

OpenVPN Setup in Cloud-Vm

First we need cloud instance. We have many options like AWS, Azure, Google cloud, Digital ocean, Linode, etc. Just create Ubuntu VM with a free tier, and allow SSH (22), http (80), https (443) ports.

Microsoft Azure portal interface showing the 'Create a virtual machine' wizard. The 'Inbound port rules' section is active, showing 'Public inbound ports' set to 'Allow selected ports' with 'HTTP (80), HTTPS (443), SSH (22)' selected. A warning message states: 'This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.'

Next, In Networking tab under public ip box click on "create new" then a dialog box will appear on the right side :

Microsoft Azure portal interface showing the 'Create a virtual machine' wizard with the 'Networking' tab selected. The 'Public IP' dropdown is set to '(new) openvpn1-ip' with a 'Create new' link. A dialog box titled 'Create public IP address' is open on the right, showing 'Name' as 'openvpn1-ip', 'SKU' as 'Basic', and 'Assignment' as 'Dynamic'. The 'OK' button is visible at the bottom of the dialog.

In Assignment, change it from dynamic to Static and hit ok :

Create public IP address ×

Name *

openvpn1-ip ✓

SKU ?


☒ Basic ☐ Standard

Assignment


☐ Dynamic ☒ Static

OK

Continue next till review & create, review your VM and create it. After deploying VM, go to networking tab :

 **openvpn1** ✈ ...

Virtual machine

 Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Disks

Size

Security

Advisor recommendations

Extensions + applications

Continuous delivery

Click on Add Inbound Port Rules :

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20211205021508 > openvpn1

openvpn1 | Networking

Virtual machine

Search (Ctrl+ /) « Attach network interface Detach network interface Feedback

Virtual network/subnet: openvpn1-vnet/default NIC Public IP: 20.115.127.134 NIC Private IP: 10.1.0.4 Accelerated networking: Disabled

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group openvpn1-nsg (attached to network interface: openvpn1517)
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
320	HTTP	80	TCP	Any	Any	Allow
340	HTTPS	443	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Add Inbound port rules :

Source	Destination	Permission
Any	943/tcp	Allow
Any	1194/udp	Allow

It is very important to allow these ports as they are default ports used by OpenVPN access server. If you will not allow them then your client will not be able to connect to the VPN server.

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20211205021508 > openvpn1

openvpn1 | Networking

Virtual machine

Search (Ctrl+ /) « Attach network interface Detach network interface Feedback

IP configuration ⓘ
ipconfig1 (Primary)

Network Interface: openvpn1517 Effective security rules Troubleshoot

Virtual network/subnet: openvpn1-vnet/default NIC Public IP: 20.115.127.134

Inbound port rules Outbound port rules Application security groups

Network security group openvpn1-nsg (attached to network interface: openvpn1517)
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol
300	SSH	22	TCP
320	HTTP	80	TCP
340	HTTPS	443	TCP
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalan...	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule

openvpn1-nsg

Source ⓘ
Any

Source port ranges * ⓘ
*

Destination ⓘ
Any

Service ⓘ
Custom

Destination port ranges * ⓘ
943 ✓

Protocol
☐ Any
☒ TCP
☐ UDP
☐ ICMP

Add Cancel

First Port you have to add is 943, type it in destination port ranges and choose protocol as TCP. Then Scroll down and write name of the port rule and priority value. Then hit on Add button.

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20211205021508 > openvpn1

openvpn1 | Networking

Virtual machine

Search (Ctrl+/)

Attach network interface Detach network interface Feedback

IP configuration ⓘ
ipconfig1 (Primary)

Network Interface: openvpn1517 Effective security rules Troubleshooting
Virtual network/subnet: openvpn1-vnet/default NIC Public IP: 20.115.127.134

Inbound port rules Outbound port rules Application security groups

Network security group openvpn1-nsg (attached to network interface: openvpn1517)
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol
300	SSH	22	TCP
320	HTTP	80	TCP
340	HTTPS	443	TCP
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalanc...	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule openvpn1-nsg

