**Setting up Site-to-Site VPN between Cisco ASA and Microsoft Azure Virtual Network using a Static Routing VPN Gateway**

* Introduction
* Prerequisites
  + Cisco ASA
* Topology
* Creating S2S VPN in Azure Virtual Network
  + Creating virtual network
  + Creating gateway
* Configure Cisco ASA
  + CISCO ASA 9.1 and above
  + Verifying ASA configuration
* Establishing VPN
* Verification
  + Virtual network side verification
  + On premises side Verification

**Introduction:**

With a CISCO ASA we can establish a site-to-site VPN between an on premises network and a Microsoft Azure Virtual Network. In this blog we’ll provide step-by-step procedure to establish site-to-site VPN (with Static Routing VPN Gateway) between Cisco ASA and Microsoft Azure Virtual Network.

**Prerequisites:**

Before we move on to configure site-to-site VPN, let’s make sure we have the minimum prerequisites to establish site-to-site VPN.

**ASA Prerequisites:**

1) We recommend ASA version 9.1 or above and the version can be verified with CLI “Show Version”.

2) AES Encryption License should be enabled. Make sure AES license is enabled on ASA, which can be verified using “Show version” or “Show version | include Encryption-3DES-AES” CLI on ASA.

**Topology:**

Use the below topology as a reference for site-to-site VPN configuration.



**Azure Virtual Network**

**Virtual Network**

**Address Space**

192.168.10.0/24

**Subnet**-1 192.168.10.0/27

**Gateway** 192.168.10.32/29

On Premises Network

10.10.10.0/24

Site-to-Site VPN

Internet

Cloud

ASA Inside

10.10.10.1/24

Host

10.10.10.20/24

Azure virtual network address space:

192.168.10.0/24

ASA side network:

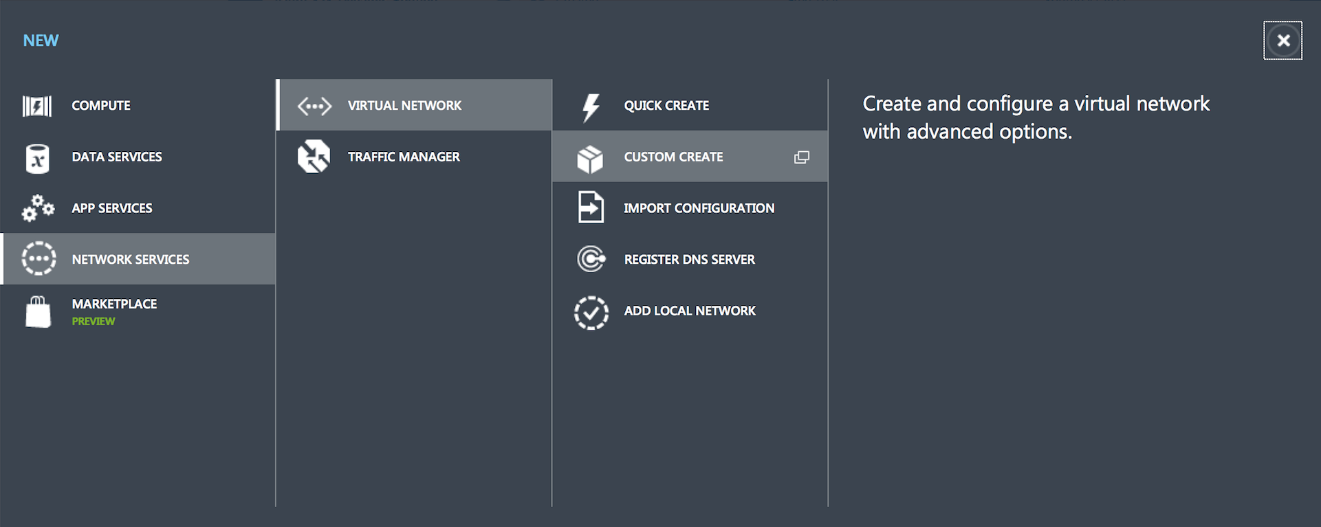
On-premises network inside network 10.10.10.0/24

