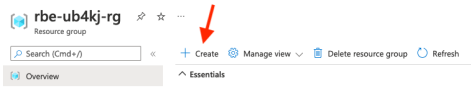
Azure VPN Configuration – Manual Method

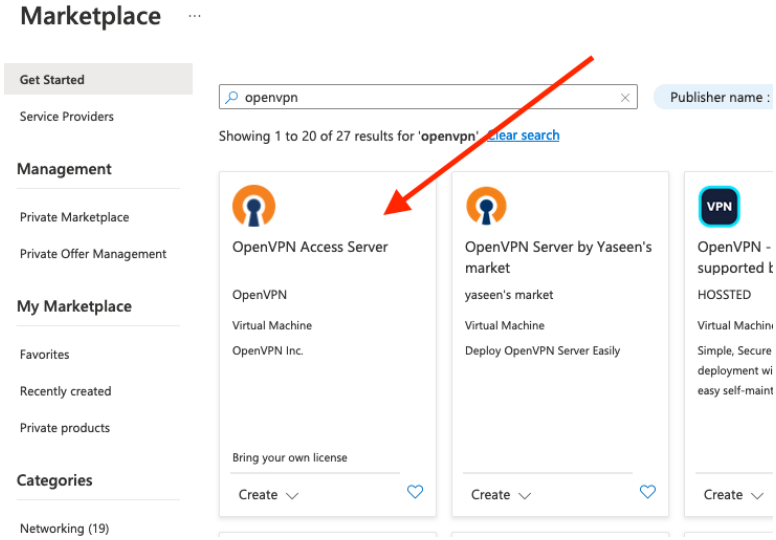
This document will walk through how to manually create an OpenVPN server on Azure for use with a private VNet.

1. Create the base VNet with an ingress subnet at a minimum

2. From the Azure Portal, navigate to the resource group of the created base VNet and select “+Create”



3. Search the marketplace for OpenVPN Access Server



4. Enter a valid name for the virtual

5. Select the region that matches the other resources in the resource group

6. Select either a new ssh key or an existing one for secure ssh logon

7. Move to the networking tab and select the required existing VNet, ingress subnet, network security group and either create a new public IP or use an existing one.

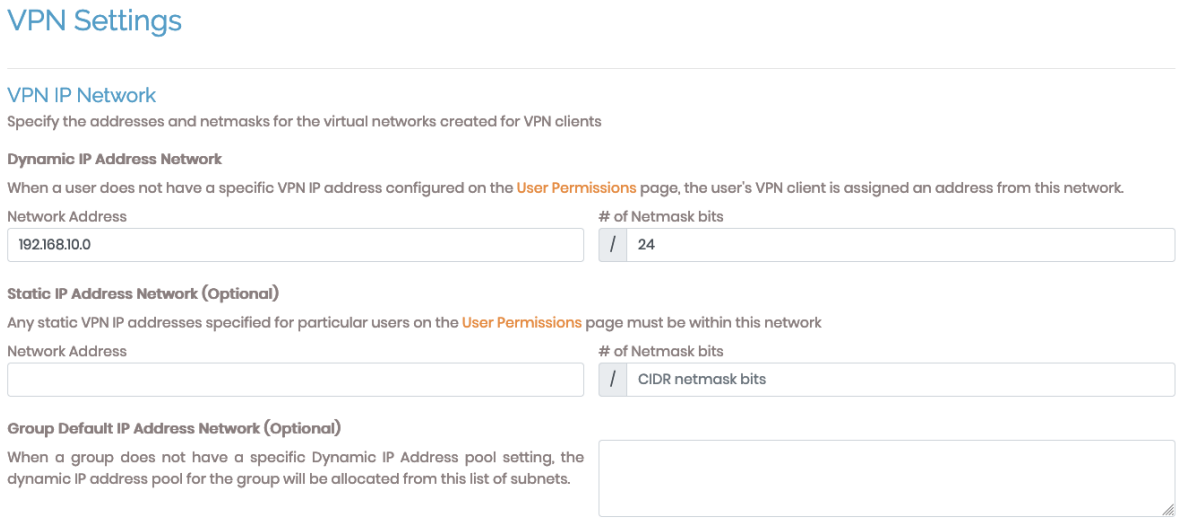
8. Move to the review and create tab. Review VM, then select create.

