**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**

10.0.0.0/16

**AzureVnet** 10.0.0.0/24

**Gateway** 10.0.200.0/29

On Premises Network

192.168.1.0/24

Site-to-Site VPN

Internet

Cloud

ASA Inside

192.168.1.0/24

Host

192.168.1.10

Azure virtual network address space:

10.0.0.0/16

ASA side network:

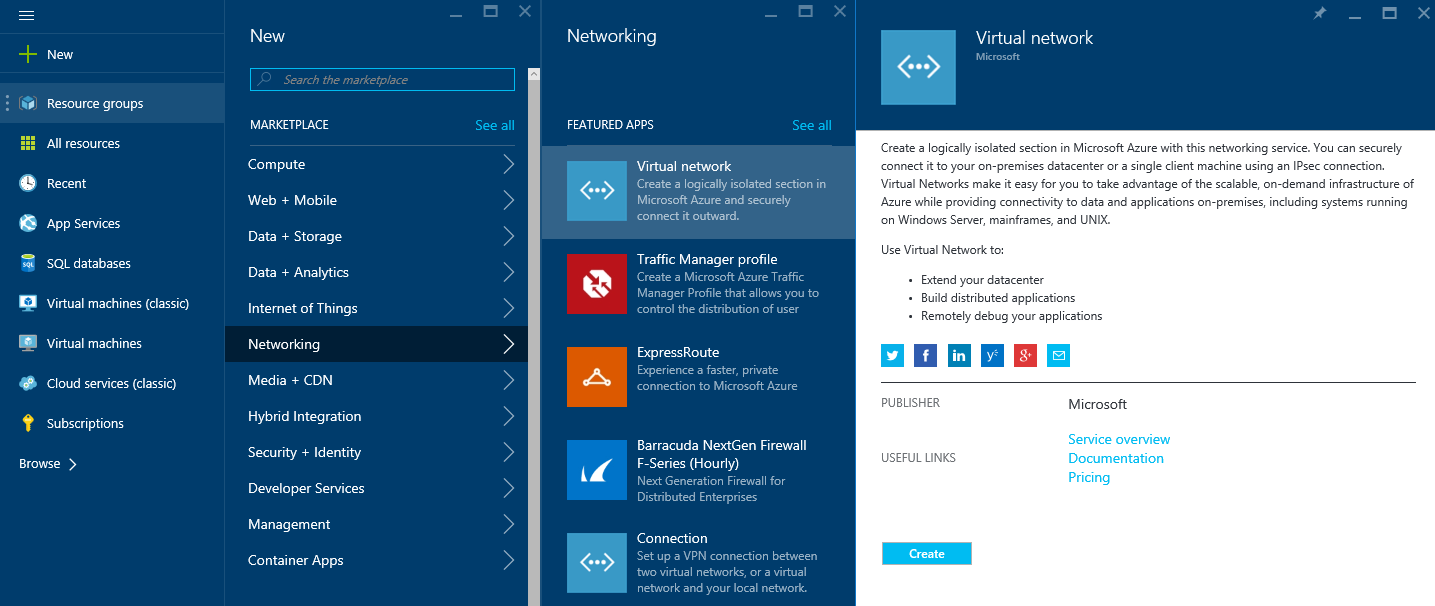
On-premises network inside network 192.168.1.0/24

**Creating the Azure VPN**

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

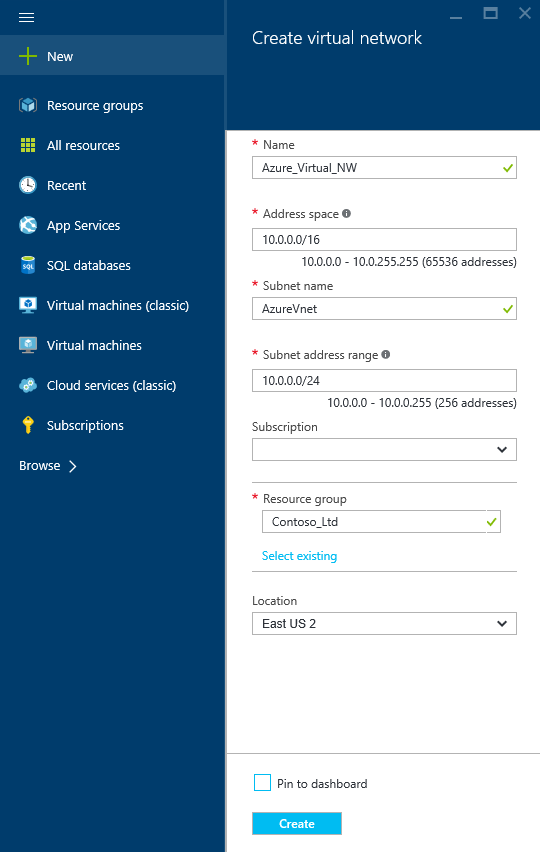
**Step 1:** Create the virtual network:

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

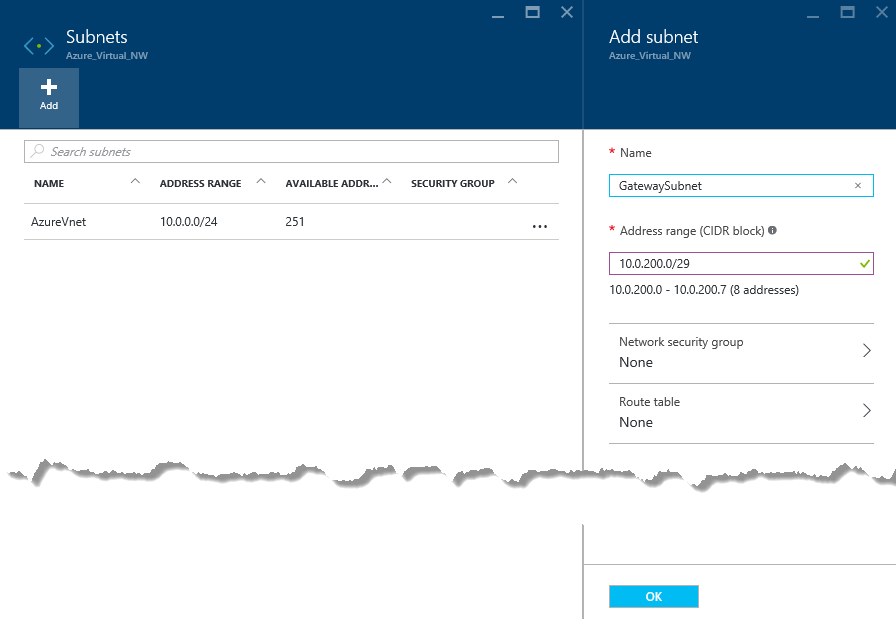


**Step 2:** Create new virtual network

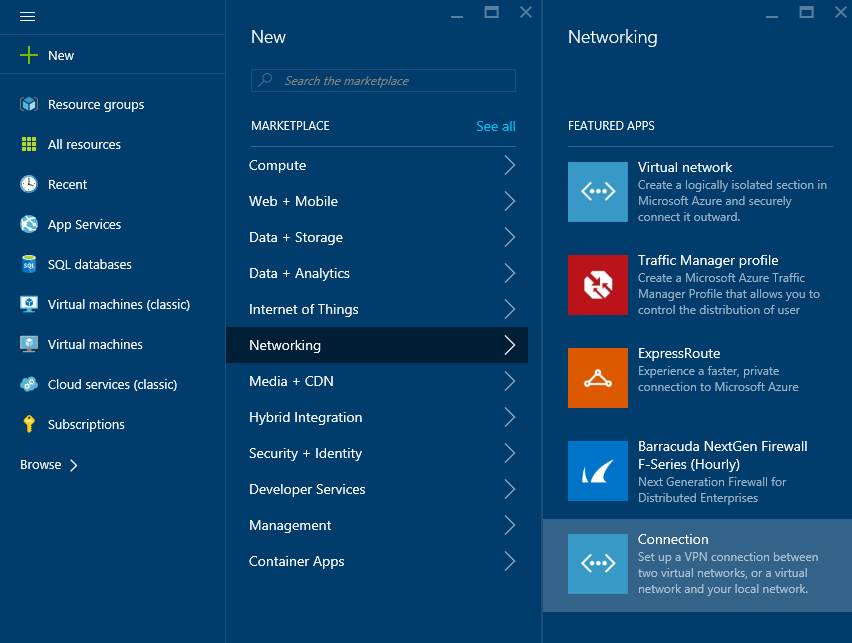
Fill in the name of Virtual Network, the Address range you wish to use in Azure, and the location.



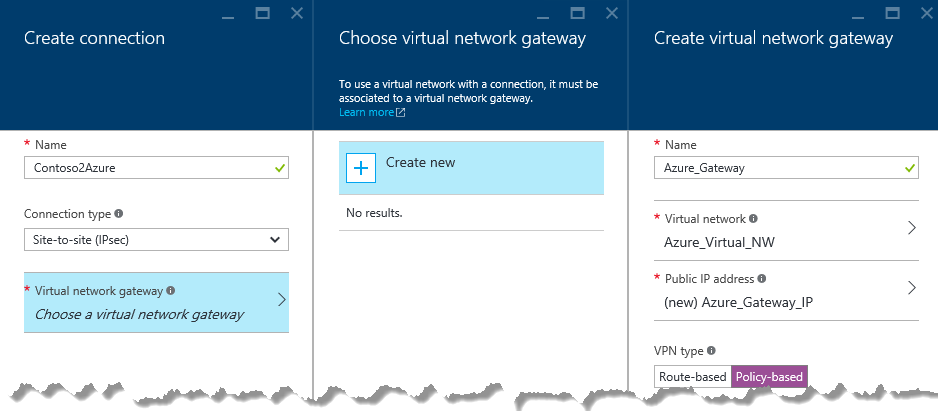
**Step 3:** After creation of a virtual network add a gateway subnet named GatewaySubnet