**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 Network -> Click NEW -> CUSTOM CREATE



**Step 2:** Create new virtual network

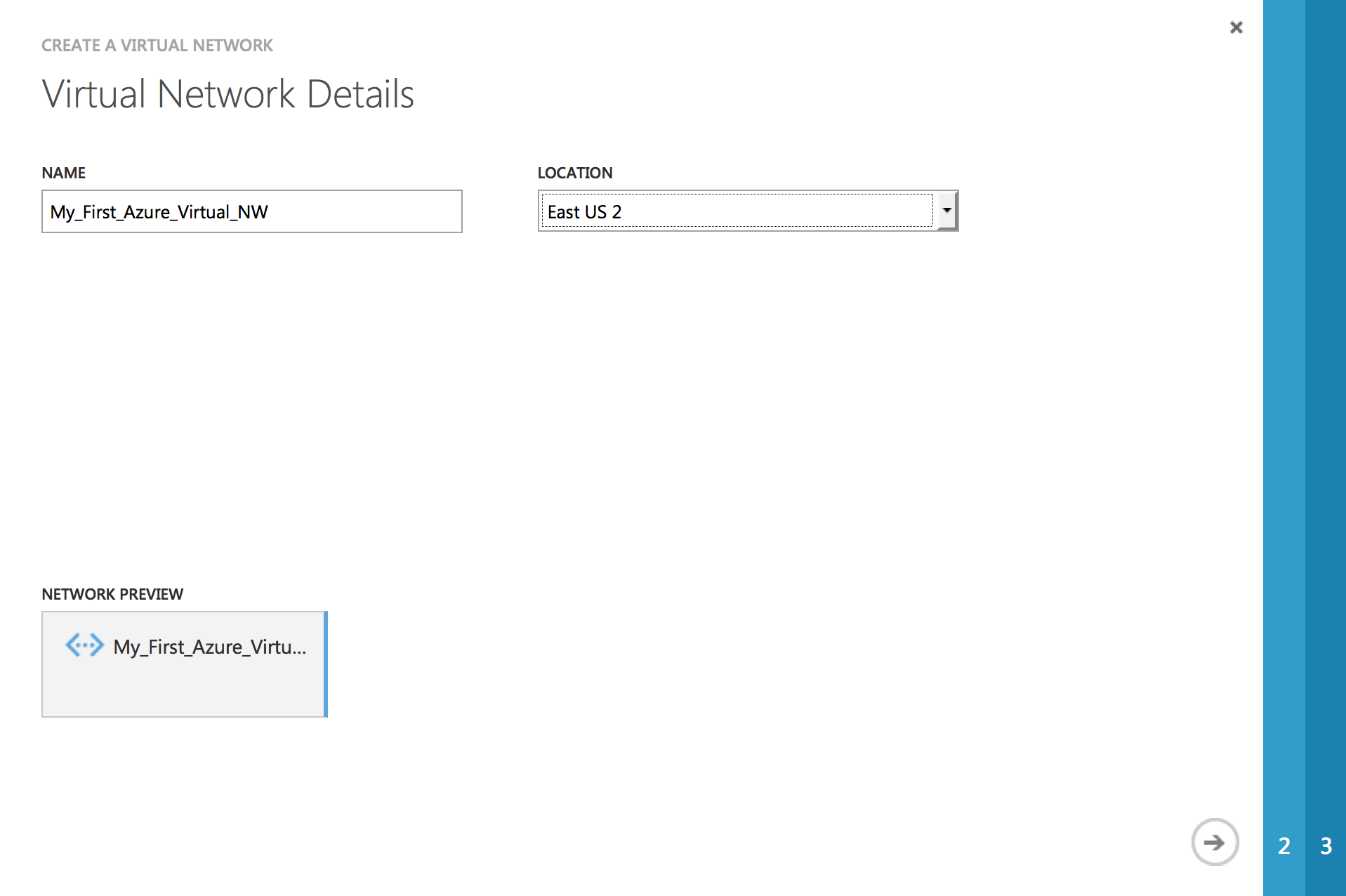
Page 1: Virtual network details

In this first page fill in the name of virtual network and the location of your on premises network.

e.g. Name: My\_First\_Azure\_Virtual\_NW

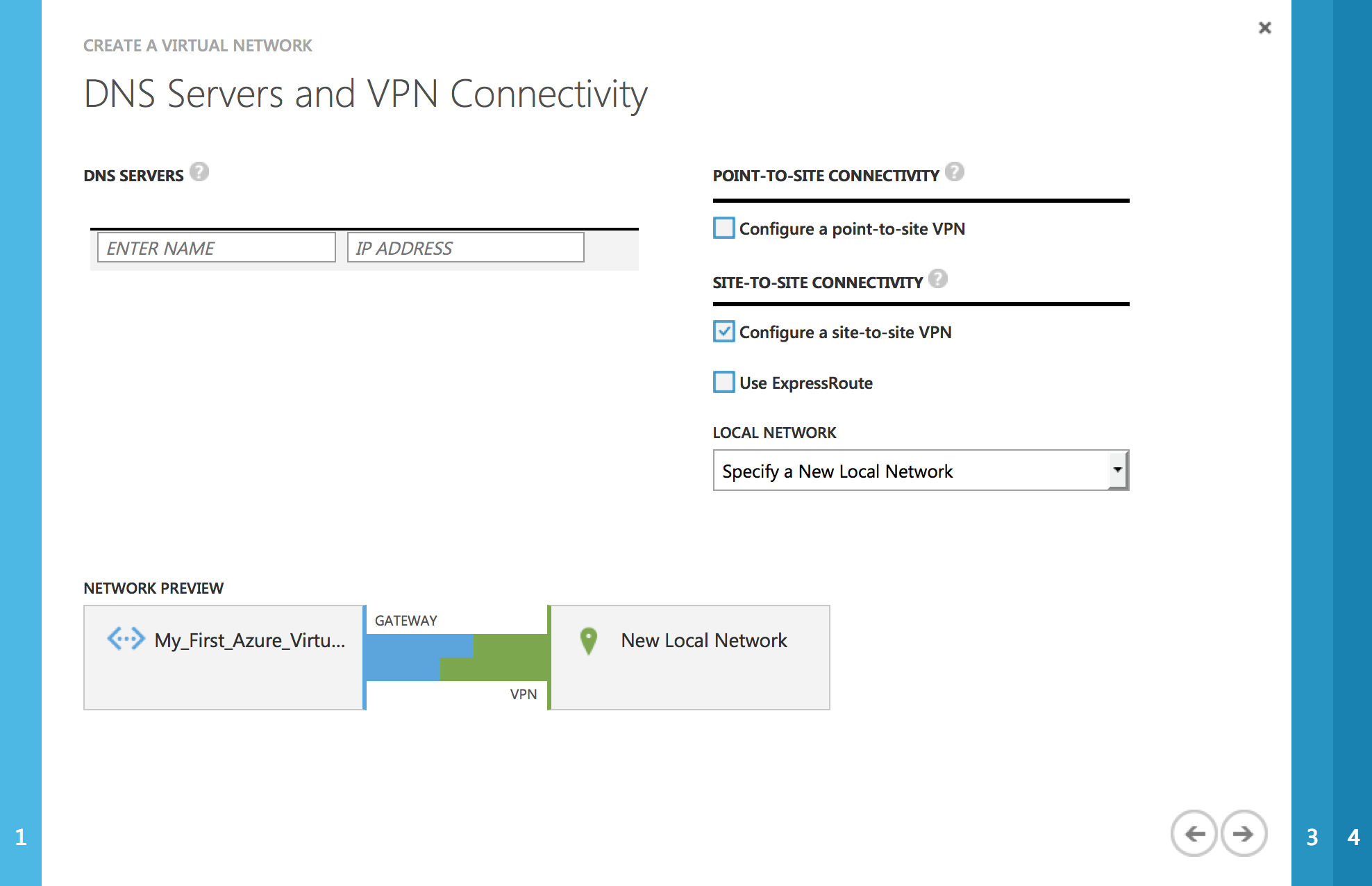
Location: East US 2

Click Next ->



**Page 2:** DNS Server and VPN Connectivity

At this point the DNS server detail is optional. Select check box “Configure a site-to-site VPN” and click Next ->



