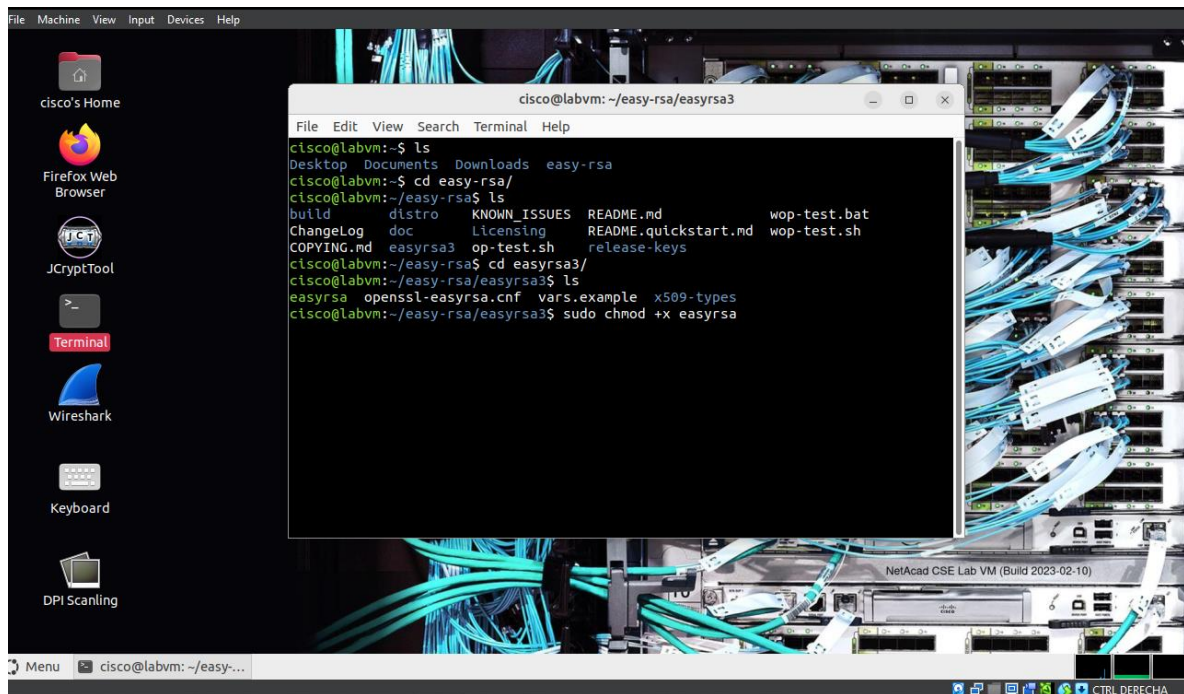


LABORATORIO 8

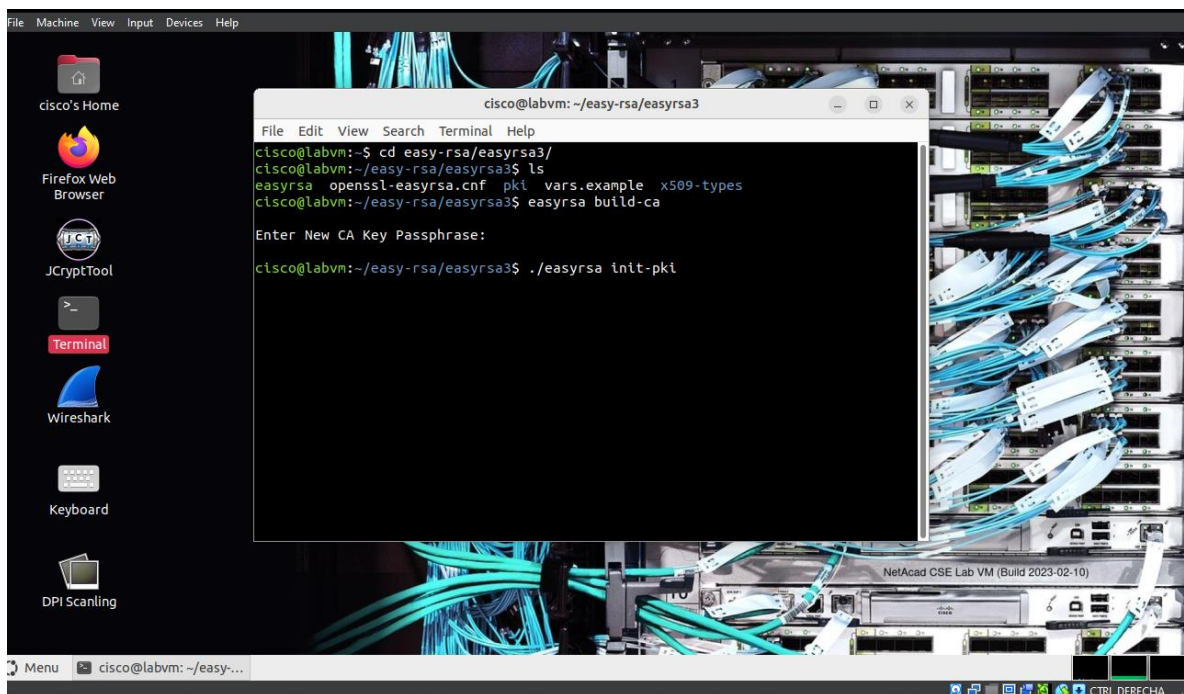
HECTOR DIAZ

PARTE 1: ACTUALIZACIÓN DEL SISTEMA E INSTALACIÓN DEL SERVIDOR



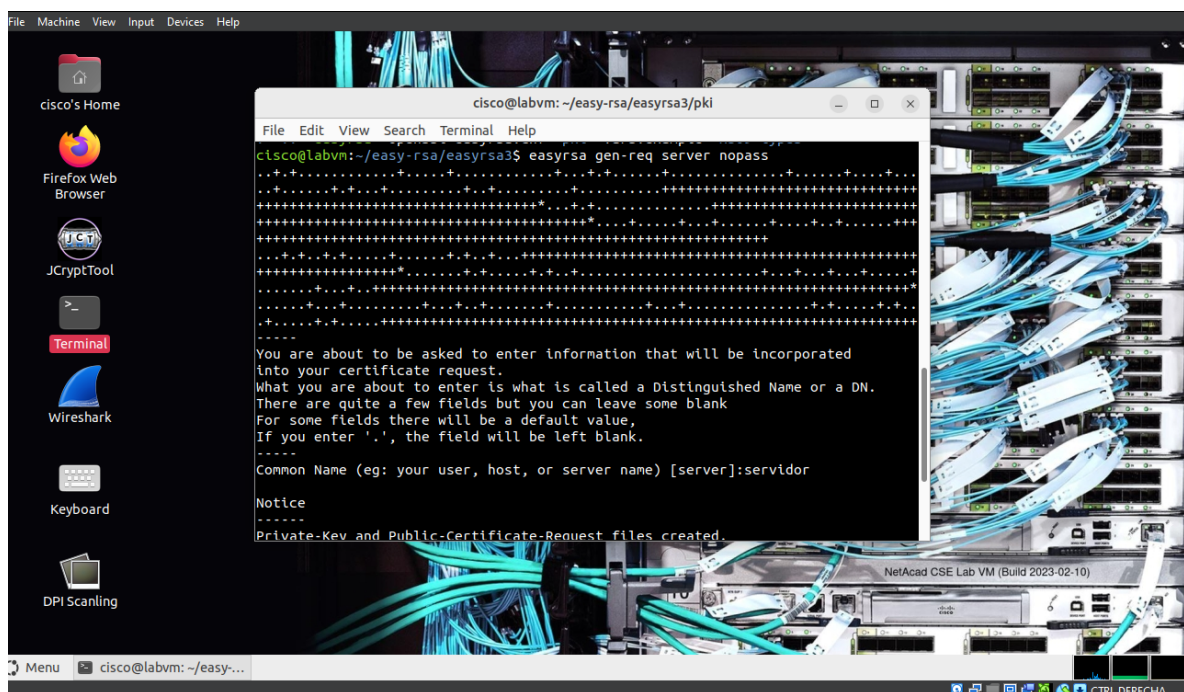
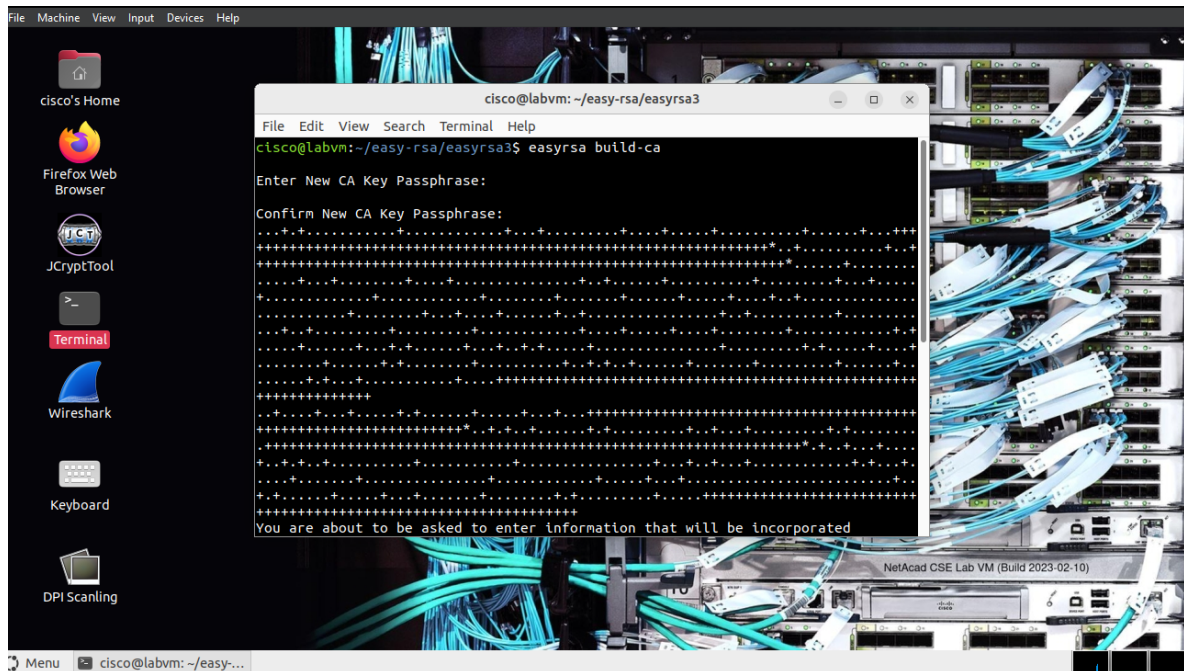
```
cisco@labvm: ~/easy-rsa/easyrsa3
File Edit View Search Terminal Help
cisco@labvm:~$ ls
Desktop Documents Downloads easy-rsa
cisco@labvm:~$ cd easy-rsa/
cisco@labvm:~/easy-rsa$ ls
build      distro      KNOWN_ISSUES  README.md      wop-test.bat
ChangeLog  doc         licensing     README.quickstart.md  wop-test.sh
COPYING.md easyrsa3    op-test.sh    release-keys
cisco@labvm:~/easy-rsa$ cd easyrsa3/
cisco@labvm:~/easy-rsa/easyrsa3$ ls
easyrsa  openssl-easyrsa.cnf  vars.example  x509-types
cisco@labvm:~/easy-rsa/easyrsa3$ sudo chmod +x easyrsa
```

