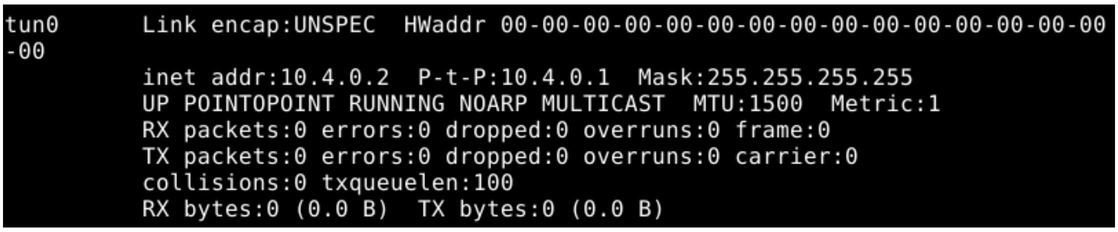
Seguridad en Redes
Practica 3.6

David Antuña Rodríguez
Javier Carrión García

1 OpenVPN

1.1 Clave estática compartida

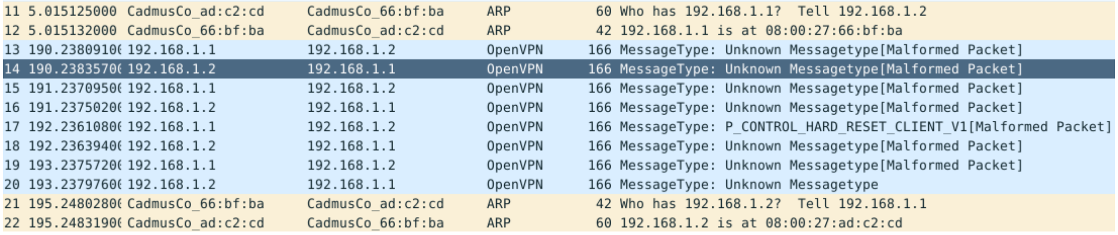
```
Tue Apr 24 12:11:50 2018 us=815937   shared_secret_file = ’static.key’
Tue Apr 24 12:11:50 2018 us=860926 Local Options hash (VER=V4): ’8addc3e6’
Tue Apr 24 12:11:50 2018 us=860938 Expected Remote Options hash (VER=V4):
  ’04a219ce’
Tue Apr 24 12:11:50 2018 us=860950 UDPv4 link local (bound): [undef]
Tue Apr 24 12:11:50 2018 us=860958 UDPv4 link remote: [AF_INET]192.168.1.1:1194
^[[1;5CTue Apr 24 12:11:59 2018 us=856274 Peer Connection Initiated with
  [AF_INET]192.168.1.1:1194
Tue Apr 24 12:12:00 2018 us=923036 Initialization Sequence Completed
^CTue Apr 24 12:18:53 2018 us=251659 event_wait : Interrupted system call
  (code=4)
Tue Apr 24 12:18:53 2018 us=251728 TCP/UDP: Closing socket
Tue Apr 24 12:18:53 2018 us=251761 Closing TUN/TAP interface
Tue Apr 24 12:18:53 2018 us=251787 /sbin/ifconfig tun0 0.0.0.0
Tue Apr 24 12:18:53 2018 us=264076 SIGINT[hard,] received, process exiting
```



```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:10.4.0.2  P-t-P:10.4.0.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

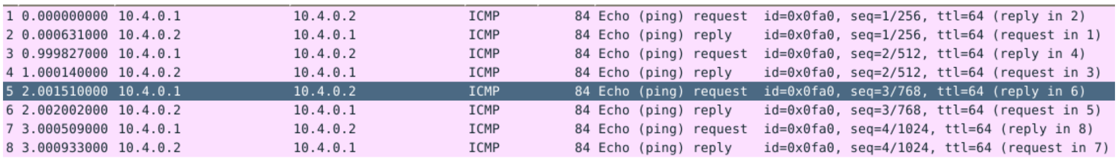
Figure 1.1.1 : Características de tun0.

Los paquetes que vemos por eth1 no se pueden leer (figura 1.1.2), en cambio por tun0 si podemos ver su contenido (figura 1.1.3).