**Page 3:** Site-to-site Connectivity

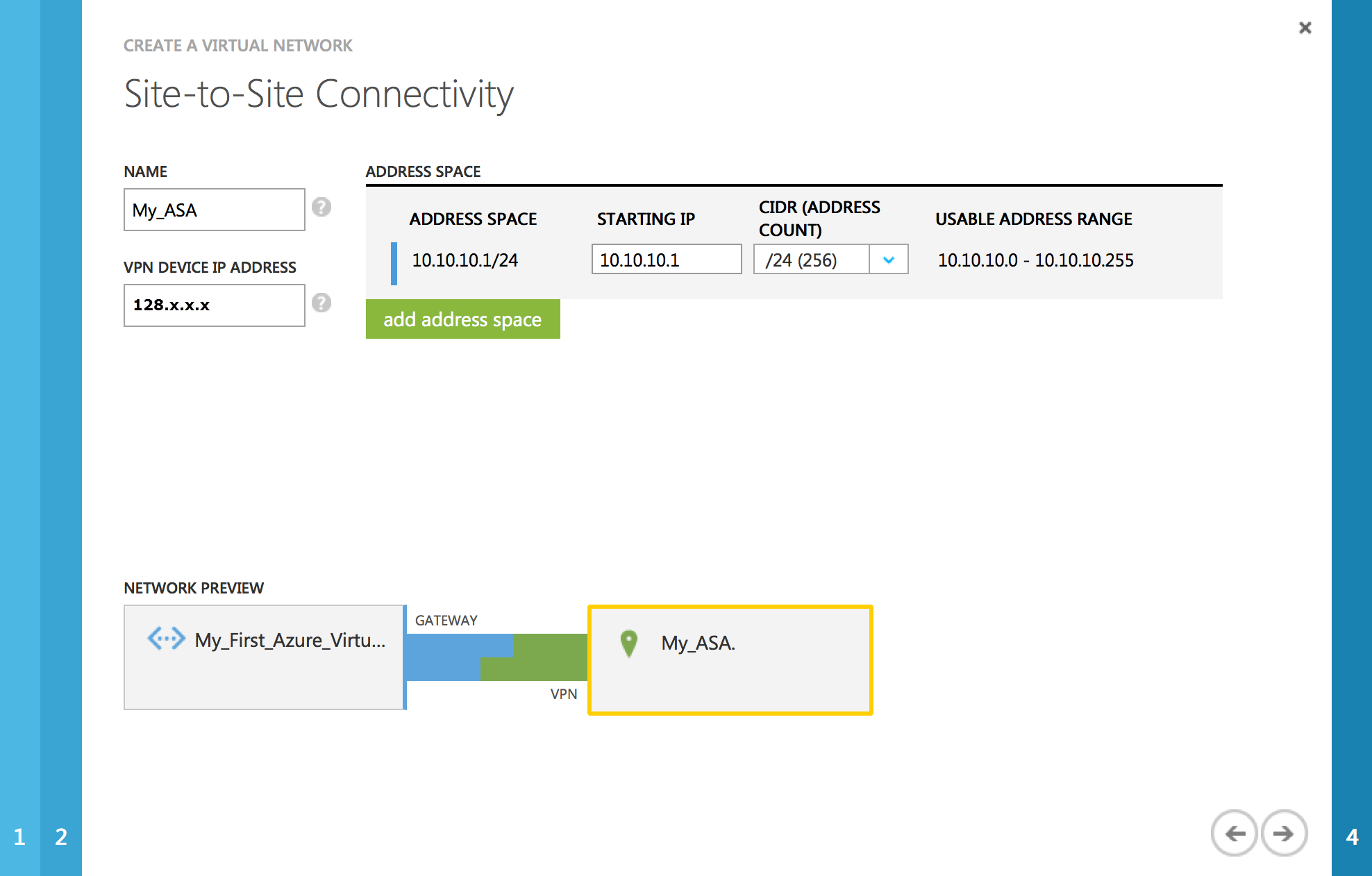
In this page, fill in the name for on-premises and detail such as the ASA Outside (Public IP address) and Inside Network.

In our example:

**Name:** My\_ASA *(User defined name for the on-premises network)*

**VPN Device IP Address:** 128.X.X.X *(ASA outside interface IP (Public IP address)*

**Address:** 10.10.10.1/24 *(Your on-premises local network. Specify starting IP address of your network.)*



Click Next ->

**Page 4:** Virtual Network Address Spaces

In this page you have to allocate IP address that will be used for Azure Virtual Network. In our e.g. 192.168.10.0/24 is used

