Working with Barracuda F-Series Firewall on Microsoft Azure

Lab Guide

January 2016

© 2016 Microsoft Corporation. All rights reserved. This document is confidential and proprietary to Microsoft. Internal use only. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

Table of Contents

©2016 Microsoft Corporation

Overview

In this lab you will learn how to:

- Deploy a Barracuda NG virtual appliance
- Configure Azure networking with the Barracuda NG virtual appliance
- Set user defined roles, create traffic routing rules, and control the flow of traffic between virtual machines

You will start the labs by deploying an Azure Resource Manager template consisting of three Windows Server 2012 R2 virtual machines, each residing on a separate subnet within the same virtual network.

With this template, you will implement User Defined Route and IP forwarding rules, in order to enforce traffic routing in a particular pattern: traffic originating from the first virtual machine and destined for the third virtual machine, will route via the second one.

Next, you will replace the second virtual machine with a virtual machine hosting a Barracuda NextGen Firewall F-Series virtual appliance from the Azure Marketplace. By modifying existing network security groups, configuring the network interface of the new virtual machine, and defining firewall rules of the Barracuda appliance, you will allow for a controlled traffic flow between the two remaining virtual machines.

Requirements:

Microsoft Azure Subscription

Local workstation configured with the following:

- Windows operating system (Windows 8.1+ or Windows Server 2012+)
- Azure PowerShell module 1.0.2 or newer from https://github.com/Azure/azure-powershell/releases/download/v1.1.0-January2016/azure-powershell.1.1.0.msi
- Barracuda NG Admin 6.2 downloadable from here: http://bit.ly/1Szy7em

Technical Support

Having trouble with this lab or have a question? Please contact SuperHuman_Help@microsoft.com for technical assistance.

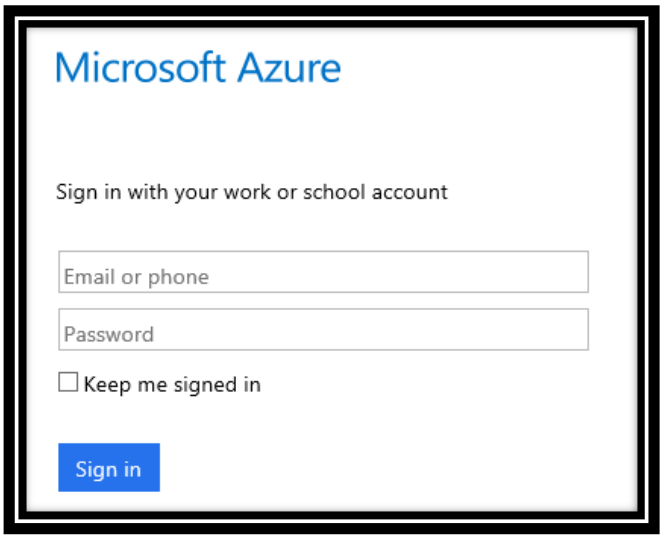
©2016 Microsoft Corporation

Exercise 1: Login to the Microsoft Azure Portal

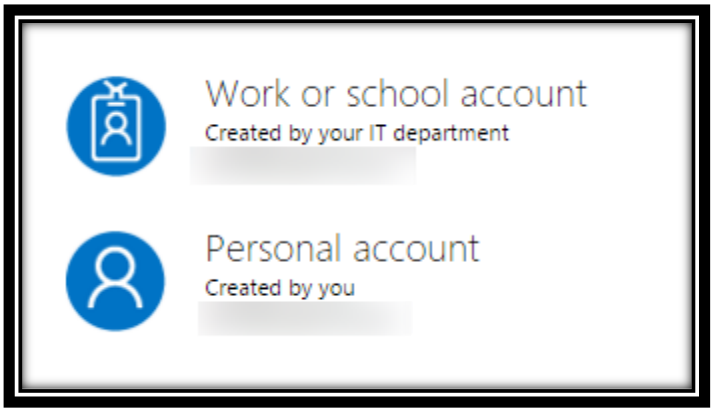
In this exercise, you will use your Microsoft or Organization account to login to the Azure portal to start the lab exercise.

1. Open your browser and navigate to https://portal.azure.com/

2. Enter the account associated with your Microsoft Azure subscription.



3. If your account is associated with an organization account and a Microsoft account, you may be prompted to choose which one to authenticate with for your Microsoft Azure account.



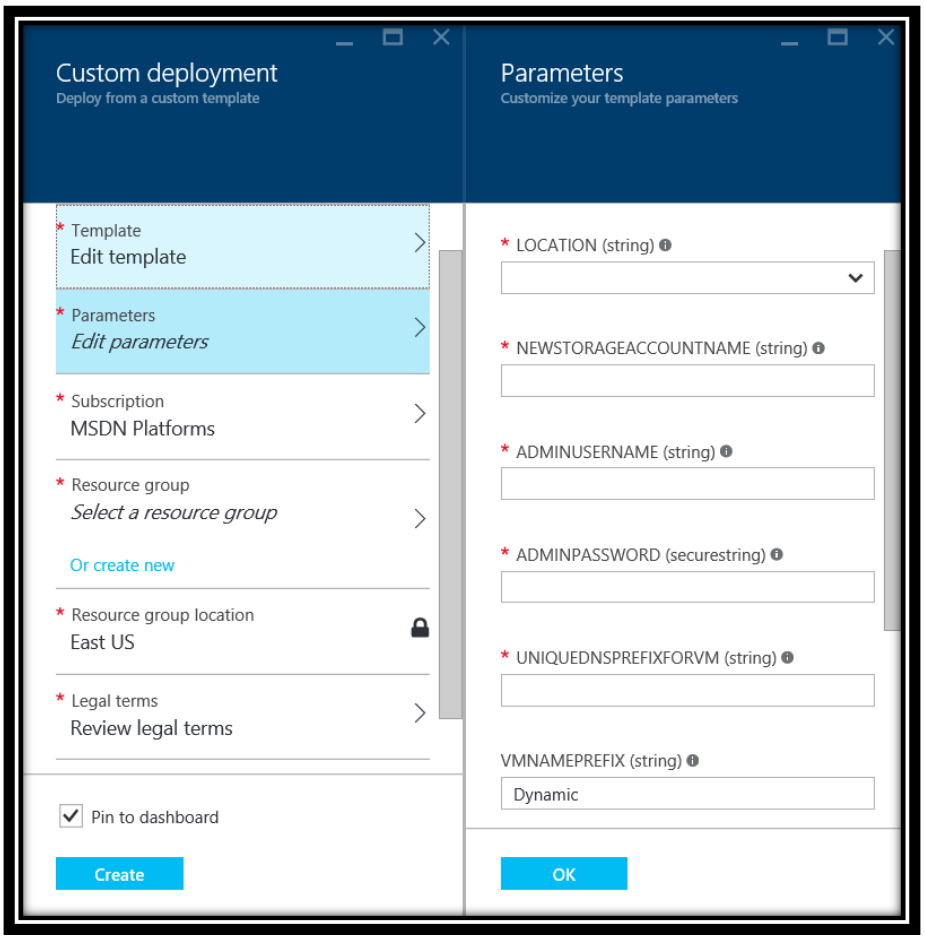
©2016 Microsoft Corporation

Exercise 2: Deploy an Azure Resource Manager Template

In this task, you will deploy an Azure Resource Manager Template, which implements three Windows Server 2012 R2 virtual machines, each of them residing on a separate subnet within the same virtual network. The deployment defines User Defined Route and IP forwarding, enforcing traffic originating from the first virtual machine and destined for the third virtual machine to be routed via the second one.

1. In your browser navigate to https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fgithub.com%2FNarayanAnnamalai%2Fazure-quickstart-templates%2Fraw%2Fmaster%2F201-userdefined-routes-appliance%2Fazuredeploy.json

2. This will automatically initiate deployment in the Azure portal, displaying the **Parameters** blade.



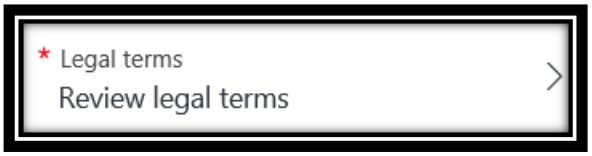
©2016 Microsoft Corporation

3. In the **Parameters** blade, specify the following and click **OK**:
    - LOCATION (string): *an available Azure region close to your location*
    - NEWSTORAGEACCOUNTNAME (string): *unique string consisting of 3-24 lower-case characters and digits.*
    - ADMINUSERNAME (string): **demouser**
    - ADMINPASSWORD (securestring): **demo@pass1**
    - UNIQUEDNSPREFIXORVM (string): *unique string consisting of 3-24 lower-case characters and digits.*
    - VMNAMEPREFIX (string): **DemoVM**
    - PUBLICIPADDRESSTYPE (string): **Dynamic**
    - WINDOWSOSVERSION (string): 2012-R2-Datacenter

4. In the **Custom Deployment** blade, click **Or create new** in the **Resource Group** section.

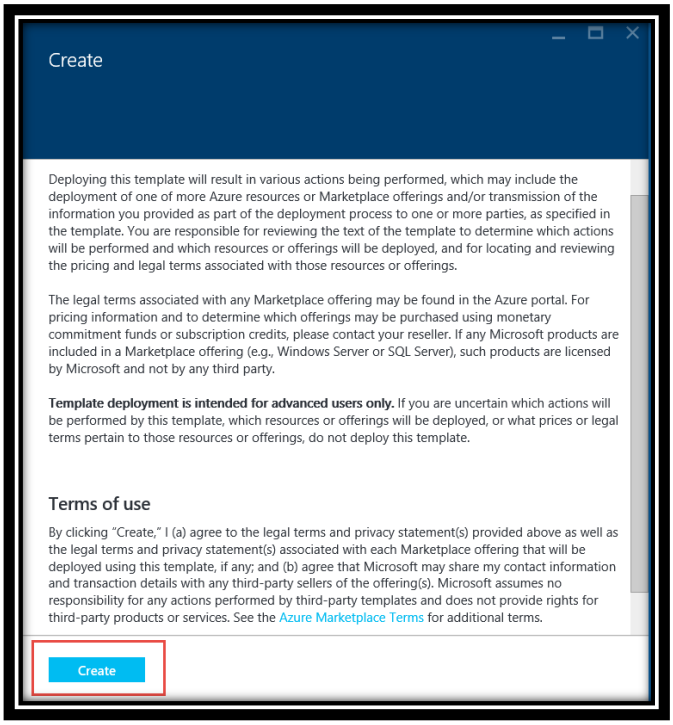
5. Type **BarracudaRG** in the textbox.

6. Click **Review legal terms**

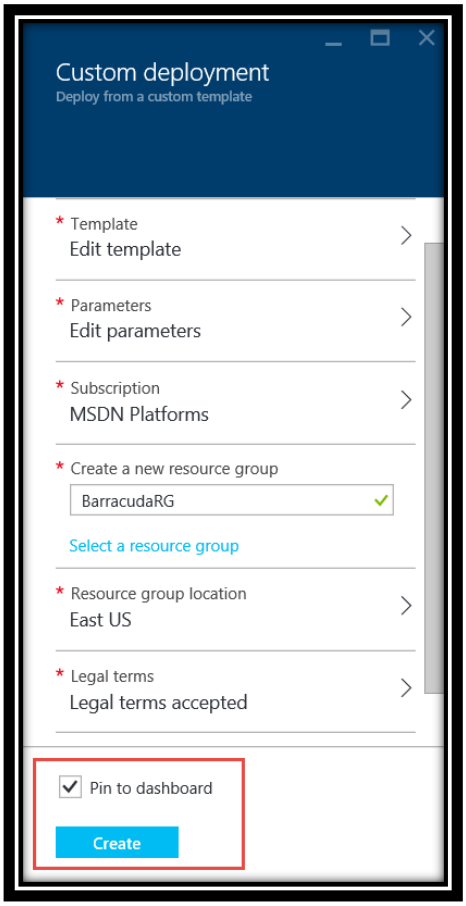


7. In the **Create** blade, click **Create.**

©2016 Microsoft Corporation



8. In the **Custom Deployment** blade, click **Create**



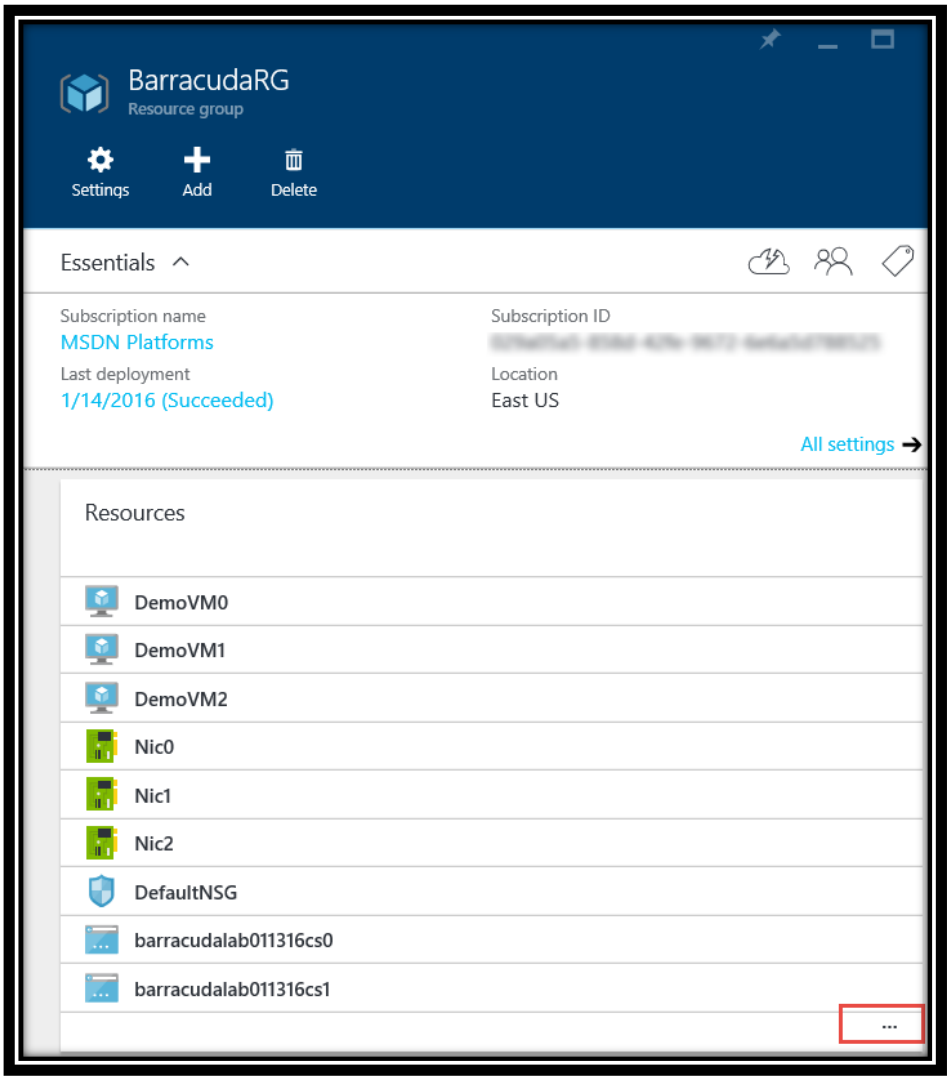
©2016 Microsoft Corporation

NOTE: Wait for the deployment to complete. This may take about 10 minutes.

