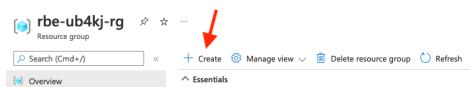


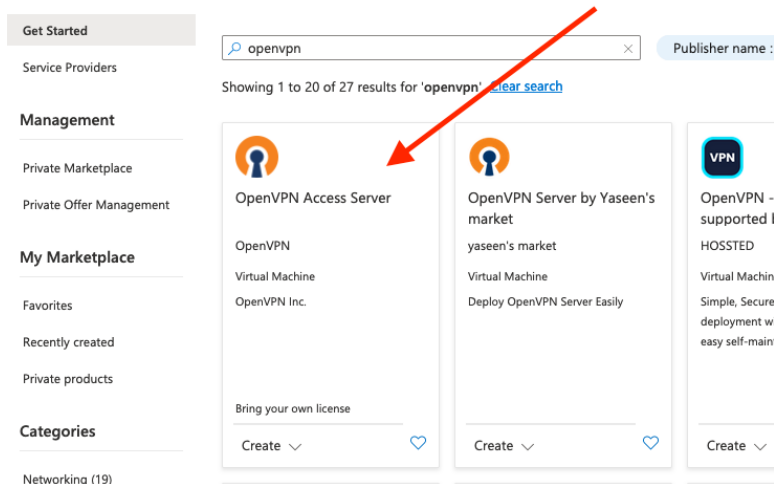
Azure VPN Configuration – Manual Method

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
Marketplace ...



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 login
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
VPN Settings

VPN IP Network

Specify the addresses and netmasks for the virtual networks created for VPN clients

Dynamic IP Address Network

When a user does not have a specific VPN IP address configured on the [User Permissions](#) page, the user's VPN client is assigned an address from this network.

Network Address

192.168.10.0

of Netmask bits

/ 24

Static IP Address Network (Optional)

Any static VPN IP addresses specified for particular users on the [User Permissions](#) page must be within this network

Network Address

of Netmask bits

/ CIDR netmask bits

Group Default IP Address Network (Optional)

When a group does not have a specific Dynamic IP Address pool setting, the dynamic IP address pool for the group will be allocated from this list of subnets.

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

Routing

Should VPN clients have access to private subnets (non-public networks on the server side)?

☐ No
 ☐ Yes, using NAT
 ☒ Yes, using Routing

Specify the private subnets to which all clients should be given access (one per line):

10.0.32.0/20
10.0.0.0/20
10.0.16.0/20
10.0.48.0/20

Allow access from these private subnets to all VPN client IP addresses and subnets

☒ Yes

Should client Internet traffic be routed through the VPN?

☐ No

Should clients be allowed to access network services on the VPN gateway IP address?

☒ Yes

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

DNS Settings

Pushing DNS servers to clients is optional, unless clients' Internet traffic is to be routed through the VPN

Do not alter clients' DNS server settings

☐ No

Have clients use the same DNS servers as the Access Server host

☐ No

Have clients use specific DNS servers

☒ Yes

Primary DNS Server

168.63.129.16

Secondary DNS Server

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.

Microsoft Azure

Home > Resource groups > rbe-ub4kj-rg > rbe-ub4kj-rtb | Routes >

vpn-return ...

rbe-ub4kj-rtb

Address prefix destination * ⓘ

IP Addresses

Destination IP addresses/CIDR ranges * ⓘ

192.168.10.0/24

Next hop type * ⓘ

Virtual appliance

Next hop address * ⓘ

10.0.32.4

ⓘ Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by r

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.

Local Password

Password: (Change Password)

Allow password change from CWS: ☒ Default ☐ Yes ☐ No

Enable password strength checking in CWS: ☒ Default ☐ Yes ☐ No

IP Addressing

Select IP Addressing: ☒ Use Dynamic ☐ Use Static

Access Control

Select addressing method: ☐ Use NAT ☒ Use Routing

Allow Access To these Networks: 10.0.0/16

Allow Access From: ☐ all server-side private subnets

Allow Access From: ☐ all other VPN clients

VPN Gateway

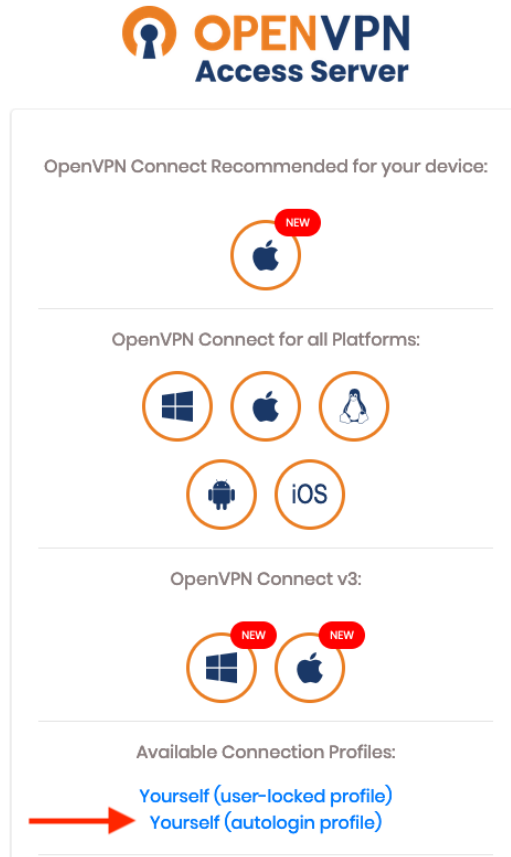
Configure VPN Gateway: ☒ No ☐ Yes

DMZ settings

Configure DMZ IP address: ☒ No ☐ Yes

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: LZ0 commands are pushed by the Access Server at connect time.
# NOTE: The below line doesn't disable LZ0.
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`