Networking requirements for connecting to Azure

VERITAS
The truth in information.

This article walks you through the networking requirements for connecting your on-premises data center to Azure cloud. The steps in this article shows you how to use the Azure portal to create a Site-to-Site VPN gateway connection from your on-premises network to the VNet in Azure cloud. This article does not describe the use of ExpressRoute connection method.

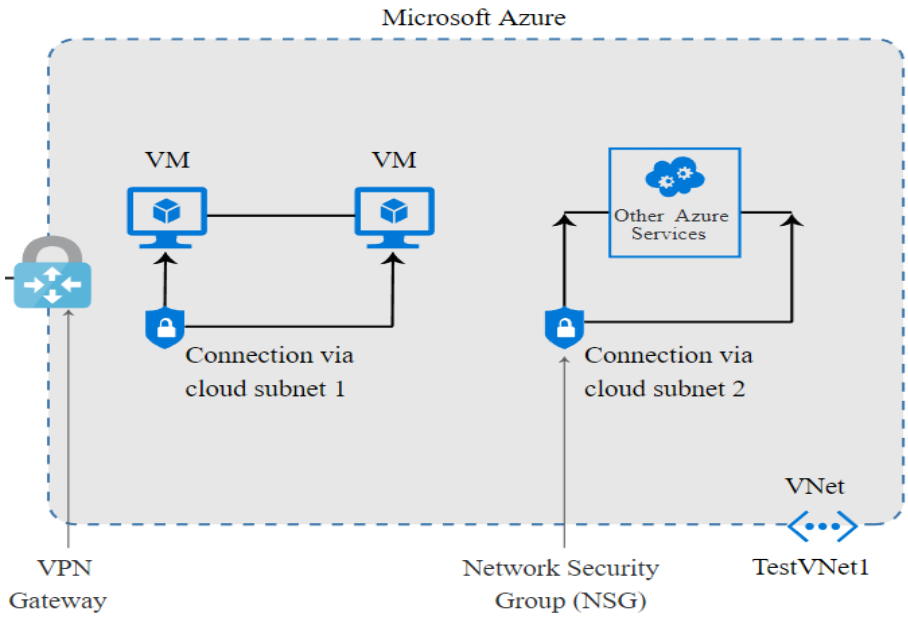
We will discuss basic terminologies like: VNet, VPN Gateway, Local network gateway, Network security group (NSG) and DNS.

Networking Glossary:
Before we begin, we must understand some common terms that you will see throughout this article:

VNet:
VNet stands for "Virtual Network" of Microsoft Azure service which enables Azure resources to securely communicate with each other in a virtual network. It is an interpretation of your isolated network in the cloud, based on your Azure subscription.

Windows Azure subscription is a provision which grants you access to Windows Azure services and to the Windows Azure Platform Management Portal. Using the Management Portal, you can create your own virtual network.

You can also connect virtual networks to other isolated virtual networks, or to your on-premises network. The below picture depicts the VNet structure:



VPN Gateway:

A VPN gateway is a type of virtual network gateway that sends encrypted data between your virtual network and your on-premises location across a public connection.

Local network gateway:

This refers to your on-premises location by which Azure can create a connection.

Network security group (NSG):

A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet).

NSGs can be associated to subnets or individual network interfaces (NIC) attached to virtual machines. When an NSG is associated to a subnet, the rules apply to all the resources connected to the subnet. Traffic can further be restricted by also associating an NSG to a VM or NIC.

© 2017 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo and NetBackup are trademarks or registered trademarks of Veritas Technologies or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

DNS server:

DNS server is not required when you are setting up Site-to-Site connection. But if you want to have user friendly names to the resources it is much simpler to use names that can be easily remembered and do not change.

For more information on the DNS, refer to the below link:

Site to site connection in the Azure portal

Note:

- The source, destination ports should be opened, and IP addresses need to be unblocked with the help of your IT help desk.
- Address space and subnets needs to be decided with the help of IT, which will be used while creating virtual network.