Exercise 3: Review networking configuration of the new deployment

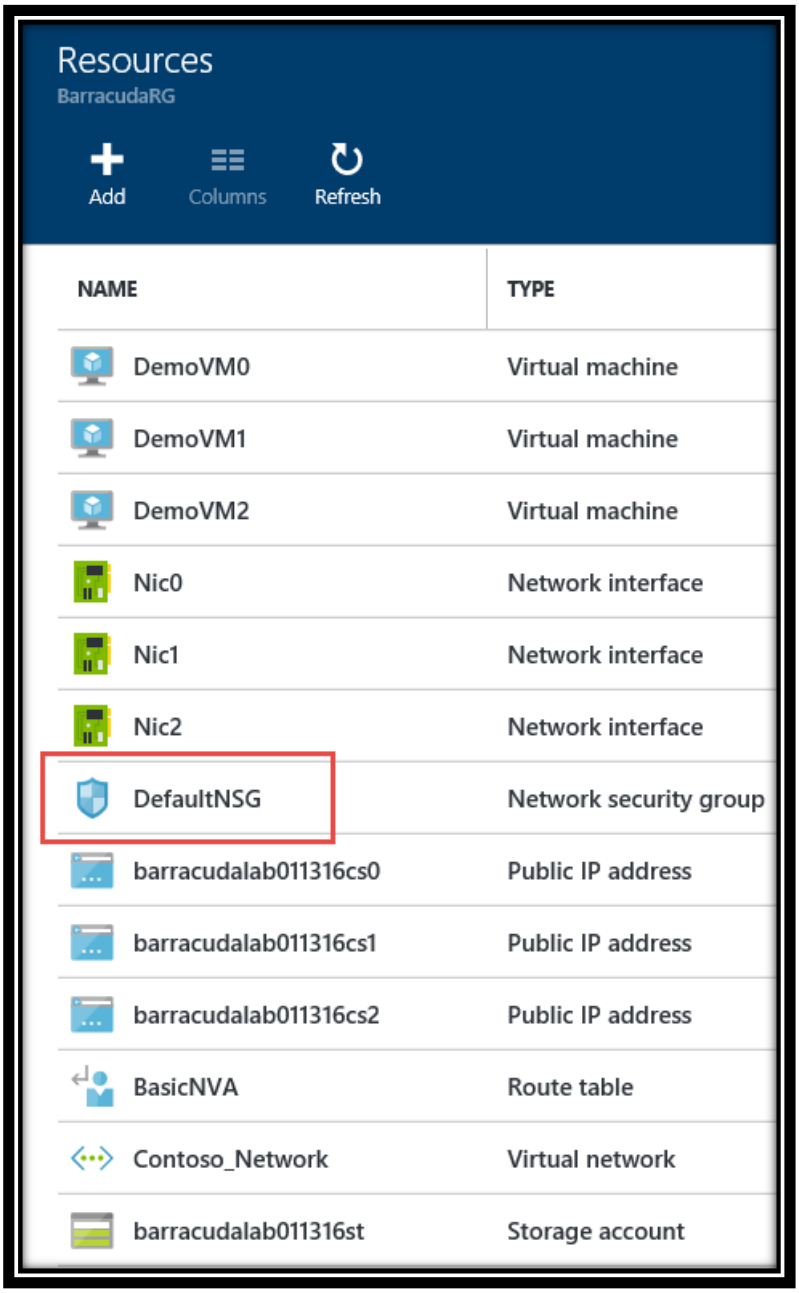
In this task you will review the settings of the new deployment and prepare it for deployment of the Barracuda NG virtual appliance.

1. In the Azure Portal, in the **Resources** lens of the **BarracudaRG** resource group, click ellipsis (...).



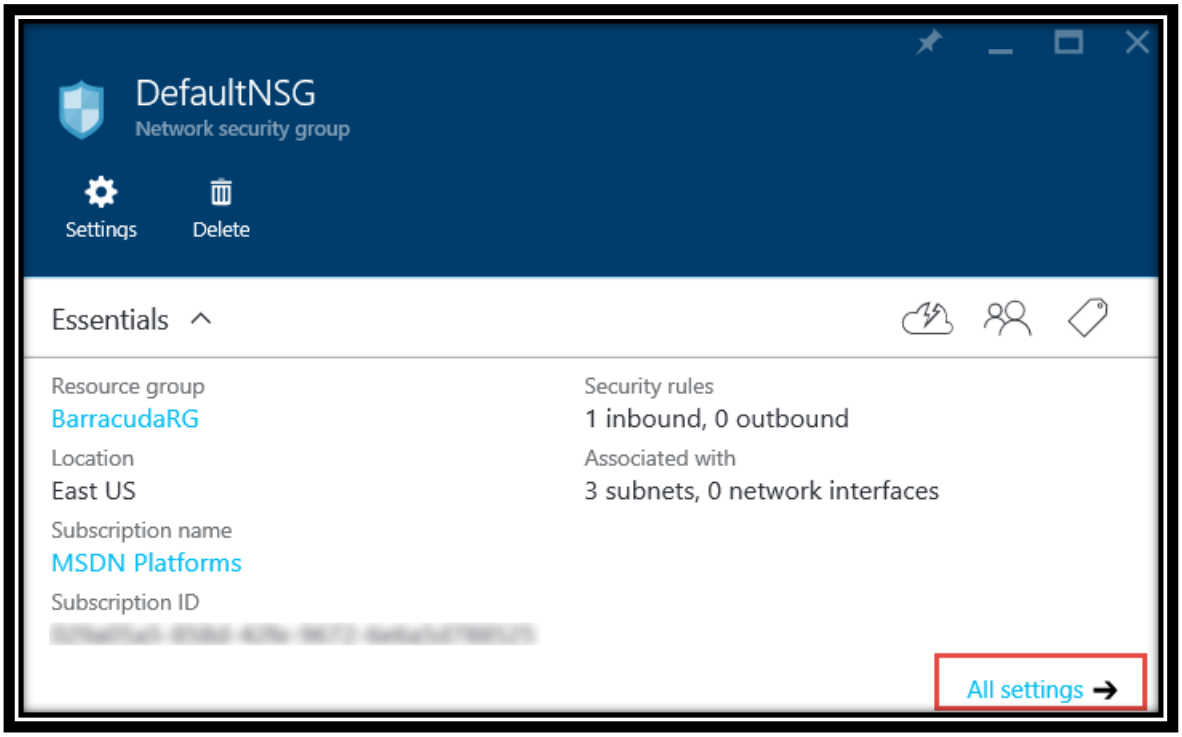
©2016 Microsoft Corporation

2. In the **Resources** blade, note that the resource group contains three virtual machines, three network interfaces (one per each VM), one default network security group, one route table, virtual network, and a storage account. Click **DefaultNSG.**

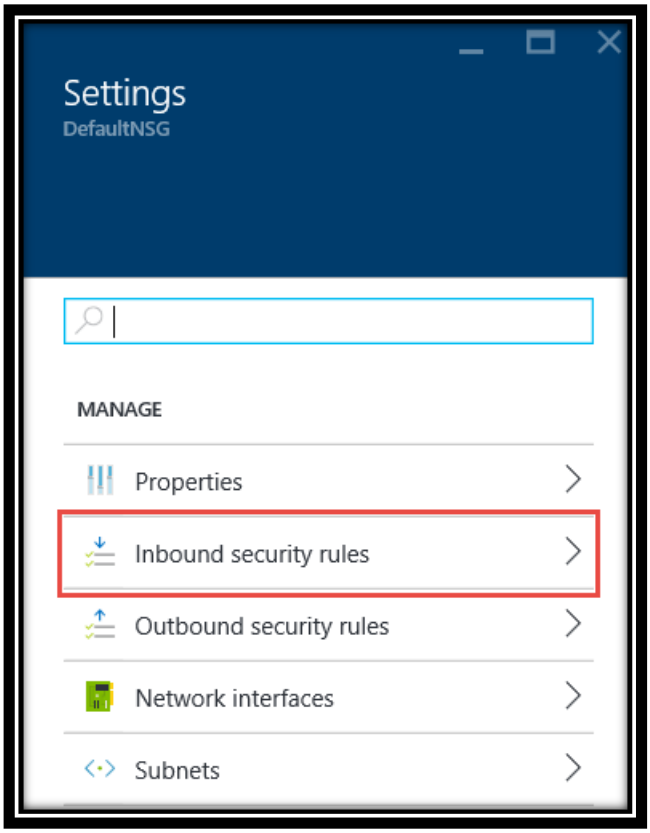


3. In the **DefaultNSG** blade, click **All settings**.

©2016 Microsoft Corporation



4. In the **Settings** blade, click **Inbound security rules**.

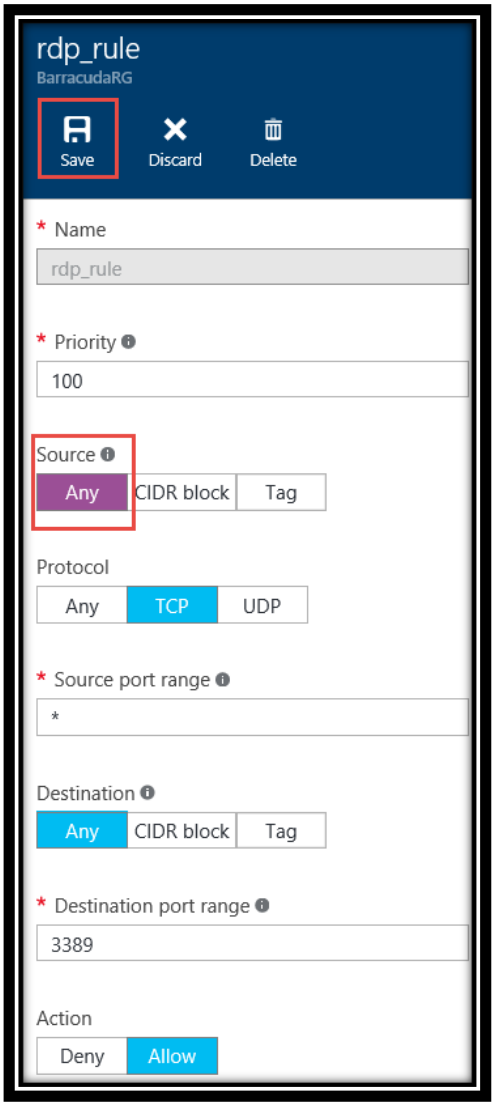


©2016 Microsoft Corporation

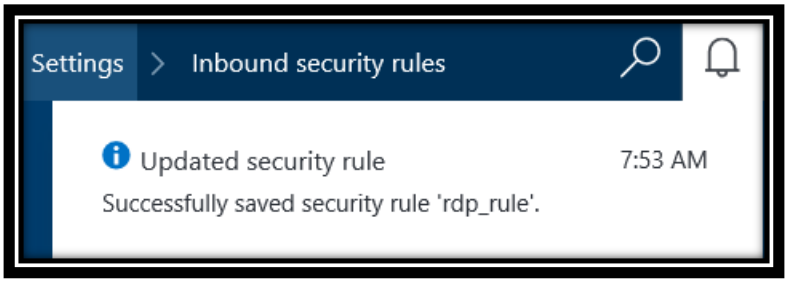
5. In the **Inbound security rules** blade, note that the network security group **DefaultNSG** consists of a single rule that allows RDP connectivity to each VM from the Internet. We will modify it to allow RDP connectivity from anywhere, including connections initiated from within the same virtual network. Click **ellipsis (...)**.

