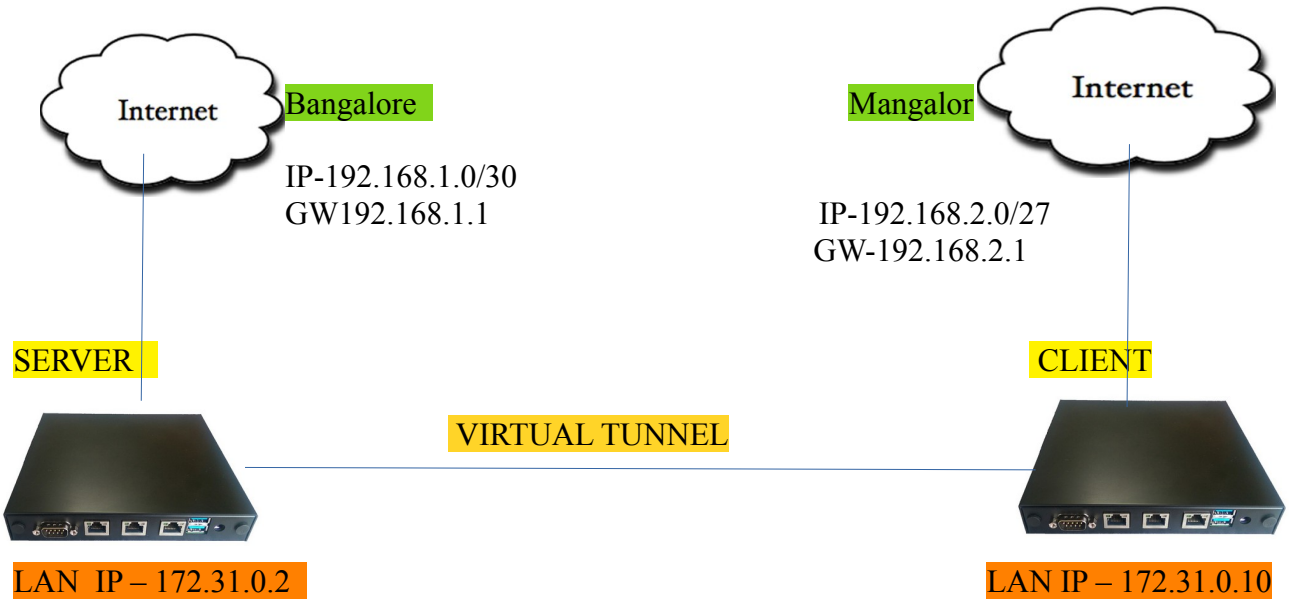

OpenVPN Bridging config:L2 VPN – when both side lan ip same

Firewall 1:

Server Mode: Peer to Peer (Shared Key)
Protocol: UDP
Device Mode: Tap
Interface: WAN (external interface)
Local Port: 1194
Shared Key: I let it auto generate…you can paste your own if you like (if you let it auto-generate, copy it as we will need to input it on Firewall2)
Encryption: I left at default AES-128-CBC again you can change to suit your environment
Tunnel Network: choose something NOT in use here, 10.20.30.0/24

SAVE

Go to Interfaces > assign > click the + symbol to add an interface and choose the 'ovpns1' from the drop down (this is the openvpn tap interface for the openvpn server we just setup)
Now go to Interface > OPT1 (or whatever NEW interface it appears as) > check the box for 'enable this interface' > rename to OVPN (for simplicity)
Now Interfaces > assign > bridges > hit the + > add LAN and OVPN to BRIDGE0

Navigate to Firewall > Rules
Create a new rule under WAN Action 'pass' > Interface WAN > protocol UDP > src:any > dst:any > dest port range: OpenVPN (1194)
Create a rule under OpenVPN to allow ALL traffic: proto * src * dest *
Create a rule under OVPN to allow ALL traffic: proto * src * dest *
Create a rule under OVPN to DENY traffic: proto udp src * dest * port 67-68(this is to deny DHCP from coming from the other side of the bridge)

now in my troubleshooting I had to edit the server conf file (/var/etc/openvpn/server1.conf use Diagnostics > edit file > browse to find it) and change the 'ifconfig' option
because it would input it as ifconfig 10.0.8.1 10.0.8.2 when instead it should have been ifconfig 10.0.8.1 255.255.255.248, I have since seen it appear to work with this step but it doesn't hurt (and it cleans up the logs).

SAVE

Firewall2

This is almost the same config > navigate to OpenVPN > 'client'

Server Mode: Peer to Peer: Shared Key
Protocol: UDP
Device Mode: tap
Interface: WAN
Server Host or address: input the public IP of Firewall1 here
Server port: 1194
Shared key: paste key here from Firewall1
Encryption: match it with Firewall1 in my case AES-128-CBC
Tunnel Network: 10.0.8.0/29 (same as on Firewall1)

SAVE

Edit the client config file /var/etc/openvpn/client1.conf and change the ifconfig to:
ifconfig 10.0.8.2 255.255.255.248

SAVE

Go to Interfaces > assign > click the + symbol to add an interface and choose the 'ovpnc1' from the drop down (this is the openvpn tap interface for the openvpn client we just setup)
Now go to Interface > OPT1 (or whatever NEW interface it appears as) > check the box for 'enable this interface' > rename to OVPN (for simplicity)
Now Interfaces > assign > bridges > hit the + > add LAN and OVPN to BRIDGE0

Navigate to Firewall > Rules
Create a new rule under WAN Action 'pass' > Interface WAN > protocol UDP > src:any > dst:any > dest port range: OpenVPN (1194) (I don't think you need this on the client side, but I did it just to be safe)
Create a rule under OpenVPN to allow ALL traffic: proto * src * dest *
Create a rule under OVPN to allow ALL traffic: proto * src * dest *
Create a rule under OVPN to DENY traffic: proto udp src * dest * port 67-68(this is to deny DHCP from coming from the other side of the bridge)

At this point you should be able to ping resources across the bridge!

below are my server1.conf and client1.conf respectively in case you would like to reference (Public IPs masked)

dev ovpns1
dev-type tap
dev-node /dev/tap1

writepid /var/run/openvpn_server1.pid
#user nobody
#group nobody
script-security 3
daemon
keepalive 10 60
ping-timer-rem
persist-tun
persist-key
proto udp
cipher AES-128-CBC
up /usr/local/sbin/ovpn-linkup
down /usr/local/sbin/ovpn-linkdown
local 11.x.x.x
ifconfig 10.0.8.1 255.255.255.248
lport 1194
management /var/etc/openvpn/server1.sock unix
secret /var/etc/openvpn/server1.secret

and client

dev ovpnc1
dev-type tap
dev-node /dev/tap1
writepid /var/run/openvpn_client1.pid
#user nobody
#group nobody
script-security 3
daemon
keepalive 10 60
ping-timer-rem
persist-tun
persist-key
proto udp
cipher AES-128-CBC
up /usr/local/sbin/ovpn-linkup
down /usr/local/sbin/ovpn-linkdown
local 24.x.x.x
lport 0
management /var/etc/openvpn/client1.sock unix
remote 11.x.x.x 1194
ifconfig 10.0.8.2 255.255.255.248
secret /var/etc/openvpn/client1.secret