Pràctica 2 – Accés als recursos de xarxa

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

Alumnes:
Mariona Farré Tapias,
Adrian Garcia Campillo

- 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
- 1 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. (tcpdump)

- 2 Qüestions a respondre
  - 2.1 On es situen, en un escenari general, el servidor VPN i els clients?

En un escenari general, el servidor VPN sol estar ubicat en un centre de dades que ofereix alta disponibilitat, amplies connexions a Internet i altes mesures de fortes. Això pot incloure ubicacions físiques segures amb recursos com control d'accés, alimentació de reserva i connectivitat redundada per assegurar un servei constant i segur. El servidor actua com un punt central a través del qual tots els clients VPN es connecten, permetent així un control centralitzat de la política de seguretat i accés a la xarxa.
Els clients VPN poden estar situats pràcticament en qualsevol lloc del món, sempre que tinguin accés a Internet per connectar-se al servidor VPN. Això inclou treballadors remots, sucursals d'empreses, dispositius mòbils en trànsit, i fins i tot usuaris en llars particulars. La flexibilitat de ubicació dels clients és una de les principals avantatges de l'ús de VPNs, ja que proporciona accessibilitat i seguretat no importa on es trobi el client.

Evidència d'ús: 2-1.txt
Es pot veure un esquema de com seria un escenari general.

Bibliografia: Web debian opnen vpn: https://wiki.debian.org/OpenVPN

- 2. 2 Quina és la configuració IP del servidor i els clients?

Per veure la ip del servidor i del client el que farem sera fer un ping desdel movil cap a la màquina amb debian.
Capturarem el tràfic amb tcpdump.
A les captures podrem veure com la ip 192.168.1.49 (ip del móvil) fa una petició a la ip 192.168.1.229 (ip de la màquina) o la ip 192.168.2.100 (ip de la màquina servidor en els següents exercicis)

Evidència d'ús: 2-2.txt
Es pot veure l'execució de les comandes anteriors.
Es pot veure que es un mòbil perque hi ha un paquet de spotifiy: `_spotify-social-listening._tcp.local. (54)` Assegurant que es pot establir una connexió entre el mòbil i el servidor.

Bibliografia: Web debian opnen vpn: https://wiki.debian.org/OpenVPN

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

Si com en el nostre cas el servidor és una màquina debian, es poden fer diferents canvis en els routers i possibles tallafocs que tinguem en la xarxa.
Es important fer un renviament dels ports per aquest específic protocol, la configuració del servidor Openvpn es realitza en el fitxer: server.conf
On es especificar el port el qual el servidor Openvpn ha d'escoltar, així que modificar executar: root@seax1:# nano /etc/openvpn/server/server.conf
posant en el fitxer: port 1194

Fer que el server pugui fer un renviament de paquets IP entre els interfícies de xarxa, en el fitxer /etc/sysctl.conf descomentar la següent línia:
net.ipv4.ip_forward = 1
I aplicar els canvis executant:: root@seax1:# sysctl -p

També es necessari configurar les regles del tràfic del VPN pel servidor OpenVPN, per això utilitzarem l'eina: nfttables
Si aquesta no està instalada instalar amb: root@seax1:#apt install nftables
Es pot comprovar que esta instalada executant la següent comanda, on ens retorna totes les regles configurades: root@seax1:# nft list tables
En el nostre cas, no ens retorna res ja que no tenim cap regla o taula especificada amb nftables.
Per configurar una nova regla per el servidor OpenVPN, s'han de crear les taules i regles necessàries:
root@seax1:# nft add table ip filter
root@seax1:# nft add chain ip filter input {type filter hook input priority 0 \; }
root@seax1:# nft add rule ip filter input ct state new udp dport 1194 accept

Comprovar amb: root@seax1:# nft list chain ip filter input
On si esta configurat malament no sortirà res, però si sha fet correctament sortirà la cadena 1194 creada correctament.