Steps for setting up the networking environment from your on-premises data center to Azure cloud:

Step 1: Create Azure cloud subscription:

You should have an Azure subscription to access the management portal. For more information about Azure subscription, see Azure subscription

Step 2: To create Virtual Network (VNet) at Azure cloud:

1. Login to Azure portal with your account.
2. Search for the keyword "virtual networks". Click "+ Add" to create a new virtual network.
3. Complete the "Create virtual network" wizard with required fields. Refresh the portal to locate your VNet. Note that, it is required to use "Custom" DNS rather than the "Default" DNS server which is provided by Microsoft Azure. "Custom" DNS can also be set at NIC level; however, it is recommended to set it at VNet level.

   For more information on the VNet, refer to the below link:
   Site to site connection in the Azure portal

© 2017 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo and NetBackup are trademarks or registered trademarks of Veritas Technologies or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Step 3: To create a VPN Gateway:

1. After VNet is ready, from the Azure portal, search for "virtual network gateway" and click "+ Add".
2. Complete the "Create virtual network gateway" wizard with the required fields.

   For more information on creating VPN Gateway, refer to the below link:

   Site to site connection in the Azure portal

Step 4: To create Local network gateway:

1. After VPN Gateway is created, from the Azure portal, search for "Local network gateway" and click "+ Add". This refers to your on-premises location by which Azure can create a connection.
2. Complete the "Create local network gateway" wizard with the required fields.

   For more information on creating local network gateway, refer to the below link:

   Site to site connection in the Azure portal

After you are done with creating Local network gateway, using VPN connection create a link between Azure and on-premises data center.

Step 5: Creating link between Azure and on-premises environment through VPN connection:

To create a link between Azure and on-premises environment, we need to create a connection between the VPN Gateway and the Local network gateway created in **step 2** and **step 3** using Site-to-Site (IPSec) protocol.

1. From the Azure portal, search the keyword as "Connections". Click "+Add" and fill in all the mandatory fields.
2. Provide the Secret Shared Key (any combination of alphabets and numbers) (if required).
3. Complete the wizard. You can see the "Creating Connection" flash on your screen.
4. Connection status changes from **Unknown** to **Connecting**, and then to **Succeeded**.

   For more information on creating VPN connection, refer to the below link.

   Site to site connection in the Azure portal

Step 6: To verify the VPN connection:

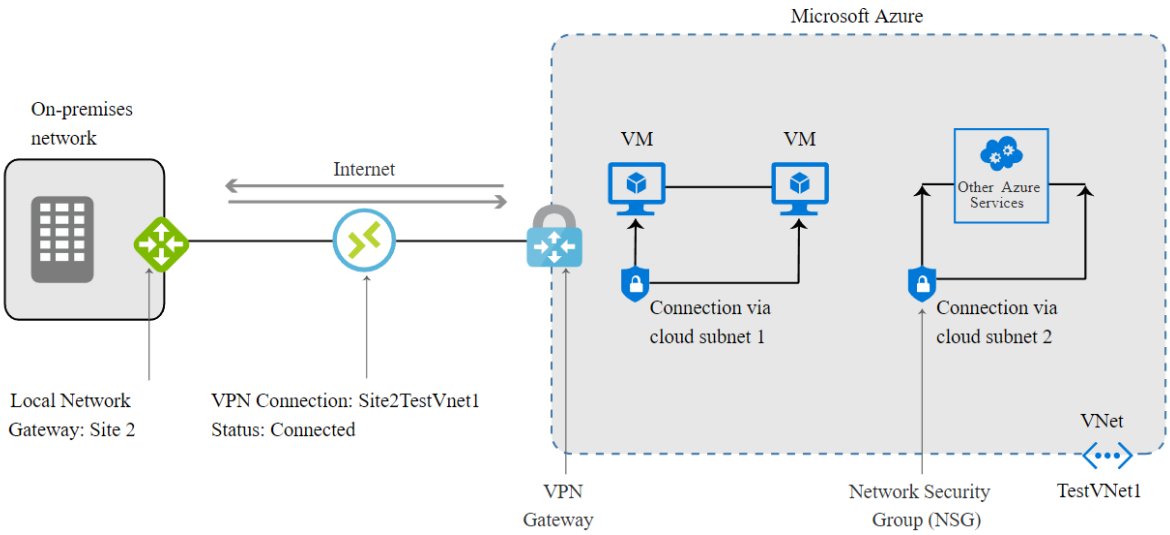
In the Azure portal, you can view the connection status of a VPN Gateway by navigating to the connection. The **Status** is **'Succeeded'** and **'Connected'** when you have made a successful connection.