6. In the **rdp_rule** blade, click **Any** Source and click **Save** to save the change.

©2016 Microsoft Corporation



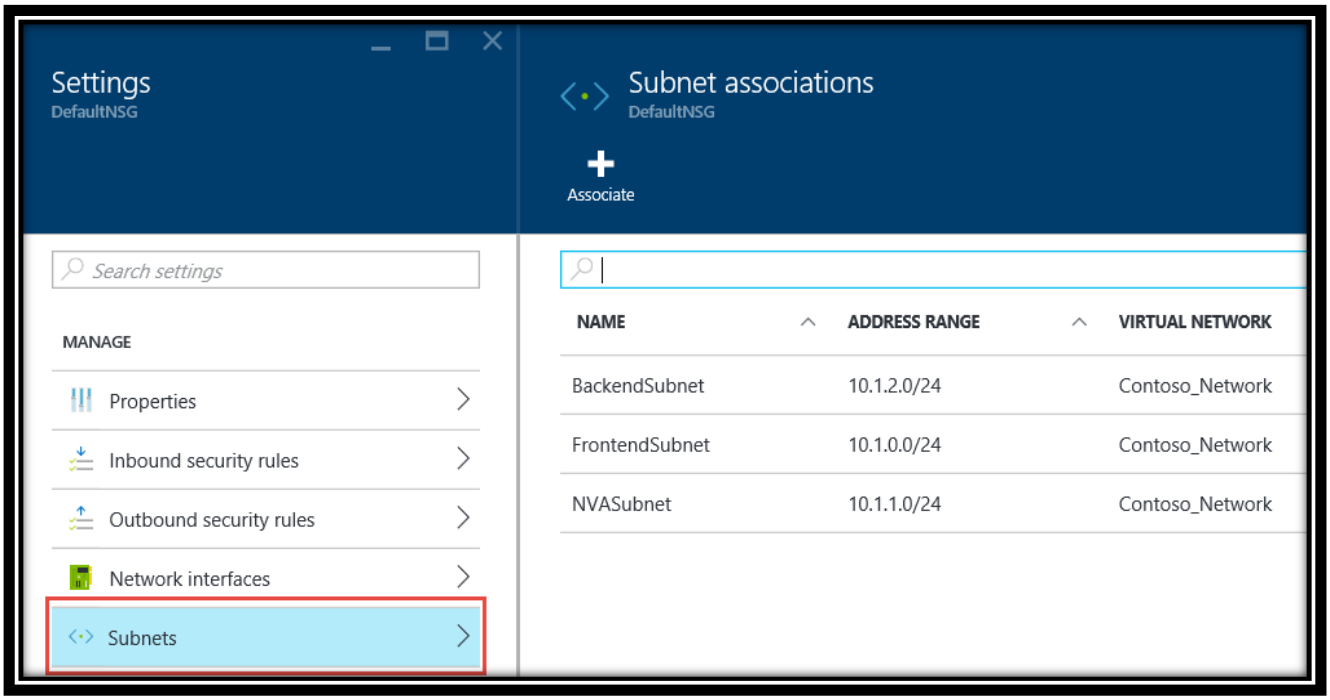
7. Wait for the rule to be successfully saved.



8. Click **Settings** at the top of the Azure Portal page.

©2016 Microsoft Corporation

9. In the **Settings** blade, click **Subnets** and examine the content of the **Subnets** blade. Note that the network security group is applied to all three subnets on our virtual network.

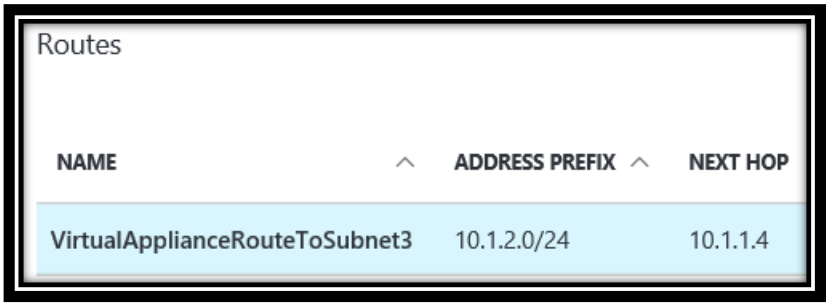


10. Click **Resources** at the top of the Azure Portal page.

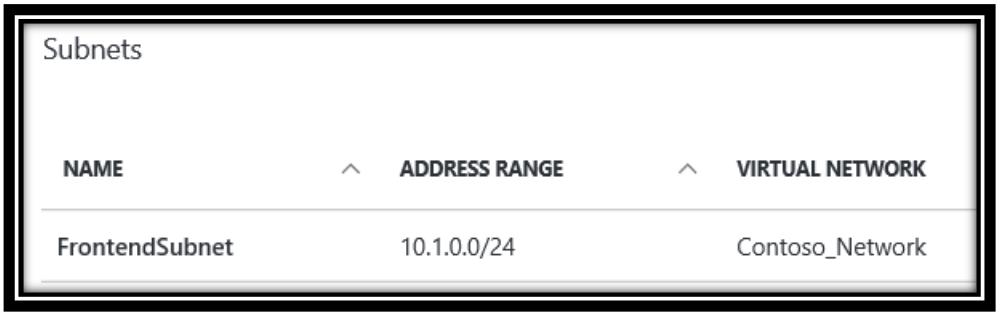
11. In the **Resources** blade, click **BasicNVA** route table.

12. In the **BasicNVA** blade, review the **Routes** lens. Note that the route table contains a single user defined route, which forces the traffic to Subnet3 (10.1.2.0/24) via the virtual machine with the IP address of 10.1.1.4. This is the second virtual machine (**DemoVM1)** which we will replace with the Barracuda NG appliance.

©2016 Microsoft Corporation

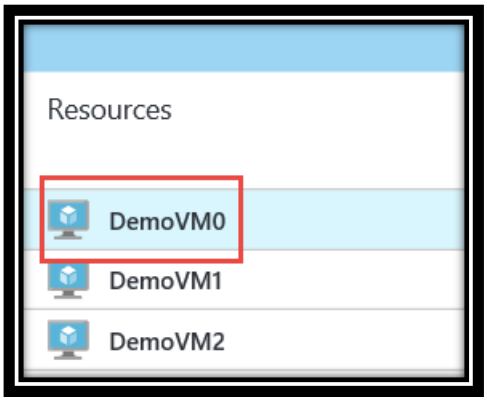


13. In the **BasicNVA** blade, review the **Subnets** lens. Note that the route table is associated with the FrontEndSubnet (containing the **DemoVM0** virtual machine).



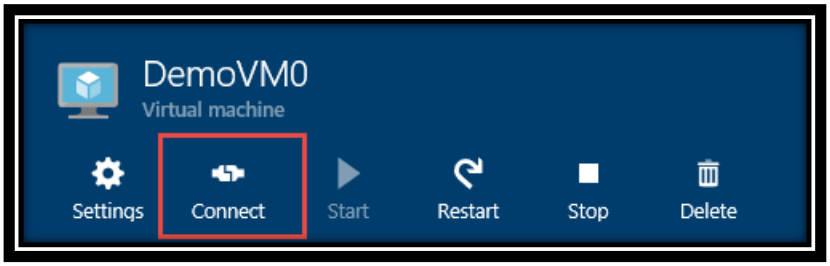
14. Click **Resources** at the top of the Azure Portal page.

15. In the **Resources** lens of the **Resources** blade, click **DemoVM0**.



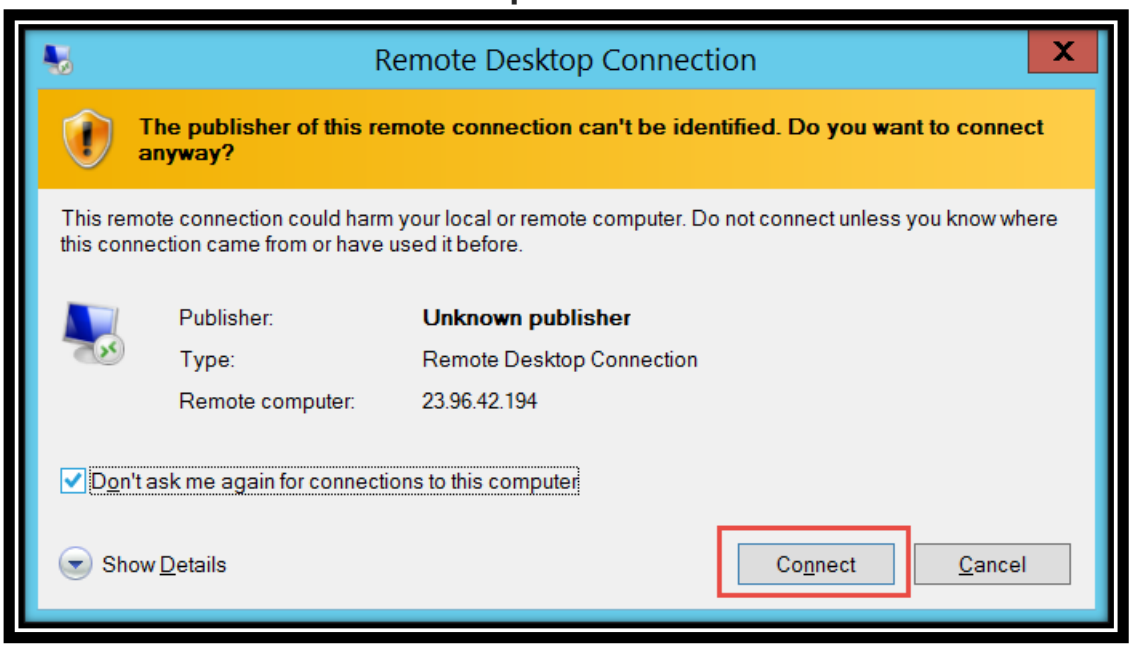
16. In the **DemoVM0** blade, click **Connect**.

©2016 Microsoft Corporation



17. When prompted, click **Open**.

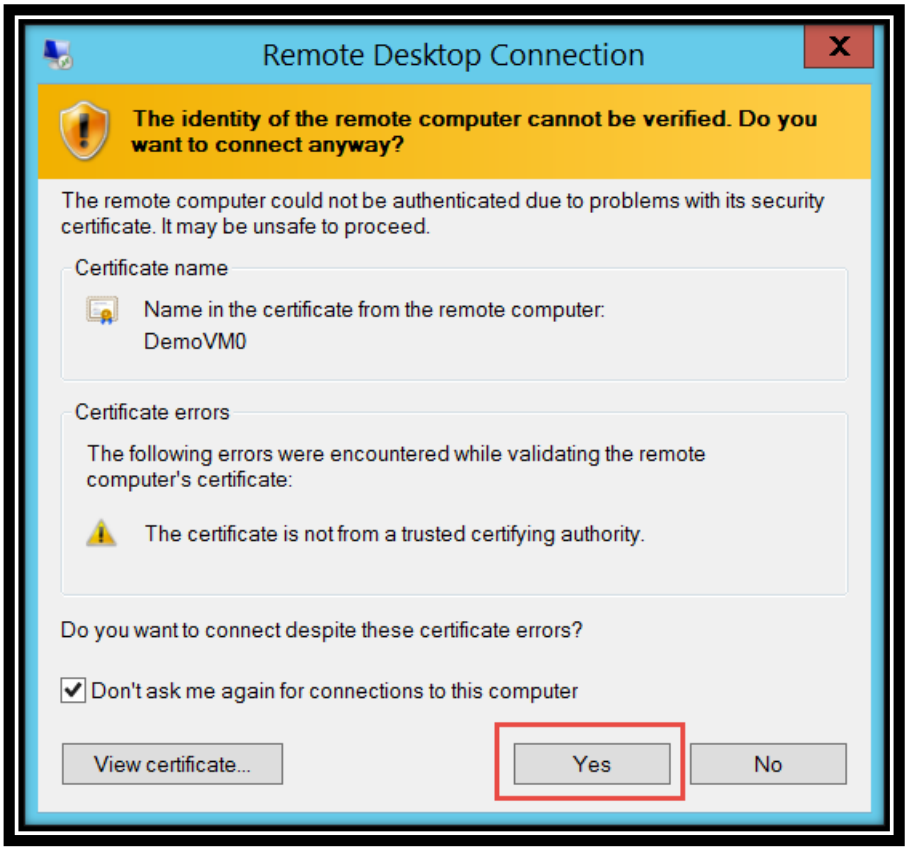
18. In the **Remote Desktop Connection** dialog box, enable the **Don't ask me again for connections to this computer** checkbox and click **Connect**.



19. In the **Windows Security** dialog box, sign in with the **demouser** username and **demo@pass1** password credentials.

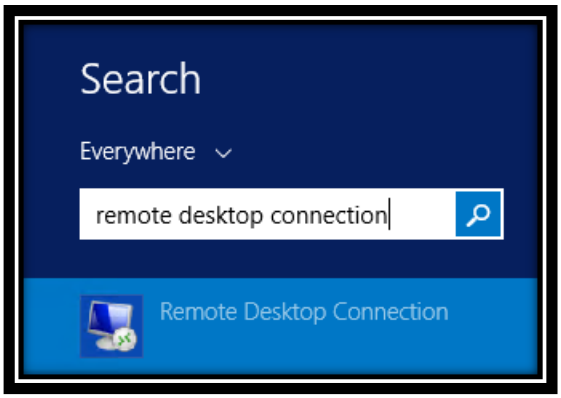
©2016 Microsoft Corporation

20. In the **Remote Desktop Connection** dialog box, enable the **Don't ask me again for connections to this computer** checkbox and click **Yes**.

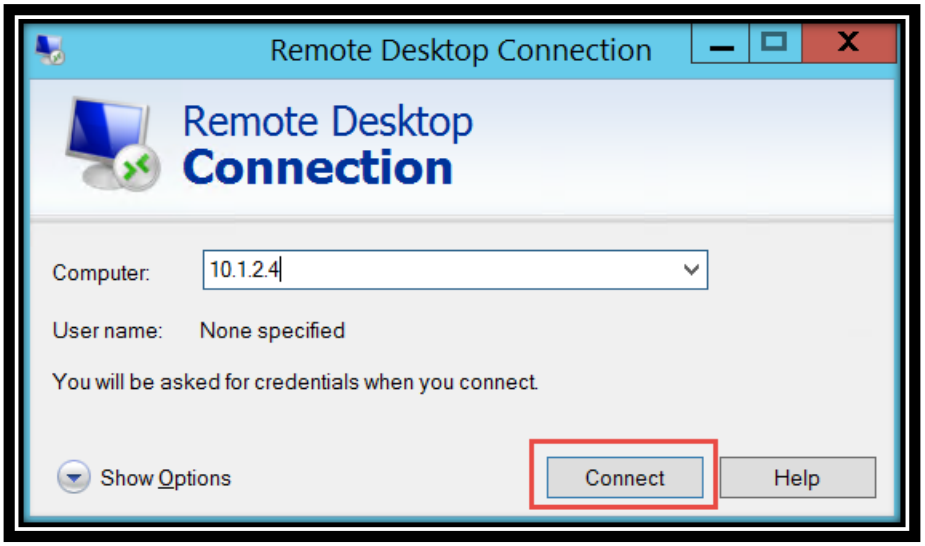


©2016 Microsoft Corporation

21. Once you log on to **DemoVM0**, from within the RDP session, from the **Start** screen, launch Remote Desktop Connection

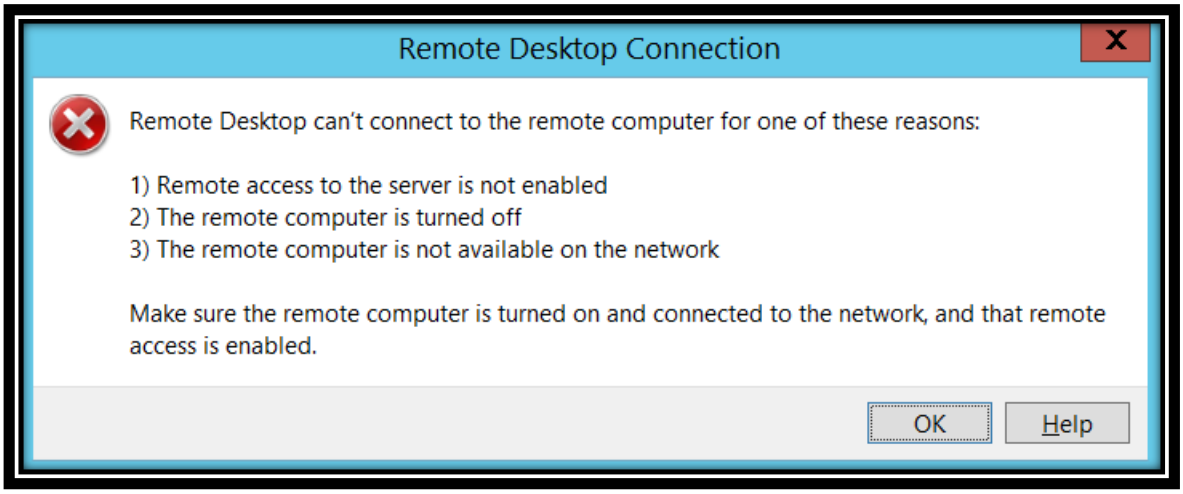


22. In the **Remote Desktop Connection** dialog box, type in **10.1.2.4** (the private IP address of **DemoVM2** in the **Computer** text box and click **Connect**.