Fitxers involucrats:

- server.conf

Tenir configurat correctament el renviament de ports, en el cas del OpenVPN port: 1194

```
…
 local 192.168.2.100
port 1194
proto udp
…
```

- /etc/sysctl.conf

Descomentar la següent línia:

```
net.ipv4.ip_forward = 1
```

Evidència d'ús: 2-3.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian opnen vpn: https://wiki.debian.org/OpenVPN
Instalar openvpn debian:
https://www.webhi.com/how-to/how-to-install-openvpn-server-on-linux-debian-11-12/

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

Per instal·lar OpenVPN en la màquina servidor fer:
Actualitzar la màquina executant: root@seax1:# apt update
Descarregar el paquet de openvpn per debian, executant:
root@seax1:# apt install openvpn
Triar interfície estàtica, decidir quina interfície de xarxa utilitzarà OpenVPN com a punt d'entrada/sortida. En aquest cas, has triat la interfície estàtica enp0s8 amb l'adreça IP 192.168.2.100.
Crea un fitxer de configuració per al servidor OpenVPN manualment en la ruta /etc/openvpn/server/server.conf.
executant: root@seax1:# nano /etc/openvpn/server/server.conf
Aqui es on s'introduiran i modificaran les opcions de configuració necessàries, com ara la localització, el port, els certificats, les claus, etc.

Abans d'iniciar el OpenVpn, shan de crear vàries coses:
Crear Diffie-Hellman, aquests paràmetres són essencials per a l'establiment de la connexió VPN segura. Aquest procés genera els paràmetres DH que s'utilitzaran per a l'intercanvi de claus durant l'iniciació de la connexió. Això permet la generació compartida de claus segures entre el servidor i els clients.
root@seax1:# openssl dhparam -out /etc/openvpn/server/dh.pem 2048

Easy-RSA és una eina que facilita la gestió de certificats i claus en una infraestructura de claus pública (PKI). Amb aquesta eina, es poden crear i gestionar els certificats de manera fàcil i segura.
Instalar els paquets easy-rsa:
root@seax1:#: apt-get install easy-rsa

Inicialitzar la infraestructura de les claus públiques PKI (Public Key Infrastructure) utilitzant Easy-RSA: i directori de treball on es guardarà tota la informací relacionada amb els certificats i les claus:
root@seax1:#:/usr/share/easy-rsa/easyrsa init-pki

Crear una nova Autoritat de Certificació (CA) utilitzant Easy-RSA. La opció nopass indica que no es demanarà una contrasenya per a la CA. La CA és responsable de signar els certificats del servidor i dels clients.
root@seax1:#: /usr/share/easy-rsa/easyrsa build-ca nopass

Crear un certificat i una clau per al servidor VPN. Utilitza el nom server per al certificat. La opció nopass indica que no es demanarà una contrasenya per al certificat del servidor.
root@seax1:#: /usr/share/easy-rsa/easyrsa easyrsa build-server-full server nopass

Això generarà el certificat i la clau del servidor, nomenats server.crt i server.key, respectivament.

Generar els paràmetres Diffie-Hellman utilitzats per a l'establiment de la connexió VPN segura. Aquests paràmetres són importants per a la seguretat de la connexió.
root@seax1:#: /usr/share/easy-rsa/easyrsa gen-dh

Finalment, Copiar els fitxers generats a la carpeta d'OPENVPN:
root@seax1:#: cp pki/ca.crt /etc/openvpn/server/
root@seax1:#: cp pki/issued/server.crt /etc/openvpn/server/
root@seax1:#: cp pki/private/server.key /etc/openvpn/server/
root@seax1:#: cp pki/dh.pem /etc/openvpn/server/

Protegir la clau del server: root@seax1:#: chmod 600 /etc/openvpn/server/server.key

Finalment configurar el fitxer del server.conf a la nostra necessitat, en el nostre cas ho hem fet seguint els requisits donats:

- local 192.168.2.100:Indica la IP del servidor OpenVPN.
- port 1194: Especifica el port UDP al qual el servidor escoltarà les connexions entrants dels clients.
- proto udp: Utilitza el protocol UDP per a les connexions VPN.
- dev tun: Utilitza l'interfície de xarxa virtual TUN per a les connexions VPN.
- ca /etc/openvpn/server/ca.crt: Indica la ruta del fitxer del certificat de l'Autoritat de Certificació (CA) utilitzat per autenticar els clients.
- cert /etc/openvpn/server/server.crt: Indica la ruta del fitxer del certificat del servidor.
- key /etc/openvpn/server/server.key: Indica la ruta del fitxer de la clau privada del servidor.
- dh /etc/openvpn/server/dh.pem: Indica la ruta del fitxer dels paràmetres Diffie-Hellman utilitzats per a l'establiment de la connexió segura.
- server 10.10.10.0 255.255.255.0: Especifica la configuració del servidor VPN amb l'adreça de xarxa 10.10.10.0 i la màscara de subxarxa 255.255.255.0.
- ifconfig-pool-persist ipp.txt: Guarda de forma persistent la assignació d'adreces IP als clients en el fitxer ipp.txt.
- push "redirect-gateway def1 bypass-dhcp": Empenta la configuració de l'encaminament VPN als clients per redirigir tot el trànsit de xarxa a través de la connexió VPN.
- push "dhcp-options DNS 8.8.8.8": Empenta la configuració dels servidors DNS als clients.
- keepalive 10 120: Manté viva la connexió VPN amb pings cada 10 segons i es tanca si no hi ha resposta durant 120 segons.
- cipher AES-256-CBC: Utilitza l'algoritme de xifrat AES amb una clau de 256 bits per a la comunicació VPN.
- user nobody: Especifica l'usuari sota el qual s'executarà el servidor OpenVPN per motius de seguretat.(en aquesta practica no cal)
- group nogroup: Especifica el grup sota el qual s'executarà el servidor OpenVPN per motius de seguretat. (en aquesta practica no cal)
- persist-key: Manté la clau privada del servidor en memòria després de l'arrencada.
- persist-tun: Manté l'interfície TUN en memòria després de l'arrencada.
- status openvpn.status.log: Indica la ruta del fitxer de registre de l'estat del servidor OpenVPN.
- verb 3: Estableix el nivell de verbositat del registre del servidor OpenVPN a 3, que és moderat.

Fer un reset de openvpn:
root@seax1:#: systemctl restart openvpn
root@seax1:#: systemctl restart openvpn@server

També es pot iniciar automàticament executant.
root@seax1:#: systemctl enable openvpn@server
root@seax1:#: systemctl start openvpn@server

Comprovar que la configuració és correcte amb la comanda:
root@seax1:#: openvpn --config /etc/openvpn/server/server.conf

Iniciar servidor nova configuració: root@seax1:#: openvpn --config /etc/openvpn/server.conf
Executar en segona banda:
root@seax1:#: openvpn --config /etc/openvpn/server.conf --dameon

Comprovar que el funcionament és correcte executant: root@seax1:#: systemctl status openvpn, que sortirà active si tot esta correctament configurat.

Fitxers involucrats:

- server.conf

Tenir configurat correctament el server OpenVPN:
root@seax1:#: cat /etc/openvpn/server.conf

```
local 192.168.2.100
port 1194
proto udp
dev tun
topology subnet
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/server.crt
key /etc/openvpn/server/server.key
dh /etc/openvpn/server/dh.pem
server 10.10.10.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-options DNS 8.8.8.8"
keepalive 10 120
data-ciphers AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305
;user nobody
;group nogroup
persist-key
persist-tun
status openvpn.status.log
verb 3
```

Evidència d'ús: 2-4.txt
Es pot veure l'execució de les comandes anteriors.
Si tot això es correcte, en el ip show de la màquina servidor, sortirà una nova interfície anomenada: tun0

La sortida de la interfície virtual tun0 del servidor OpenVPN. Aquesta interfície té una adreça IP (10.10.10.1) i una adreça IP del punt final (10.10.10.2) per a la connexió VPN punt a punt. Utilitza el protocol UDP i té una MTU de 1500. La disciplina de cues és fq_codel, amb una longitud de cua de 500. La interfície està activa i no té connexió física associada.