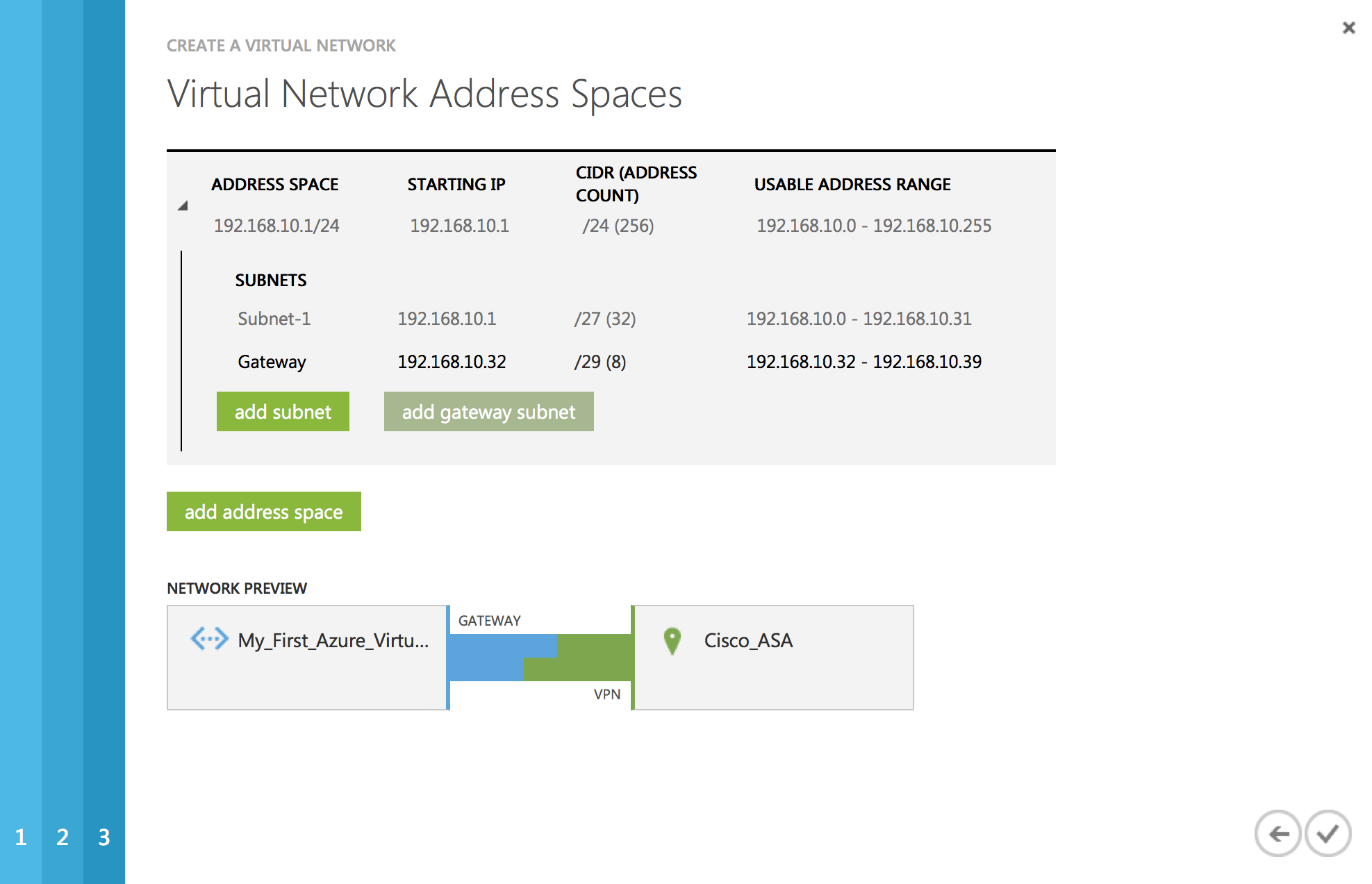
**Starting IP:** 192.168.10.1 (Starting IP address of your Virtual Network)

**CIDR:** 24 (Subnet Mask for the IP range)

Subnets:

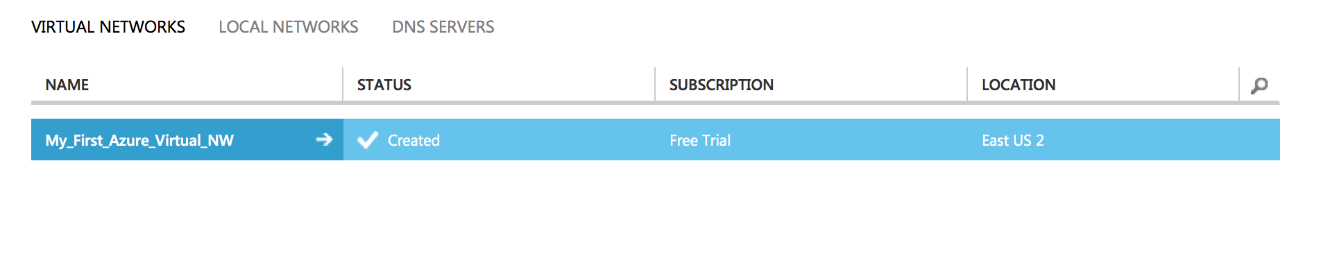
**Subnet-1:** 192.168.10.1 / 27 (This Network will be used for Virtual Host in Azure Virtual Network)

**Gateway:** 192.168.10.32 / 29 (This Network will be used for Virtual Azure Gateway)



Once done click complete.

