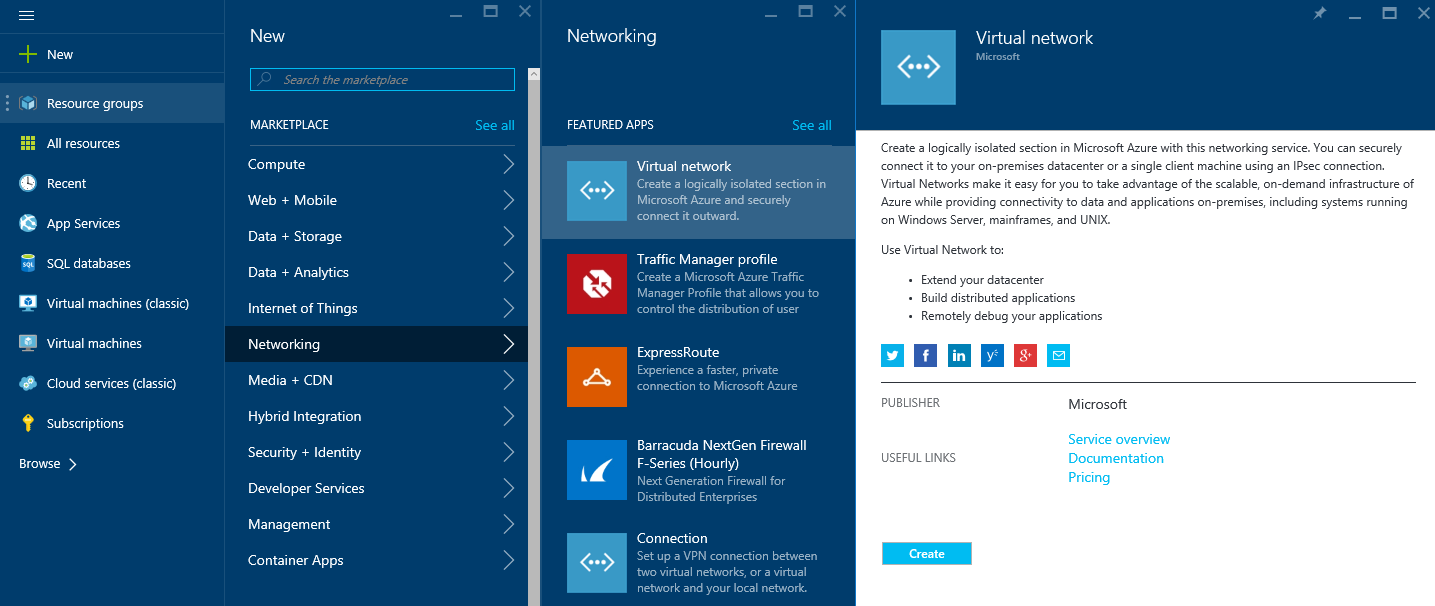
**Creating the Azure VPN**

In this section, we’ll be creating a virtual network in the Azure portal.

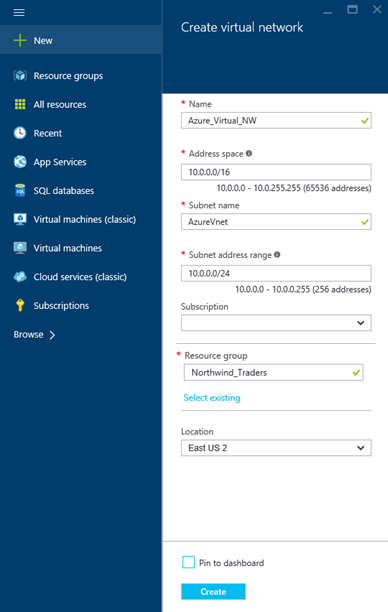
**Step 1:** Create the virtual network:

After login to Azure portal, click New -> Networking -> Virtual Network, Create

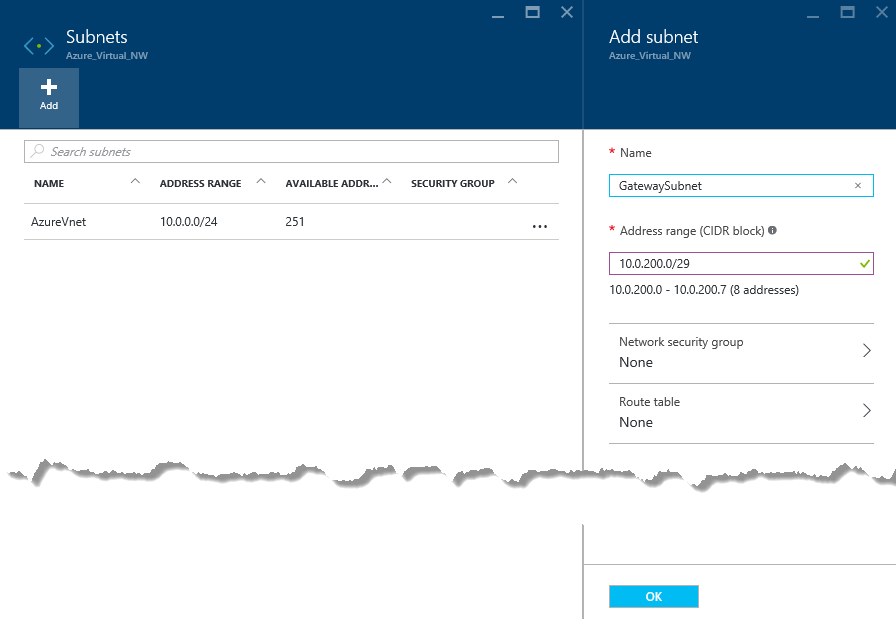


**Step 2:** Create new virtual network

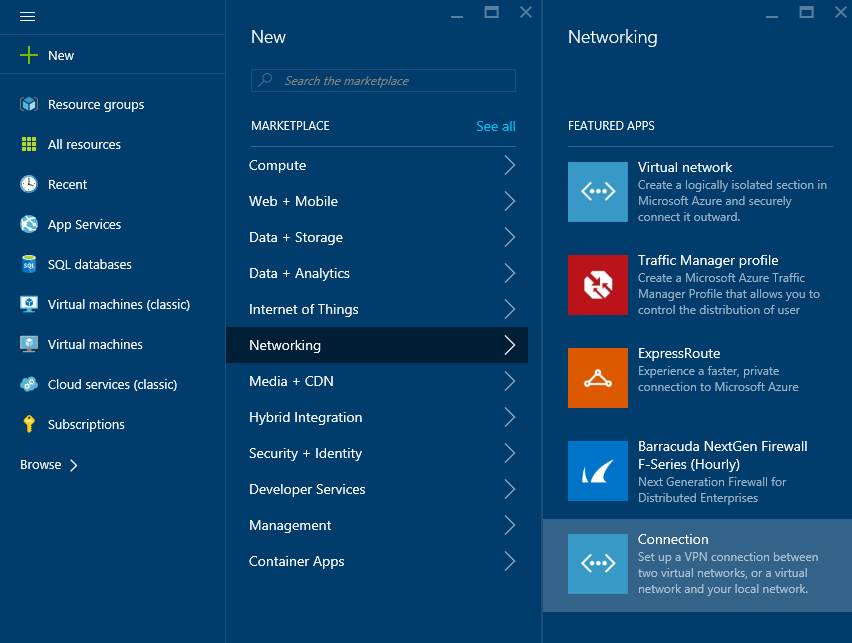
Fill in the name of Virtual Network, the Address range you wish to use in Azure, and the location.



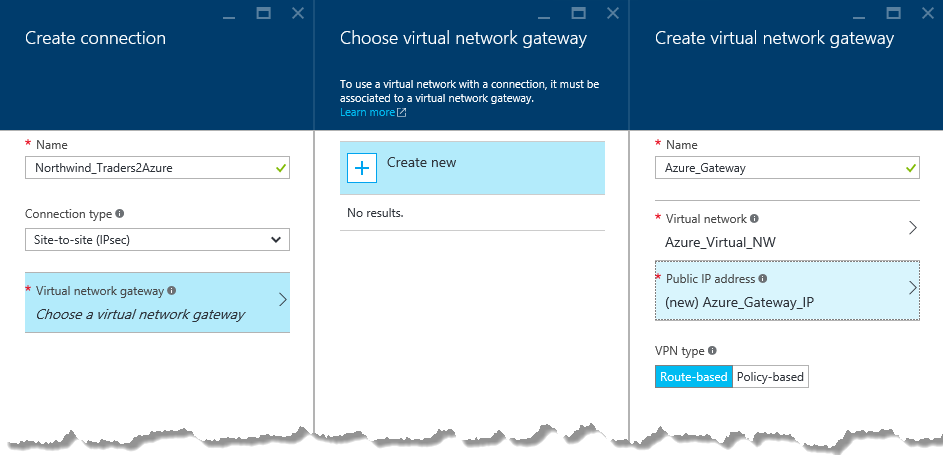
**Step 3:** After creation of a virtual network add a gateway subnet named GatewaySubnet