© 2017 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo and NetBackup are trademarks or registered trademarks of Veritas Technologies or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

For more information on verifying VPN connection, refer to step 8 in the below link.

[Site to site connection in the Azure portal]

Diagram depicts the VPN connection between on-premises to Azure cloud



How to deploy and configure Veritas Resiliency Platform:

Veritas Resiliency Platform is deployed as a virtual appliance. A virtual appliance is a virtual machine image consisting of a pre-configured operating system environment with a software application installed on it.

There are four virtual appliances available for Resiliency Platform to deploy:

1. Resiliency Manager

2. Infrastructure Management Server (IMS)

3. Replication Gateway

4. YUM virtual appliance.

Veritas Resiliency Platform must be deployed on both the sites, i.e. on your on-premises and on Azure cloud.

Steps to deploy Veritas Resiliency Platform as a virtual **appliance on on-premises**:

[To deploy on on-premises]

Steps to deploy Veritas Resiliency Platform as a virtual appliance **on cloud**:

[To deploy on cloud]

© 2017 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo and NetBackup are trademarks or registered trademarks of Veritas Technologies or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Steps to configure the virtual appliances as Veritas Resiliency Platform components:

1. Prerequisites for configuring Resiliency Platform components

    Prerequisites

2. About configuring the Resiliency Platform components

    Configuring the Resiliency Platform components

3. Configuring the Resiliency Manager or IMS

    Configuring Resiliency Manager or IMS

4. Configuring the Replication Gateways

    Configuring Replication Gateways

5. Configuring the YUM repository server

    Configuring the YUM repository server

Configuring Azure cloud in Veritas Resiliency Platform:

To access the Azure cloud resources, you need to configure the cloud credentials:

Configure Azure cloud

For more information on recovering virtual machine to Azure, refer:

Recovering VMware virtual machines to Azure

Configuring Veritas Resiliency Platform with Azure through networking settings:

1. Login to Resiliency Platform console.
2. From the **Quick Actions**, click **Manage Asset Infrastructure**. Here you can view information about the on-premises data center and the cloud data center which you have configured.
3. In the cloud data center, click **Access Profile** > **Network** tab.
4. In the **Type** dropdown, select **Subnets**. List of all the discovered subnets is displayed.

    Example: Discovered subnets for this cloud data centers is "MyVNet".
5. Similarly, in the on-premises data center, click **Access Profile > Network** tab.
6. In the **Type** dropdown, select **Subnet**. List of all the discovered subnets is displayed.

© 2017 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo and NetBackup are trademarks or registered trademarks of Veritas Technologies or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Example: Discovered subnet for the on-premises data centers is "192.168.0.0/16" with Purpose as "Production". Note that, the purpose does not appear automatically along with the discovered subnets. The purpose is explicitly assigned by the user during the network pairing.

Using the above discovered subnets and the discovered Azure subnets, we can create a network pair between on-premises and cloud data center.

For more information on the network objects, see:
About network objects

Using Veritas Resiliency Platform create network pairs between on-premises and the Azure cloud for disaster recovery:

1. Navigate to **Disaster Recovery Settings** page.
2. Do one of the following:
    - On the **Overview** tab, click + **New Network Pair**.
    - On the **Network** tab, click + **Create Pair**.

   Previously created network pairs are listed in the table.
3. In the **Network Mapping** page, select the source and the target data centers, and the network types that should be the part of your network pair. In this case we will select the network type as subnet on the on-premises data center and Azure subnet on the cloud data center.
4. Click **Move selected** button. The above selected network types are listed in the below space given.
5. Click **Next** to submit your selections.

   This network pairing feature helps you to perform all the disaster recovery operations on Azure data center.

© 2017 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo and NetBackup are trademarks or registered trademarks of Veritas Technologies or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.