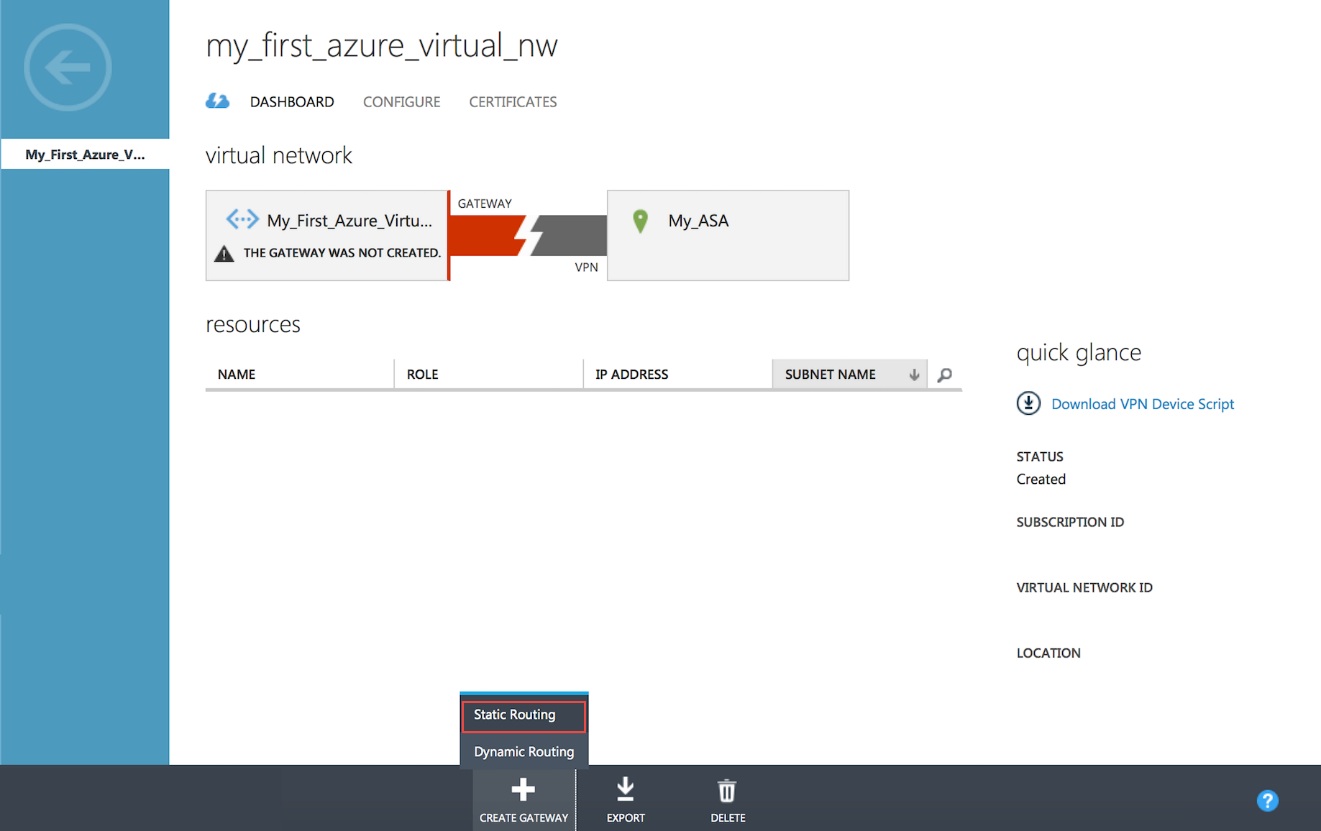
It takes couple of minutes to create Virtual Network. Once created you’ll see created Virtual Network under Network.



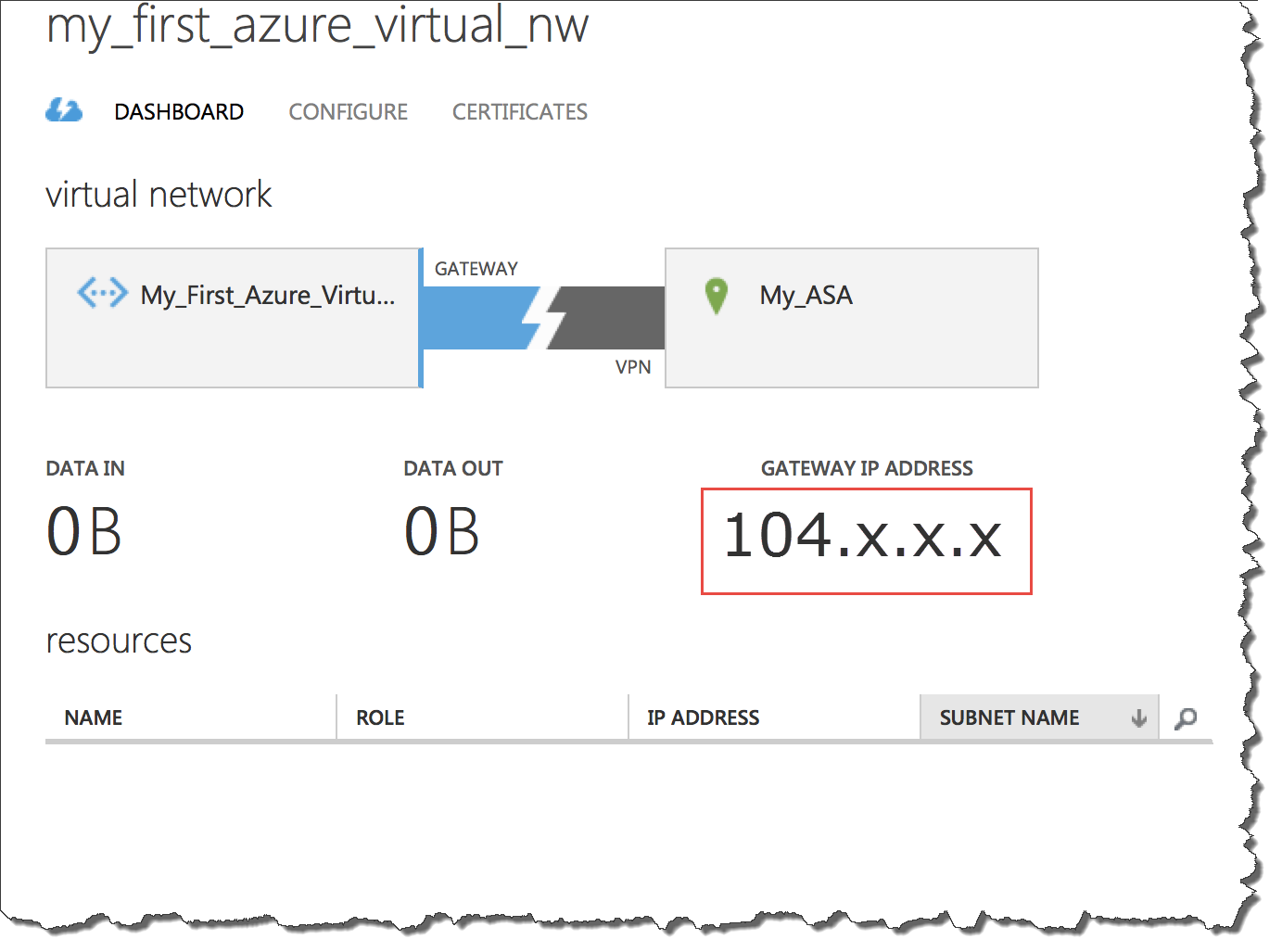
**Creating Gateway:**

Once Virtual Network is created, we should create Gateway. Click on the newly created Virtual Network. e.g. Click “My\_First\_Azure\_Virtual\_NW”.