9. When the VM is built, ssh to server and reset openvpn password
   `$ sudo passwd azureuser`

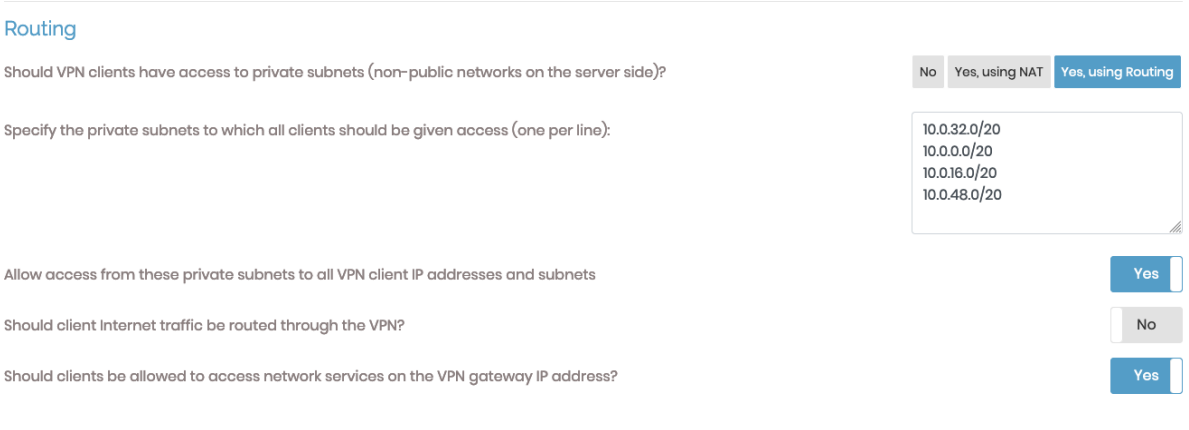
10. Connect to the admin portal at https://<public_ip>:943/admin
    Use the credentials for azureuser and the reset passwd

11. Navigate to CONFIGURATION -> VPN Settings

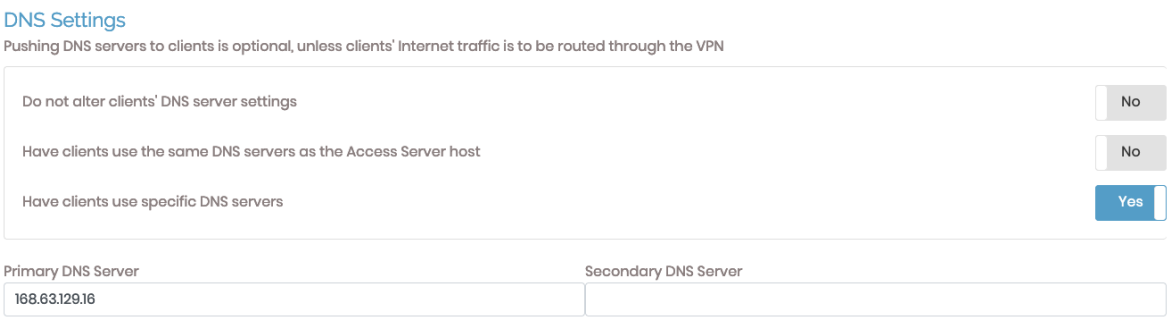
12. Change VPN Settings to use a unique Dynamic IP Address Network