```
11 5.015125000 CadmusCo_ad:c2:cd  CadmusCo_66:bf:ba  ARP       60 Who has 192.168.1.1?  Tell 192.168.1.2
12 5.015132000 CadmusCo_66:bf:ba  CadmusCo_ad:c2:cd  ARP       42 192.168.1.1 is at 08:00:27:66:bf:ba
13 190.2380910( 192.168.1.1       192.168.1.2        OpenVPN  166 MessageType: Unknown Messagetype[Malformed Packet]
14 190.2383570( 192.168.1.2       192.168.1.1        OpenVPN  166 MessageType: Unknown Messagetype[Malformed Packet]
15 191.2370950( 192.168.1.1       192.168.1.2        OpenVPN  166 MessageType: Unknown Messagetype[Malformed Packet]
16 191.2375020( 192.168.1.2       192.168.1.1        OpenVPN  166 MessageType: Unknown Messagetype[Malformed Packet]
17 192.2361080( 192.168.1.1       192.168.1.2        OpenVPN  166 MessageType: P_CONTROL_HARD_RESET_CLIENT_V1[Malformed Packet]
18 192.2363940( 192.168.1.2       192.168.1.1        OpenVPN  166 MessageType: Unknown Messagetype[Malformed Packet]
19 193.2375720( 192.168.1.1       192.168.1.2        OpenVPN  166 MessageType: Unknown Messagetype[Malformed Packet]
20 193.2379760( 192.168.1.2       192.168.1.1        OpenVPN  166 MessageType: Unknown Messagetype
21 195.2480280( CadmusCo_66:bf:ba CadmusCo_ad:c2:cd  ARP       42 Who has 192.168.1.2?  Tell 192.168.1.1
22 195.2483190( CadmusCo_ad:c2:cd CadmusCo_66:bf:ba  ARP       60 192.168.1.2 is at 08:00:27:ad:c2:cd
```

Figure 1.1.2 : Paquetes por eth1.



```
1 0.000000000 10.4.0.1        10.4.0.2        ICMP      84 Echo (ping) request  id=0x0fa0, seq=1/256, ttl=64 (reply in 2)
2 0.000631000 10.4.0.2        10.4.0.1        ICMP      84 Echo (ping) reply    id=0x0fa0, seq=1/256, ttl=64 (request in 1)
3 0.999827000 10.4.0.1        10.4.0.2        ICMP      84 Echo (ping) request  id=0x0fa0, seq=2/512, ttl=64 (reply in 4)
4 1.000140000 10.4.0.2        10.4.0.1        ICMP      84 Echo (ping) reply    id=0x0fa0, seq=2/512, ttl=64 (request in 3)
5 2.001510000 10.4.0.1        10.4.0.2        ICMP      84 Echo (ping) request  id=0x0fa0, seq=3/768, ttl=64 (reply in 6)
6 2.002002000 10.4.0.2        10.4.0.1        ICMP      84 Echo (ping) reply    id=0x0fa0, seq=3/768, ttl=64 (request in 5)
7 3.000509000 10.4.0.1        10.4.0.2        ICMP      84 Echo (ping) request  id=0x0fa0, seq=4/1024, ttl=64 (reply in 8)
8 3.000933000 10.4.0.2        10.4.0.1        ICMP      84 Echo (ping) reply    id=0x0fa0, seq=4/1024, ttl=64 (request in 7)
```

Figure 1.1.3 : Paquetes por tun0.

1.2 TLS con certificados

Salida del comando:
sudo openvpn –remote 192.168.1.1 –dev tun –ifconfig 10.4.0.2 10.4.0.1 –tls-server –dh dh1024.pem –ca ca.crt –cert server.crt –key server.key –verb 4