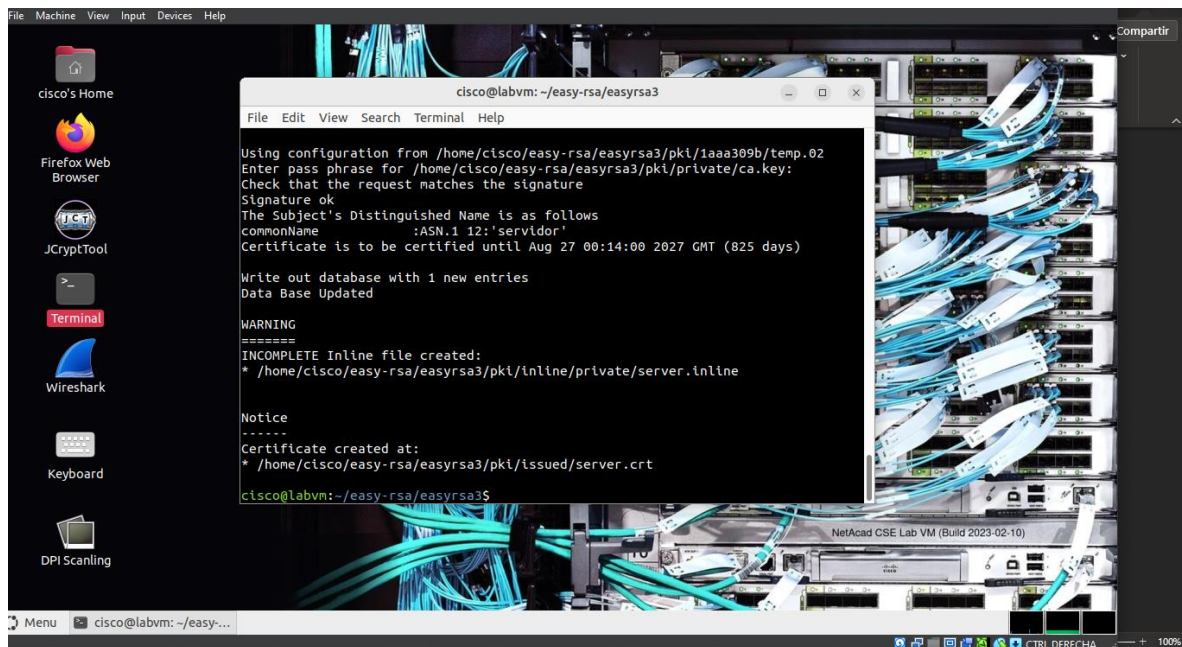
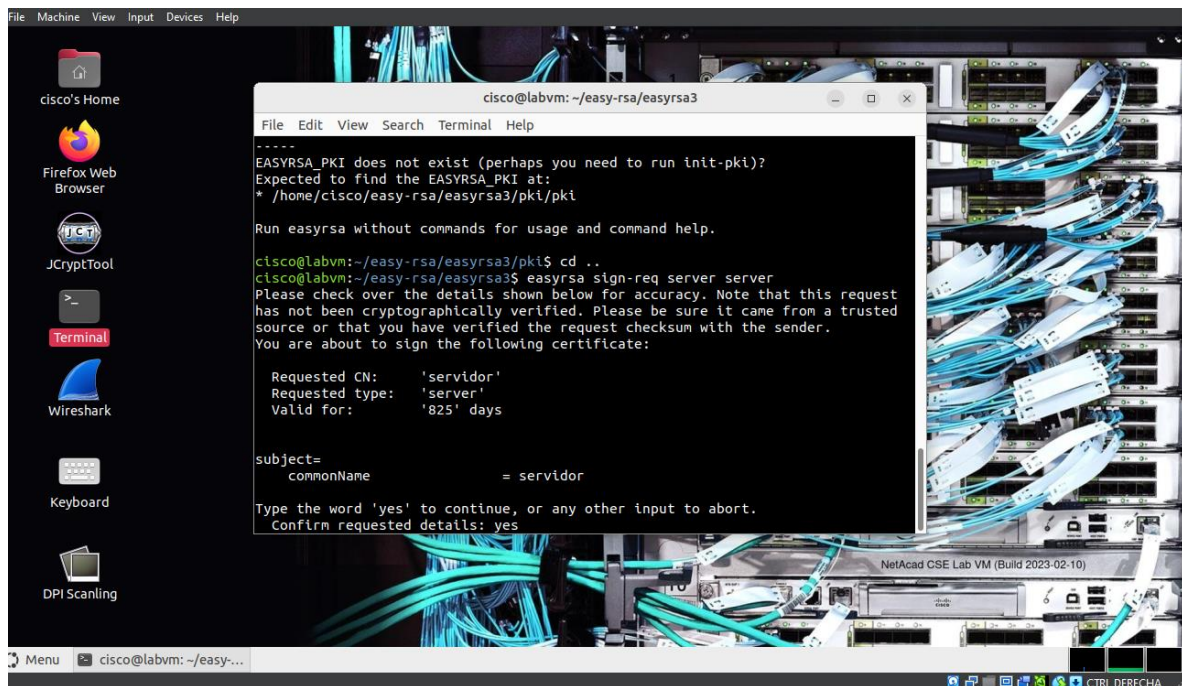
PARTE 2 PASO 3: CONFIGURACIÓN DE LA INFRAESTRUCTURA DE CERTIFICADOS



```
cisco@labvm: ~/easy-rsa/easyrsa3
File Edit View Search Terminal Help
cisco@labvm:~$ cd easy-rsa/easyrsa3/
cisco@labvm:~/easy-rsa/easyrsa3$ ls
