Understand Azure VM Endpoint, Access Control List (ACL), Network Secutiry Group (NSG)

## **What is Azure VM Endpoint?**

Once virtual machines are created in Azure, in order to access the applications installed in machine, need to login physically to view the applications every time.

In order to access that application from outside of the virtual box, we need to add the endpoint to the machine.

e.g. Customer hosts on-premises (or IaaS) version of SQL Server instance in the cloud. The natural question then is, “How do I connect to the SQL server using SQL Server Management Studio (SSMS) from outside Azure environment?” Solution to this is VM endpoint. it is a mapping of public port to the private port on specific protocol.

## **What are public ports?**

The [Internet Assigned Numbers Authority](https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority) (IANA) is responsible for maintaining the official assignments of port numbers for specific uses. The range of port numbers from 1024 to 49151 are the registered ports. They are assigned by [IANA](https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority) for specific service upon application by a requesting entity. On most systems, registered ports can be used without super user privileges. E.g. port 1433 is officially assigned for MSSQL communication on TCP and UDP. So we can safely assume public port for SQL Server is 1433 while configuring VM end point.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Port | TCP | UDP | Description | Status |
| 1433 | TCP | UDP | [Microsoft SQL Server](https://en.wikipedia.org/wiki/Microsoft_SQL_Server) [database management system](https://en.wikipedia.org/wiki/Database_management_system) (MSSQL) server | Official |

[Transmission Control Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) (TCP) provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating by an IP network. Major Internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP. Applications that do not require reliable data stream service may use the [User Datagram Protocol](https://en.wikipedia.org/wiki/User_Datagram_Protocol) (UDP), which provides a  connectionless datagram service that emphasizes reduced latency over reliability.

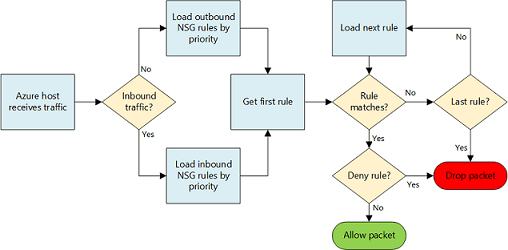
## **New approach of endpoints**

The approach to Azure endpoints works a little differently between the Classic and Resource Manager Deployment models. In the Resource Manager Deployment model, now have the flexibility to create network filters that control the flow of traffic in and out of VMs using Network Security Group (NSG).

## **Network Security Group**

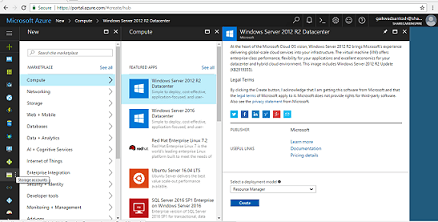
A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager). When an NSG is associated to a subnet, the rules apply to all resources connected to the subnet. Traffic can further be restricted by also associating an NSG to a VM or NIC.

Following image depicts how NSG rules are processed.

How NSG rules are processed

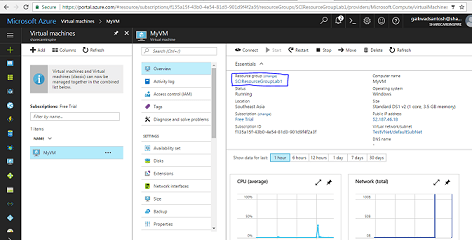
## **Steps to setup NGS Rules**

**1.** Create VM  
New -> Compute -> Select Windows Server 2012

Create VM

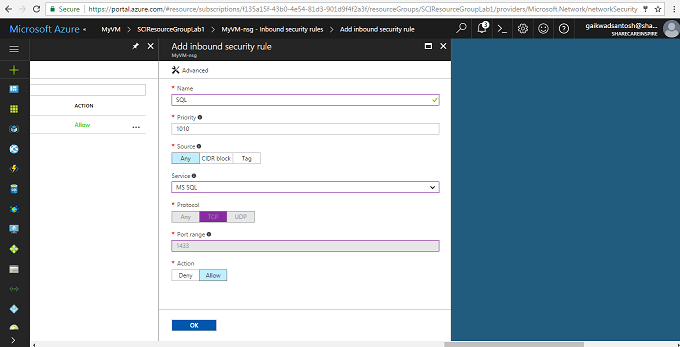
Follow further instructions to create VM.

**2.** Select resource group of VM  
Click on Virtual Machines -> Get the list of all virtual machines -> Select VM -> Overview -> click on resource group name

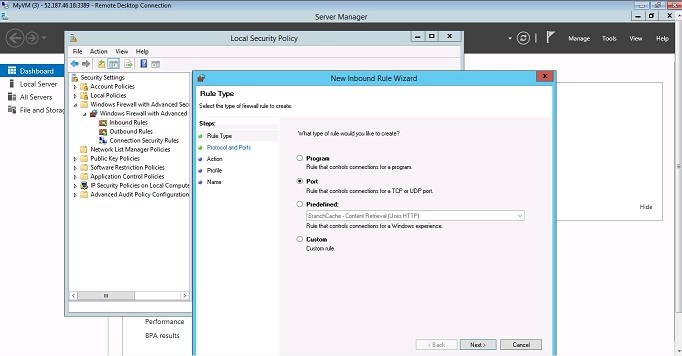
VM Resource Group

Further click on public IP address and provide appropriate DNS name.

**3.** Add inbound security rules on NSG  
Navigate back to resource group and click on Network security group

NSG Inbound Rule

**4.**Install SQL Server in VM and add Local security policy  
**i.** Install SQL Server in VM and make appropriate settings to enable communication on port 1433 (default)  
**ii.** Server Manager -> Tools -> Local Security Policy

Local Secutiry Policy in VM

**5.**Connect to SQL Server  
Using SQL Server management studio connect to SQL Server from your local machine. (make sure SQL client settings are configured properly to communicate on 1433 with TCP)

## **Access control list (ACL)**

It is recommended to use Network Security Groups (NSGs) instead of ACLs whenever possible.

Access Control List (ACL) is a security enhancement available for your Azure deployment. An ACL provides the ability to selectively permit or deny traffic for a virtual machine endpoint. This packet filtering capability provides an additional layer of security. You can specify network ACLs for endpoints only. You can’t specify an ACL for a virtual network or a specific subnet contained in a virtual network.