Bibliografia: Web debian opnen vpn: https://wiki.debian.org/OpenVPN
Instalacio de openvpn en debian:
https://www.webhi.com/how-to/how-to-install-openvpn-server-on-linux-debian-11-12/
Certificats digitals open vpn:
https://openvpn.net/community-resources/setting-up-your-own-certificate-authority-ca/

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

La configuració del servidor VPN implica establir les opcions de xarxa, seguretat i autenticació a través del fitxer de configuració del servidor OpenVPN (server.conf). Diferenciar el cas d'ús de clau compartida del de certificats digitals implica comprendre les diferències en l'autenticació i la seguretat que ofereixen.

Configuració amb clau compartida:
Es genera una clau compartida única, que es comparteix tant pel servidor com pels clients per autenticar-se mútuament durant l'establiment de la connexió VPN.

root@seax1:#: openvpn --genkey secret /etc/openvpn/server/ta.key
Per configurar dins del servidor al fitxer server.conf, s'especificar la ruta de la clau compartida utilitzant el paràmetre tls-auth per millorar la seva seguretat en el TLS:

```
tls-auth /etc/openvpn/server 0
```

Els clients també han d'incloure la mateixa clau compartida en els seus fitxers de configuració, aquesta clau ha de ser traspassada de manera segura, nosaltres utilitzarem scp:
root@seax1:#: scp /etc/openvpn/server/ta.key
root@192.168.2.100:/etc/openvpn/client/client1/
I en la seva configuració client1.conf també posar els paràmetres de tls-auth, però ara amb un 1 per senyalar que és client:

```
tls-auth /etc/openvpn/client/client1/ta.key 1
```

Per la configuració amb el client mòbil s'haurà de passar en mail.

Configuració amb certificats digitals:
Es crea un conjunt de certificats digitals, incloent un certificat per al servidor i certificats únics per a cada client.
Com s'ha fet anteriorment en el punt 2.4 la generació d'aquests fitxers s'ha d'indicar al fitxer server.conf la ruta del certificat del servidor (cert) i la clau privada (key). També s'especifica la ruta del certificat d'autoritat de certificació (CA) utilitzat per verificar la identitat dels clients.
Per configurar dins del servidor al fitxer server.conf, s'especificar la ruta dels certificats:

```
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/server.crt
key /etc/openvpn/server/server.key
```

Com s'ha farà en el punt 2.6 la generació d'aquests fitxers, els clients hauran de tenir els seus propis certificats digitals, incloent un certificat signat per l'autoritat de certificació (CA) i la seva pròpia clau privada.

ca /etc/openvpn/client/client1/ca.crt
cert /etc/openvpn/client/client1/client1.crt
key /etc/openvpn/client/client1/client1.key

Per la configuració amb el client mòbil s'haurà de passar en mail.

La configuració d'OpenVPN amb clau compartida és fàcil de configurar i gestionar, però és menys segura perquè si la clau s'obté de manera il·lícita, tots els usuaris es veuen afectats. En canvi, la configuració amb certificats digitals és més complexa i requereix una gestió més detallada, però ofereix major seguretat al permetre una verificació individualitzada del servidor i dels clients, a més de la capacitat de revocar certs sense afectar tota la xarxa.

Fitxers involucrats:

- server.conf

Per la clau compartida introduir:

tls-auth /etc/openvpn/server 0

Pels certificats digitals introduir:

ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/server.crt
key /etc/openvpn/server/server.key

- client.conf

Per la clau compartida introduir:

tls-auth /etc/openvpn/client/client1/ta.key 1

Pels certificats digitals introduir:

ca /etc/openvpn/client/client1/ca.crt
cert /etc/openvpn/client/client1/client1.crt
key /etc/openvpn/client/client1/client1.key

Evidència d'ús: 2-5.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian open vpn: https://wiki.debian.org/OpenVPN
Clau compartida open vpn: https://openvpn.net/community-resources/static-key-mini-howto/
Certificats digitals open vpn:
https://openvpn.net/community-resources/setting-up-your-own-certificate-authority-ca/

