IURRETA INSTITUTUA
Goi-mailako Lanbide-Heziketako Berariazko Institutua

EUSKO JAURLARITZA
GOBIERNO VASCO
HEZKUNTZA UNIBERTSITATE ETA IKERKETA SAILA
DEPARTAMENTO DE EDUCACIÓN, UNIVERSIDADES E INVESTIGACIÓN

OpenVPN

Tunel Zifratuak Eskolara

Bertsioa: 1.0.1

Alfredo Barrainkua Zallo

2009.eko Abendua

Aurkibidea

1. Sarrera....3
2. TUN / TAP....4
2.1. Zer da bridging?....4
2.2. Zein da bridgingi eta routing arteko ezberdintasuna?....4
2.2.1. Bridging-aren abantailak....4
2.2.2. Bridging-aren desabantailak....4
2.2.3. Routing-aren abantailak....4
2.2.4. Routing-aren desabantailak....5
2.2.5. Ezberdintasunak konfigurazio mailan....5
3. Suhesia konfiguratzen....6
4. Zerbitzaria....9
4.1. Zerbitzaria instalatzen....9
4.2. Zerbitzariaren ziurtagiria sortzen....9
4.3. Zerbitzaria Konfiguratzen....10
4.4. OpenVPN erabiltzaileak sortzen....11
5. Erabiltzaileen ziurtagiriak sortzen....13
6. Bezeroak....15
6.1. Mac OSX....15
6.2. Windows....16
6.3. Ubuntu Linux....18
7. Egiteke....21
8. Egilea....22
9. A Eranskina. Aginte ziurtagiri-emailea sortzen....23

1. Sarrera

Gero eta ohikoagoa ikusten da erabiltzaileek edozein tokitatik atzitzea enpresaren sarea. Errepidean dabiltzan langileek (**Road Warriors**) bezeroen sareetatik edo hoteletatik euren enpresetako sareakatzitzen dituzte, eskabideak betetzeko, salneurriak kontsultatzeko, katalogoak jaisteko, etab.

Sarrera hau erosoa izan behar da. Sarean bertan egongo balira bezala aurkitu behar dute lan egiteko aukera izan behar dute. Bestalde, enpresek segurtasun neurriak mantendu behar dituzte.

Guzti hau ahalbidetzen duen teknologia **VPN**a da. VPNen bitartez, informazio guztia enkriptatuta garraiatzen da. Enpresako ordenagailuak (normalean eramangarriak) baino ezin dira sartu, eta gainera, erabiltzaileak kautotu behar dira. Sarritan, "**tunnel**" esaten zaie VPNei, zeren informazioa tunelaren alde batetik bestera baino ez doa. Ezin daiteke kanpotik ikusi.

VPNak egiteko era ezberdinak daude. Hemen erabiliko denak **SSL/TLS** teknologia erabiltzen du informazioa enkriptatzeko. Produktu hau **OpenVPN** da. Gogoratu behar da teknologia honekin eginiko VPNak aplikazio mailakoak direla.

/dev/tun gailua A konputagailuan eta **/dev/tun** gailua B konputagailuan konektatzeko **OpenVPN**-k erabiltzen duen mekanismoa honakoa da: zifraturiko **UDP** (TCP) konexio bakarra sortzen du Internet-en bidez, A eta B konputagailuen artean, eta trafikoa birbidali egiten du A eta B makinen artean. **TUN** eta **TAP** interfazeen diseinu berezia dela eta, posible da erabiltzaile espazioan dagoen programa batek lotura hau ezartzea. Horrela, **OpenVPN**, plataforma-arteko "**portablea"** den ***deabru*** bihurtzen da, **SSH** bezala, eta ez erabiltzaile-sistema baten modulu espezifiko, **IPSec** bezala.

Apunte hauetan, **GNU/Debian Linux 4.0** (Etch) erabiliko da **OpenVPN** zerbitzari bezala eta Windows, Mac OSX eta Ubuntu bezero bezala,. Windows bezeroek Win2000, WinXP, WinVista edo Win7 izan behar dute.

2. TUN / TAP

TUN gailua, puntuz-puntuko IP lotura birtuala da. TAP gailua ordea, ethernet gailu birtuala. Ezin daitezke nahasi. Bata edo bestea erabili behar dira konexioaren bi muturretan. Beraz, ezin daitezke jarri **-dev-tun** eta **-dev-tap** konexioaren muturretan. Bietariko bat erabili behar da.

2.1. Zer da bridging?

Teknika honekin, eremu zabaleko ethernet LAN bat sortzen da, azpisare batean funtzionatzen duena. Informazio praktiko gehiago nahi izanez gero, Ethernet Bridging Mini-HOWTO ikus daiteke.

2.2. Zein da bridgingi eta routing arteko ezberdintasuna?

Bridging eta routing, VPN bitartez sistemak lotzeko metodo bi dira.

2.2.1. Bridging-aren abantailak

- Broadcast mezuak VPN osora garraiatzen dira. Honela, ahalbidetzen da LAN broadcast-ek behar dituzten softwareak, hau da: Windows NETBIOS fitxategi konpartitzea eta sare bilaketak, funtzionatzea.
- Ez dago bideraketa konfiguratu beharrik.
- Ethernet-ean funtziona dezakeen edozein protokolorekin funtziona dezake, Ipv4, Ipv6, Netware IPX, AppleTalk, etab.
- Oso konfigurazio erraza du Road Warriors-entzat.