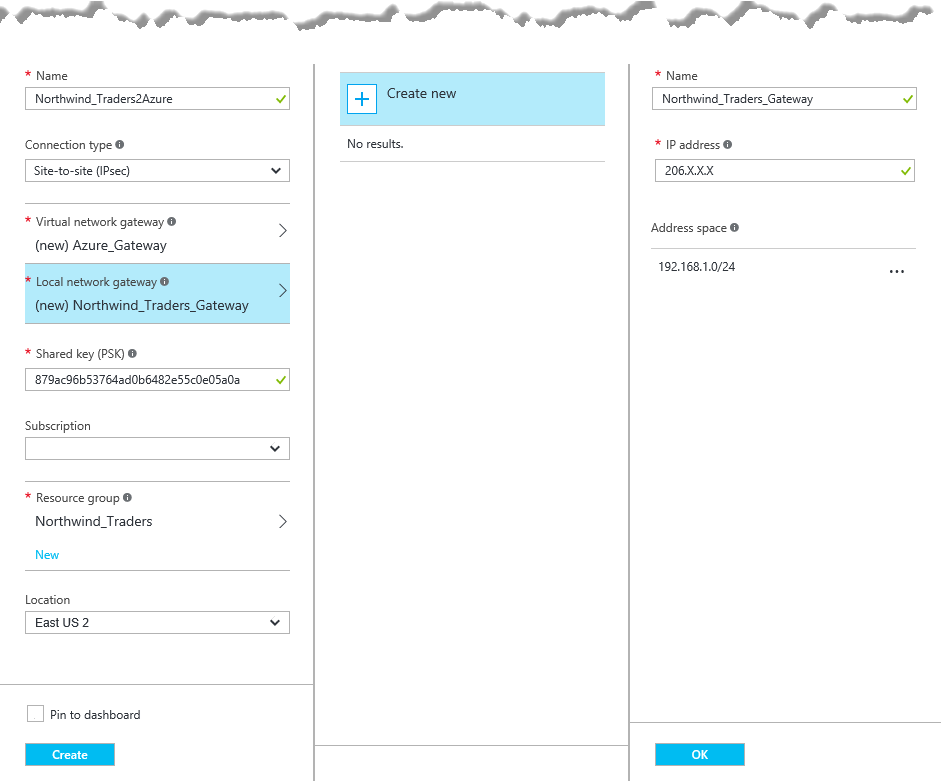
**Step 4:** Create a VPN Connection



**Step 5**: Setup Azure Route-based gateway



**Step 6:** Setup Local Gateway



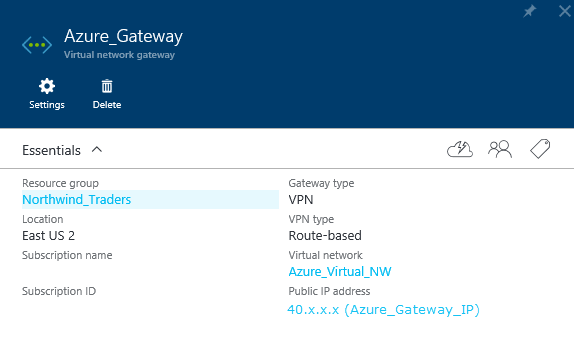
In our example:

**Local virtual network gateway:** 206.X.X.X *(SRX external interface IP (Public IP address)*

**Local Network Address:** 192.168.1.0/24 *(Your on-premises local network. Specify starting IP address of your network.)*

**Shared Key:** 879ac96b53764ad0b6482e55c0e05a0a

It takes couple of minutes to create Gateway Connection. Once created review the Virtual Network Gateway IP Address



**Configuring the SRX**

Now we need to configure the SRX. If you log in to the device as the root user, you enter the UNIX shell, which is indicated by the percent sign (%) as the prompt.