```
Sat Apr 21 20:07:46 2018 us=825293 Diffie-Hellman initialized with
1024 bit key
Sat Apr 21 20:07:46 2018 us=825524 WARNING: file ’server.key’ is
group or others accessible
Sat Apr 21 20:07:46 2018 us=825784 Control Channel MTU parms
[ L:1541 D:138 EF:38 EB:0 ET:0 EL:0 ]
Sat Apr 21 20:07:46 2018 us=825848 Socket Buffers:
R=[229376->131072] S=[229376->131072]
Sat Apr 21 20:07:46 2018 us=826308 TUN/TAP device tun0 opened
Sat Apr 21 20:07:46 2018 us=826320 TUN/TAP TX queue length set
to 100
Sat Apr 21 20:07:46 2018 us=826328 do_ifconfig, tt->ipv6=0,
tt->did_ifconfig_ipv6_setup=0
Sat Apr 21 20:07:46 2018 us=826340 /sbin/ifconfig tun0
10.4.0.2 pointopoint 10.4.0.1 mtu 1500
Sat Apr 21 20:07:46 2018 us=827384 Data Channel MTU parms
[ L:1541 D:1450 EF:41 EB:4 ET:0 EL:0 ]
Sat Apr 21 20:07:46 2018 us=827400 Local Options String:
’V4,dev-type tun,link-mtu 1541,tun-mtu 1500,proto UDPv4,
ifconfig 10.4.0.1 10.4.0.2,cipher BF-CBC,auth SHA1,
keysize128,key-method 2,tls-server’
Sat Apr 21 20:07:46 2018 us=827404 Expected Remote Options
String: ’V4,dev-type tun,link-mtu 1541,tun-mtu 1500,
proto UDPv4,ifconfig 10.4.0.2 10.4.0.1,cipher BF-CBC,
auth SHA1,keysize 128,key-method 2,tls-client’
Sat Apr 21 20:07:46 2018 us=827415 Local Options hash
(VER=V4): ’bd0285da’
Sat Apr 21 20:07:46 2018 us=827420 Expected Remote Options
hash (VER=V4): ’599bc3b6’
Sat Apr 21 20:07:46 2018 us=827425 UDPv4 link local (bound):
[undef]
Sat Apr 21 20:07:46 2018 us=827429 UDPv4 link remote:
[AF_INET]192.168.1.1:1194
Sat Apr 21 20:07:46 2018 us=827755 TLS: Initial packet from
[AF_INET]192.168.1.1:1194, sid=77b8cb72 79f522af
Sat Apr 21 20:07:46 2018 us=835973 VERIFY OK: depth=1,
/C=KG/ST=NA/L=BISHKEK/O=OpenVPN-TEST/emailAddress=me@myhost.mydomain
Sat Apr 21 20:07:46 2018 us=836137 VERIFY OK: depth=0,
/C=KG/ST=NA/O=OpenVPN-TEST/CN=Test-Client/emailAddress=me@myhost.mydomain
Sat Apr 21 20:07:46 2018 us=845402 Data Channel Encrypt:
Cipher 'BF-CBC' initialized with 128 bit key
Sat Apr 21 20:07:46 2018 us=845452 Data Channel Encrypt:
Using 160 bit message hash 'SHA1' for HMAC authentication
Sat Apr 21 20:07:46 2018 us=845501 Data Channel Decrypt:
Cipher 'BF-CBC' initialized with 128 bit key
Sat Apr 21 20:07:46 2018 us=845524 Data Channel Decrypt:
Using 160 bit message hash 'SHA1' for HMAC authentication
Sat Apr 21 20:07:46 2018 us=846128 Control Channel: TLSv1,
cipher TLSv1/SSLv3 DHE-RSA-AES256-SHA, 2048 bit RSA
Sat Apr 21 20:07:46 2018 us=846170 [Test-Client] Peer
Connection Initiated with [AF_INET]192.168.1.1:1194
Sat Apr 21 20:07:48 2018 us=70028 Initialization
Sequence Completed
```

Para configurar la VPN cliente-servidor hemos modificado el archivo left, configurandolo como cliente.

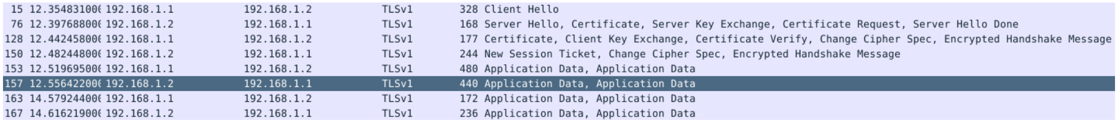
```
client