2.2.2. Bridging-aren desabantailak

- Ez da routing-a bezain eraginkorra eta ez da hain ongi eskalatzen.

2.2.3. Routing-aren abantailak

- Eraginkortasuna eta eskalabilitatea.

- MTUaren afinazio hobea ahalbidetzen du, eta horrela, eraginkortasuna.

2.2.4. Routing-aren desabantailak

- Bezeroek, WINS zerbitzaria erabili behar dute sare-arteko bilaketak funtziona dezan. Adibidez, Samba erabiliz.

- Bideak jarri behar dira sare guztiak lotzeko.

- Broadcast-aren menpekotasuna duen softwareak ez ditu ikusiko VPNaren sareko beste aldeko makinak.

- Normalean, soilik funtzionatuko du Ipv4-arekin, eta kasu berezietan IPv6, konexioaren bi muturretako TUN driver-rek, esplizitoki onartzen badute.

2.2.5. Ezberdintasunak konfigurazio mailan

Bezeroa urruneko sare batera bridge bitartez konektatzen denean, urruneko ethernet sareko IP helbide bat esleitzen zaio, eta beraz, gai da urruneko makinekin konektatzeko, lokalki konektatuta balego bezala. Bridging ezarpenak, sistema eragileko tresna berezi bat behar dute lotzeko ethernet portu fisikoa eta TAP gailua. Linux-ean adibidez, tresna hori, **brtcl** da. Windows XP-ean, aukeratu zuten TAP-Win32 gailua eta ethernet txarteleko **Control Panel -> Network Connections** aukeran eskuineko botoiarekin klikatu eta aukeratu **Bridge Connections**.

Bezero bat konektatzen denean routing bidez, bere azpisare propioa erabiltzen du, eta bideraketa ezartzen da, bai bezeroan eta bai zerbitzarian. Honela, paketeek VPN-a zeharkatzen dute. Bezeroa ez da zertan makina bat izan behar. Makina anitzeko sarea izan daiteke.

Bridging eta routing, funtzionalki, oso antzekoak dira. Ezberdintasun nagusia: bideratutako (Routing) VPNak ez ditu zabaltzen IP broadcast mezuak eta Bridged VPN-ak bai.

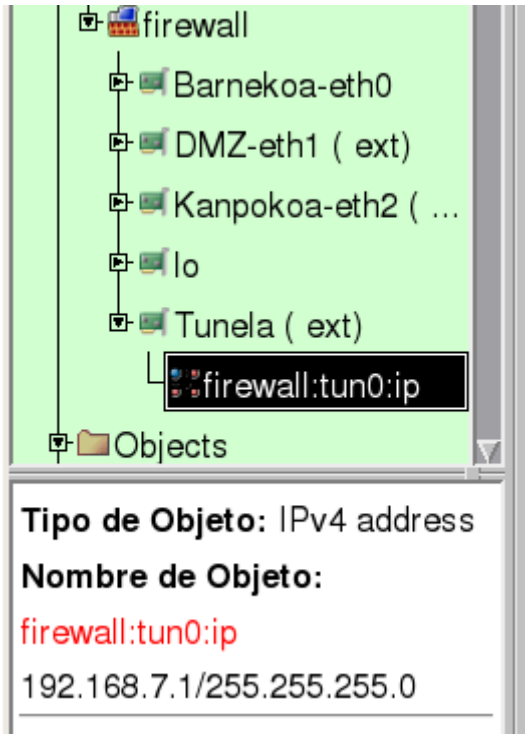
Bridging egiten denean, beti erabili behar da **-dev tap** konexioaren mutur bietan. Routing egiten bada, **-dev tap** edo **-dev tun**, erabil daiteke, baina berdina erabili behar da konexioaren mutur bietan. **-dev tun** pixka bat eraginkorragoa da bideraketaren kasurako.

3. Suhesia konfiguratzen

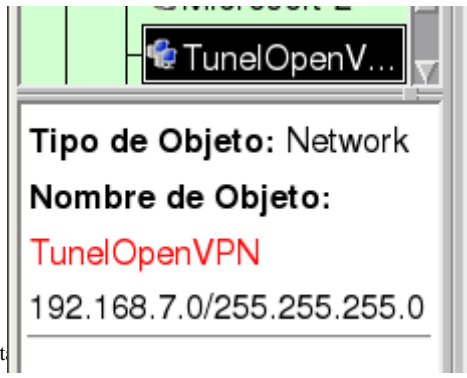
Komunikazioak ahalbidetzeko VPN sarearen eta eskolako sareen bitartean, **FWBuilder**-en konfigurazioa aldatu behar da. FWBuilder 2.0.9 eta 2.1.19 bertsioekin egingo dugu.

VPNaren sarea **192.168.7.0/24** da. Sare honi utzi egingo zaio gure interfaze publikotik sartzen. Hori, Interfazearen fitxan egin behar da. Gero, baimendu egingo da sare hotatik, barne sareetara eta DMZra konexioa, beharrezkoak ditugun protokoloentzat.

Interfasea, sarea, errglak etab. Zehaztuko ditugu FWBuilder 2.0.9 aplikazioan.