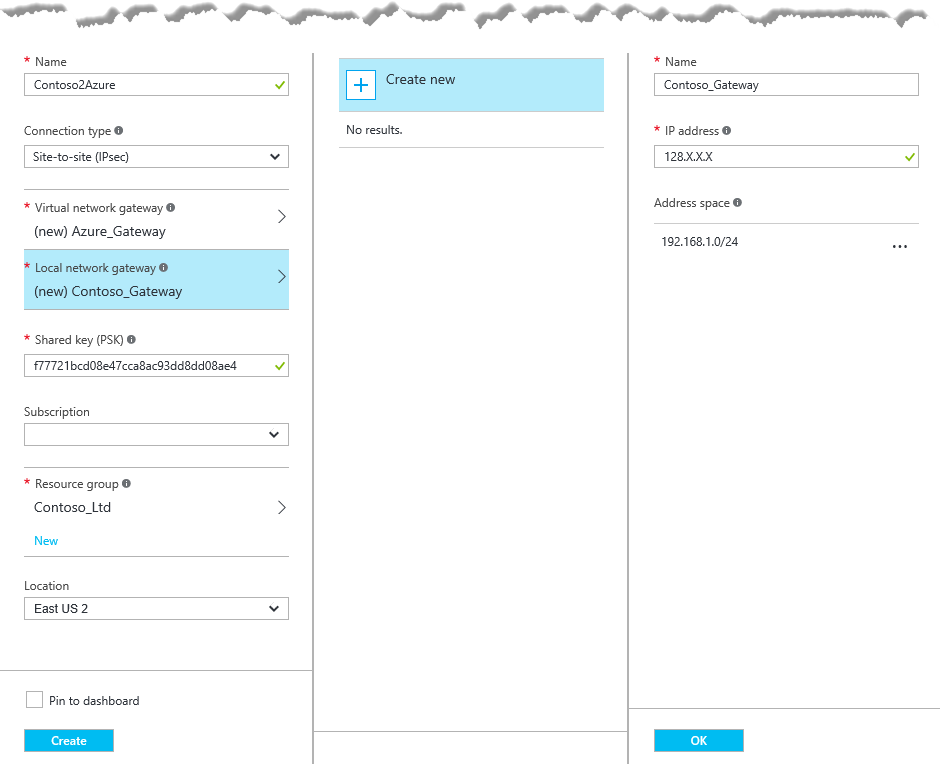
**Step 4:** Create a VPN Connection



**Step 5**: Setup Azure Policy based gateway



**Step 6:** Setup Local Gateway

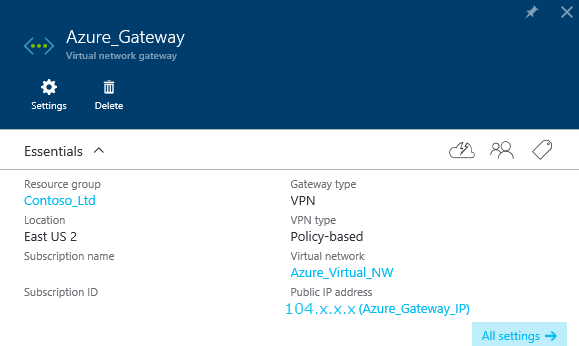


In our example:

**Local virtual network gateway:** 128.X.X.X *(ASA outside 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.)*

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



**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 10.0.0.0 255.255.255.0**

**exit**

**object-group network onprem-networks**

**description On-premises Network**

**network-object 192.168.1.0 255.255.255.0**

**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**

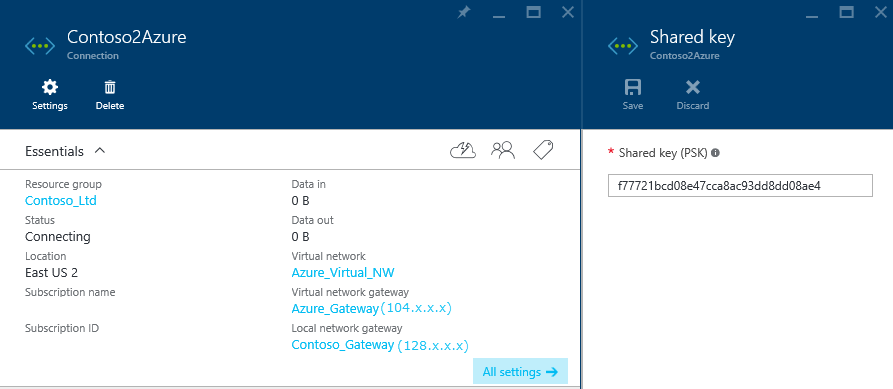
**lifetime 28800**

**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 Virtual network gateway, which is available under the connection object <Pre-Share-Key> should be replaced by Share Key (PSK), which is available on same object, under All settings, 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 10.0.0.0 255.255.255.0

object-group network onprem-networks

network-object 192.168.1.0 255.255.255.0

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.x.x.x type ipsec-l2l

tunnel-group 104.x.x.x ipsec-attributes

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

My-ASA(config)#

**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 Machine in Azure network using the created Virtual Network address space. Virtual Host will get an on IP from AzureVnet 10.0.0.0/24 range.

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

**Azure Connection view:**