Click “Create GATEWAY” which is available in the bottom of the screen and choose Static Routing and click “YES”. It will take couple of minutes to create the gateway.



Once the gateway is created, the gateway IP address will be displayed in the dashboard.



**Configuring Cisco ASA:**

In this section we’ll configure site-to-site VPN on ASA 8.4 & 9.x and above.

**Step 1:** Access-list

**Step 1a:**

Create two object-group one with Azure Virtual Network subnet another object-group for On-Premises network, e.g.

**object-group network azure-networks**

**description Azure-Virtual-Network**

**network-object 192.168.10.0 255.255.255.0**

**exit**

**object-group network onprem-networks**

**description On-premises Network**

**network-object 10.10.10.0 255.255.255.0**

**exit**

**Step 1b:** Creating the access-list with the above object-group for identifying interesting traffic for the VPN.

**access-list azure-vpn-acl extended permit ip object-group onprem-networks object-group azure-networks**

Step 2: Creating Identity NAT

With same object-group create identity NAT for this VPN traffic

**Nat (inside,outside) 1 source static onprem-networks onprem-networks destination static azure-networks azure-networks**

**Step 3:** Configuring IKEv1 Internet Key Exchange

Creating IKEv1 policy parameters for phase I.

**crypto ikev1 policy 5**

**authentication pre-share**

**encryption aes-256**

**hash sha**

**group 2**

**lifetime 28800**

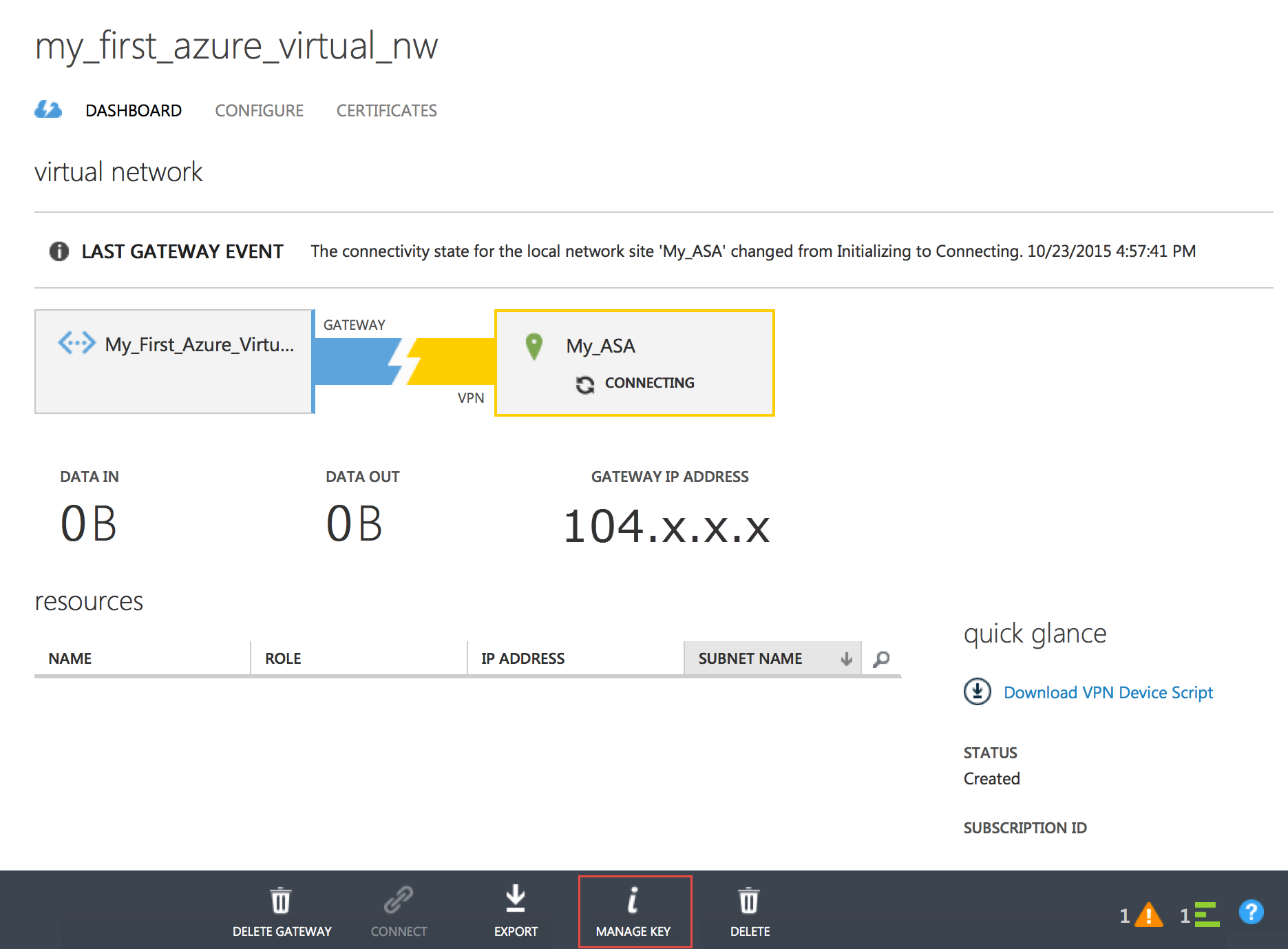
**crypto ikev1 enable outside** *(Outside is the interface nameif)*

**Step 4:** Configuring IPSec

Configuring IPSec parameters for Phase II.