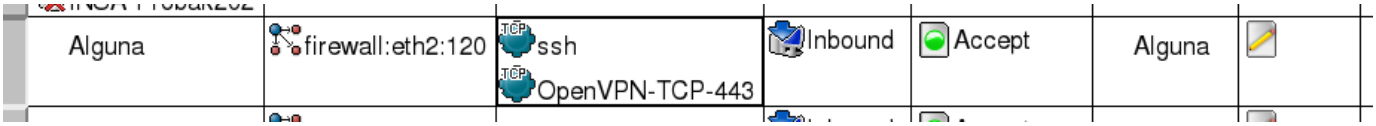


Suhesiaren interfasea zehaztua.

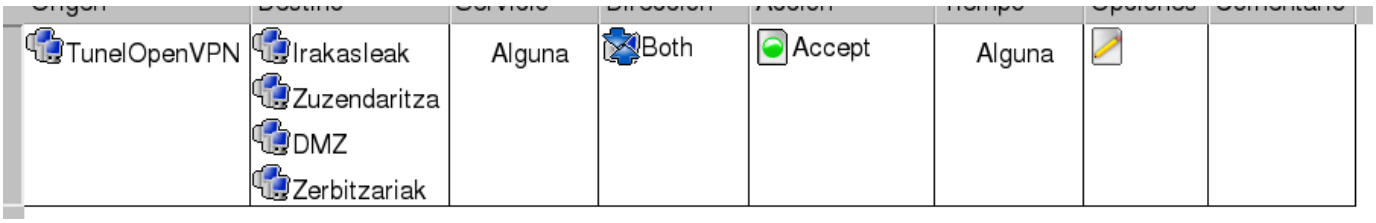


Iurret 88 00

VPNrako den 192.168.7.0/24 sarea zehaztu dugu.

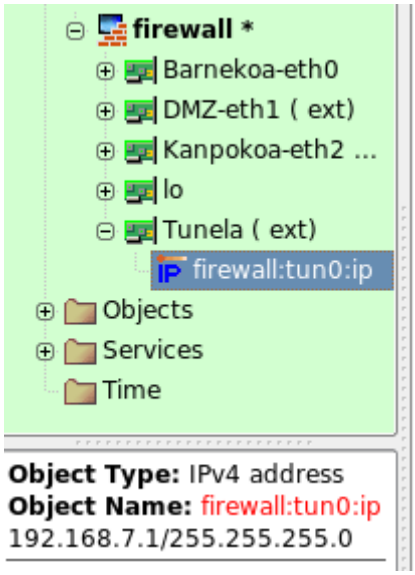


Konpotik atzipena suhesiaren openvpn-k eta ssh-k (lehendik zegoen) erabiliko duten IP helbiderara.

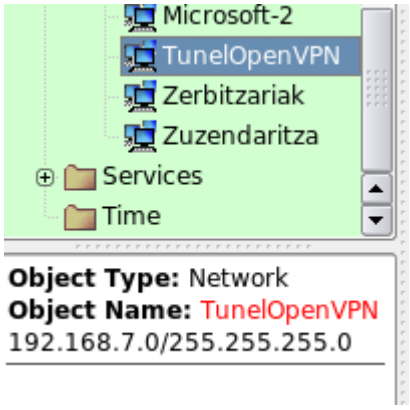


Tunelaren interfasetik konexio baimenak.

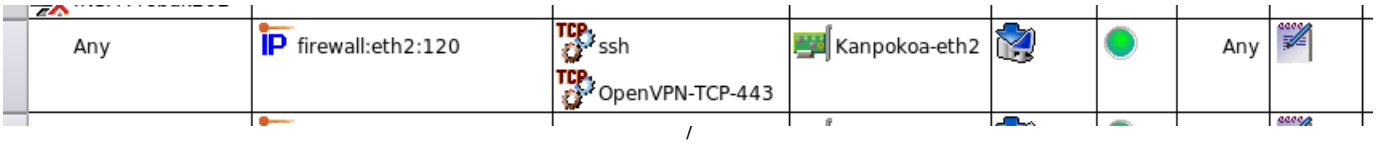
FWBuilderren 2.1.19 bertsioarekin ere, gauza bera egingo dugu. Bertsiko honetak, ez dira sortzen interfaseen fitxak. Politiken fitxan sartzen dira, baina bertan, zein interfaseri dagokion zehazten da.



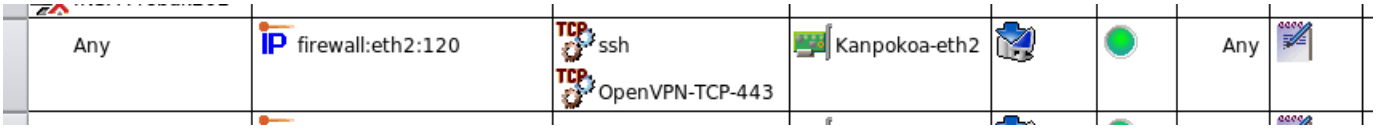
Suhesiaren interfasea.



Tunelaren sarea zehaztua.



Kanpotik konektatzeko baimenak zehaztuak.



Tunelaren komunikazio politikak zehaztuak.