To access the Junos CLI, enter the cli command at the shell prompt:

Machine generated alternative text:
root e * cli 
root n •ure SR_» 

After logging in, you enter operational mode, which is indicated by the right angle bracket (>) From operational mode, use the configure command to enter configuration mode, which is indicated by the pound sign (#):

Machine generated alternative text:
root Azure SR_» configure 
Entering configuration mode 
(edit) 
root Azure SRX# 

One we have logged into Junos CLI we need to see what route can reach the Dynamic Azure Gateway

The Junos command is **run show route**

Machine generated alternative text:
root Azure SRX# run show route 
inet.O: S destinations, S routes (S active, 
ho I ddown , 
hidden) 
Active Route, 
o.o.o.o/o 
192.168 .1.0/24 
192.168.1.1/32 
Last Active, 
Both 
• (Static,'sl 
to 206.165.220.1 via fe-O/O/O.O 
• (Direct,'ol 
via vIan.I 
• (Local ,'01 
Local via VI an. I 
206.x.x.x/24 
206.x.x.x/32 
• (Direct,'ol 
via fe—O/O/O 
• (Local ,'01 
Local via fe— 
0/0/0 0 

In this example **fe-0/0/0.0** is the name of the External interface, **vlan.1** is the name of the Internal interface

We will need to show zone(s) with interface **fe-0/0/0.0**

The Junos command is **show security zones | display set | match fe-0/0/0.0**

Machine generated alternative text:
(edit) 
root"zure SRX# show security zones dis lay set I match fe—O/O/O.O 
set security zones security—zone Internet interfaces fe—O/O/O .0 

In this example Zone **Internet** is associated with interface **fe-0/0/0.0**

We will need to show zone(s) with interface **vlan.1**

The Junos command is **show security zones | display set | match vlan.1**

Machine generated alternative text:
root@Äzure SRX# show security zones I display set I match 
Vlan. I 
host — inbound —t raffi c 
host — inbound —t raffi c 
host — inbound —t raffi c 
host — inbound —t raffi c 
host — inbound —t raffi c 
host — inbound —t raf f i c 
system 
system 
system 
system 
system 
system 
— se ces 
p 1 ng 
https 
s sh 
te I net 
set 
set 
set 
set 
set 
security 
security 
security 
security 
security 
security 
zone s 
zone s 
zone s 
zone s 
zone s 
zone s 
security 
security 
security 
security 
security 
security 
— zone 
— zone 
— zone 
— zone 
— zone 
— zone 
Internal 
Inte rna I 
Inte rna I 
Inte rna I 
Inte rna I 
Inte rna I 
interfaces 
interfaces 
interfaces 
interfaces 
interfaces 
interfaces 
vIan . 
vIan . 
vIan . 
vIan . 
vIan . 

In this example Zone **Internal** is associated with interface **vlan.1**

The follow script may need to be modified to suit your device

*###Script Begin###*

*set security ike proposal azure-proposal authentication-method pre-shared-keys*

*set security ike proposal azure-proposal authentication-algorithm sha1*

*set security ike proposal azure-proposal encryption-algorithm aes-256-cbc*

*set security ike proposal azure-proposal lifetime-seconds 28800*

*set security ike proposal azure-proposal dh-group group2*

*set security ike policy azure-policy mode main*

*set security ike policy azure-policy proposals azure-proposal*

*set security ike policy azure-policy pre-shared-key ascii-text* ***879ac96b53764ad0b6482e55c0e05a0a***

*set security ike gateway azure-gateway ike-policy azure-policy*

*set security ike gateway azure-gateway address* ***40.X.X.X***

*set security ike gateway azure-gateway external-interface* ***fe-0/0/0.0***

*set security ike gateway azure-gateway version v2-only*

*set security ipsec proposal azure-ipsec-proposal protocol esp*

*set security ipsec proposal azure-ipsec-proposal authentication-algorithm hmac-sha1-96*

*set security ipsec proposal azure-ipsec-proposal encryption-algorithm aes-256-cbc*

*set security ipsec proposal azure-ipsec-proposal lifetime-seconds 3600*

*set security ipsec policy azure-vpn-policy proposals azure-ipsec-proposal*

*set security ipsec vpn azure-ipsec-vpn ike gateway azure-gateway*

*set security ipsec vpn azure-ipsec-vpn ike ipsec-policy azure-vpn-policy*

*set security zones security-zone* ***Internal*** *interfaces* ***vlan.1***

*set security zones security-zone* ***Internal*** *host-inbound-traffic system-services ike*

*set security zones security-zone* ***Internal*** *address-book address onprem-networks-1* ***192.168.1.0/24***

*set security zones security-zone* ***Internet*** *interfaces* ***fe-0/0/0.0***

*set security zones security-zone* ***Internet*** *host-inbound-traffic system-services ike*

*set security zones security-zone* ***Internet*** *address-book address azure-networks-1* ***10.0.0.0/16***