easyrsa  openssl-easyrsa.cnf  vars.example  x509-types
cisco@labvm:~/easy-rsa/easyrsa3$ easyrsa build-ca
Enter New CA Key Passphrase:
cisco@labvm:~/easy-rsa/easyrsa3$ ./easyrsa init-pki
```

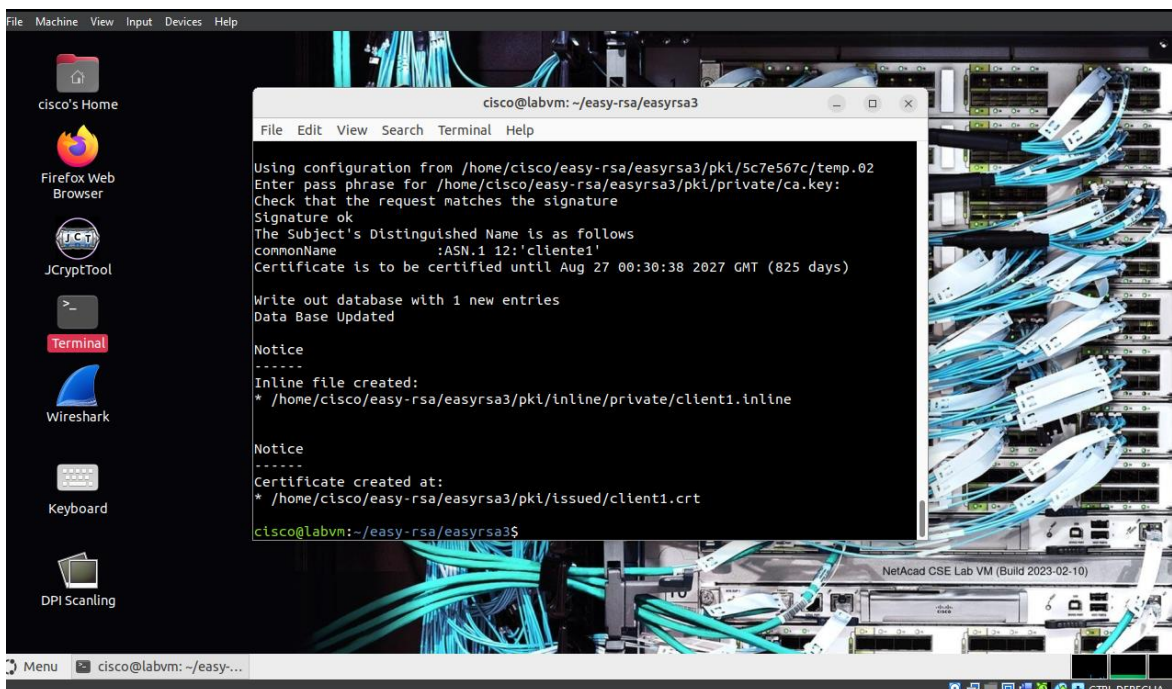
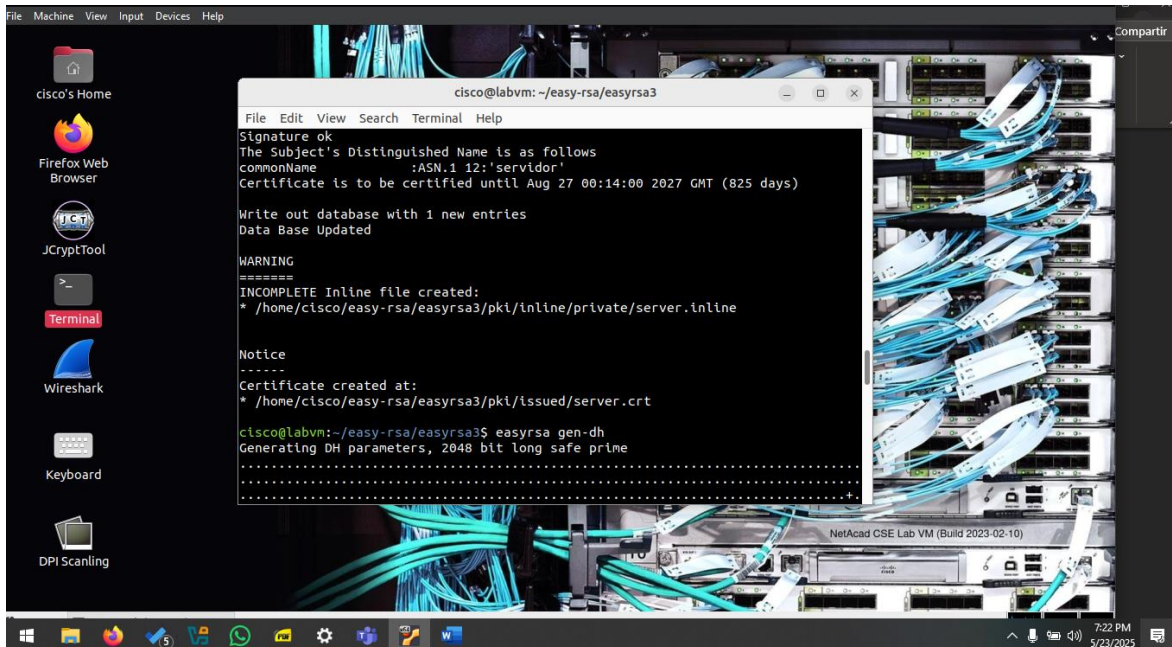
PASO 4: CONFIGURACIÓN DEL SERVIDOR VPN