Zehatzago egin daitezke gauzak. Adibide bat soilik da hau, eta segurtassuna administratzaile bakoitzaren ardura da. Beste era bnatzuetan ere egin daiteke lan hau. Adibidez, tunelaren interfasea sortu gabe. Kasu honetan, politikak ez dagokizkio tunelaren interfaseari, baizik eta orokorrak izanen lirateke.

4. Zerbitzaria

Zerbitzaria, **GNU/Linux Debian 4.0 (Etch)** sistema bat izango da. Erabiltzaileek, ziurtagiri baten beharra izango dute, eta gainera, euren erabiltzaile izena eta pasahitza sartu beharko dute.

VPN kanalerako, **TUN** interfaze bat erabiliko da. Ez badu bridge eran funtzionatu behar, ez bada erabiltzen sareko lokaleko DHCP zerbitzaria IP helbideak banatzeko, edo ez bada erabili behar broadcast mezurik, hobe da TUN interfazea erabiltzea. Gaur egun, Windows sistemek ere, **DNS** zerbitzua erabiltzen dute zerbitzariak eta zerbitzuak bilatzeko. Hau dela eta, ez dago hainbat broadcast mezuren beharra. OpenVPN konexioen sarea eta eskolako barneko sareen arteko bideraketa suhesian burutuko da.

4.1. Zerbitzaria instalatzen

OpenVPN erabiltzeko eta ziurtagiriak sortzeko, hurrengo paketeak instalatu behar dira:

```
aptitude install vtun openssl liblzo2-2 openvpn
```

4.2. Zerbitzariaren ziurtagiria sortzen

A eranskinean sortu den autoritate ziurtagiri-emailearekin sortuko da zerbitzariaren ziurtagiria. Ziurtagiria suhesiarentzat izango da, eta beraz, **fw-cert.pem** izena izango du.

```
cd /etc/zertifikatuak
openssl req -new -days 1095 -keyout fw-key.pem -out fw-req.pem
```

Lehenetsitako baloreak aukeratu behar dira. Gero, eskatuko da erabiltzailearen izena "**Common Name**", eta "**suhesia.iurreta-institutua.net**" sartuko da. Gero, honen posta helbidea eskatuko da. "**sare-admin@iurreta-institutua.net**" sartuko da.

Sinatu egingo da ziurtagiri eskabidea, sortutako autoritate ziurtagiri-emailearen bitartez. Honen gako pribatuaren pasa-esaldia eskatuko da. Zertifikatu agintearen pasahitza eskatuko digu. Sartu.

```
openssl ca -policy policy_anything -out fw-cert.pem -in fw-req.pem
```

Orain, pasahitza kendu behar zaio gako pribatuari. Honela, ez du eskatuko pasahitza gakoa erabili behar den bakoitzean. Zertifikatu eskaera egiterakoan sartu dugun pasahitza eskatuko digu. Sartu.

```
openssl rsa -out fw-priv.pem -in fw-key.pem
```

Orain bere tokira kopiatuko dira suhesiaren ziurtagiria eta gako pribatua. Baita autoritate ziurtagiri-emailearen ziurtagiria ere.

```
cp /etc/zertifikatuak/fw-cert.pem /etc/openvpn/fw-cert.pem
cp /etc/zertifikatuak/fw-priv.pem /etc/openvpn/fw-priv.pem
cp /etc/zertifikatuak/iurretaCA/cacert.pem /etc/openvpn/ca-cert.pem
```

Ziurtagiriak beste ordenagailu batean sortzen badira, beste era batera kopiatu beharko dira.

Suhesiaren gako pribatuaren fitxategi baimenak aldatu eginbehar dira:

```
chmod 600 /etc/openvpn/fw-priv.pem
```

Beharrezkoa da DH (Diffie-Hellman) parametroak sortzea. **OpenVPN** gakoak dauden tokian sortuko da fitxategia.

```
cd /etc/openvpn
openssl dhparam -out dh1024.pem 1024
```