23. The connection will fail due to the user defined route which forces the traffic from 10.1.0.0/24 (on which **DemoVM0** resides) to 10.1.2.0/24 (on which **DemoVM2** resides) via 10.1.1.4, assigned to **DemoVM1**, which at this point, is not configured to allow routing.

©2016 Microsoft Corporation



NOTE: Leave the RDP session to DemoVM0 open. We will use it again later in this lab.

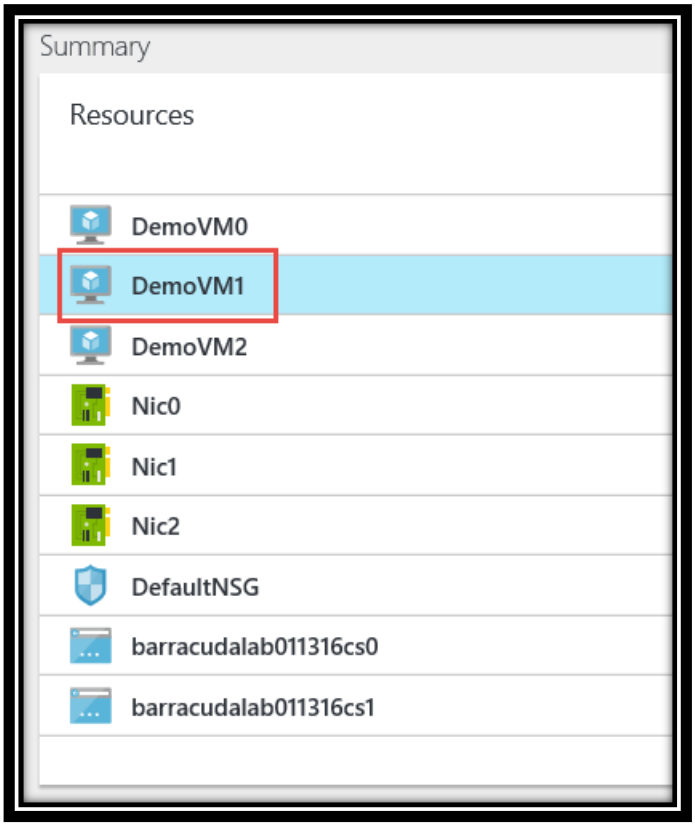
Exercise 4: Deploy Barracuda NG virtual appliance

In this exercise, you will replace the second virtual machine with a Barracuda NG virtual appliance from Azure Marketplace.

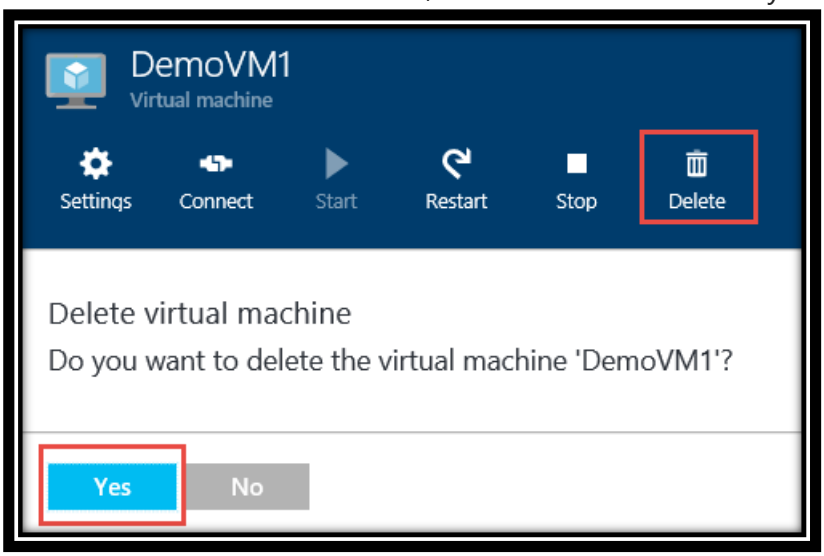
1. Return to the Azure Portal page on your lab computer. Click **BarracudaRG** at the top of the page.

2. In the **Summary** lens of the **BarracudaRG** blade, click **DemoVM1**.

©2016 Microsoft Corporation

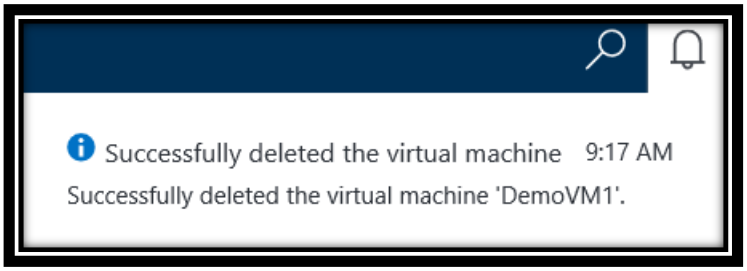


3. In the **DemoVM1** blade, click **Delete** followed by **Yes** when prompted to confirm.

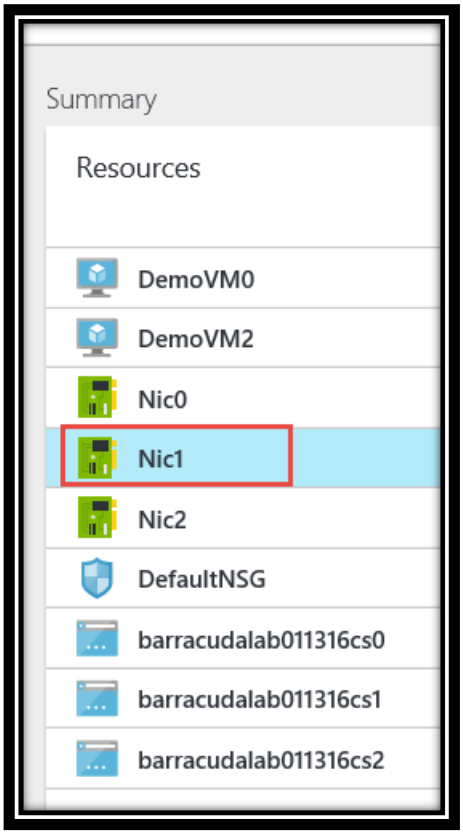


4. Wait for the confirmation that the **DemoVM1** has been successfully deleted.

©2016 Microsoft Corporation

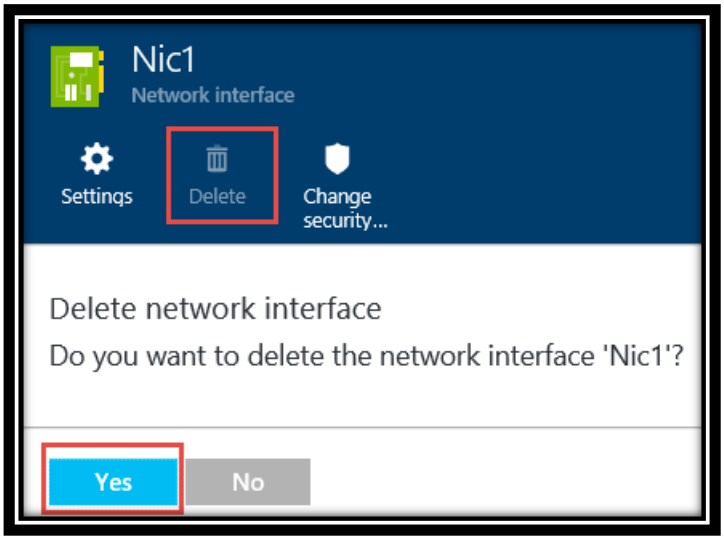


5. In the **Summary** lens of the **BarracudaRG** blade, click **Nic1**.



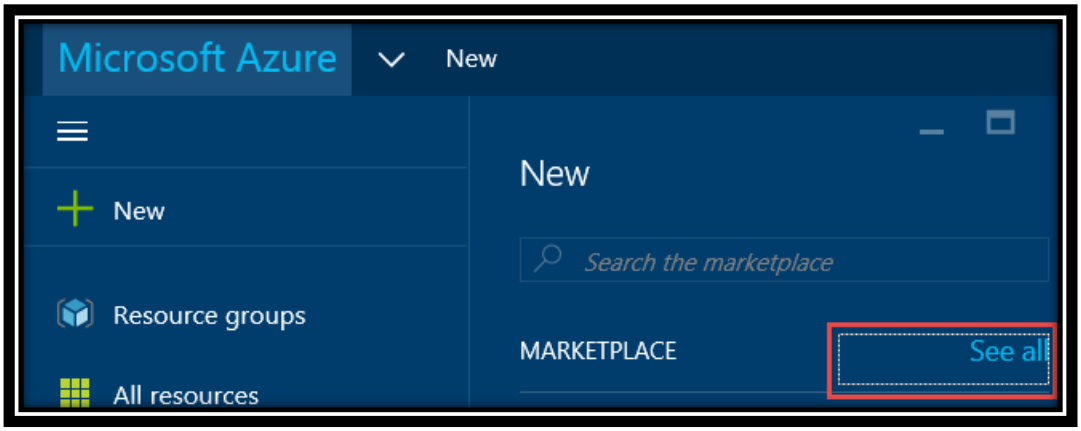
6. In the **Nic1** blade, click **Delete** followed by **Yes** when prompted to confirm.

©2016 Microsoft Corporation



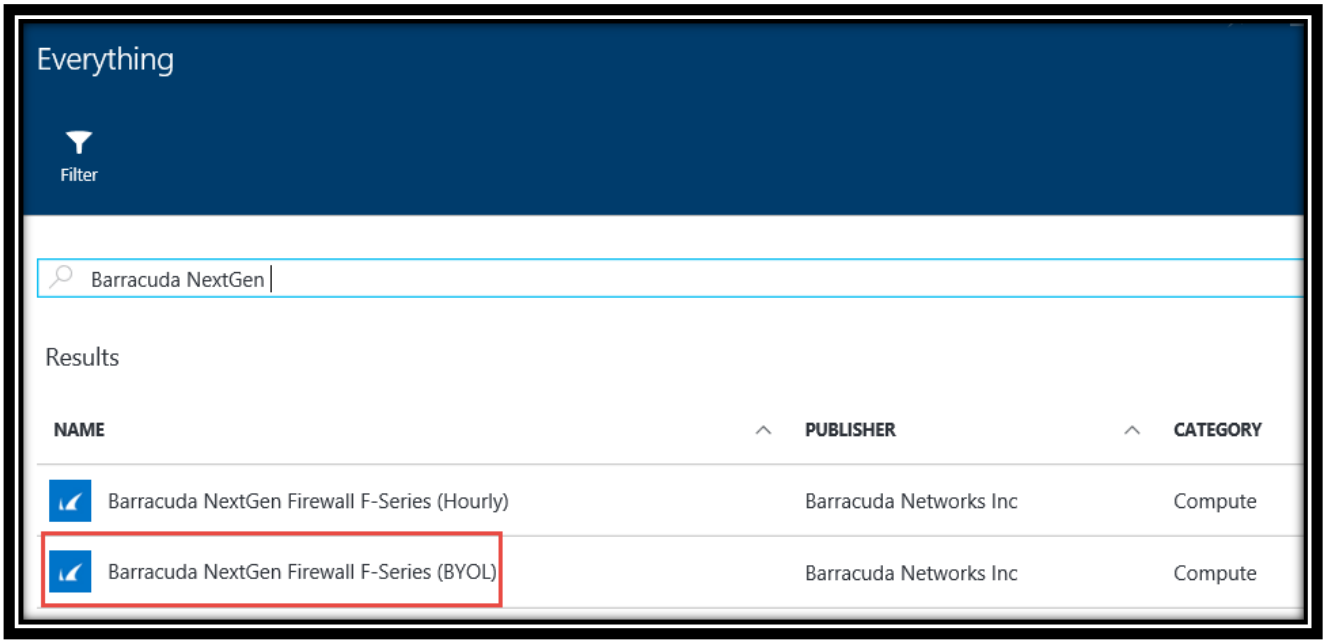
7. Wait for the confirmation that the **Nic1** is successfully deleted.

