**Pràctica 2 – Accés als recursos de xarxa**

**Sessió 3 - Accés al servidor mitjançant un servei de xarxa privada virtual (VPN)**

**Marc Gamboa Martin**

**Marc Pascual Desentre**

------------------------------------------------------------------------------------------------------------------------------

- Respon a cadascuna de les següents preguntes tot seguint aquesta estructura:

- Breu raonament de la resposta.

- Comanda / menú / opció a utilitzar.

- Fitxers de configuració involucrats, si s’escau.

- Evidència d'ús.

- Bibliografia.

**1 - Servei VPN**

**- Accions i requeriments**

* Implementa un servidor i un client OPENVPN.
* Utilitza clau compartida i certificats.
* Utilitza el rang d'adreces ip 10.10.10.xx.
* Configura dos clients (1 màquina linux i 1 terminal mòbil) per verificar la connectivitat.
* Realitza les captures de xarxa que validen el bon funcionament.

**- Qüestions a respondre**

**- On es situen, en un escenari general, el servidor VPN i els clients?**

El servidor acostuma a estar situat en un lloc centralitzat, el més aprop posible de la majoria de clients. Per exemple podria ser una oficina corporativa o un centre de dades.

Els clients per altra banda poden estar dispersos per altres ubicacions preferiblement el més aprop posible del servidor VPN. Però no és necessari que estigui en un punt concret o fixa.

**- Quina és la configuració IP del servidor i els clients?**

Primerament hem de configurar tant el servidor com el client amb una IP estática per l'adaptador de xarxa principal, en el nostre cas utilitzem la IP 10.0.2.4 al servidor i la IP 10.0.2.8 per al client.

Per provar la connexió entre client i servidor farem servir la següent comanda:

Al servidor:

openvpn --remote 10.0.2.4 --dev tun1 --ifconfig 10.10.10.1 10.10.10.2

Al client:

openvpn --remote 10.0.2.8 --dev tun1 --ifconfig 10.10.10.2 10.10.10.1

Per comprovar que funciona al executar les comandes ens apareixerà el següent missatge: TUN/TAP device tun1 opened.

Podem verificar-ho si obrim una nova terminal i fem ip a podem veure com apareix la nova interfície tun1, evidencia ipa.txt.

A més si fem obrim una nova terminal a qualsevol de les dues màquines i fem un ping podem comprovar el correcte funcionament de la interfície, evidencia ping1.txt

**- Cal fer algun canvi a la configuració de routers/tallafocs? Quins?**

Per poder assegurar una connexió segura i funcional hem de configurar el firewall de tal forma que només permeti tràfic pel port UDP 1194 i el tràfic relacionat o establert, això ho farem de la següent manera:

Creem un arxiu anomenat openvpn.nft en el nostre cas ho crearem a /etc/nftables/:

nano /etc/nftables/openvpn.nft

En aquest arxiu posarem el següent:

#!/usr/sbin/nft -f

table ip filter {

chain input {

type filter hook input priority 0; policy drop;

ct state { established, related } accept

udp dport 1194 accept

# Agrega más reglas según sea necesario

}

chain forward {

type filter hook forward priority 0; policy drop;

ct state { established, related } accept

# Agrega más reglas según sea necesario

}

}

Un cop tenim l’arxiu guardem i sortim.

Ara hem de carregar les regles a nftables, això ho farem fent la següent comanda:

nft -f /etc/nftables/openvpn.nft

I per últim ens queda habilitar el reenviament de ports, això ho farem amb la següent comanda:

sysctl -w net.ipv4.ip\_forward=1

**- Com s'instal·la OPENVPN en el servidor?**

Per instalar openvpn hem d’utilitzar la següent comanda:

apt install openvpn

Un cop realitzem la comanda podem comprovar que ha estat instal·lat correctament utilitzant la comanda:

openvpn –version

Evidencia version.txt

**- Com es configura el servidor VPN? Diferencia el cas d'ús de clau compartida del de certificats digitals.**

Per tal de poder configurar el servidor VPN amb una clau compartida farem el següent, primerament a la maquina servidor, anem a /etc/openvpn i un cop aquí fem la següent comanda:

openvpn --genkey secret static.key

Un cop generada la clau, desde la maquina client farem:

scp static.key root@10.0.2.8:/etc/openvpn

Ara que ja tenim la clau tant al client com al servidor podem seguir, el següent pas serà crear el tunel, això ho farem de la següent manera, primerament dins del directori /etc/openvpn, on ja hi érem hem de fer el següent:

nano tun0.conf

Aquí dintre haurem de posar la informació pertinent al túnel VPN. En cas del client sera la que trobarem a la evidencia tun0client.txt, i en cas del servidor hem de posar el que trobem a la evidencia tun0server.txt. (En el nostre cas hem utilitzat el port 1193, ja que el port 1194 ens indica que esta ocupat i dona error).