4.3. Zerbitzaria Konfiguratzen

Konfigurazio fitxategia **/etc/openvpn/openvpn.conf** izango da. Hona hemen bere edukia:

```
# TCP edo UDP zerbitzaria? TCP/443 (HTTPS) erabiliko dugu. Oso zaila da portu hau itxita
aurkitzea.
;proto tcp
proto udp

# Zein helbitan onartu behar ditu konexioak?
local 212.142.138.120

# Zein portu erabiliko du OpenVPN-k
port 443


# Erabiliko duen interfase mota. TUN aukeratuko da.
# Horrela, sare arteko bideraketa egin daiteke
dev tun
;tun-mtu 1500

# Ziurtagiriak. Autoritate ziurtagiri-emailearena eta suhesiaren ziurtagiria eta gako pribatua
ca /etc/openvpn/ca-cert.pem
cert /etc/openvpn/fw-cert.pem
key /etc/openvpn/fw-priv.pem

# Diffie-hellman parametroak
dh /etc/openvpn/dh1024.pem

# Zerbitzaria da eta 192.168.7.0/24 sarea
# erabiliko du bezeroekin konektatzeko
# Zerbitzariak 192.168.7.1 helbidea hartuko du
server 192.168.7.0 255.255.255.0

# Bezeroei, beti emango zaie helbide berdina
# ipp.txt fitxategian apuntatuko da bezero bakoitzaren helbidea
ifconfig-pool-persist /var/run/ipp.txt

# Bezeroentzako bideraketa informazioa
# Bezeroek aldatu behar dituzte euren bideraketa taulak
push "route 10.22.0.0 255.255.255.0"
push "route 10.22.2.0 255.255.255.0"
push "route 10.22.3.0 255.255.255.0"
push "route 172.31.249.0 255.255.255.240"

# Bezeroentzat DHCP aukerak
push "dhcp-option DNS 10.22.0.7"
```

```
push "dhcp-option DNS 10.22.2.7"
push "dhcp-option DNS 10.22.3.7"
push "dhcp-option WINS 10.22.0.7"
push "dhcp-option WINS 10.22.2.7"
push "dhcp-option WINS 10.22.3.7"
push "dhcp-option DOMAIN iurreta-institutua.net"

# Konexio anitz bezero bakoitzeko, ziurtagiri berdinarekin onartzeko
duplicate-cn

# Jakiteko konexioko beste partaidea bizirik dagoen
# 10 segundoro bidali “ping” antzerako bat. 120 segundotan ez bada jasotzen horrelako bat,
# partaidea “hilik” dago
keepalive 10 120

# Zifraketa mota
cipher AES-256-CBC
auth SHA1

# Gaitu konpresioa
comp-lzo

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute
status /var/run/openvpn-status.log

# Erregistro fitxategia. Ezer ez bada jartzen, “syslog” sistema erabiliko da.
# “log” erabiltzen bada, berrabiarazterakoan, gainidatzi egingo da fitxategia.
# “log-append” erabiltzen bada, berrabiarazterakoan, erantsi egingo zaio fitxategiari.
# Ez erabili biak
;log         /var/log/openvpn.log
log-append  /var/log/openvpn.log

# Erregistro maila
# 0 → 9
verb 3

# Bezeroekin klabeak birnegoziatu denbora hau pasa ondoren
reneg-sec 28800

# Erabiltzaile eta pasahitza sartu behar da
plugin /usr/lib/openvpn/openvpn-auth-pam.so login
# root erabiltzailea ezin daiteke sartu OpenVPN bitartez
#plugin /usr/lib/openvpn/openvpn-down-root.so login ???
```

4.4. OpenVPN erabiltzaileak sortzen

Lehenago aipatu denez, erabiltzaileek euren ziurtagiria izan beharko dute, eta gainera euren erabiltzaile izena eta pasahitza sartu. Hori gauzatzeko, **OpenVPN** zerbitzariak, hau da, **suhesiak**, erabiltzaile izenak eta pasahitzak egiaztatu behar ditu. Horretarako, erabiltzaile lokalak zein OpenLDAP edo ActiveDirectory directorio zerbitzu bateko erabiltzaileak izan daiterzke. Lehenengo, erabiltzaile lokalak ikusiko ditugu, errazagoa bait da.

Adibidean jarritako **alfredobz** erabiltzailea sortzeko suhesian, hurrengo agintea egikaritu behar da:

```
useradd -m -k /etc/skel -s /bin/bash alfredobz
```

```
passwd alfredobz
```

Listo! Orain **OpenVPN** berrabiarazi behar da.

```
/etc/init.d/openvpn restart
```

Martxan zerbitzaria!

5. Erabiltzaileen ziurtagiriak sortzen

Prozesua, zerbitzariaren ziurtagiria sortzeko egin den berdina izango da. Ziurtagiriak sortzeko, autoritate ziurtagiri-emailea behar da. Suposatzen da, autoritate hori sortuta dagoela. Honela sortuko da ziurtagiria **alfredobz** erabiltzailearentzat:

```
cd /etc/zertifikatuak
openssl req -new -days 1095 -keyout alfredobz-key.pem -out alfredobz-req.pem
openssl ca -policy policy_anything -out alfredobz-cert.pem -in alfredobz-req.pem
openssl rsa  -out alfredobz-priv.pem -in alfredobz-key.pem
```

Lehenetsitako baloreak aukeratu. Gero, eskatuko da erabiltzailearen izena "**Common Name**", eta "**Alfredo Barrainkua**" sartuko da. Gero, honen posta helbidea eskatuko da. "**alfredobz@iurreta-institutua.net**" sartuko da.

Gako pribatua sortu du eta ziurtagiri eskabidea. Gero, autoritate ziurtagiri-emaileak sinatu du ziurtagiria. Hortarako, ziurtagiri-emalearen pasahitza eskatuko digu. Azkenik, klabea kendu zaio gako pribatuari, bestela, erabili behar den bakoitzean, gakoa eskatuko lukeelako, berau irakurtzeko. Azken hau egiteko, zihurtagiri eskabidea sortzerakoan sartutako pasahitza eskatuko digu.

Suhesia ez den ordenagailu batean sortzen badugu ziurtagiria, suhesira kopiatu behar dugu. Suhesiko **/usr/lib/ssl/misc** direktoriora kopiatu behar dugu. Suhesian sortu badugu aldiz, ez dugu ezer egin behar. Baimenak 644 izan behar dure. Honela egingo genuke:

```
cp alfredobz-cert.pem /usr/lib/ssl/misc/
chmod 644 /usr/lib/ssl/misc/ alfredobz-cert.pem
```

Gako pribatua urruneko ordenagailuan jarri behar da. Baina hori, hurrengo kapituluan ikusiko dugu.