In the below e.g. 104.x.x.x IP should be replaced by Gateway IP address, which is available under Network -> Virtual Network -> Click (Newly created Virtual Network) Under dashboard you’ll get “GATEWAY IP ADDRESS”

<Pre-Share-Key> should be replaced by Managed Share Key, which is available on same dashboard, click “Manage Key” available at bottom of the screen, copy “managed shared key” and replace “Pre-shared-key”



**crypto ipsec ikev1 transform-set azure-ipsec-proposal-set esp-aes-256 esp-sha-hmac**

**crypto ipsec security-association lifetime seconds 3600**

**crypto ipsec security-association lifetime kilobytes 102400000**

**tunnel-group 104.x.x.x type ipsec-l2l**

**tunnel-group 104.x.x.x ipsec-attribute**

**ikev1 pre-shared-key <Pre-Shared-Key>**

**Step 5:** Creating Crypto Map

Configure crypto map using below configuration, if your ASA already has existing crypto map use the same name with different priority number. Using “show run crypto map” CLI you can verify If ASA has existing crypto map, if it existing use same name instead of “**azure-crypto-map”**

**crypto map azure-crypto-map 1 match address azure-vpn-acl**

**crypto map azure-crypto-map 1 set peer 104.x.x.x**

**crypto map azure-crypto-map 1 set ikev1 transform-set azure-ipsec-proposal-set**

**crypto map azure-crypto-map interface outside**

**Step 6:** Adjusting TCPMMS value

To avoid fragmentation set TCPMMS value to 1350, use below CLI

**“sysopt connection tcpmss 1350”**

**Step 7:** Allowre-establishment of the L2L VPN Tunnel

To avoid tunnel drops use below CLI

**“sysopt connection preserve-vpn-flows”**

ASA configuration is now complete!

**Verifying ASA configuration:**

Once above configuration is completed, you can verify it

**Verifying Object-group and Access-list:**

Using “show run object-group” and “show run access-list” to verify object-group and Access-list.

My-ASA(config)# **show run object-group**

object-group network azure-networks

network-object 192.168.10.0 255.255.255.0

object-group network onprem-networks

network-object 10.10.10.0 255.255.255.0

My-ASA(config)# **show run access-list**

access-list azure-vpn-acl extended permit ip object-group onprem-networks object-group azure-networks

**Verifying Crypto configuration:**

To verify all crypto configuration, use “show run crypto” to verify configured crypto CLI.

My-ASA(Config)#**Show run crypto**

crypto ipsec ikev1 transform-set azure-ipsec-proposal-set esp-aes-256 esp-sha-hmac

crypto ipsec security-association lifetime seconds 3600

crypto ipsec security-association lifetime kilobytes 102400000

crypto map azure-crypto-map 1 match address azure-vpn-acl

crypto map azure-crypto-map 1 set peer 104.X.X.X

crypto map azure-crypto-map 1 set ikev1 transform-set azure-ipsec-proposal-set

crypto map azure-crypto-map interface outside

crypto ikev1 enable outside

crypto ikev1 policy 1

authentication pre-share

encryption aes-256

hash sha

group 2

lifetime 28800

**Verify Tunnel group:**

To verify tunnel group configuration, use CLI “Show run tunnel-group”

My-ASA(config)# **show run tunnel-group**

tunnel-group 104.210.13.15 type ipsec-l2l

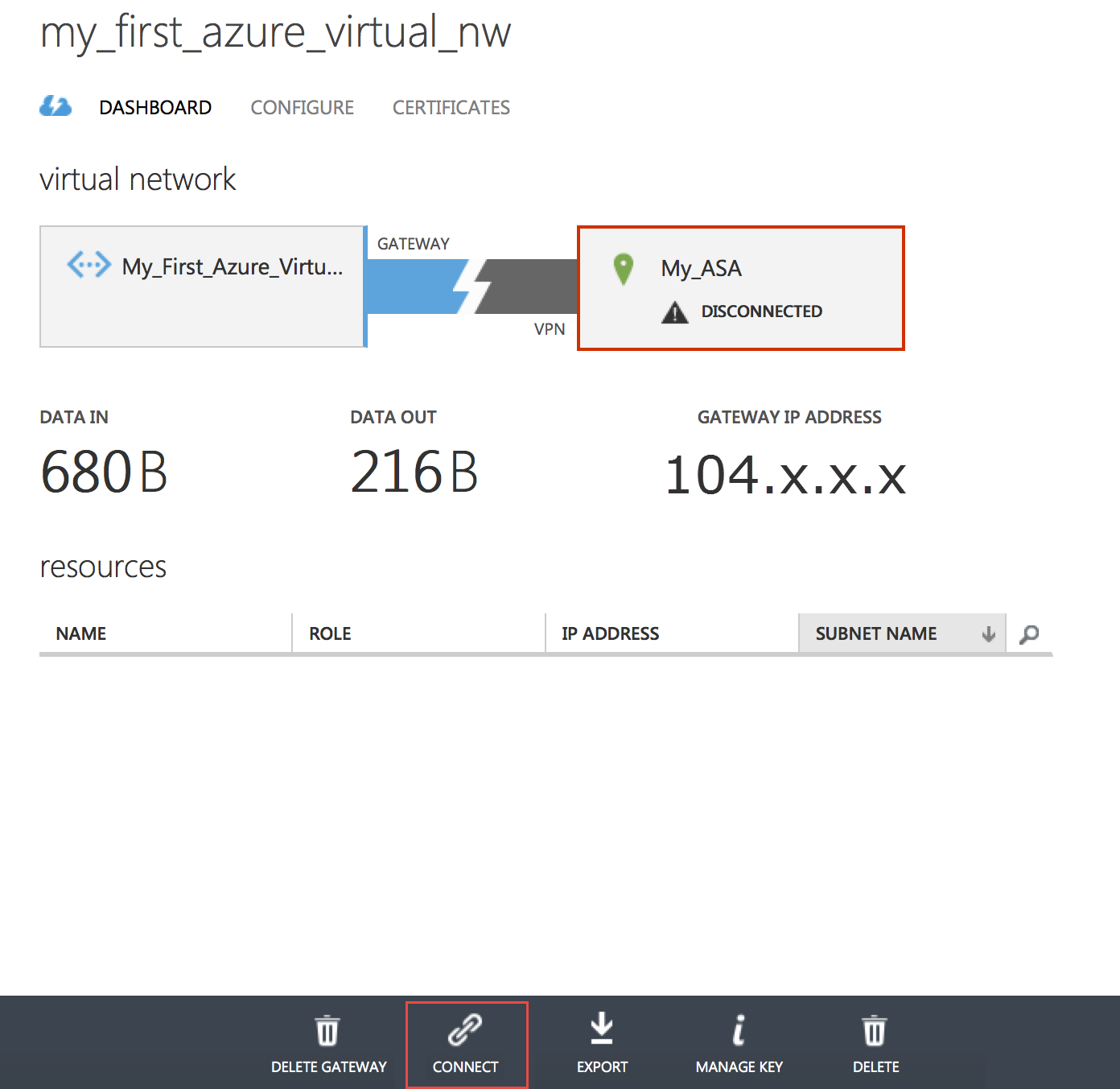
tunnel-group 104.210.13.15 ipsec-attributes

