Network Security Group Demo Walkthrough

This guide provides a walkthrough for Network Security Group.

Contents

[Pre-Requisites 1](#_Toc435631906)

[Setup 1](#_Toc435631907)

[Demo Steps 3](#_Toc435631908)

[Clean Up 4](#_Toc435631909)

## Pre-Requisites

This section lists the pre-requisites required for this demonstration.

* An Azure subscription
* Download PSTools - <https://technet.microsoft.com/en-us/sysinternals/jj729731.aspx>

## Setup

Estimated time: 10 minutes

|  |  |
| --- | --- |
| 1. Open Windows Explorer. 2. Copy the folder **.\Demos\1\_NSG** to **c:\azurecoe\demos\networking**. 3. Open Visual Studio. 4. Using Visual Studio, open the solution at **C:\azurecoe\demos\networking\2\_NSG\** **NSG-Demo-Solution\NSG-Demo-Solution.sln**. 5. Select **<Create New>** for the **Resource Group Name**.    1. Set the **Resource Group location** to a region close to you.    2. Click **Create**. |  |
| 1. Click **Edit Parameters**.    1. Keep the default values with should look as shown here.    2. Click **Save**.   **Note:** RDP user name is **demouser** and pwd is **demouser@123**   1. Click **Deploy**.   **Note: This deployment will take approx. 15 minutes to complete.** |  |
| 1. Once the deployment is completed, you can view the resources created. This template creates a VNet with 3 Subnets, Frontend, App Subnet and Database subnet. It also creates three Network Security groups one per each subnet. |  |
|  |  |

## Demo Steps

Estimated time: 5 minutes

|  |  |
| --- | --- |
| 1. Sign-in to the Azure portal. 2. Open the **NSG-Demo-Solution** resource group blade. 3. In the **Resource** tile, click front end server **fewinvm**. |  |
| 1. Click Connect (RDP) and login to the front end server. |  |
| 1. Copy utility “PSTools” to the front end window server. |  |
| 1. Go to the “PSTool” folder location using command prompt (Administrator). Execute below command:   **psping –t <<DB Server 1>>:3389**  **e.g. psping –t 168.63.248.133:3389**   1. You will get the response from the server. |  |
| 1. Open the **NSG-Demo-Solution** resource group blade. Select the database NSG rule (e.g. dbnsg) and click on settings > you should be able to see the rule “rdp\_rule” which allows traffic on port 3389. |  |
| 1. Select the rule and change the Action to the “Deny” from “Allow”. |  |
| 1. After denying incoming traffic on port 3389 on db server, you will receive time out response. **(note: wait for a minute to rule to take effect)** |  |

## Clean Up

Delete the created resource group “NSG-Demo-Solution” to clean up.