TRUKUA: Guaaa! La **letxe** litzateke **sor-ovpn-erab.sh** izena duen hurrengo skripta izatea **/root/bin** direktorioan:

```
# sor-ovpn-erab.sh
# Alfredo Barrainkua 2009, GPLv3 Lizentziapean
# OpenVPN erabiltzaileak sortzeko eskripta

if [ $# -lt 1 ]; then

        echo -n "Erabilpena: $0 erabiltzailea"
        echo
        exit 1
fi

        echo
        echo "Erabiltzailea sortzen ::: Erabiltzailearen pasahitza behar duzu sartu"
        useradd -m -k /etc/skel -s /bin/null $1
```

```
	passwd $1

	cd /usr/lib/ssl/misc

	echo
	echo "Zertifikatu eskabidea sortzen ::: Erabiltzailearen pasahitza eta datuak behar
dituzu sartu"
	openssl req -new -days 1095 -keyout $1-key.pem -out $1-req.pem

	echo
	echo "Zertifikatu eskabidea sinatzen ::: Zertifikatu agintearen pasahitza behar duzu
sartu"
	openssl ca -policy policy_anything -out $1-cert.pem -in $1-req.pem

	echo
	echo "Gako pribatuaren pasahitza kentzen ::: Erabiltzailearen pasahitza behar duzu
sartu"
	openssl rsa -out $1-priv.pem -in $1-key.pem

	cp $1-cert.pem /etc/openvpn/

	cd /root/bin

	exit 0
```

6. Bezeroak

Erabilienak diren Windows, Linux eta Mac OSX sistema eragileetan instalatuko da **OpenVPN**.

6.1. Mac OSX

MAC OSX sistema eragilearentzat, **TunnelBlick** deituriko aplikazioa dago. Helbide honetatik deskarga daiteke:

http://tunnelblick.googlecode.com/files/Tunnelblick_3.0b10.dmg

Gero, instalatu eta kito!

Zerbitzariaren zihurtagiriaren datu bat behar dugu. Zihurtagiria ikusteko, honela egingo dugu:

```
openssl x509 -noout -text -in fw-cert.pem
```

Irteeran, honen antzeko lerro bat agertuko da:

Subject: E=EH, ST=Bizkaia, L=Iurreta, OU=Sarea, CN=suhesia.iurreta-institutua.net/emailAddress=sare-admin@iurreta-institutua.net

Bezeroa konfiguratzeko beharko dugu.

Orain konfiguratu egin behar da. Erabiltzaile bakoitzak bere konfigurazio fitxategia dauka. Fitxategia **~/Library/openvpn\openvpn.conf** da. Hona hemen bere edukia:

```
# Bezeroa!, noski.
client

# Interfaze mota
dev tun

# Konexio mota
proto tcp

# Zerbitzariaren helbidea eta portua
remote 212.142.138.120 443

# Zerbitzariaren TLS-a. Zerbitzariaren ziurtagiritik aterako da (fw-cert.pem).
# Ziurtagiriaren informazioa ,lortzeko:
# openssl x509 -noout -text -in fw-cert.pem
# Aldatu eremu barneko zuriuneak "_" karakterearekin
# Banandu eremuak "/" karakterearekin. Jarri hasieran ere!!!
# Dena lerro batean.
```

```
tls-remote "/C=EH/ST=Bizkaia/L=Iurreta/O=Iurreta_Institutua/OU=Sarea/CN=suhesia.iurreta-
institutua.net/emailAddress=sare-admin@iurreta-institutua.net"

# Beti egon zerbitzariaren hostalari izena erresolbitzen saiatzen
resolv-retry infinite

# Ez erabili portu berezi bat
nobind

# Utzi pribilegioak hasieratzearen ostean. Windows ez direnak soilik.
user nobody
group nobody

# Berrabiarazteen artean, mantendu zenbait gauza
persist-key
persist-tun

# SSL/TLS parametroak
ca /etc/openvpn/ca-cert.pem
cert /etc/openvpn/alfredobz-cert.pem
key /etc/openvpn/alfredobz-priv.pem

# Erabiltzaile eta pasahitza erabili
auth-user-pass

# Zifraketa metodoa
cipher AES-256-CBC
auth SHA1

# Konpresioa
comp-lzo

# Erregistro fitxategia
log-append   /var/log/openvpn.log

# Erregistro maila
verb 3

# Birnegoziazioa
reneg-sec 0

# Kanpoko skriptak egikaritzeko (Linux)
#script-security 2

# Abiaraztean eta ixtean, hurrengo skripta erabili (Soilik Linux)
#up /etc/openvpn/update-resolv-conf
#down /etc/openvpn/update-resolv-conf
```

Editatu nahi bada:

```
sudo /Applications/TextEdit.app/Contents/MacOS/TextEdit ~/Library/openvpn/openvpn.conf
```

Direktorio berean jarri behar dira autoritate ziurtagiri-emailearen ziurtagiria duen **ca-cert.pem** fitxategia, eta erabiltzailearen ziurtagiria eta gako pribatua. Azken fitxategi honen baimenak 600 izan behar dira.

TunnelBlick abiarazi ikonoan klikatuz. Aukeratu "**Set Nameserver**" aukeraketa kutxa.