13. Change to routing and add all the private subnets:

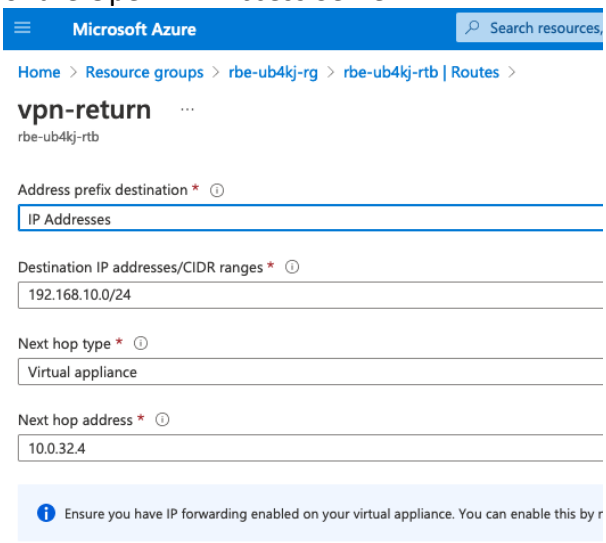


14. Change DNS Settings so that clients point to the Azure DNS



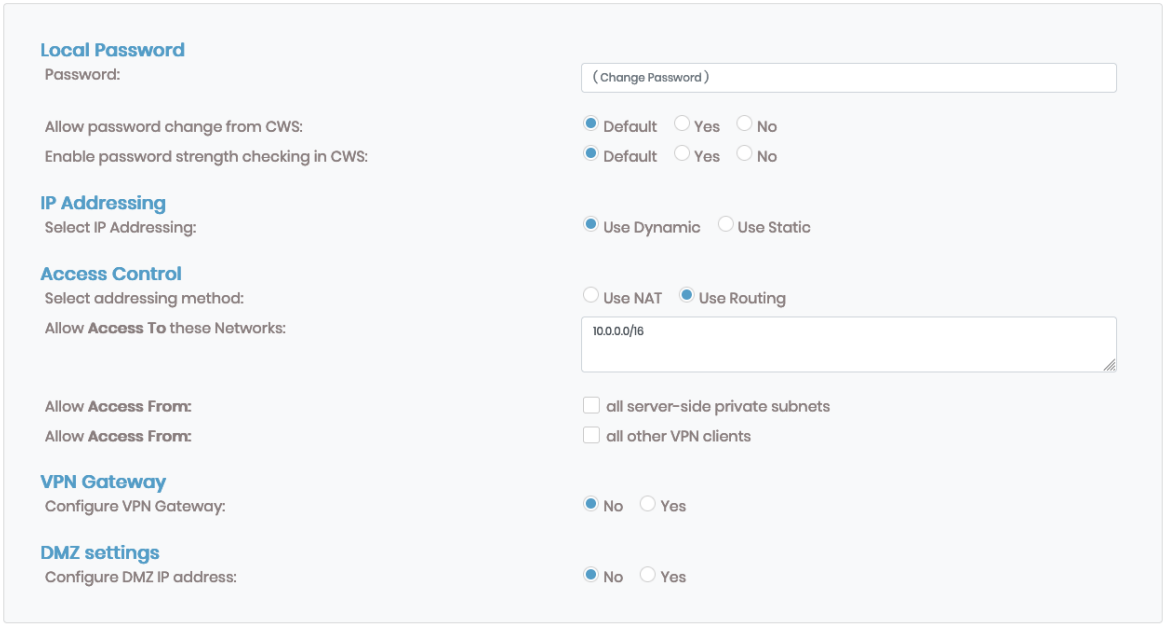
15. Press “Save Settings” button at the bottom of the page and then at the top of the page restart the server.

16. Create a return route in the VNet route table where the destination IP addresses is the CIDR of the VPN client group and the next hop address is the internal IP address of the OpenVPN Access Server.