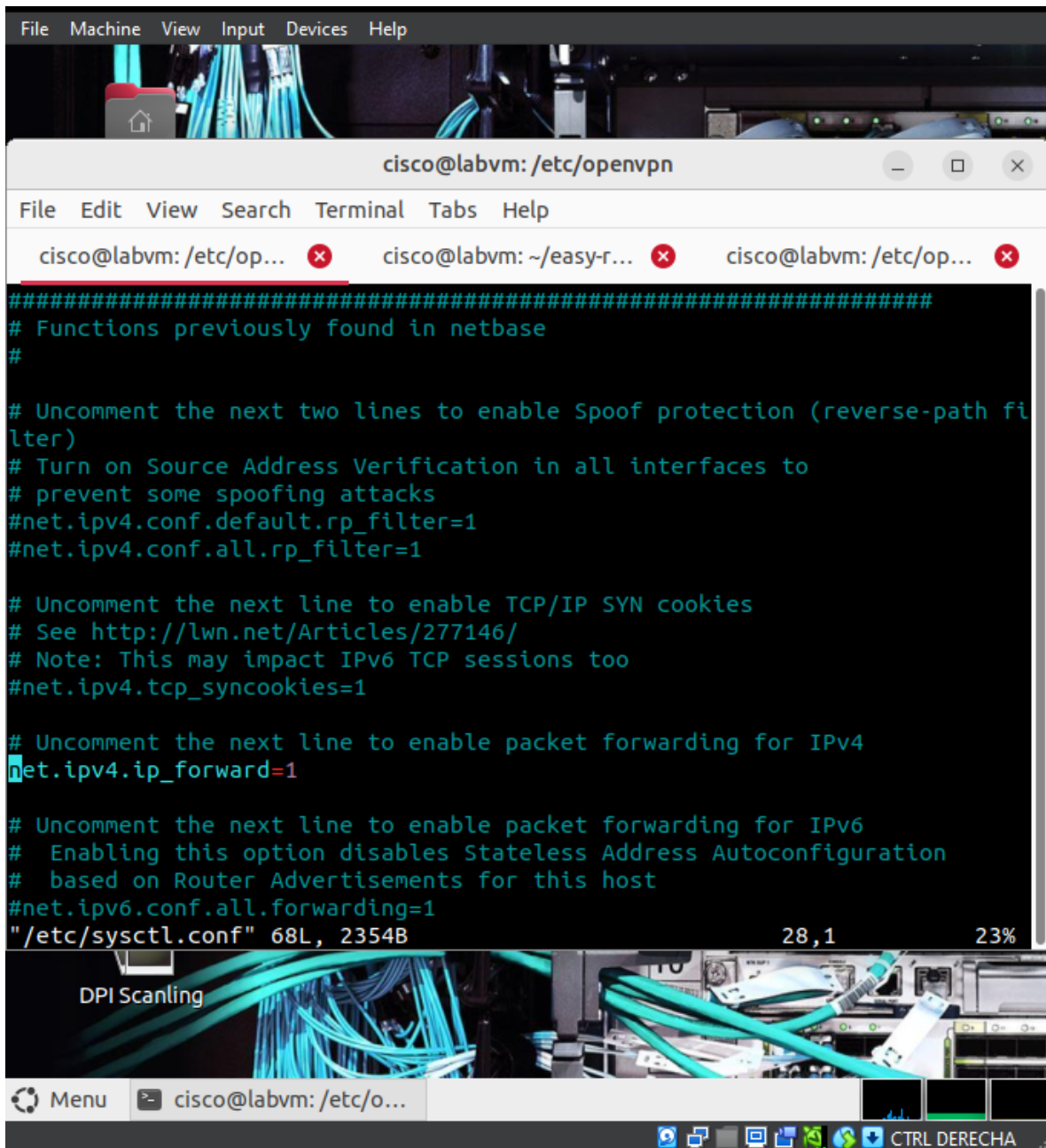


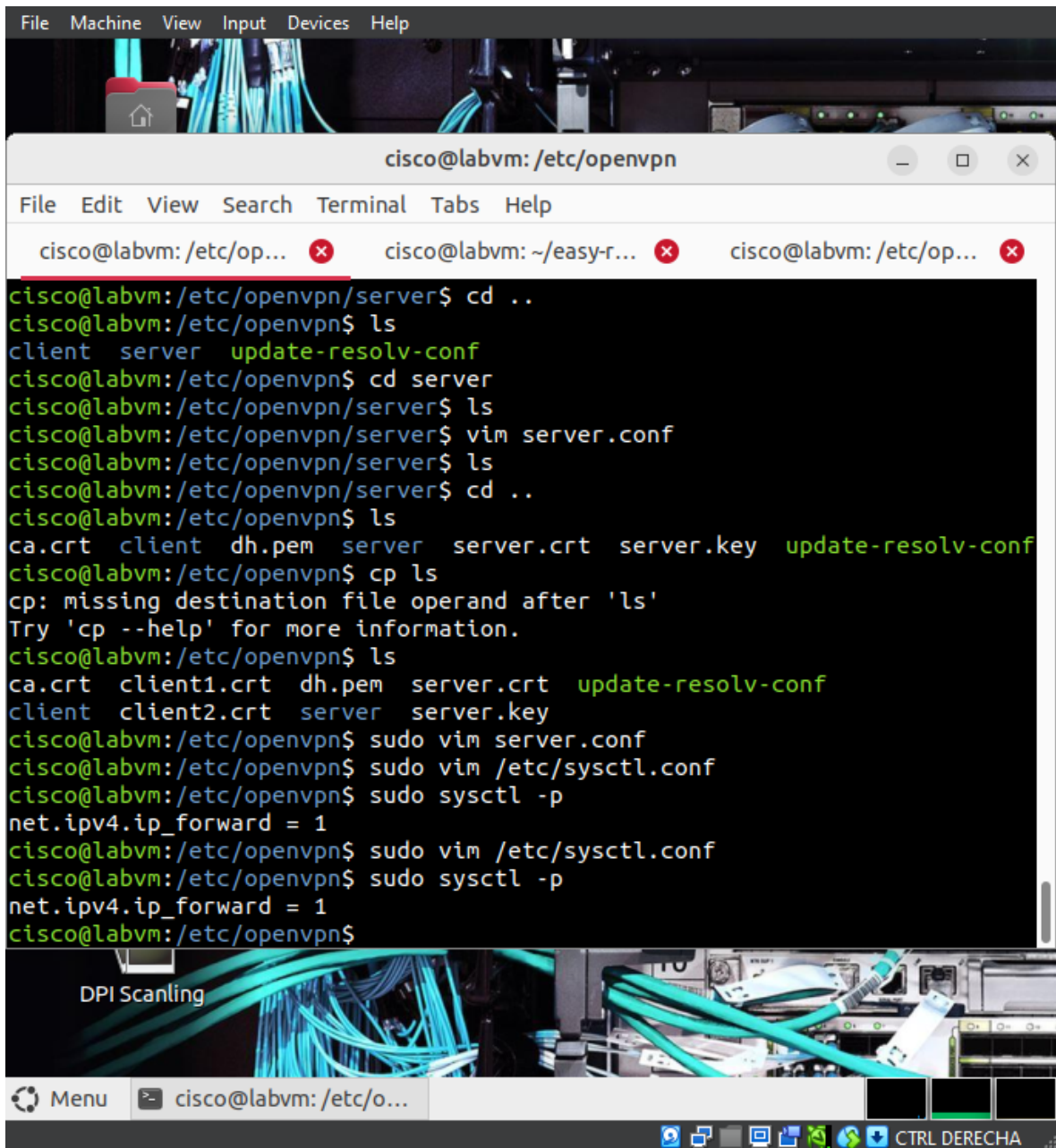


}

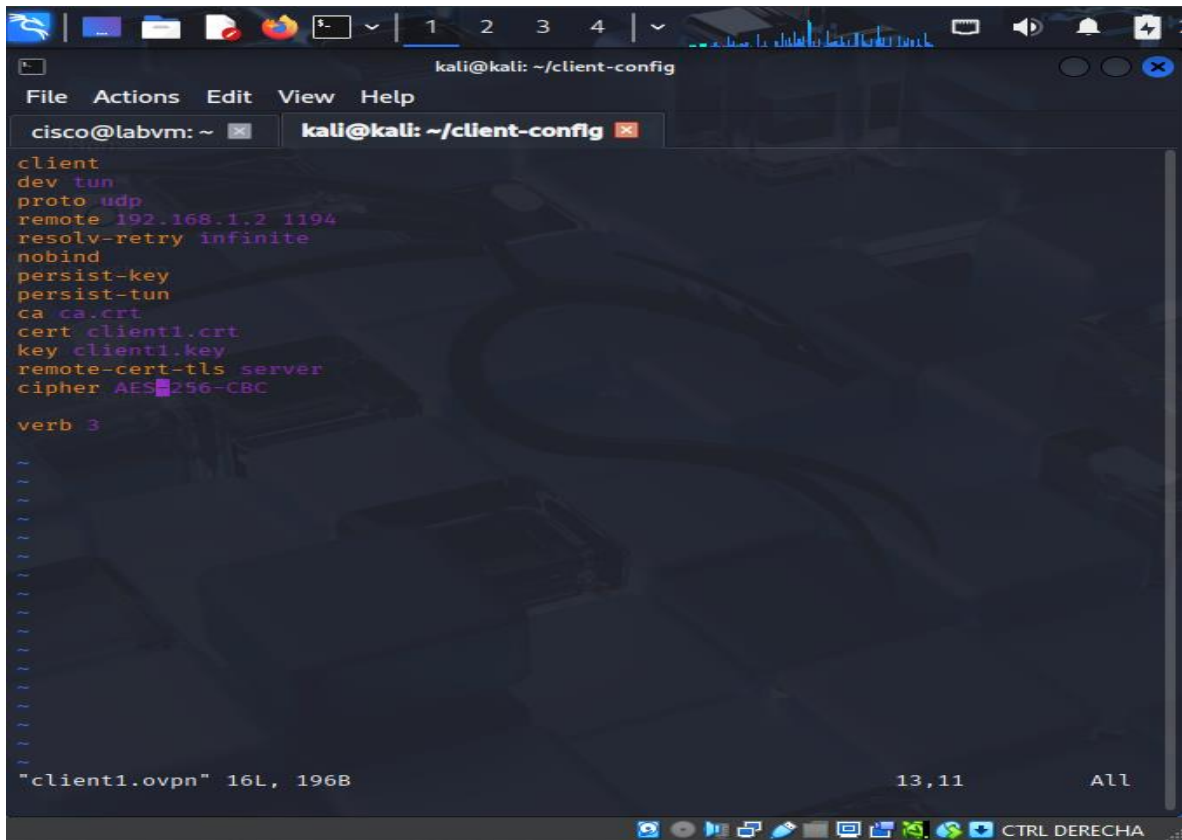
PARTE 4: CONFIGURACIÓN DEL SERVIDOR







PASO 5: CONFIGURACIÓN DEL CLIENTE



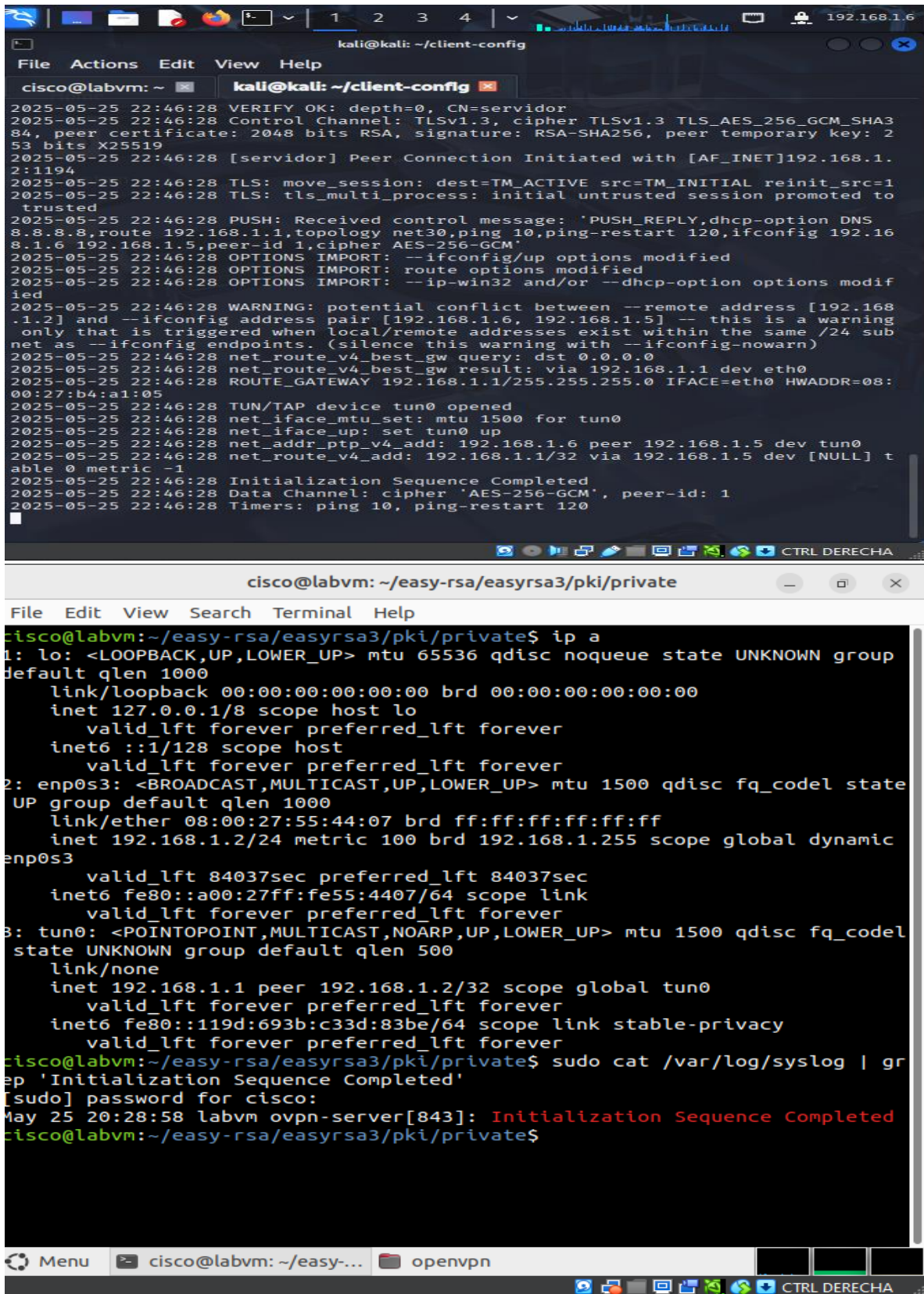
The screenshot shows a terminal window titled "kali@kali: ~/client-config". The window contains the following configuration for an OpenVPN client:

```
client
dev tun
proto udp
remote 192.168.1.2 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client1.crt
key client1.key
remote-cert-tls server
cipher AES-256-CBC

verb 3
```

At the bottom of the terminal, there is a status bar that reads: "client1.ovpn" 16L, 196B 13,11 All. The terminal window is part of a desktop environment with a taskbar at the bottom showing various application icons and the text "CTRL DERECHA".