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

En el servidor de OpenVPN, s'ha de configurar el fitxer de configuració del client, per això crear el fitxer client.ovpn /etc/openvpn/client/client-mobil.ovpn
Aqui es on s'introduiran i modificaran les opcions de configuració necessàries, com ara la localització, el port, els certificats, les claus, etc.
Com en el servidor, haurem de crear els diferents certificats i claus necessaris per configurar un client OpenVPN (ca.crt, client.crt, client.key)

Donem per suposat que ja sha fet el pas 2-4.txt on es crea amb EasyRSA el servidor i els fitxers server.crt, server.key i dh.pem

Tenint ja la CA, només generar els certificats i claus per cada client:
En el nostre cas client1:
root@seax1:#: /usr/share/easy-rsa/easyrsa build-client-full client1 nopass
Fer-li la seva carpeta per guardar tots els certificats digitals i la seva configuració:
root@seax1:#: mkdir -p /etc/openvpn/client/client1

Copiar tots els certificats digitals en la seva carpeta:
root@seax1:#: cp /scripts/pki/issued/client1.crt /etc/openvpn/client/client1/
root@seax1:#: cp /etc/openvpn/server/ca.crt /etc/openvpn/client/client1/
root@seax1:#:cp /scripts/pki/private/client1.key /etc/openvpn/client/client1/

Protegir la clau del client: root@seax1:#: chmod 600 /etc/openvpn/client/client1/client1.key
root@seax1:#: chown root:root /etc/openvpn/client/client1/client1.key

Finalment configurar el nou fitxer de configuració del client1, en el nostre cas per una connexió amb un mòbil:
root@seax1:#: nano /etc/openvpn/client/client1/client1-mobil.ovpn

Introduir la següent configuració:

- client: Indica que aquest sistema serà un client OpenVPN.
- dev tun: Especifica el dispositiu de xarxa a utilitzar, en aquest cas, tun per a túnels.
- proto udp: Defineix el protocol de transport, en aquest cas, UDP.
- remote 192.168.2.100 1194: Indica la direcció IP i el port del servidor OpenVPN al qual es connectarà el client.
- resolv-retry infinite: Especifica el comportament de resolució de DNS en cas de fallada de connexió.
- nobind: Evita que el client es vinculi a una adreça IP o port específic.
- persist-key: Indica que s'han de mantenir les claus en cas de reconfiguració.
- persist-tun: Similar a persist-key, però per al dispositiu de xarxa (tun).
- ca /etc/openvpn/client/client1/ca.crt: Especifica la ruta de l'arxiu de certificat d'autoritat (CA) utilitzat per verificar l'autenticitat del servidor.
- cert /etc/openvpn/client/client1/client1.crt: Ruta de l'arxiu de certificat del client.
- key /etc/openvpn/client/client1/client1.key: Ruta de l'arxiu de clau privada del client.
- remote-cert-tls server: Requereix que el servidor presenti un certificat vàlid per a l'autenticació.
- cipher AES-256-CBC: Defineix l'algorisme de xifrat a utilitzar.

- comp-lzo: Habilita la compressió LZO per millorar l'eficiència de la transferència de dades.
- verb 3: Estableix el nivell de detall dels registres (verbosity) a 3, la qual cosa significa registres detallats.
- redirect-gateway def1: Redirigeix tot el trànsit a través del túnel VPN.
- dhcp-option DNS 8.8.8.8: Especifica el servidor DNS que s'utilitzarà mentre es connecta al túnel VPN. En aquest cas, s'està utilitzant el servidor DNS de Google (8.8.8.8).