ikev1 pre-shared-key \*\*\*\*\*

My-ASA(config)#

**Establishing VPN:**

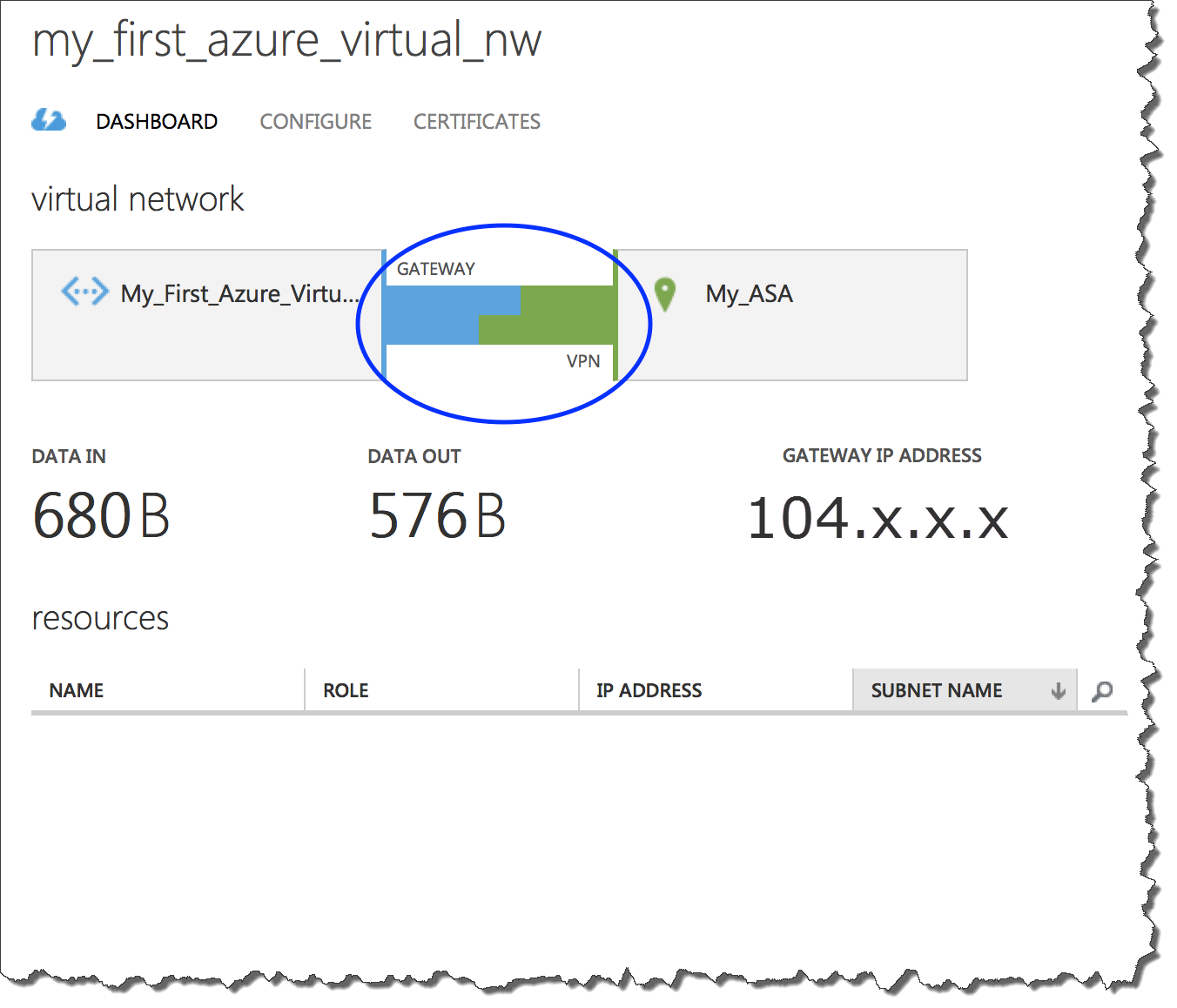
Once the virtual network is created on Azure portal and the ASA is configured, its time to establish the VPN. You can establish/start VPN by clicking “**Connect**” under the Virtual Network Dashboard.



**Verification:**

**Verification on Azure Portal:**

Once the VPN is established, Virtual Network Dashboard would appear as below.



**Verification on Cisco ASA:**

On ASA you can verify use CLI “Show Crypto isakmp”

The output should show “MM\_ACTIVE”

IKE Peer: 104.X.X.X

Type : L2L Role : responder

Rekey : no State : MM\_ACTIVE

Also additionally you can verify using “Debug ICMP trace”. Once you enable this Debug, we can see ICMP echo request packet coming from Azure Virtual Network

“ ICMP echo request from outside:192.168.10.0 to inside:10.10.10.0 ID=1 seq=427 len=4 “

To Turn off Debug CLI “undebug all”

**Testing with Traffic:**

In order to test VPN with traffic, create a Virtual Host in Azure network using the created Virtual Network address space. Virtual Host will get an on IP from Subnet-1 192.168.10.4 – 30 range.

After turning off the firewall on the Virtual Host, you should be able to ping or RDP to the virtual host from host in on-premises network.