8. In the upper left corner of the Azure Portal, click **+New** followed by **See all** next to the **MARKETPLACE** entry

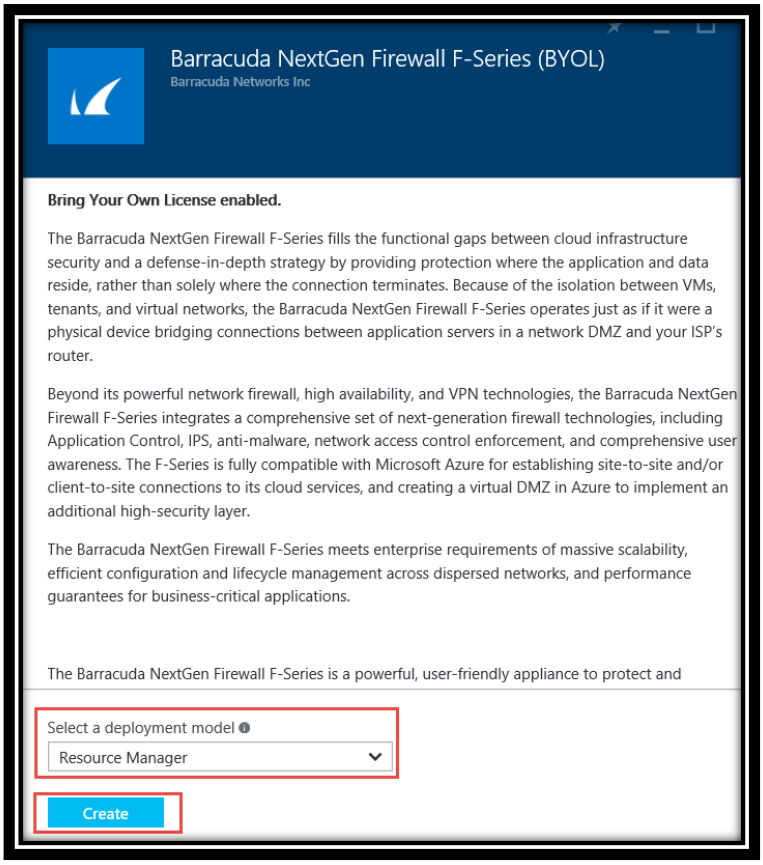


9. In the **Everything** blade, in the Search textbox, type in **Barracuda NextGen** and press the **Enter** key. Next, in the result list, click **Barracuda NextGen Firewall F-Series (BYOL)**

©2016 Microsoft Corporation

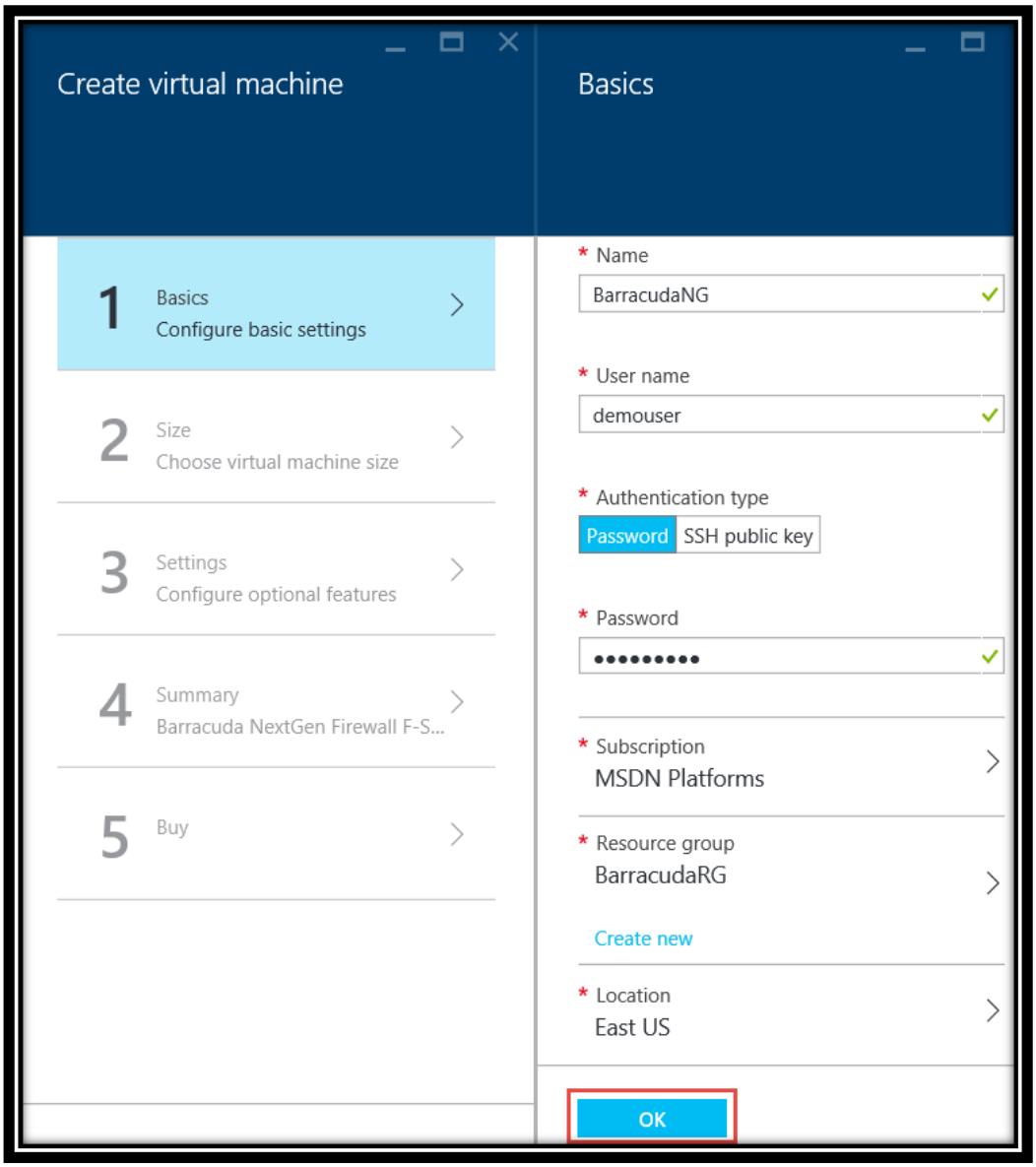


10. In the **Barracuda NextGen Firewall F-Series (BYOL)** blade, make sure that **Resource Manager** is selected in the **Select a deployment model** drop down list and click **Create**.



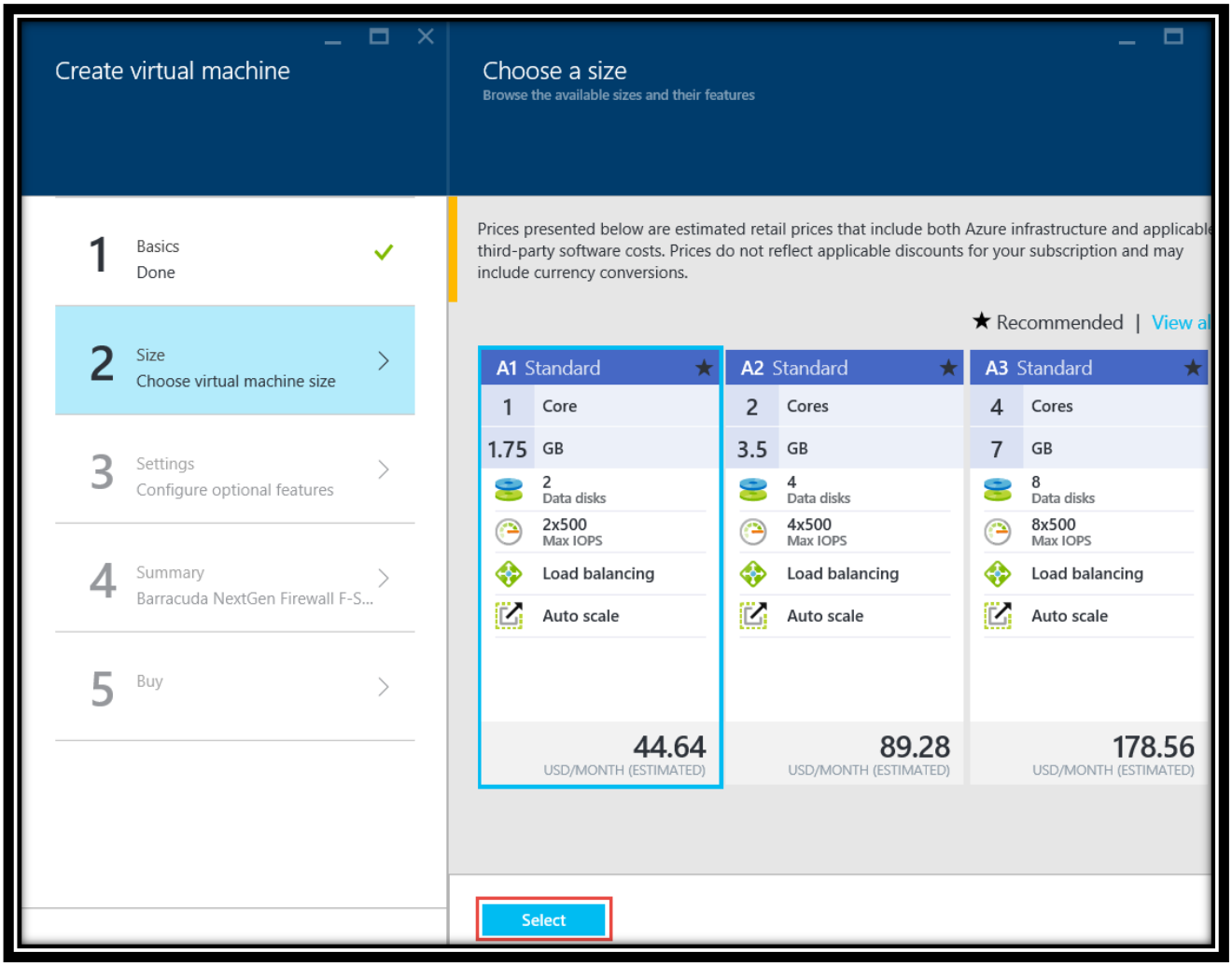
©2016 Microsoft Corporation

11. In the **Basics** blade, specify the following and click **OK**.
    - Name: **BarracudaNG**
    - User name: **demouser**
    - Authentication type: **Password**
    - Password: **demo@pass1**
    - Resource group: *click* **Select existing** *and select* **BarracudaRG**
    - Location: *choose the same location to which you deployed the virtual machines in this lab*



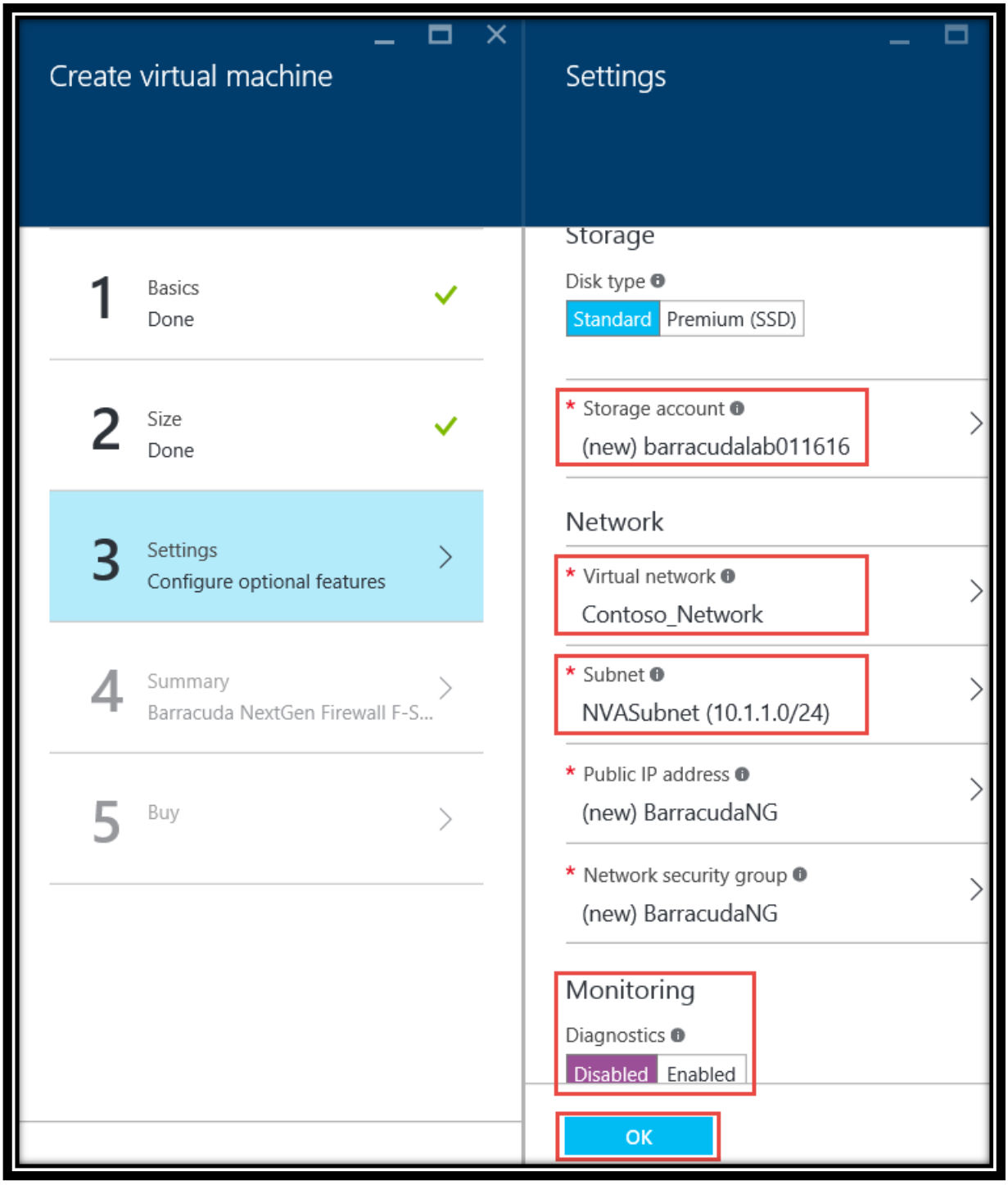
12. In the **Choose a size** blade, select **A1 Standard** and click **Select**