Per activar el openvpn client fer:
root@seax1:#: openvpn --config /etc/openvpn/client/client1/client1-mobile.ovpn --daemon

Per mirar el seu estat executar: root@seax1:#: systemctl status openvpn@client1

Fitxers involucrats:
- client-mobil.conf

root@seax1:#: cat /etc/openvpn/client/client1/client1-mobil.ovpn

```
client
dev tun
proto udp
remote 192.168.2.100 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca /etc/openvpn/client/client1/ca.crt
cert /etc/openvpn/client/client1/client1.crt
key /etc/openvpn/client/client1/client1.key
remote-cert-tls server
data-ciphers AES-256-GCM:AES-128-GCM:CHACHA20-POLY1305
verb 3
redirect-gateway def1
dhcp-option DNS 8.8.8.8
```

Evidència d'ús: 2-6.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian open vpn: https://wiki.debian.org/OpenVPN

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

La configuració del client implica establir les rutes cap als fitxers de certificats i claus necessaris, així com ajustar les opcions específiques de connexió com ara el servidor a connectar i les opcions de xarxa. En dispositius mòbils, aquest procés sovint es simplifica a través de l'ús d'aplicacions específiques que gestionen aquests ajustos.
En Linux, editaríem el fitxer de configuració manualment amb un editor de text:
“sudo nano /etc/openvpn/client/client.conf”

Aplicacio en mobil

Per instal·lar OpenVPN en un dispositiu mòbil iOS, seguirem aquests pasos:
Descarreguem l'aplicació OpenVPN Connect des de l'App Store
Obrim l'App
Cerquem "OpenVPN Connect" i descarreguem l'aplicació.
Configurem el client OpenVPN Connect amb els fitxers de configuració del servidor: (certificats, claus, fitxers de configuració).
Enviem aquests fitxers al teu dispositiu iOS (per exemple, a través de correu electrònic, AirDrop o transferència de fitxers mitjançant iTunes).
Obrim l'aplicació OpenVPN Connect.
Importem els fitxers de configuració.
Després d'importar tots els fitxers de configuració necessaris, t'apareixeran a la pantalla principal de l'aplicació OpenVPN Connect.
Senyalitzem el perfil del servidor OpenVPN al qual volem connectar.
Si es requereix autenticació, introduim les credencials (nom d'usuari i contrasenya).
Un cop connectat, veurem una icona de connexió activa a la barra de notificacions del teu dispositiu.
Podem verificar la connexió accedint a recursos de xarxa a través de l'aplicació o navegador del teu dispositiu.

Fitxers involucrats:
Per a Linux: /etc/openvpn/client/client.conf o un fitxer .ovpn proporcionat pel servidor VPN.
Per a dispositius mòbils: un fitxer .ovpn que es pot importar a l'aplicació d'OpenVPN.

Bibliografia: Web debian open vpn: https://wiki.debian.org/OpenVPN

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

La verificació de la configuració es basa en assegurar-se que tots els paràmetres i fitxers de configuració són correctes i que el servei es pot iniciar sense errors. A més, cal confirmar que la connectivitat entre el client i el servidor és operativa. El mètode de clau compartida utilitza una única clau simètrica, mentre que l'ús de certificats implica una infraestructura de clau pública amb certificats i claus privades individuals per a cada usuari i el servidor.

Per comprovar el correcte funcionament de la nostra vpn utilitzarem les següents comandes:
systemctl status openvpn
openvpn --config /etc/openvpn/server/server.conf

També podem mirar si tenim la interfaç tun0, la cual funciona quan tenim la vpn en funcionament.

Fitxers involucrats:
/etc/openvpn/server/server.conf per al servidor.
/etc/openvpn/client/client.conf per als clients.
Fitxers de clau i certificats especificats dins aquests fitxers de configuració, com ca.crt, server.crt, server.key, i ta.key per tls-auth.

Evidència d'ús: 2-8.txt
Es pot veure l'execució de les comandes anteriors.

Bibliografia: Web debian open vpn: https://wiki.debian.org/OpenVPN

- Lliura els resultats mitjançant Atenea (2 fitxers).
  - Fitxer 1: Redactar l'informe de la pràctica p2_s2_cognom1_nom.txt.
  - Fitxer 2: Realitzar les proves necessàries per justificar els resultats i encapsular els fitxers necessaris en el fitxer p2_s3_cognom1_nom.zip.