Egina! Eskolako sarean, bertan egongo bazina bezala!

6.2. Windows

Windows bezeroarentzat interfaze grafiko bat dago. Interfaze grafiko hori duen paketeak, OpenVPN bera programa ere badauka, baina arazoak eman ditzake. Beraz, aplikazioa eta interfaze grafikoa deskargatu eta instalatuko dira. **ORDENA HONETAN!**

Helbide hauetatik deskargatuko dira:

http://openvpn.net/release/openvpn-2.0.9-install.exe

http://openvpn.se/files/install_packages/openvpn-2.0.9-gui-1.0.3-install.exe

Gero, Windows ingurunean ohikoa den bezala, aplikazioak egikaritu, eta dena instalatuko da.

Zerbitzariaren zihurtagiriaren datu bat behar dugu. Zihurtagiria ikusteko, honela egingo dugu:

```
openssl x509 -noout -text -in fw-cert.pem
```

Irteeran, honen antzeko lerro bat agertuko da:

Subject: E=EH, ST=Bizkaia, L=Iurreta, OU=Sarea, CN=suhesia.iurreta-institutua.net/emailAddress=sare-admin@iurreta-institutua.net

Bezeroa konfiguratzeko beharko dugu.

Orain konfiguratu egingo da. Konfigurazio fitxategia **c:\Archivos de Programa\openvpn\config\openvpn.ovpn** izango da. Hona hemen bere edukia:

```
# Bezeroa!, noski.
client

# Interfaze mota
dev tun

# Konexio mota
proto tcp

# Zerbitzariaren helbidea eta portua
remote 212.142.138.120 443

# Zerbitzariaren TLS-a. Zerbitzariaren ziurtagiritik aterako da (fw-cert.pem).
# Ziurtagiriaren informazioa ,lortzeko:
# openssl x509 -noout -text -in fw-cert.pem
# Aldatu eremu barneko zuriuneak "_" karakterearekin
# Banandu eremuak "/" karakterearekin. Jarri hasieran ere!!!
# Dena lerro batean.
tls-remote "/C=EH/ST=Bizkaia/L=Iurreta/O=Iurreta_Institutua/OU=Sarea/CN=suhesia.iurreta-
institutua.net/emailAddress=sare-admin@iurreta-institutua.net"

# Beti egon zerbitzariaren hostalari izena erresolbitzen saiatzen
resolv-retry infinite

# Ez erabili portu berezi bat
nobind

# Utzi pribilegioak hasieratzearen ostean. Windows ez direnak soilik.
#user nobody
#group nobody

# Berrabiarazteen artean, mantendu zenbait gauza
```

```
persist-key
persist-tun

# SSL/TLS parametroak
ca C:\Archivos de Programa\openvpn\config\ca-cert.pem
cert C:\Archivos de Programa\openvpn\config\alfredobz-cert.pem
key C:\Archivos de Programa\openvpn\config\alfredobz-priv.pem

# Erabiltzaile eta pasahitza erabili
auth-user-pass

# Zifraketa metodoa
cipher AES-256-CBC
auth SHA1

# Konpresioa
comp-lzo

# Erregistro fitxategia (Ez Windows)
#log-append  /var/log/openvpn.log

# Erregistro maila
verb 3

# Birnegoziazioa
reneg-sec 0
```

Direktorio berean jarri behar dira autoritate ziurtagiri-emailearen ziurtagiria duen **ca-cert.pem** fitxategia, eta erabiltzailearen ziurtagiria eta gako pribatua. Azken fitxategi honen baimenak 600 izan behar dute.

Orain, OpenVPN ikonoan klikatu eta "**Conectar**" aukeratu.

6.3. Ubuntu Linux

Bezeroaren instalazioa, zerbitzariarena bezalakoa da:

```
aptitude install vtun openssl liblzo2-2 openvpn
```

Zerbitzariaren zihurtagiriaren datu bat behar dugu. Zihurtagiria ikusteko, honela egingo dugu:

```
openssl x509 -noout -text -in fw-cert.pem
```

Irteeran, honen antzeko lerro bat agertuko da:

Subject: E=EH, ST=Bizkaia, L=Iurreta, OU=Sarea, CN=suhesia.iurreta-institutua.net/emailAddress=sare-admin@iurreta-institutua.net

Bezeroa konfiguratzeko beharko dugu.