dev tun
proto tcp
remote 192.168.1.2 1194

ca ca.crt
cert client.crt
key client.key

remote-cert-tls server
tls-remote Test-Server
```

Y right lo hemos configurado como servidor.

```
local 192.168.1.2
port 1194
proto tcp

dev tun

ca ca.crt
cert server.crt
key server.key

dh dh2048.pem

server 10.8.0.0 255.255.255.0
```

```
ifconfig-pool-persist ipp.txt
```

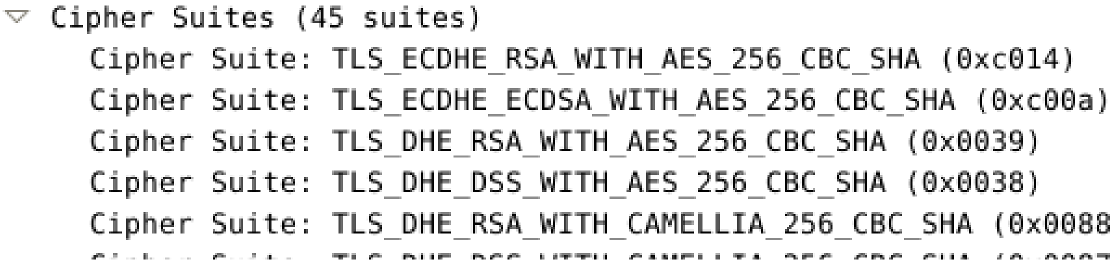
Una vez iniciada la VPN y aplicado el filtro en Wireshark vemos los siguientes mensajes, figura 1.2.1 . En primer lugar el cliente saluda al servidor para inciar la conexión y este le contesta enviando sus datos de autenticación. Una vez autenticado el cliente envia sus datos y el servidor contesta enviando la información de la sesión.



```
 15 12.35483100( 192.168.1.1     192.168.1.2     TLSv1     328 Client Hello
 76 12.39768800( 192.168.1.2     192.168.1.1     TLSv1     168 Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
128 12.44245800( 192.168.1.1     192.168.1.2     TLSv1     177 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
150 12.48244800( 192.168.1.2     192.168.1.1     TLSv1     244 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
153 12.51969500( 192.168.1.1     192.168.1.2     TLSv1     480 Application Data, Application Data
157 12.55642200( 192.168.1.2     192.168.1.1     TLSv1     440 Application Data, Application Data
163 14.57924400( 192.168.1.1     192.168.1.2     TLSv1     172 Application Data, Application Data
167 14.61621900( 192.168.1.2     192.168.1.1     TLSv1     236 Application Data, Application Data
```

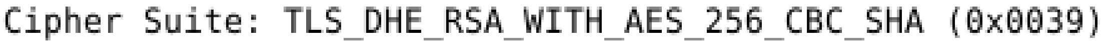
Figure 1.2.1 : Acuerdo TLS.

Se puede escoger entre 45 conjuntos distintos, figura 1.2.2 , de los cuales finalmente escogen solo uno que se puede ver en la figura 1.2.3 .



