# ***PRÁCTICA 5 - VPN***

~~(no me apetece reordenarlo esta vez, xd)~~

1. Pasos previos:

a. 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)

sudo iptables -F

sudo iptables -t nat -F

sudo iptables -P INPUT ACCEPT

sudo iptables -P OUTPUT ACCEPT

sudo iptables -P FORWARD ACCEPT

(Esto hace que se acepten todos los mensajes que pasen por el firewall, ya sea para dentro, fuera o como intermediario)

■ Habilitar la redirección de tráfico.

sudo echo 1 > /proc/sys/net/ipv4/ip_forward :->Habilita el enrutamiento en firewall3

b. Escaneo desde la máquina fuera para verificar los servicios accesibles inicialmente [Tarea 1]

nmap -T4 10.10.10.11

nmap -T4 10.20.20.22

nmap -T4 193.147.87.47

2. Creación de un enlace VPN

a. Creación de la CA y de los certificados de servidor y cliente.

■ Crear la autoridad certificadora” (CA) en el firewall

cd /usr/share/easy-rsa :->Ir al directorio

sudo cp vars.example vars :-> :-> Hacer copia de vars.example

sudo nano vars :-> Copiamos en el archivo los siguientes datos

...

set_var EASYRSA_REQ_COUNTRY "ES"

set_var EASYRSA_REQ_PROVINCE "Ourense"

set_var EASYRSA_REQ_CITY "Ourense"

set_var EASYRSA_REQ_ORG "ESEI"

set_var EASYRSA_REQ_EMAIL "cda@cda.net"

set_var EASYRSA_REQ_OU "CDA"

sudo /usr/share/easy-rsa/easyrsa init-pki :->Iniciar CA

sudo /usr/share/easy-rsa/easyrsa build-ca nopass :-> Generar claves... el nombre de la CA es prueba

■ Crear el certificado del equipo ”servidor” OpenVPN.

sudo /usr/share/easy-rsa/easyrsa build-server-full firewall3.cda.net nopass

■ Crear el certificado del equipo ”cliente” OpenVPN.

sudo /usr/share/easy-rsa/easyrsa 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

sudo /usr/share/easy-rsa/easyrsa gen-dh

b. Configuración y creación del enlace OpenVPN.

■ Configuración del servidor: en la máquina firewall3, directorio /etc/openvpn/server.

cd /etc/openvpn/server/

sudo openvpn --genkey secret ta.key :-> Crear una clave secreta para la autenticación HMAC de los paquetes TLS/SSL

sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf .

sudo nano server.conf (editar las lineas visibles que aparecen)

■ Configuración de los clientes: en la máquina fuera (193.147.87.33), directorio /etc/openvpn/client

sudo /etc/openvpn/client

sudo scp root@firewall3.cda.net:/etc/openvpn/pki/{ca.crt,issued/fuera.crt,private/fuera.key} . :-> Copiar las claves de firewall al cliente

sudo scp root@firewall3.cda.net:/etc/openvpn/server/ta.key . :-> Copiar tambien las claves secretas

sudo cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf . :->Crear fichero conf clente

sudo nano client.conf :-> Editamos el fichero las lineas que se indican)

■ Crear el túnel OpenVPN

sudo systemctl restart openvpn-server@server

sudo systemctl restart openvpn-client@client

■ Comprobar el túnel creado [Tarea 2]

nmap -T4 10.10.10.11

nmap -T4 10.20.20.22

3. Integración del enlace OpenVPN con Shorewall:

a. Preparación de Shorewall

■ Copiar los ficheros de configuración en /etc/shorewall

cd /etc/shorewall

sudo cp /usr/share/doc/shorewall/examples/three-interfaces/* .

(Esto es lo mismo que configurar los ficheros del shorewall para asociar las zonas con sus respectivas reglas y políticas (como la practica de firewall de rcii)

■ Configurar las zonas

nano zones (y añadir en el fichero lo que se pide)

■ Configurar los interfaces

nano interfaces (y añadir en el fichero lo que se pide)

- Definir el enmascaramiento (conversión dirección privada↔pública)

nano snat (y añadir en el fichero lo que se pide)

- Definir las políticas restrictivas (denegación de paquetes entre zonas)

nano polity (y añadir en el fichero lo que se pide)

nano rules (y añadir en el fichero lo que se pide)

(El resto es modificar los mismos ficheros, pero esta vez para añadir el túnel cifrazo por el que se conectará con firewall3

b. Crear una nueva zona (road) para los clientes conectados con OpenVPN en el fichero /etc/shorewall/zones

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

d. Definir las políticas y reglas que afectan a los clientes OpenVPN

e. Dar de alta el túnel OpenVPN /etc/shorewall/tunnels

f. Comprobar la configuración del firewall y el funcionamiento del túnel OpenVPN [Tarea 3]