Any
☒ TCP
UDP
ICMP

Action
☒ Allow
Deny

Priority * ⓘ
350

Name *
tcp_openvpn ✓

Description

Add Cancel

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20211205021508 > openvpn1

openvpn1 | Networking

Virtual machine

Search (Ctrl+/)

Attach network interface Detach network interface Feedback

IP configuration ⓘ
ipconfig1 (Primary)

Network Interface: openvpn1517 Effective security rules Troubleshooting
Virtual network/subnet: openvpn1-vnet/default NIC Public IP: 20.115.127.134

Inbound port rules Outbound port rules Application security groups

Network security group openvpn1-nsg (attached to network interface: openvpn1517)
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol
300	SSH	22	TCP
320	HTTP	80	TCP
340	HTTPS	443	TCP
350	tcp_openvpn	943	TCP
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalanc...	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule openvpn1-nsg

Source ⓘ
Any

Source port ranges * ⓘ
*

Destination ⓘ
Any

Service ⓘ
Custom

Destination port ranges * ⓘ
1194 ✓

Protocol
Any
TCP
☒ UDP
ICMP

Add Cancel

After that you have to add second port which is UDP port 1194, type 1194 in destination port ranges and select protocol UDP. Scroll down and give priority value and name for the port rule and hit Add button.

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20211205021508 > openvpn1

openvpn1 | Networking

Virtual machine

Search (Ctrl+/)

Attach network interface Detach network interface Feedback

IP configuration ⓘ
ipconfig1 (Primary)

Network Interface: openvpn1517 Effective security rules Troubleshooting
Virtual network/subnet: openvpn1-vnet/default NIC Public IP: 20.115.127.134

Inbound port rules Outbound port rules Application security groups

Network security group openvpn1-nsg (attached to network interface: openvpn1517)
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol
300	SSH	22	TCP
320	HTTP	80	TCP
340	HTTPS	443	TCP
350	tcp_openvpn	943	TCP
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalanc...	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule openvpn1-nsg

Any
TCP
☒ UDP
ICMP

Action
☒ Allow
Deny

Priority * ⓘ
360 ✓

Name *
udp_openvpn ✓

Description

Add Cancel

Now you can see the inbound port rules added in the list along with other ports.

Home > CreateVm-canonical.0001-com-ubuntu-server-focal-2-20211205021508 > openvpn1

openvpn1 | Networking ...

Virtual machine

Search (Ctrl+/) << Attach network interface Detach network interface Feedback

Network Interface: openvpn1517 Effective security rules Troubleshoot VM connection issues Topology

Virtual network/subnet: openvpn1-vnet/default NIC Public IP: **20.115.127.134** NIC Private IP: **10.1.0.4** Accelerated networking: **Disabled**

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group **openvpn1-nsg** (attached to network interface: openvpn1517)
Impacts 0 subnets, 1 network interfaces **Add inbound port rule**

Priority	Name	Port	Protocol	Source	Destination	Action	
300	SSH	22	TCP	Any	Any	Allow	...
320	HTTP	80	TCP	Any	Any	Allow	...
340	HTTPS	443	TCP	Any	Any	Allow	...
350	tcp_openvpn	943	TCP	Any	Any	Allow	...
360	udp_openvpn	1194	UDP	Any	Any	Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

Get back to Overview tab and there you can that you have public IP address of the machine, copy it.

Open your terminal/cmd/PowerShell.

Log into your machine via SSH :

```
$ ssh user@public_ip_address
```

In place of,

user = your username which you have set while creating the VM.

public_ip_address = public ip address of your VM.