```
▽ Cipher Suites (45 suites)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
    Cipher Suite: TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088
```

Figure 1.2.2 : Conjuntos de algoritmos.



```
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
```

Figure 1.2.3 : Conjunto escogido.

En certificate el cliente envia un certificado firmado que contiene su clave pública.

2 OpenSSH

2.1 Autentificación con clave pública

La salida del comando ssh -v 192.168.1.2 es la siguiente.

```
OpenSSH_6.0p1 Debian-4+deb7u7, OpenSSL 1.0.1e 11 Feb 2013
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug1: Connecting to 192.168.1.2 [192.168.1.2] port 22.
debug1: Connection established.
```

```
debug1: identity file /home/usuario/.ssh/id_rsa type 1
debug1: Checking blacklist file /usr/share/ssh/blacklist.RSA-2048
debug1: Checking blacklist file /etc/ssh/blacklist.RSA-2048
debug1: identity file /home/usuario/.ssh/id_rsa-cert type -1
debug1: identity file /home/usuario/.ssh/id_dsa type -1
debug1: identity file /home/usuario/.ssh/id_dsa-cert type -1
debug1: identity file /home/usuario/.ssh/id_ecdsa type -1
debug1: identity file /home/usuario/.ssh/id_ecdsa-cert type -1
debug1: Remote protocol version 2.0, remote software version
  OpenSSH_6.0p1 Debian-4+deb7u7
debug1: match: OpenSSH_6.0p1 Debian-4+deb7u7 pat OpenSSH*
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u7
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: server->client aes128-ctr hmac-md5 none
debug1: kex: client->server aes128-ctr hmac-md5 none
debug1: sending SSH2_MSG_KEX_ECDH_INIT
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: Server host key: ECDSA c5:9d:97:b8:6e:87:e4:e3:cc:ec:3b:a8:bc:9e:8b:12
debug1: Host '192.168.1.2' is known and matches the ECDSA host key.
debug1: Found key in /home/usuario/.ssh/known_hosts:1
debug1: ssh_ecdsa_verify: signature correct
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey,password
debug1: Next authentication method: publickey
debug1: Offering RSA public key: /home/usuario/.ssh/id_rsa
debug1: Server accepts key: pkalg ssh-rsa blen 279
debug1: key_parse_private_pem: PEM_read_PrivateKey failed
debug1: read PEM private key done: type <unknown>
Enter passphrase for key '/home/usuario/.ssh/id_rsa':
debug1: read PEM private key done: type RSA
debug1: Authentication succeeded (publickey).
Authenticated to 192.168.1.2 ([192.168.1.2]:22).
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: Sending environment.
debug1: Sending env LANG = es_ES.UTF-8
Linux debian 3.2.0-4-amd64 #1 SMP Debian 3.2.63-2 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Apr 21 19:29:26 2018
```

2.2 Reenvío de puertos

ssh -v -N -L 8080:www.ucm.es:80 usuario@192.168.1.2, se ha conetado a la pagina principal de la complutense.

```
Enter passphrase for key '/home/usuario/.ssh/id_rsa':
debug1: read PEM private key done: type RSA
debug1: Authentication succeeded (publickey).
Authenticated to 192.168.1.2 ([192.168.1.2]:22).
debug1: Local connections to LOCALHOST:8080 forwarded to remote address www.ucm.e
debug1: Local forwarding listening on ::1 port 8080.
debug1: channel 0: new [port listener]
debug1: Local forwarding listening on 127.0.0.1 port 8080.
debug1: channel 1: new [port listener]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: Connection to port 8080 forwarding to www.ucm.es port 80 requested.
debug1: channel 2: new [direct-tcpip]
debug1: Connection to port 8080 forwarding to www.ucm.es port 80 requested.
debug1: channel 3: new [direct-tcpip]
debug1: Connection to port 8080 forwarding to www.ucm.es port 80 requested.
debug1: channel 4: new [direct-tcpip]
debug1: Connection to port 8080 forwarding to www.ucm.es port 80 requested.
debug1: channel 5: new [direct-tcpip]
debug1: Connection to port 8080 forwarding to www.ucm.es port 80 requested.
debug1: channel 6: new [direct-tcpip]
debug1: Connection to port 8080 forwarding to www.ucm.es port 80 requested.
debug1: channel 7: new [direct-tcpip]
```

ssh -v -X -R 8080:www.ucm.es:80 usuario@192.168.1.2 chromium
Se abre en left el programa, en este caso chromium, por ser la que ejecuta el comando.
El puerto 8080 que está escuchando es el de right.