Konfigurazio fitxategia **/etc/openvpn/openvpn.conf** izango da. Edukia, Windows eta MacOS bezalakoa da, baina berezitasun batekin: azkenengo bi lerroak. OpenVPN abiarazi eta geldiarazi egiten denean, script hau egikaritzen da. Honen helburua, DNS zerbitzariak aldatzea.

```
# Bezeroa!, noski.
client

# Interfaze mota
```

```
dev tun

# Konexio mota
proto tcp

# Zerbitzariaren helbidea eta portua
remote 212.142.138.120 443

# Zerbitzariaren TLS-a. Zerbitzariaren ziurtagiritik aterako da (fw-cert.pem).
# Ziurtagiriaren informazioa ,lortzeko:
# openssl x509 -noout -text -in fw-cert.pem
# Aldatu eremu barneko zuriuneak "_" karakterearekin
# Banandu eremuak "/" karakterearekin. Jarri hasieran ere!!!
# Dena lerro batean.
tls-remote "/C=EH/ST=Bizkaia/L=Iurreta/O=Iurreta_Institutua/OU=Sarea/CN=suhesia.iurreta-
institutua.net/emailAddress=sare-admin@iurreta-institutua.net"

# Beti egon zerbitzariaren hostalari izena erresolbitzen saiatzen
resolv-retry infinite

# Ez erabili portu berezi bat
nobind

# Utzi pribilegioak hasieratzearen ostean. Windows ez direnak soilik.
user nobody
# Ubuntu/Debian-entzat, taldea nogroup da
;group nobody
group nogroup

# Berrabiarazteen artean, mantendu zenbait gauza
persist-key
persist-tun

# SSL/TLS parametroak
ca /etc/openvpn/ca-cert.pem
cert /etc/openvpn/alfredobz-cert.pem
key /etc/openvpn/alfredobz-priv.pem

# Erabiltzaile eta pasahitza erabili
auth-user-pass

# Zifraketa metodoa
cipher AES-256-CBC
auth SHA1

# Konpresioa
comp-lzo

# Erregistro fitxategia
log-append   /var/log/openvpn.log

# Erregistro maila
verb 3

# Birnegoziazioa
reneg-sec 0

# Kanpoko skriptak egikaritzeko (Linux)
script-security 2

# Abiaraztean eta ixtean, hurrengo skripta erabili (Soilik Linux)
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
```

Direktorio berean jarriko dira autoritate ziurtagiri-emailearen ziurtagiria duen **ca-cert.pem** fitxategia, eta erabiltzailearen ziurtagiria eta gako pribatua. Azken fitxategi honen baimenak 600 izan behar dute.

Listo. Orain, berrabiarazteko OpenVPN, hurrengo hau egikaritu:

```
/etc/init.d/openvpn restart
```

Erabiltzaile izena eta pasahitza eskatuko ditu, eta listo! Eskolan!

7. Egiteke

- Sare bi konektatu. Bi eraikuntza duten eskolentzat.
- OpenLDAP erabili azpi-sistema bezala erabiltzaileentzat

8. Egilea

Alfredo Barrainkua Zallo, Iurreta Institutuko IKT Arduraduna

Kritikak, hobekuntzak aldaketa proposamenak edota galderak, hurrengo posta helbidera bidali:

alfredobz@iurreta-institutua.net

9. A Eranskina. Aginte ziurtagiri-emailea sortzen

Ziurtagiriak baieztatzeko, aginte ziurtagiri-emaile bat behar da. Aginte hau **nireeskolaCA** izango da. Hiru urtetarako sortuko da agintea.

Konfigurazio fitxategian (**/etc/ssl/openssl.cnf**), aldaketa hauek egin behar dira:

[CA_default] atalean:

```
dir = ./demoCA                          -> iurretaCA
default_days = 365                      -> 1095
```

[req_distinguished_name] atalean aldaketa hauek egin:

```
countryName_default = AU                    -> EH
stateOrProvinveName_default = Some State    -> Bizkaia
O.organizationName_default = Internet ... Ltd -> Iurreta GLHB Institutua
organizationalUnitName_default = Sarea
```

Lerro hau gehitu atal berean:

```
localityName_default = Iurreta
```

Konfigurazio fitxategia den **/etc/ssl/openssl.cnf** fitxategiak eskatzen duen fitxategi egitura sortu behar da, nahi den direktorioan. Adibidez, **/etc/zertifikatuak** direktorioan.

```
mkdir /etc/zertifikatuak
chmod 700 /etc/zertifikatuak
cd /etc/zertifikatuak
mkdir -p iurretaCA/certs
mkdir -p iurretaCA/crl
mkdir -p iurretaCA/newcerts
mkdir -p iurretaCA/private
echo 00 > iurretaCA/serial
touch iurretaCA/index.txt
```

Aginte ziurtagiri-emailearen ziurtagiria sortu behar da. Hiru bat parametro baino ez dira txertatu behar. Besteak beste, pasa-esaldia. Beste guztiak lehenetsiak hartuko ditu konfigurazio fitxategitik.

KONTUZ! Konfigurazio fitxategian jarrita dagoenez era lehenetsian, 20 karaktere izan ditzake gehienez pasa-esaldiak. Adibidez: **Toki ona da eskola**.

```
openssl req -new -keyout iurretaCA/private/ca-key.pem -out iurretaCA/certs/ca-req.pem
```

Lehenetsitako aukerak dauden tokian, aurrera egin. Gero, eskatuko da arduradunaren izena "**Common Name**", eta "**Sare Admninistraria**" sartuko da. Gero, honen posta helbidea eskatuko da. "**sare-admin@iurreta-institutua.net**" sartuko da.

Orain eskabidea sinatuko da.

```
openssl ca -days 1095 -batch -selfsign -extensions v3_ca -keyfile iurretaCA/private/ca-key.pem -out iurretaCA/newca.pem -in iurretaCA/certs/ca-req.pem
```

Orain x509-an jarriko da ziurtagiria.

```
openssl x509 -days 1095 -signkey iurretaCA/private/ca-key.pem -out iurretaCA/ca-cert.pem -in iurretaCA/newca.pem
```

Egina. Prest ziurtagiriak sortzeko.