If port of ssh is defined is different then :

```
# ssh -P port_number user@public_ip_address
```

First, update and upgrade your repo :

```
$ sudo apt update
$ sudo apt upgrade
```

Setup the password for the root :

```
$ sudo passwd root
```

You need to download the GitHub script of OpenVPN access server, for more guide you can visit <https://github.com/Nyr/openvpn-install>

```
$ wget https://git.io/vpn -O openvpn-install.sh
```

```
axer@openvpn1: ~
axer@openvpn1:~$ wget https://git.io/vpn -O openvpn-install.sh
--2021-12-04 20:57:01-- https://git.io/vpn
Resolving git.io (git.io)... 52.204.242.176, 18.205.36.100, 54.157.58.70, ...
Connecting to git.io (git.io)|52.204.242.176|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh [following]
--2021-12-04 20:57:01-- https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh [following]
--2021-12-04 20:57:01-- https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.110.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23501 (23K) [text/plain]
Saving to: 'openvpn-install.sh'

openvpn-install.sh      100%[=====>] 22.95K  --.-KB/s  in 0s

2021-12-04 20:57:01 (83.4 MB/s) - 'openvpn-install.sh' saved [23501/23501]

axer@openvpn1:~$
```

Then you have to run the script, If you are using CMD/PowerShell then :

```
$ sudo bash openvpn-install.sh
```

```
axer@openvpn1: ~  
axer@openvpn1:~$ sudo bash openvpn-install.sh_
```

But if your using Linux Terminal then, first you may have to make it executable first and then run it :

```
$ sudo chmod +x openvpn-install.sh  
$ sudo ./openvpn-install.sh
```

```
axer@openvpn1: ~  
axer@openvpn1:~$ sudo ./openvpn-install.sh_
```

Then you will be prompted with the installer welcome!

Here you will find the first option about your ip address, put in your VM's public ip address and hit enter. Then you will be asked about the port number where you want your server to listen on, you can keep it default 1194 as we have allowed that port earlier so no need to change it and hit enter. Then, choose the DNS of your choice, Best DNS from the security perspective is of Cloudflare (1.1.1.1), so will recommend in using that otherwise, there are tons of options you can choose whichever you are comfortable with. Then you will be asked the first client name. Give it a name and your client configuration file will be created.

```
axer@openvpn1: ~  
Welcome to this OpenVPN road warrior installer!  
  
This server is behind NAT. What is the public IPv4 address or hostname?  
Public IPv4 address / hostname [20.115.127.134]:  
  
Which protocol should OpenVPN use?  
1) UDP (recommended)  
2) TCP  
Protocol [1]:  
  
What port should OpenVPN listen to?  
Port [1194]:  
  
Select a DNS server for the clients:  
1) Current system resolvers  
2) Google  
3) 1.1.1.1  
4) OpenDNS  
5) Quad9  
6) AdGuard  
DNS server [1]: 3  
  
Enter a name for the first client:  
Name [client]: axer
```



```

axer@openvpn1: ~
.....+++++
writing new private key to '/etc/openvpn/server/easy-rsa/pki/easy-rsa-3419.Sxes16/tmp.xMzrBP'
-----
Using configuration from /etc/openvpn/server/easy-rsa/pki/easy-rsa-3419.Sxes16/tmp.qj8Rzj
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'server'
Certificate is to be certified until Dec  2 20:59:06 2031 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated

Using SSL: openssl OpenSSL 1.1.1f  31 Mar 2020
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/openvpn/server/easy-rsa/pki/easy-rsa-3494.rmTJTv/tmp.YW6PAA'
-----
Using configuration from /etc/openvpn/server/easy-rsa/pki/easy-rsa-3494.rmTJTv/tmp.1avNhN
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'axer'
Certificate is to be certified until Dec  2 20:59:07 2031 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated

Using SSL: openssl OpenSSL 1.1.1f  31 Mar 2020
Using configuration from /etc/openvpn/server/easy-rsa/pki/easy-rsa-3550.Ihscix/tmp.WTuabt

An updated CRL has been created.
CRL file: /etc/openvpn/server/easy-rsa/pki/crl.pem

Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-iptables.service → /etc/systemd/system/openvpn-iptables.service.
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-server@server.service → /lib/systemd/system/openvpn-server@.service.

Finished!

The client configuration is available in: /root/axer.ovpn
New clients can be added by running this script again.
axer@openvpn1:~$

```

In the picture above, you can see that configuration file of the first client is saved under /root/axer.ovpn
So we can copy it to the home folder with :

```
# sudo cp /root/axer/axer.ovpn /home/axer
```