*set security policies from-zone* ***Internal*** *to-zone* ***Internet*** *policy azure-security-****Internal****-to-****Internet****-0 match source-address onprem-networks-1*

*set security policies from-zone* ***Internal*** *to-zone* ***Internet*** *policy azure-security-****Internal****-to-****Internet****-0 match destination-address azure-networks-1*

*set security policies from-zone* ***Internal*** *to-zone* ***Internet*** *policy azure-security-****Internal****-to-****Internet****-0 match application any*

*set security policies from-zone* ***Internal*** *to-zone* ***Internet*** *policy azure-security-****Internal****-to-****Internet****-0 then permit*

*set security policies from-zone* ***Internet*** *to-zone* ***Internal*** *policy azure-security-****Internet****-to-****Internal****-0 match source-address azure-networks-1*

*set security policies from-zone* ***Internet*** *to-zone* ***Internal*** *policy azure-security-****Internet****-to-****Internal****-0 match destination-address onprem-networks-1*

*set security policies from-zone* ***Internet*** *to-zone* ***Internal*** *policy azure-security-****Internet****-to-****Internal****-0 match application any*

*set security policies from-zone* ***Internet*** *to-zone* ***Internal*** *policy azure-security-****Internet****-to-****Internal****-0 then permit*

*set interfaces st0 unit 0 family inet*

*set security zones security-zone* ***Internet*** *interfaces st0.0*

*set security ipsec vpn azure-ipsec-vpn bind-interface st0.0*

*set routing-options static route* ***10.0.0.0/16*** *next-hop st0.0*

*set security flow tcp-mss ipsec-vpn mss 1350*

*###Script End###*

###Script Key###

***879ac96b53764ad0b6482e55c0e05a0a is the Azure Gateway preshared key******40.X.X.X is the IP address of the Dynamic Azure gateway***

***fe-0/0/0.0 in the external interface***

***vlan.1 the name of the internal interface***

***Internal is the zone is associated with interface vlan.1***

***Internet is the zone is associated with interface fe-0/0/0.0***

***192.168.1.0/24 this is IP address range of the onprem-networks***

***10.0.0.0/16 this is the IP address rage of the azure-networks***

We will need to use the text typed at the terminal as input to the configuration

The Junos command is **load set terminal**

Machine generated alternative text:
root Azure SRX# load set terminal 
L Type AD at a new line to end input I 

Copy and paste the edited script into the Juniper console window when completed press "Control D" to end input

The Junos command is **commit full**

Machine generated alternative text:
root Azure SRX# comit 
t comple te 

We need to show the default security policy

The Junos command is **show security policies from-zone Internal to-zone Internet**

Machine generated alternative text:
root"zure SRX# show security policies 
policy All Internal Internet 
mat ch 
source—address any ; 
destination—address any ; 
appl cat ion any ; 
then 
pe rmi t ; 
policy 
f rom— z one 
Internal 
to— zone 
Int e t 
mat ch 
source—address ; 
destination—address azure—networks—I, 
appl cat ion any ; 
then 
pe rmi t ; 

The default policy name in this example is **azure-security-Internal-to-Internet-0**

\*\*If your default policy does not match **azure-security-Internal-to-Internet-0**

Run Command **insert security policies from-zone Internal to-zone Internet policy azure-security-Internal-to-Internet-0 before policy <NameOfYourDefaultTrustToUntrustPolicy>**

**commit**

How to check to see main mode is connected

The Junos command is **run show security ike security-associations**

Machine generated alternative text:
root"zure SRX# run show security ike security—associations 
Remot e 
Add re s s 
go.x.x.x 
Index State Initiator cookie 
Re sponder cookie 
1369b1d61d0260B2 
Mode 
IKEv2 
6852022 UP 
9abdB7c7bea9BB63 

How to check to see Quick Mode is connected

The Junos command is **run show security ipsec security-associations**

Machine generated alternative text:
root"zure SRX# run show security ipsec security 
Total active tunnels : I 
—associations 
Life : sec/ kb Mon 
SPI 
I sys Port 
root S 00 
root S 00 
Gat e way 
40. x. x. x 
40. x. x. x 
U 31073 ESP:aes-2S6/sha1 37eb99ba 2083/ unlim 
M 31073 ESP:aes-2S6/sha1 4649682c 2083/ unlim 

To exit configuration mode and go back to operational mode, enter exit at the prompt:

Machine generated alternative text:
root Azure SRX# exit 
Exiting configuration mode 