```
Enter passphrase for key '/home/usuario/.ssh/id_rsa':
debug1: read PEM private key done: type RSA
debug1: Authentication succeeded (publickey).
Authenticated to 192.168.1.2 ([192.168.1.2]:22).
debug1: Remote connections from LOCALHOST:8080 forwarded to local address
  www.ucm.es:80
debug1: channel 0: new [client-session]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: remote forward success for: listen 8080, connect www.ucm.es:80
debug1: All remote forwarding requests processed
debug1: Requesting X11 forwarding with authentication spoofing.
```

```
debug1: Sending environment.
debug1: Sending env LANG = es_ES.UTF-8
debug1: Sending command: chromium
debug1: client_input_channel_open: ctype x11 rchan 5 win 65536 max 16384
debug1: client_request_x11: request from ::1 41802
debug1: channel 1: new [x11]
debug1: confirm x11
debug1: client_input_channel_open: ctype x11 rchan 6 win 65536 max 16384
debug1: client_request_x11: request from ::1 41803
debug1: channel 2: new [x11]
debug1: confirm x11
debug1: client_input_channel_open: ctype x11 rchan 7 win 65536 max 16384
debug1: client_request_x11: request from ::1 41804
debug1: channel 3: new [x11]
debug1: confirm x11
OpenGL Warning: Failed to connect to host. Make sure 3D acceleration is enabled
  for this VM.
debug1: client_input_channel_open: ctype forwarded-tcpip rchan 8 win 2097152
  max 32768
debug1: client_request_forwarded_tcpip: listen localhost port 8080, originator
  ::1 port 37157
debug1: connect_next: host www.ucm.es ([147.96.1.15]:80) in progress, fd=10
debug1: channel 4: new [::1]
debug1: confirm forwarded-tcpip
debug1: client_input_channel_open: ctype forwarded-tcpip rchan 9 win 2097152
  max 32768
debug1: client_request_forwarded_tcpip: listen localhost port 8080, originator
  ::1 port 37158
debug1: connect_next: host www.ucm.es ([147.96.1.15]:80) in progress, fd=11
debug1: channel 5: new [::1]
debug1: confirm forwarded-tcpip
debug1: channel 4: connected to www.ucm.es port 80
debug1: channel 5: connected to www.ucm.es port 80
debug1: client_input_channel_open: ctype forwarded-tcpip rchan 10 win 2097152
  max 32768
debug1: client_request_forwarded_tcpip: listen localhost port 8080, originator
  ::1 port 37159
debug1: connect_next: host www.ucm.es ([147.96.1.15]:80) in progress, fd=12
debug1: channel 6: new [::1]
debug1: confirm forwarded-tcpip
debug1: client_input_channel_open: ctype forwarded-tcpip rchan 11 win 2097152
  max 32768
debug1: client_request_forwarded_tcpip: listen localhost port 8080, originator
  ::1 port 37160
debug1: connect_next: host www.ucm.es ([147.96.1.15]:80) in progress, fd=13
debug1: channel 7: new [::1]
debug1: confirm forwarded-tcpip
debug1: client_input_channel_open: ctype forwarded-tcpip rchan 12 win 2097152
  max 32768
```