©2016 Microsoft Corporation



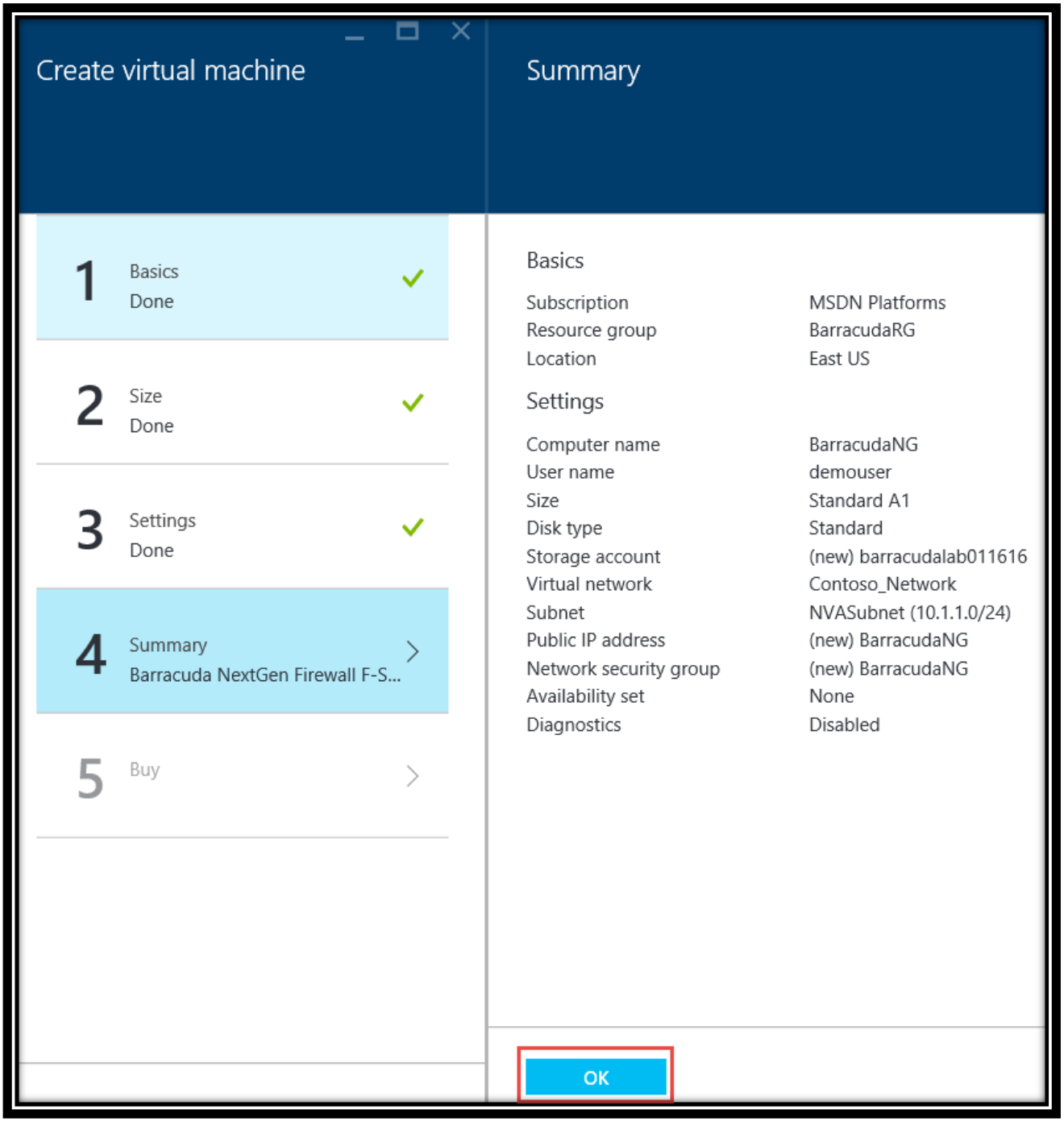
13. In the **Settings** blade, specify the following and click **OK**.
    - Disk type: **Standard**
    - Storage account: *create a new storage account. Ensure to specify a unique name consisting of a combination of lower case letters and digits.*
    - Virtual network: **Contoso_Network**
    - Subnet: **NVASubnet (10.1.1.0/24)**
    - Public IP address: *leave the default*
    - Network security group: *leave the default*
    - Diagnostics: **Disabled**
    - Availability set: **None**

©2016 Microsoft Corporation



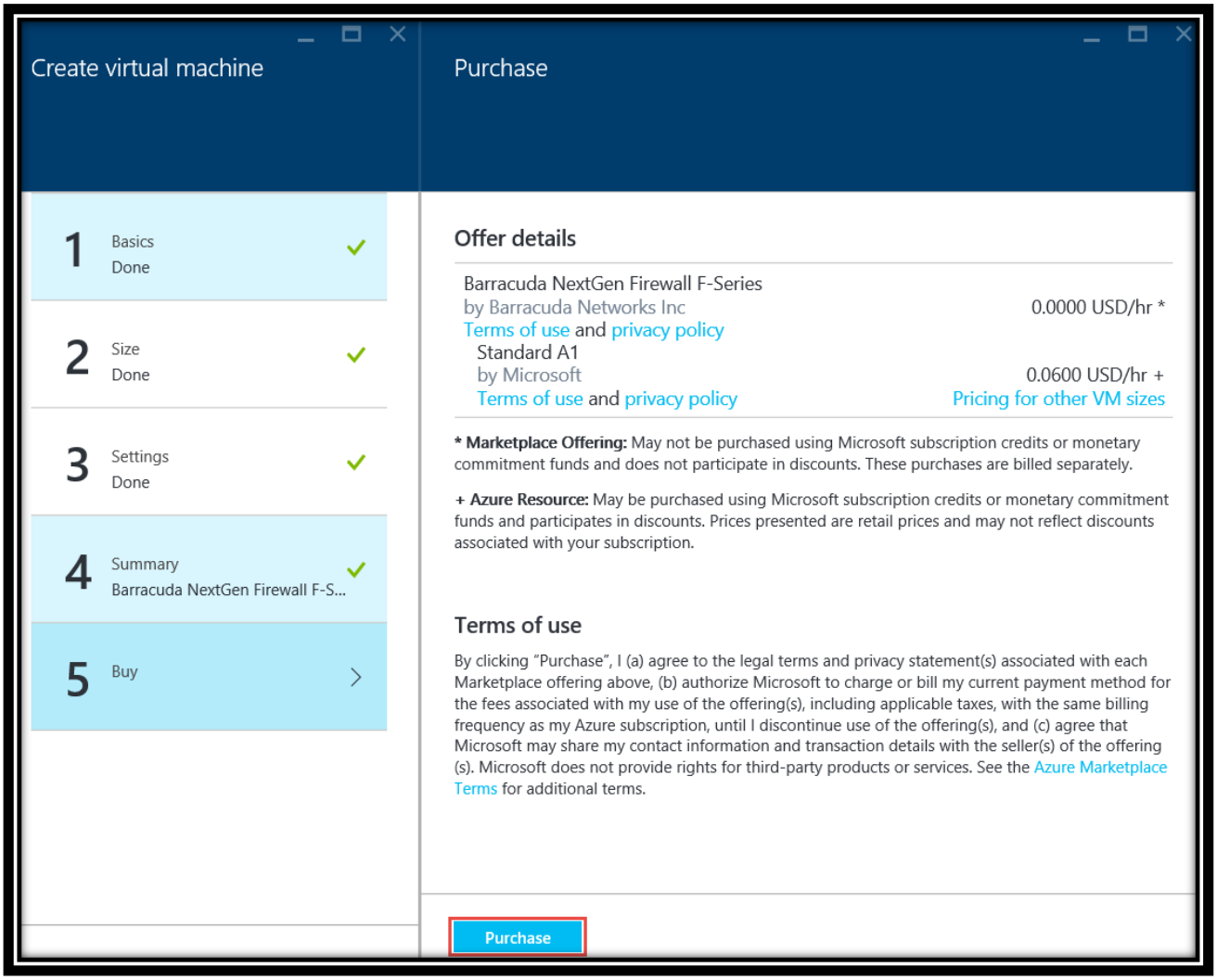
14. Review the **Summary** blade and click **OK**.

©2016 Microsoft Corporation



15. Review the **Purchase** blade and click **Purchase**.

©2016 Microsoft Corporation



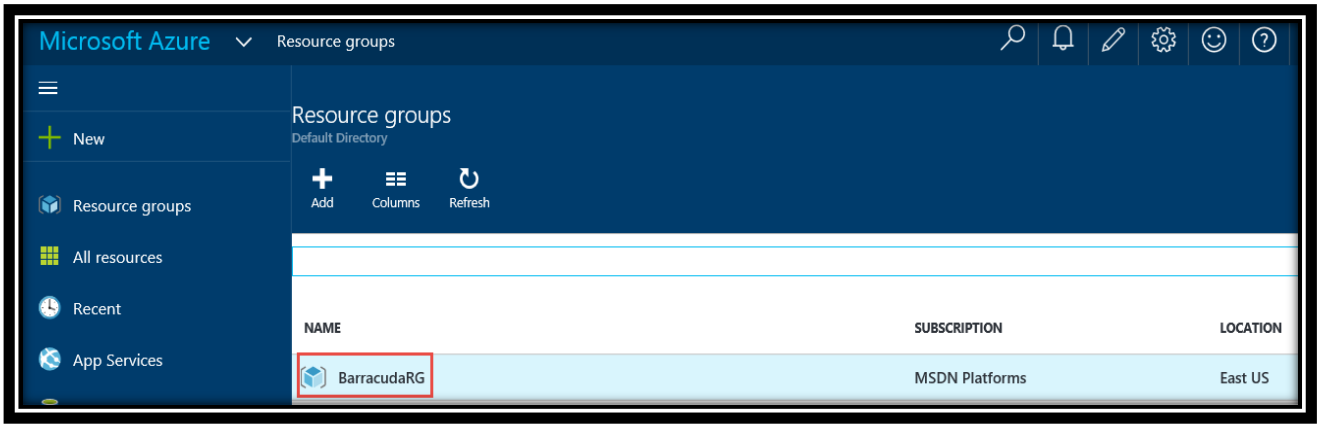
NOTE: Make sure to wait for the Barracuda NG virtual appliance to be provisioned before moving on to the next Exercise.

Exercise 5: Configure Azure networking for the Barracuda NG virtual appliance

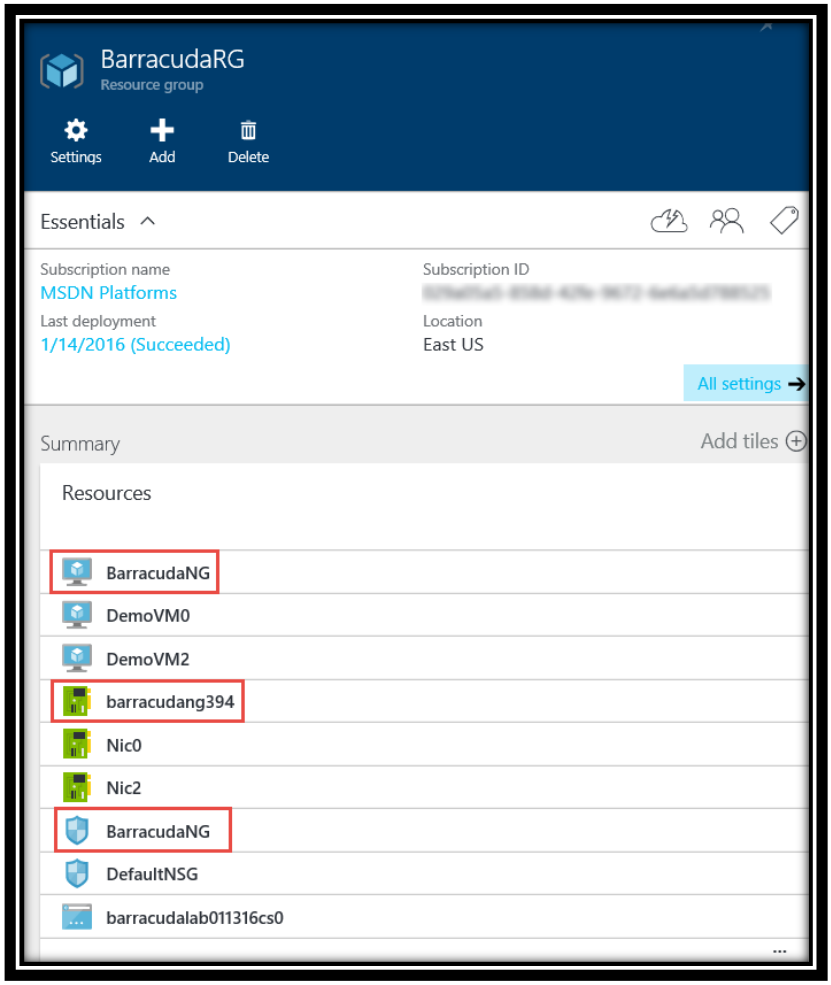
In this task, you will configure the Azure networking functionality of the Barracuda NG virtual appliance. The network interface used by the virtual machine hosting the virtual appliance must have IP Forwarding enabled.

1. In the Microsoft Azure portal, in the Hub menu on the left hand side of the page, click **Resource groups**. Then in the **Resource groups** page, click **BarracudaRG**.