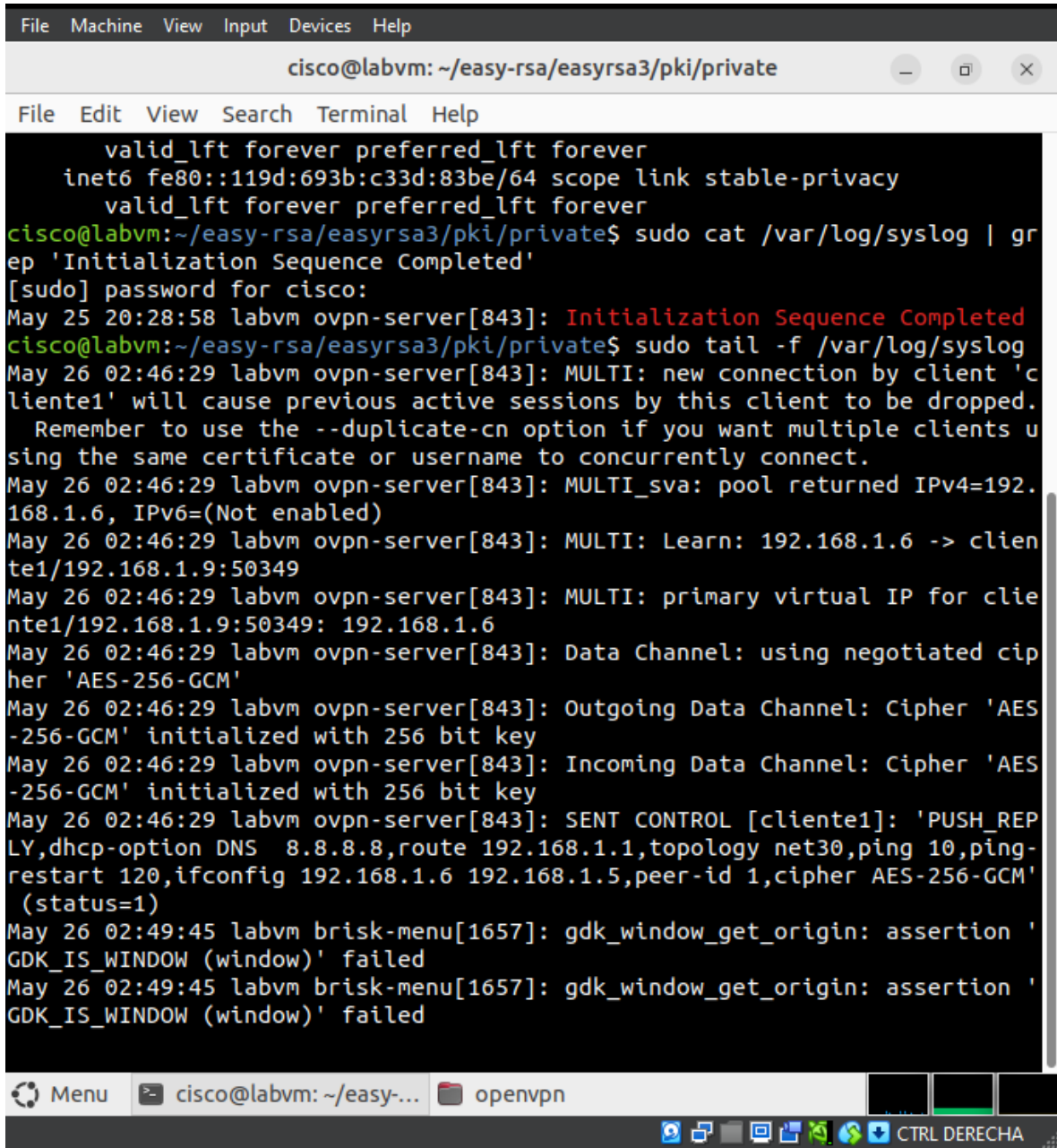
PASO 6 :VERIFICACIÓN DE CONEXIÓN



```
kali@kali: ~/client-config
File Actions Edit View Help
cisco@labvm: ~ kali@kali: ~/client-config
2025-05-25 22:46:28 VERIFY OK: depth=0, CN=servidor
2025-05-25 22:46:28 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA3
84, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporary key: 2
53 bits X25519
2025-05-25 22:46:28 [servidor] Peer Connection Initiated with [AF_INET]192.168.1.
2:1194
2025-05-25 22:46:28 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-05-25 22:46:28 TLS: tls_multi_process: initial untrusted session promoted to
trusted
2025-05-25 22:46:28 PUSH: Received control message: 'PUSH_REPLY,dhcp-option DNS
8.8.8.8,route 192.168.1.1,topology net30,ping 10,ping-restart 120,ifconfig 192.16
8.1.6 192.168.1.5,peer-id 1,cipher AES-256-GCM'
2025-05-25 22:46:28 OPTIONS IMPORT: --ifconfig/up options modified
2025-05-25 22:46:28 OPTIONS IMPORT: route options modified
2025-05-25 22:46:28 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modif
ied
2025-05-25 22:46:28 WARNING: potential conflict between --remote address [192.168
.1.2] and --ifconfig address pair [192.168.1.6, 192.168.1.5] -- this is a warning
only that is triggered when local/remote addresses exist within the same /24 sub
net as --ifconfig endpoints. (silence this warning with --ifconfig-nowarn)
2025-05-25 22:46:28 net_route_v4_best_gw query: dst 0.0.0.0
2025-05-25 22:46:28 net_route_v4_best_gw result: via 192.168.1.1 dev eth0
2025-05-25 22:46:28 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=eth0 HWADDR=08:
00:27:b4:a1:05
2025-05-25 22:46:28 TUN/TAP device tun0 opened
2025-05-25 22:46:28 net_iface_mtu_set: mtu 1500 for tun0
2025-05-25 22:46:28 net_iface_up: set tun0 up
2025-05-25 22:46:28 net_addr_ptp_v4_add: 192.168.1.6 peer 192.168.1.5 dev tun0
2025-05-25 22:46:28 net_route_v4_add: 192.168.1.1/32 via 192.168.1.5 dev [NULL] t
able 0 metric -1
2025-05-25 22:46:28 Initialization Sequence Completed
2025-05-25 22:46:28 Data Channel: cipher 'AES-256-GCM', peer-id: 1
2025-05-25 22:46:28 Timers: ping 10, ping-restart 120

cisco@labvm: ~/easy-rsa/easyrsa3/pki/private
File Edit View Search Terminal Help
cisco@labvm:~/easy-rsa/easyrsa3/pki/private$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
UP group default qlen 1000
    link/ether 08:00:27:55:44:07 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.2/24 metric 100 brd 192.168.1.255 scope global dynamic
enp0s3
        valid_lft 84037sec preferred_lft 84037sec
    inet6 fe80::a00:27ff:fe55:4407/64 scope link
        valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel
state UNKNOWN group default qlen 500
    link/none
    inet 192.168.1.1 peer 192.168.1.2/32 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::119d:693b:c33d:83be/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
cisco@labvm:~/easy-rsa/easyrsa3/pki/private$ sudo cat /var/log/syslog | gr
ep 'Initialization Sequence Completed'
[sudo] password for cisco:
May 25 20:28:58 labvm ovpn-server[843]: Initialization Sequence Completed
cisco@labvm:~/easy-rsa/easyrsa3/pki/private$
```