Un cop tenim els dos arxius .conf farem la següent comanda a la maquina servidor:

openvpn --config /etc/openvpn/tun0.conf --verb 6

Un cop executem aquesta comanda el servidor podem veure que el servidor esta actiu ja que ens indica el següent:

TUN READ [48]

Ara hem d’executar la mateixa comanda del costat del client, i si obrim una terminal i fem ping podem comprovar que s’ha connectat correctament, evidencia ping2.txt  
  
**Certificat:**

Per a configurar el servidor amb certificat haurem de seguir els següents passos:

Primerament ens dirigim a /etc/openvpn i un cop aquí farem la següent comanda:

make-cadir easy-rsa/

Acte seguit ens dirigim al directori que acabem de crear amb la comanda:

cd easy-rsa/

Un cop ens situem al directori easy-rsa/ farem la següent comanda per tal d’inicialitzar l'entorn:

./easyrsa init-pki

Ara, per tal de crear un certificat d’autoritat farem:

./easyrsa build-ca

Acte seguit farem la següent comanda per crear un certificat complert al servidor (server.crt i server.key):

./easyrsa build-server-full server

El següent pas haurem de generar un “BUILD DIFFIE-HELLMAN PARAMETERS”, que ens farà falta per la connexió SSL/TLS:

./easyrsa gen-dh

Per poder continuar movem la clau que hem creat anteriorment i l’anomenem ta.key i ho posem dins del directori /etc/openvpn/server amb la comanda:

mv /etc/openvpn/static.key /etc/openvpn/server/ta.key

Acte seguit creem un certificat complet per al client al qual anomenarem marc amb la següent comanda, ho farem amb la opcio nopass perquè no ens demani contrasenya:

./easyrsa build-client-full marc nopass

Primer de tot generem la clau compartida utilitzant la següent comanda:

openvpn --genkey secret /etc/openvpn/server/ta.key

Hem de passar marc.crt, ca.crt i marc.key al client, això ho podem fer fent ús d’una carpeta compartida (com ho hem fet nosaltres)

Després configurem el servidor creant en el directori /etc/openvpn/server un fitxer de configuració server.conf, ho podem veure a la evidencia server.conf

Per tal de poder iniciar el servei OpenVPN hem d’utilitzar les següents comandes:

systemctl start openvpn-server@server

I per tal d’habilitat el servei OpenVPN i s’inici automàticament al arrancar la maquina hem de fer el següent:

systemctl enable openvpn-server@server

Primer de tot creem un log fent:

touch /var/log/openvpn/openvpn-status.log

Ara per tal d’executar el servidor farem:

openvpn –config /etc/openvpn/server/server.conf

I a la banda del el client farem aquesta altra comanda:

openvpn –config /etc/openvpn/client/client.conf

El fitxer client.conf esta explicat en la següent pregunta.

Veiem que ens deixa connectar-nos correctament, ho podem veure en el .log, evidencia openvpn-status.log

**- Com s'instal·la OPENVPN en els clients?**

En cas del client movil podem instalar-ho tant en android com en iOS, en qualsevol cas el nom de l’aplicació que hem de descarregar es OpenVPN, que la podem trobar a la Google Play Store o a la App Store dependen del sistema operatiu que estem utilitzant.

En el cas de debian el que haurem de fer es al igual que ja hem fer amb el servidor instalar el paquet OpenVPN, això ho farem amb la següent comanda:

apt install openvpn

Podem verificar que s’ha instal·lat correctament utilitzant la comanda:

openvpn –version

Evidencia version.txt

**- Com es configuren els client (Linux i mòbil)?**

Si volem configurar el client linux amb clau hem de seguir el que hem vist a l’apartat de “com configurar el servidor VPN” (ja que per demostrar-ho hem tingut que configurar també el client).

Pero, si volem configurar el client linux amb un certificat hem de seguir els següents passos, primerament al client ens dirigim a /etc/openvpn, un cop ens trobem aquí crearem un arxiu de configuració anomenat client.conf amb la següent comanda:

nano client.conf

Dintre d’aquest arxiu hem d’afegir el següent:

client

dev tun

proto udp

remote 10.0.2.4 1193

resolv-retry infinite

nobind

persist-key

persist-tun

ca /etc/openvpn/easy-rsa/pki/ca.crt

cert /etc/openvpn/easy-rsa/pki/marc.crt

key /etc/openvpn/easy-rsa/pki/private/marc.key

remote-cert-tls server

tls-auth /etc/openvpn/server/ta.key 1

auth-nocache

cipher AES-256-CBC

data-ciphers AES-256-CBC

mute-replay-warnings

verb 3

Podem veure la evidencia client.conf.

Com ja hem explicat, estem utilitzant el port 1193, ja que el port 1194 ens genera un error que impedeix continuar.

Pel client mòbil és més senzill, únicament hem de carregar el certificat generat en .ovpn a l’aplicació desde el núvol (google drive).

Podem veure que funciona en la evidencia de la configuració del server

**- Com es comprova que la configuració del servei de VPNs es correcta? Diferencieu cas d'ús de clau compartida del de certificats.**

Podem comprovar que la configuració és correcta de diverses formes, la primera es mirant el openvpn-status.log, com podem veure ens apareix tota la informació relacionada amb la connexió.

Un altre forma de poder comprovar que la configuració del servei VPN es correcta es fent un de la comanda:

systemctl status openvpn-server@server

Aquesta comanda ens mostrarà l’estat del servidor VPN i configuració relacionada amb aquest, podem vuere-ho a la evidencia openvpn-status.txt

**Fonts:**

**Wiki Debian**:

<https://wiki.debian.org/OpenVPN#OpenVPN_Overview>

**OpenVPN Community:**

<https://openvpn.net/community-resources/how-to/>