZONE    INTERFACE       OPTIONS
#
net     enp0s9
loc     enp0s3
dmz     enp0s8
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

- Definir el enmascaramiento (`/etc/shorewall/snat`): Indica que el tráfico de la red **10.10.10.0** y de **10.20.20.0** que pretenda salir a través del interface *enp0s9* (red externa) se "reescribirá" su dirección origen con la dirección IP del interfaz *enp0s9* (IP pública de **firewall3 (193.147.87.47)**)

```
01 firewall3:/etc/shorewall# nano snat
```

```
#############################################################################
#########################################################
#ACTION      SOURCE              DEST          PROTO   PORT    IPSEC
MARK    USER    SWITCH  ORIGDEST        PROBABILITY
#
MASQUERADE   10.10.10.0/24       enp0s9
MASQUERADE   10.20.20.0/24       enp0s9
```

- Definir las políticas (`/etc/shorewall/policy`): se fijarán unas políticas restrictivas que descartarán por defecto todo el tráfico entre las zonas definidas. En el fichero `/etc/shorewall/rules` se ajustarán las excepciones pertinentes.

```
01  firewall3:/etc/shorewall# nano policy
```

```
#############################################################################
#SOURCE         DEST            POLICY          LOG LEVEL
LIMIT:BURST
#
loc             all             DROP
net             all             DROP            info
dmz             all             DROP

# THE FOLLOWING POLICY MUST BE LAST
all             all             REJECT          info
```

- Incluir las excepciones y redirecciones en `/etc/shorewall/rules`

```
01  firewall3:/etc/shorewall# nano rules
```

```
#############################################################################
#ACTION         SOURCE          DEST            PROTO   DEST    SOURCE   ORIGINAL ...
#                                                       PORT    PORT(S)  DEST

#       Accept DNS connections from the firewall to the Internet
############### COMENTAR (no nos interesa) ################
# DNS(ACCEPT)      $FW             net
#############################################################

#       Accept SSH connections from the local network to the firewall and DMZ
SSH(ACCEPT)      loc             $FW    # Cubre parte de las restricciones 3c
SSH(ACCEPT)      loc             dmz    # Cubre parte de las restricciones 3c

. (sigue)
.
.

#############################################################################################
##
## ANADIDOS para implementar reglas de filtrado  (AÑADIR al final del fichero "rules" DESDE AQUI)
##
#############################################################################################

## Anadidos para 2a, 2b: redirec. puertos (servicios publicos: http, https, smtp, pop3) a DMZ
DNAT            net             dmz:10.20.20.22   tcp     80,443
DNAT            net             dmz:10.20.20.22   tcp     25,110


## Anadidos para 3b: acceso desde local a red externa (solo WEB y SSH)
ACCEPT          loc             net               tcp     80,443
ACCEPT          loc             net               tcp     22


## Anadidos para 3c: acceso desde local a servidores web y correo de DMZ y ssh a equipos DMZ
ACCEPT          loc             dmz:10.20.20.22   tcp     80,443
ACCEPT          loc             dmz:10.20.20.22   tcp     25,110
ACCEPT          loc             dmz               tcp     22  # No sería necesario, cubierto por una regla anterior

## Anadidos para 3d: acceso del servidor SMTP de DMZ a servidores SMTP externos para (re)envío de e-mails
ACCEPT          dmz:10.20.20.22  net              tcp     25

## Anadidos para 3e: acceso del servidor web de DMZ al servidor mysql
ACCEPT          dmz:10.20.20.22  loc:10.10.10.11  tcp     3306

## Anadidos para 3f: acceso al exterior para consultas DNS desde red interna y dmz
DNS(ACCEPT)     loc             net
DNS(ACCEPT)     dmz             net

######## NOTA: Reglas 3f equivalen a:
#ACCEPT          loc             net              tcp     53
#ACCEPT          loc             net              udp     53
#ACCEPT          dmz             net              tcp     53
#ACCEPT          dmz             net              udp     53
#####################################

## Anadidos para 3f: acceso al cortafuegos mediante SSH desde local
ACCEPT          loc             fw               tcp     22
```