17. Navigate to “USER MANAGEMENT” -> “User Permissions”

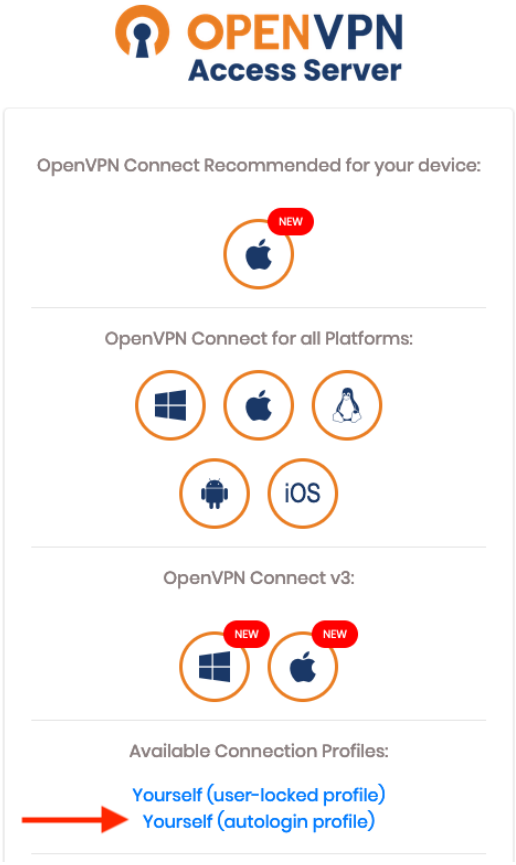
18. Add a new user by entering the details in the “New Username” box, select “Allow Auto-login” and select the “More Settings” button to drop down details. Select “Use Routing” and enter the VNet CIDR.



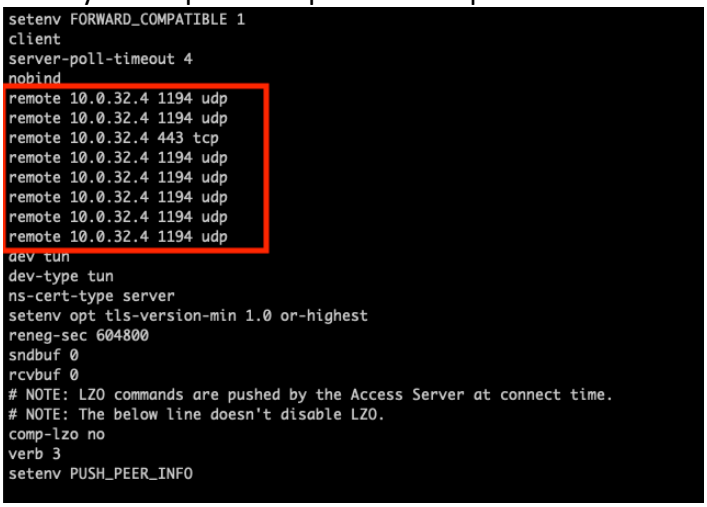
19. Change the password and save settings.

20. Login to the user portal at https://<public_ip>:943/ using the created user credentials

21. Download the openvpn configuration for autologin profile (providing you selected to allow auto-login when creating the user).



22. Modify the ovpn file to point to the public IP address of the OpenVPN Access Server.



```
setenv FORWARD_COMPATIBLE 1
client
server-poll-timeout 4
nobind
remote 10.0.32.4 1194 udp
remote 10.0.32.4 1194 udp
remote 10.0.32.4 443 tcp
remote 10.0.32.4 1194 udp
remote 10.0.32.4 1194 udp
remote 10.0.32.4 1194 udp
remote 10.0.32.4 1194 udp
remote 10.0.32.4 1194 udp
dev tun
dev-type tun
ns-cert-type server
setenv opt tls-version-min 1.0 or-highest
reneg-sec 604800
sndbuf 0
rcvbuf 0
# NOTE: LZO commands are pushed by the Access Server at connect time.
# NOTE: The below line doesn't disable LZO.
comp-lzo no
verb 3
setenv PUSH_PEER_INFO
```

With CLI:

```
$ cat client.ovpn | sed 's/<old_ip>/<new_ip>/g' > new-file.ovpn
```

23. Install openvpn client locally and run,
    ```
    $ sudo openvpn new-file.ovpn
    ```