PASO 7: MONITOREO DE CONEXIONES

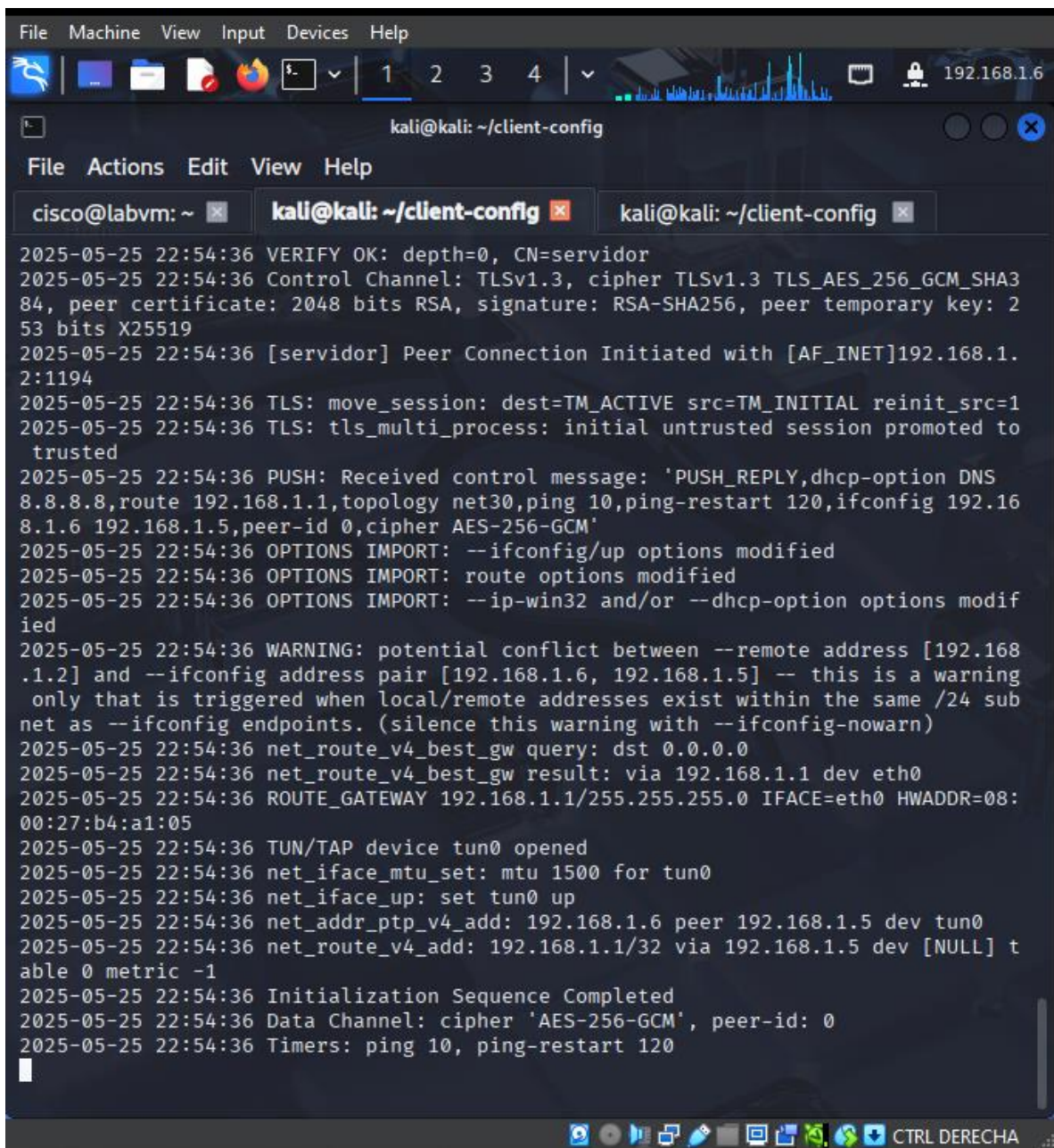


The screenshot shows a terminal window titled 'cisco@labvm: ~/easy-rsa/easyrsa3/pki/private'. The terminal displays the following commands and output:

```
File Machine View Input Devices Help
cisco@labvm: ~/easy-rsa/easyrsa3/pki/private
File Edit View Search Terminal Help

valid_lft forever preferred_lft forever
inet6 fe80::119d:693b:c33d:83be/64 scope link stable-privacy
valid_lft forever preferred_lft forever
cisco@labvm:~/easy-rsa/easyrsa3/pki/private$ sudo cat /var/log/syslog | gr
ep 'Initialization Sequence Completed'
[sudo] password for cisco:
May 25 20:28:58 labvm ovpn-server[843]: Initialization Sequence Completed
cisco@labvm:~/easy-rsa/easyrsa3/pki/private$ sudo tail -f /var/log/syslog
May 26 02:46:29 labvm ovpn-server[843]: MULTI: new connection by client 'c
liente1' will cause previous active sessions by this client to be dropped.
Remember to use the --duplicate-cn option if you want multiple clients u
sing the same certificate or username to concurrently connect.
May 26 02:46:29 labvm ovpn-server[843]: MULTI_sva: pool returned IPv4=192.
168.1.6, IPv6=(Not enabled)
May 26 02:46:29 labvm ovpn-server[843]: MULTI: Learn: 192.168.1.6 -> clien
te1/192.168.1.9:50349
May 26 02:46:29 labvm ovpn-server[843]: MULTI: primary virtual IP for clie
nte1/192.168.1.9:50349: 192.168.1.6
May 26 02:46:29 labvm ovpn-server[843]: Data Channel: using negotiated cip
her 'AES-256-GCM'
May 26 02:46:29 labvm ovpn-server[843]: Outgoing Data Channel: Cipher 'AES
-256-GCM' initialized with 256 bit key
May 26 02:46:29 labvm ovpn-server[843]: Incoming Data Channel: Cipher 'AES
-256-GCM' initialized with 256 bit key
May 26 02:46:29 labvm ovpn-server[843]: SENT CONTROL [cliente1]: 'PUSH_REP
LY,dhcp-option DNS 8.8.8.8,route 192.168.1.1,topology net30,ping 10,ping-
restart 120,ifconfig 192.168.1.6 192.168.1.5,peer-id 1,cipher AES-256-GCM'
(status=1)
May 26 02:49:45 labvm brisk-menu[1657]: gdk_window_get_origin: assertion '
GDK_IS_WINDOW (window)' failed
May 26 02:49:45 labvm brisk-menu[1657]: gdk_window_get_origin: assertion '
GDK_IS_WINDOW (window)' failed
```

The terminal window has a menu bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. The title bar shows the user 'cisco@labvm' and the current directory '~/easy-rsa/easyrsa3/pki/private'. The bottom status bar shows a 'Menu' button, the user 'cisco@labvm' and directory '~/easy-...', an 'openvpn' icon, and system icons including a network icon and a 'CTRL DERECHA' button.



```
File Machine View Input Devices Help
1 2 3 4 192.168.1.6
kali@kali: ~/client-config
File Actions Edit View Help
cisco@labvm: ~ kali@kali: ~/client-config kali@kali: ~/client-config
2025-05-25 22:54:36 VERIFY OK: depth=0, CN=servidor
2025-05-25 22:54:36 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA3
84, peer certificate: 2048 bits RSA, signature: RSA-SHA256, peer temporary key: 2
53 bits X25519
2025-05-25 22:54:36 [servidor] Peer Connection Initiated with [AF_INET]192.168.1.
2:1194
2025-05-25 22:54:36 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-05-25 22:54:36 TLS: tls_multi_process: initial untrusted session promoted to
trusted
2025-05-25 22:54:36 PUSH: Received control message: 'PUSH_REPLY,dhcp-option DNS
8.8.8.8,route 192.168.1.1,topology net30,ping 10,ping-restart 120,ifconfig 192.16
8.1.6 192.168.1.5,peer-id 0,cipher AES-256-GCM'
2025-05-25 22:54:36 OPTIONS IMPORT: --ifconfig/up options modified
2025-05-25 22:54:36 OPTIONS IMPORT: route options modified
2025-05-25 22:54:36 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modif
ied
2025-05-25 22:54:36 WARNING: potential conflict between --remote address [192.168
.1.2] and --ifconfig address pair [192.168.1.6, 192.168.1.5] -- this is a warning
only that is triggered when local/remote addresses exist within the same /24 sub
net as --ifconfig endpoints. (silence this warning with --ifconfig-nowarn)
2025-05-25 22:54:36 net_route_v4_best_gw query: dst 0.0.0.0
2025-05-25 22:54:36 net_route_v4_best_gw result: via 192.168.1.1 dev eth0
2025-05-25 22:54:36 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=eth0 HWADDR=08:
00:27:b4:a1:05
2025-05-25 22:54:36 TUN/TAP device tun0 opened
2025-05-25 22:54:36 net_iface_mtu_set: mtu 1500 for tun0
2025-05-25 22:54:36 net_iface_up: set tun0 up
2025-05-25 22:54:36 net_addr_ptp_v4_add: 192.168.1.6 peer 192.168.1.5 dev tun0
2025-05-25 22:54:36 net_route_v4_add: 192.168.1.1/32 via 192.168.1.5 dev [NULL] t
able 0 metric -1
2025-05-25 22:54:36 Initialization Sequence Completed
2025-05-25 22:54:36 Data Channel: cipher 'AES-256-GCM', peer-id: 0
2025-05-25 22:54:36 Timers: ping 10, ping-restart 120
```