- Ajustar el fichero de configuración de Shorewall (`/etc/shorewall/shorewall.conf`)

```
01  firewall3:/etc/shorewall# nano shorewall.conf
```

```
#############################################################################
#                       S T A R T U P   E N A B L E D
#############################################################################
STARTUP_ENABLED=Yes
.
.
.
```

```
##############################################################################
#                       F I R E W A L L   O P T I O N S
##############################################################################
...
IP_FORWARDING=Yes
...
```

- Configuración de la integración:
  - Crear una nueva zona (road) para los clientes conectado con OpenVPN en el fichero /etc/shorewall/zones

```
01  firewall3:/etc/shorewall$ sudo nano zones &
```

```
##############################################################################
############
#ZONE        TYPE     OPTIONS     IN            OUT
#                                  OPTIONS       OPTIONS
fw           firewall
net          ipv4
loc          ipv4
dmz          ipv4
→   road     ipv4
```

  - Asociar el interfaz tun0 a la zona road en el fichero /etc/shorewall/interfaces

```
01  firewall3:/etc/shorewall$ sudo nano interfaces &
```

```
##############################################################################
?FORMAT 2
##############################################################################
#ZONE        INTERFACE      OPTIONS
net          enp0s9
loc          enp0s3
dmz          enp0s8
→   road     tun+
```

  - Definir las políticas y reglas que afectan a los clientes OpenVPN
    - Habilitar el acceso sin restricciones a la zona interna (loc) desde los equipos que lleguen a través del túnel OpenVPN (zona road)

```
01  firewall3:/etc/shorewall$ sudo nano policy &
```

```
   ##############################################################################
   ############
   #SOURCE     DEST      POLICY     LOG LEVEL     LIMIT:BURST
   loc         all       DROP
   net         all       DROP
   dmz         all       DROP
→  road        loc       ACCEPT

   # THE FOLLOWING POLICY MUST BE LAST
   all         all       REHECT     info
```

- Replicar las entradas con origen en la zona loc, cambiando su campo origen de loc a road

```
01 firewall3:/etc/shorewall$ sudo nano rules &
```

```
   ACCEPT        road    net                  tcp         80,443
   ACCEPT        road    net                  tcp         22

   ACCEPT        road    dmz:10.20.20.22      tcp         80,443
   ACCEPT        road    dmz:10.20.20.22      tcp         25,110
   ACCEPT        road    dmz                  tcp         22

   DNS(ACCEPT)   road    net

   ACCEPT        road    fw                   tcp         22
```

- Dar de alta el túnel OpenVPN /etc/shorewall/tunnels

```
01 firewall3:/etc/shorewall$ sudo nano tunnels &
```

```
→  #TYPE                    ZONE       GATEWAY
   openvpnserver:1194       net        0.0.0.0/0
```

- Comprobar la configuración del firewall y el funcionamiento del túnel OpenVPN **[Ejercicio 3]**
  - Recompilar y arrancar el cortafuegos generado por Shorewall con las nuevas configuraciones

```
01 firewall3~$ sudo shorewall start
```

  - Reiniciar el servidor OpenVPN en firewall3

```
01 firewall3:~$ sudo systemctl restart openvpn-server@server
```

  - Reiniciar el cliente OpenVPN en fuera

```
01 fuera:~$ sudo systemctl restart openvpn-client@client
```

- Comprobar integración con Shorewall]: Repetir las comprobaciones realizadas en Ejercicio 2. ¿Qué conclusiones se pueden sacar?

Tarea 2 : Entregable (memoria)

1. Formato: PDF
2. Nombre: Practica5_(apellidos_nombre).pdf
3. Documentación a entregar:
   - Detallar la situación inicial[Ejercicio 1])
   - Detallar las comprobaciones realizadas [Ejercicio 2]
   - Detallar las comprobaciones realizadas [Ejercicio 3]