```
debug1: client_request_forwarded_tcpip: listen localhost port 8080, originator
  ::1 port 37161
debug1: connect_next: host www.ucm.es ([147.96.1.15]:80) in progress, fd=14
debug1: channel 8: new [::1]
debug1: confirm forwarded-tcpip
debug1: client_input_channel_open: ctype forwarded-tcpip rchan 13 win 2097152
  max 32768
debug1: client_request_forwarded_tcpip: listen localhost port 8080, originator
  ::1 port 37162
debug1: connect_next: host www.ucm.es ([147.96.1.15]:80) in progress, fd=15
debug1: channel 9: new [::1]
debug1: confirm forwarded-tcpip
debug1: channel 6: connected to www.ucm.es port 80
debug1: channel 7: connected to www.ucm.es port 80
debug1: channel 8: connected to www.ucm.es port 80
debug1: channel 9: connected to www.ucm.es port 80
```

ssh -v -N -D 1080 usuario@192.168.1.2

Para el servidor la maquina que quiere conectarse es right, que es la que hace de proxy.

```
Enter passphrase for key '/home/usuario/.ssh/id_rsa':
debug1: read PEM private key done: type RSA
debug1: Authentication succeeded (publickey).
Authenticated to 192.168.1.2 ([192.168.1.2]:22).
debug1: Local connections to LOCALHOST:1080 forwarded to remote address socks:0
debug1: Local forwarding listening on ::1 port 1080.
debug1: channel 0: new [port listener]
debug1: Local forwarding listening on 127.0.0.1 port 1080.
debug1: channel 1: new [port listener]
debug1: Requesting no-more-sessions@openssh.com
debug1: Entering interactive session.
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 2: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 3: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 4: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 5: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 6: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 7: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 8: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 9: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 10: new [dynamic-tcpip]
```

```
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 11: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 12: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 13: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 14: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 15: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 16: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 17: new [dynamic-tcpip]
channel 15: open failed: administratively prohibited: open failed
debug1: channel 15: free: direct-tcpip: listening port 1080 for xcsvmqbwrjy
  port 80, connect from ::1 port 51147, nchannels 18
channel 16: open failed: administratively prohibited: open failed
channel 17: open failed: administratively prohibited: open failed
debug1: channel 16: free: direct-tcpip: listening port 1080 for kpkchnuhbfv
  port 80, connect from ::1 port 51148, nchannels 17
debug1: channel 17: free: direct-tcpip: listening port 1080 for urhtjlxedlzo
  port 80, connect from ::1 port 51149, nchannels 16
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 15: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 16: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 17: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 18: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 19: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 20: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 21: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 22: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 23: new [dynamic-tcpip]
debug1: Connection to port 1080 forwarding to socks port 0 requested.
debug1: channel 24: new [dynamic-tcpip]
debug1: channel 8: free: direct-tcpip: listening port 1080 for www.google.es
  port 443, connect from ::1 port 51140, nchannels 25
debug1: channel 9: free: direct-tcpip: listening port 1080 for www.google.es
  port 443, connect from ::1 port 51141, nchannels 24
debug1: channel 10: free: direct-tcpip: listening port 1080 for www.google.es
  port 443, connect from ::1 port 51142, nchannels 23
```

```
debug1: channel 11: free: direct-tcpip: listening port 1080 for www.google.es
  port 443, connect from ::1 port 51143, nchannels 22
debug1: channel 4: free: direct-tcpip: listening port 1080 for apis.google.com
  port 443, connect from ::1 port 51136, nchannels 21
debug1: channel 5: free: direct-tcpip: listening port 1080 for ssl.gstatic.com
  port 443, connect from ::1 port 51137, nchannels 20
debug1: channel 6: free: direct-tcpip: listening port 1080 for ssl.gstatic.com
  port 443, connect from ::1 port 51138, nchannels 19
debug1: channel 12: free: direct-tcpip: listening port 1080 for www.gstatic.com
  port 443, connect from ::1 port 51144, nchannels 18
```