©2016 Microsoft Corporation

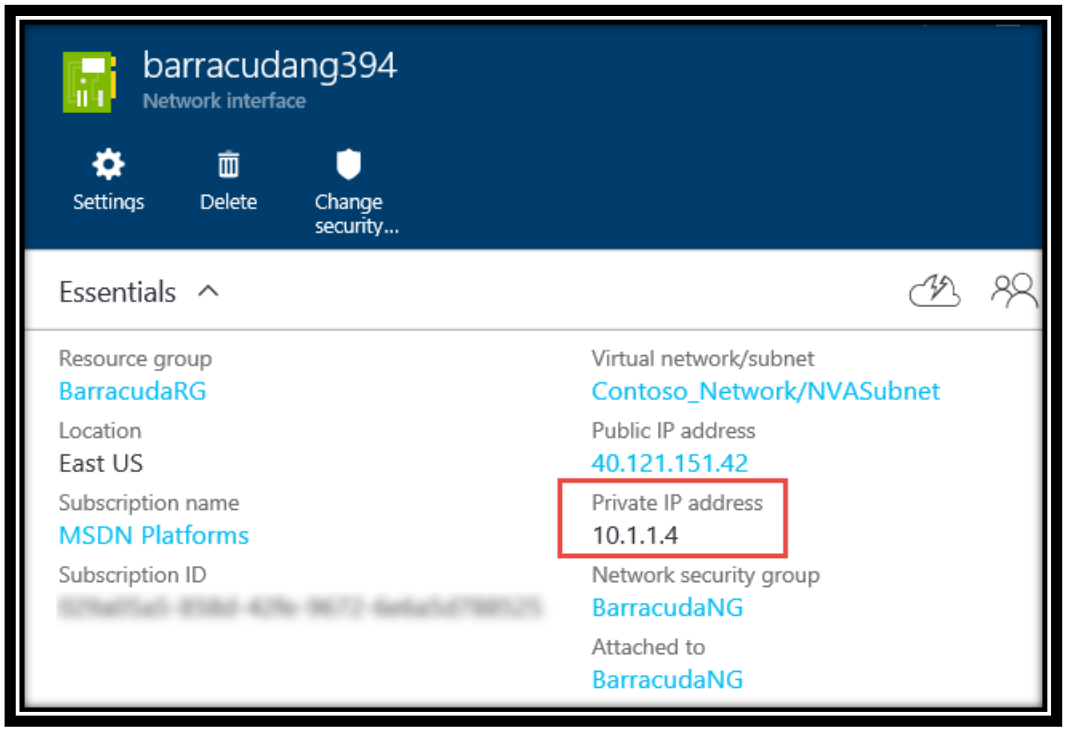


2. Note that the resource group contains a number of additional resources, including the **BarracudaNG** virtual machine, the corresponding network interface (starting with the **barracuda** prefix) and a separate network security group **BarracudaNG**.

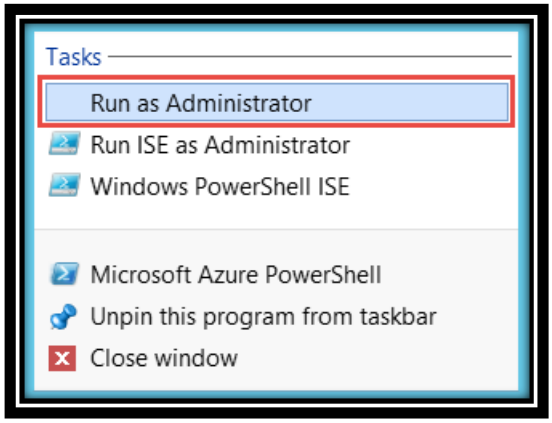


©2016 Microsoft Corporation

3. In the **Summary** lens, click the network interface (in our case, this is **barracudang394** – in yours, the last three digits are likely to differ) and note that the IP address assigned to the interface matches the one specified in our existing user defined route. This allows us to reuse it without any modifications.



4. From your lab computer, launch Microsoft Azure PowerShell as Administrator from the taskbar shortcut.

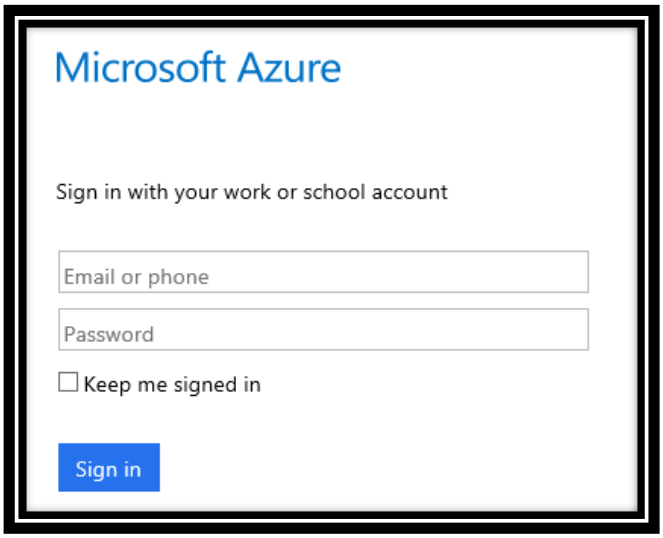


5. From the **Administrator: Microsoft Azure PowerShell** window, sign in to your Azure subscription by running the following cmdlet:

```
Login-AzureRmAccount
```

©2016 Microsoft Corporation

4. When prompted, enter the account associated with your Microsoft Azure subscription and click **Sign in**.



6. Once you are successfully signed in, set the variable representing the network interface object of the Barracuda NG virtual machine by running the following command. **<u>You will need to change the Name parameter to match the name of your Network interface</u>**:

```
$BarracudaNIC = Get-AzureRmNetworkInterface -
ResourceGroupName 'BarracudaRG' -Name 'barracudang394'
```

7. To enable IP forwarding for the network interface, set its EnableIPForwarding property to 1.

```
$BarracudaNIC.EnableIPForwarding = 1
```

8. To finalize the change, use the **Set-AzureRmNetworkInterface**

```
Set-AzureRmNetworkInterface -NetworkInterface $BarracudaNIC
```

9. The cmdlet will generate output containing the JSON representation of the updated configuration, including the **EnableIPForwarding : True** entry.

©2016 Microsoft Corporation

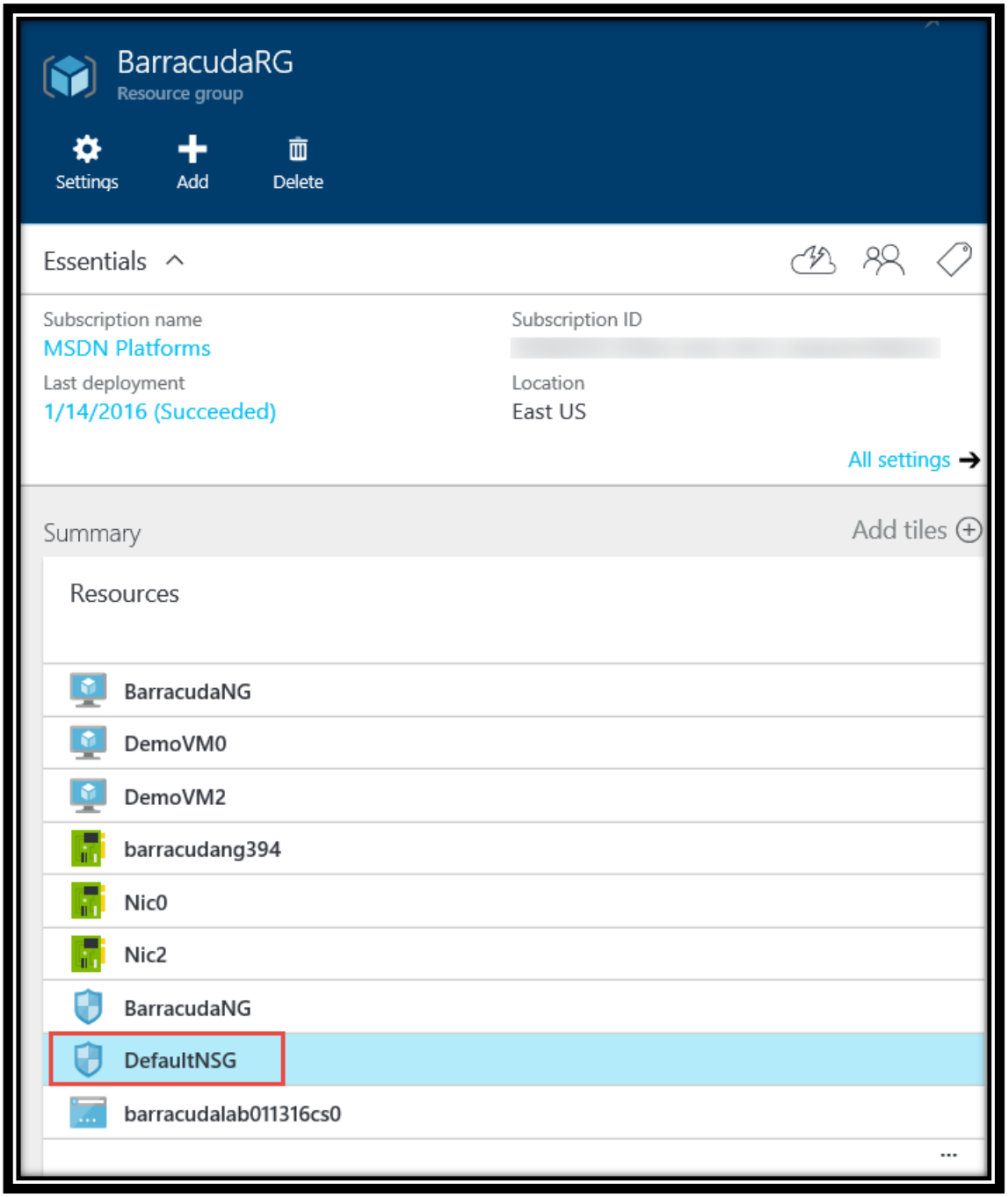
```
DnsSettings          : {
                         "DnsServers": [],
                         "AppliedDnsServers": []
                       }
EnableIPForwarding   : True
NetworkSecurityGroup : {
                         "Id": "/subscriptions/2
                       s/Microsoft.Network/netwo
                       }
Primary              : True


PS C:\>
```

10. Since the management of the Barracuda NG virtual appliance is handled by using its dedicated management utility with a designated set of ports, we will need to exclude the subnet containing the virtual appliance from the **DefaultNSG** network security group. Access to the designated ports is already implemented on the network interface level by the **BarracudaNG** network security group, included by default when deploying the appliance from the Azure Portal. To start, navigate back to the **BarracudaRG** resource group by clicking **BarracudaRG** at the top of the Azure Portal page.

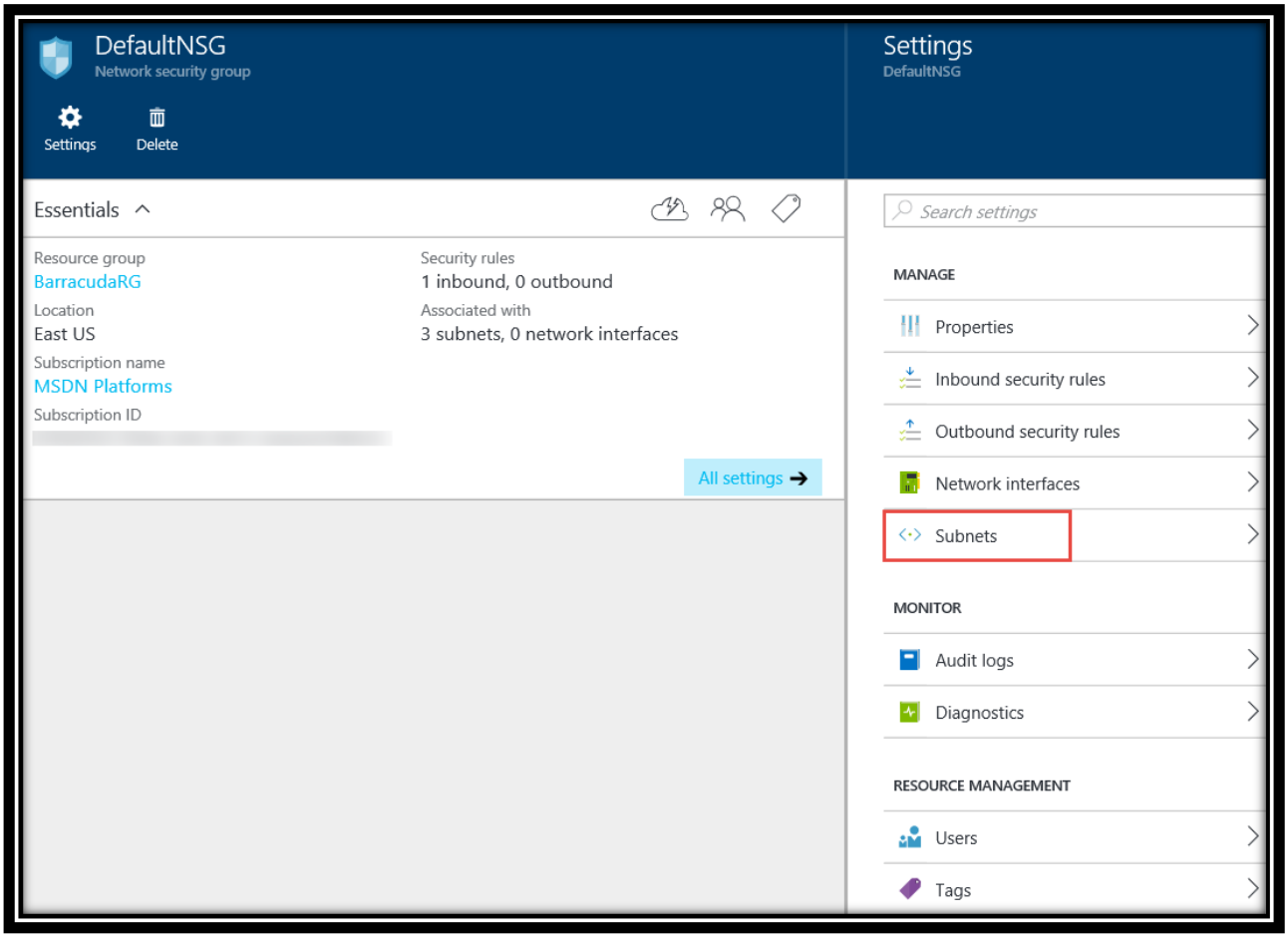
11. In the **Summary** lens on the **BarracudaRG** blade, click **DefaultNSG**.