After doing this, you need to check the status of your OpenVPN server, if its running or not, to do so :

```
$ systemctl status openvpn
```

If its not running then :

```
$ systemctl restart openvpn
```

```

axer@openvpn1:~$ sudo systemctl restart openvpn
axer@openvpn1:~$ sudo systemctl openvpn status
Unknown operation openvpn.
axer@openvpn1:~$ sudo systemctl status openvpn
● openvpn.service - OpenVPN service
   Loaded: loaded (/lib/systemd/system/openvpn.service; enabled; vendor preset: enabled)
   Active: active (exited) since Sat 2021-12-04 21:10:17 UTC; 19s ago
     Process: 4133 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 4133 (code=exited, status=0/SUCCESS)

Dec 04 21:10:17 openvpn1 systemd[1]: Starting OpenVPN service...
Dec 04 21:10:17 openvpn1 systemd[1]: Finished OpenVPN service.
axer@openvpn1:~$

```

Then you will see that OpenVPN service will start running.

Next check on the Linux Firewall status :

```
$ ufw status
```

If its inactive, then enable it :

```
$ sudo ufw enable
```

then you'll see that its status is active now.

```

axer@openvpn1: ~
axer@openvpn1:~$ sudo ufw status
Status: inactive
axer@openvpn1:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
axer@openvpn1:~$ sudo ufw status
Status: active
axer@openvpn1:~$ sudo ufw allow 80/tcp
Rule added
Rule added (v6)
axer@openvpn1:~$ sudo ufw allow 443/tcp
Rule added
Rule added (v6)
axer@openvpn1:~$ sudo ufw allow 943/tcp
Rule added
Rule added (v6)
axer@openvpn1:~$ sudo ufw allow 1194/udp
Rule added
Rule added (v6)
axer@openvpn1:~$ sudo ufw status
Status: active

To Action From
--
80/tcp ALLOW Anywhere
443/tcp ALLOW Anywhere
943/tcp ALLOW Anywhere
1194/udp ALLOW Anywhere
80/tcp (v6) ALLOW Anywhere (v6)
443/tcp (v6) ALLOW Anywhere (v6)
943/tcp (v6) ALLOW Anywhere (v6)
1194/udp (v6) ALLOW Anywhere (v6)

axer@openvpn1:~$

```

After that allow some ports :

```

$ sudo ufw allow 22/tcp
$ sudo ufw allow 80/tcp
$ sudo ufw allow 443/tcp
$ sudo ufw allow 943/tcp
$ sudo ufw allow 1194/udp

```

After doing this, if you want to add more user's/clients to the VPN or u want to revoke any client then :

```

$ sudo ./openvpn-install.sh

```

run this script again, you'll get options to do and even to delete the OpenVPN server as well.

```

axer@openvpn1: ~
OpenVPN is already installed.

Select an option:
 1) Add a new client
 2) Revoke an existing client
 3) Remove OpenVPN
 4) Exit
Option:

```

Type :

- 1 to add new client,
- 2 to revoke an existing client,
- 3 to remove OpenVPN from the server,
- 4 to exit from the script.

After this if you want no logs on the server then you can checkout these two files for logs :

```

/usr/local/openvpn_as/etc/db/log.db
/var/log/openvpnas.log

```

You can edit these log files in order to save logs or not.

Now, in the end you have to transfer that .ovpn config files to your local machine, for that we can use `scp` , open command prompt if your on windows machine and type in :


```
# scp -P 22 user@public_ip_address:/home/user/client1.ovpn .
```

here, P = port number, dot (.) in the end is important in order to tell the machine to download the file in that respective folder where we are, so you should navigate yourself to the specific folder before executing that command.

```
C:\Users\Acer\Downloads>scp -P 22 axer@20.115.127.134:/home/axer/axer.ovpn .  
axer@20.115.127.134's password:  
axer.ovpn
```

```
100% 4990 20.3KB/s 00:00
```

```
C:\Users\Acer\Downloads>
```