©2016 Microsoft Corporation

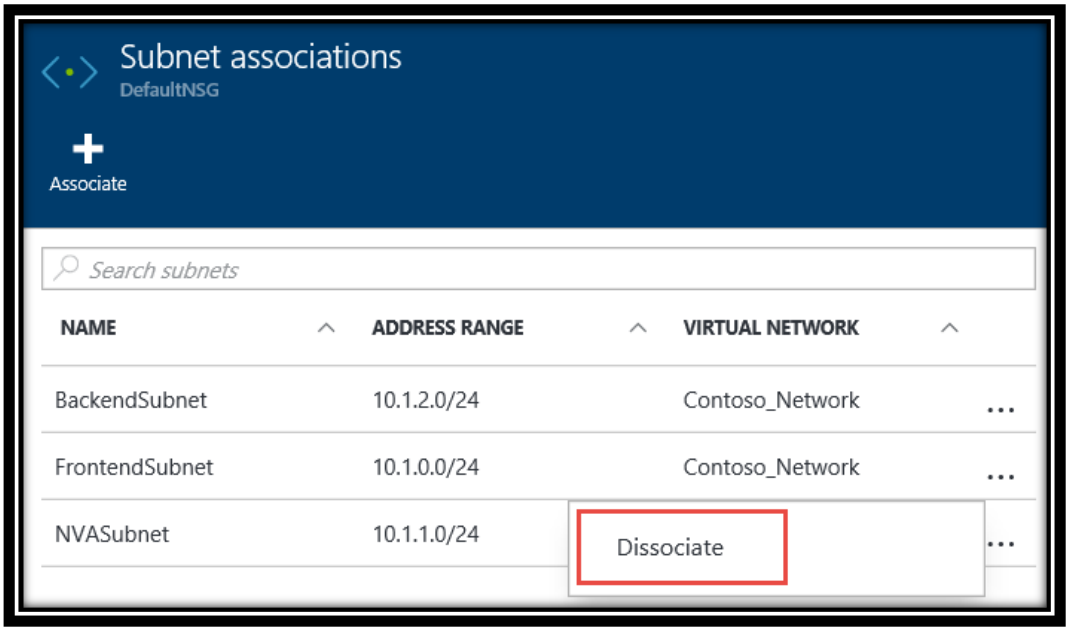


12. In the **Settings** blade of the **DefaultNSG** network security group, click **Subnets**.

©2016 Microsoft Corporation

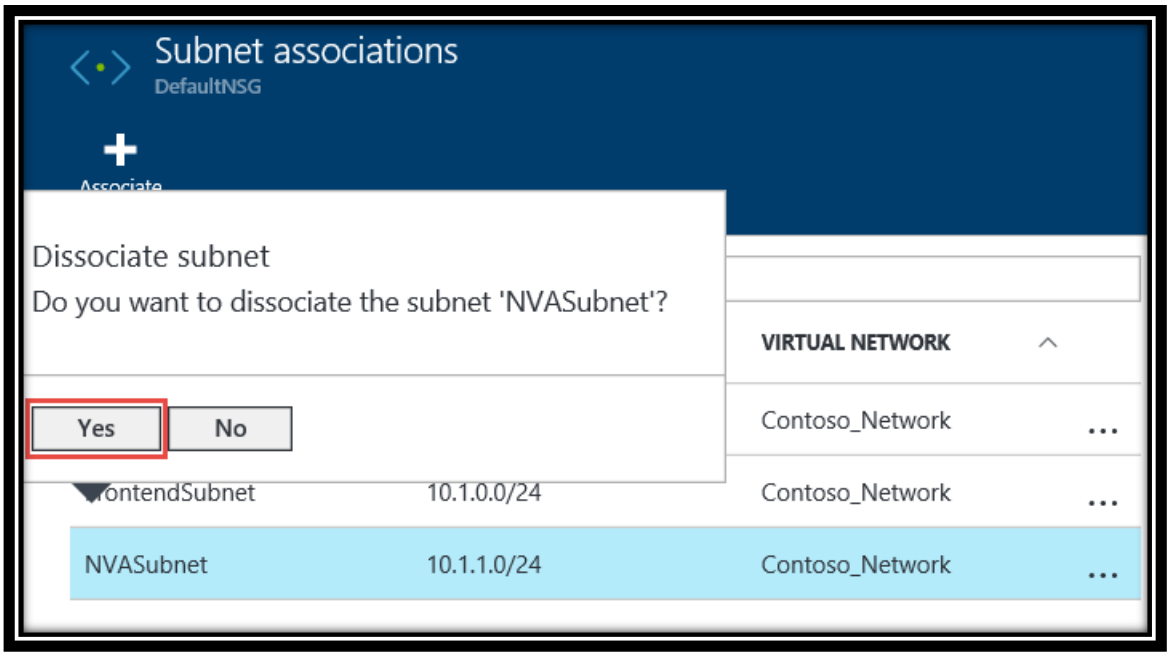


13. In the **Subnet associations** blade, click **ellipsis (...)** in the **NVASubnet** row and click **Dissociate**.

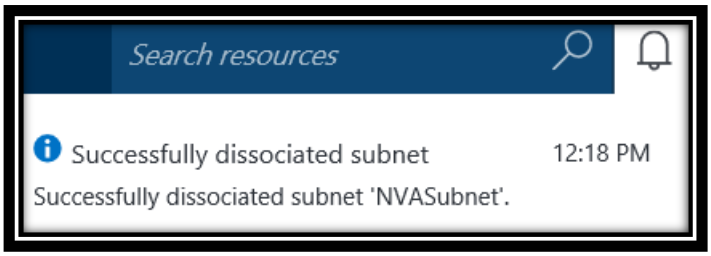


©2016 Microsoft Corporation

14. Confirm when prompted



15. Wait until the action is completed.

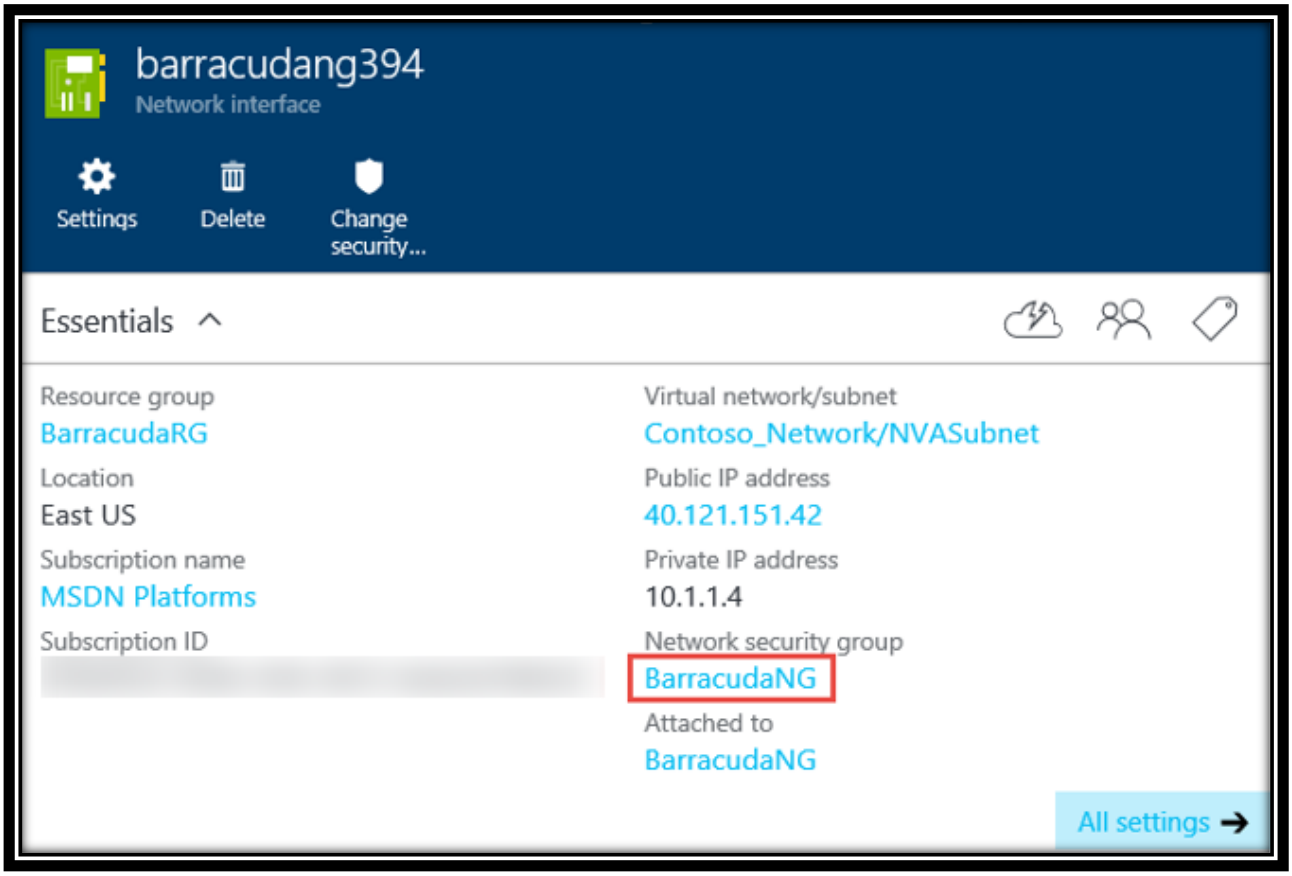


Exercise 6: Configure firewall component of the Barracuda NG virtual appliance

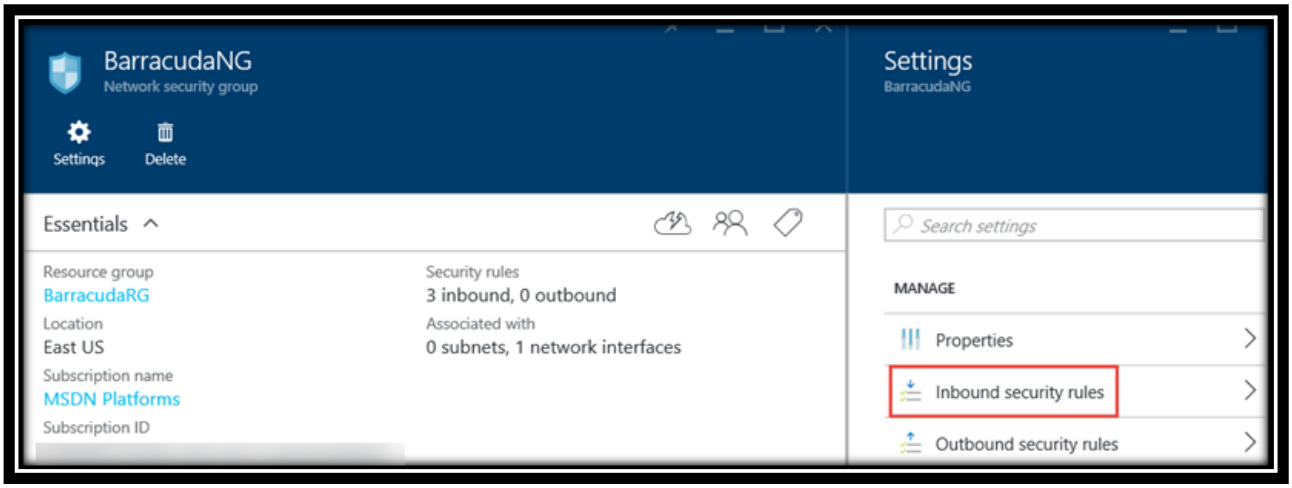
In this exercise, you will connect to the Barracuda NG virtual appliance by using the Barracuda NG Admin utility and modify firewall configuration to allow communication from **DemoVM0** to **DemoVM2**.

1. In the blade of the network interface of the virtual machine hosting the Barracuda virtual appliance (**barracuda394** in our case), click the **BarracudaNG** link under the **Network security group** label.

©2016 Microsoft Corporation

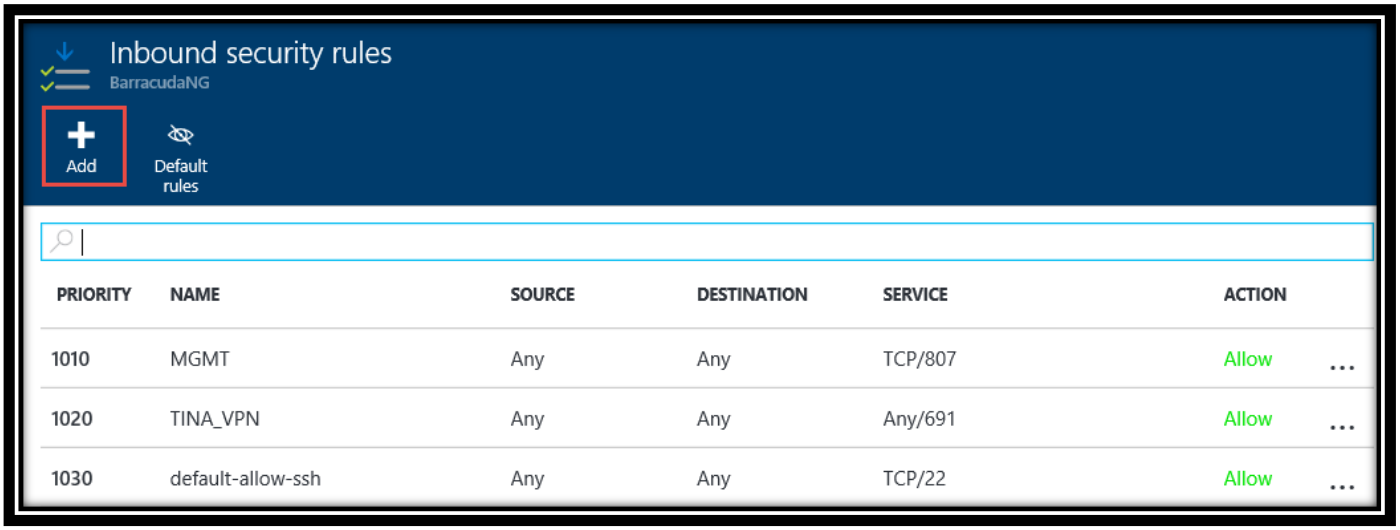


2. In the **Settings** blade of the **BarracudaNG** network security group, click **Inbound security rules**.



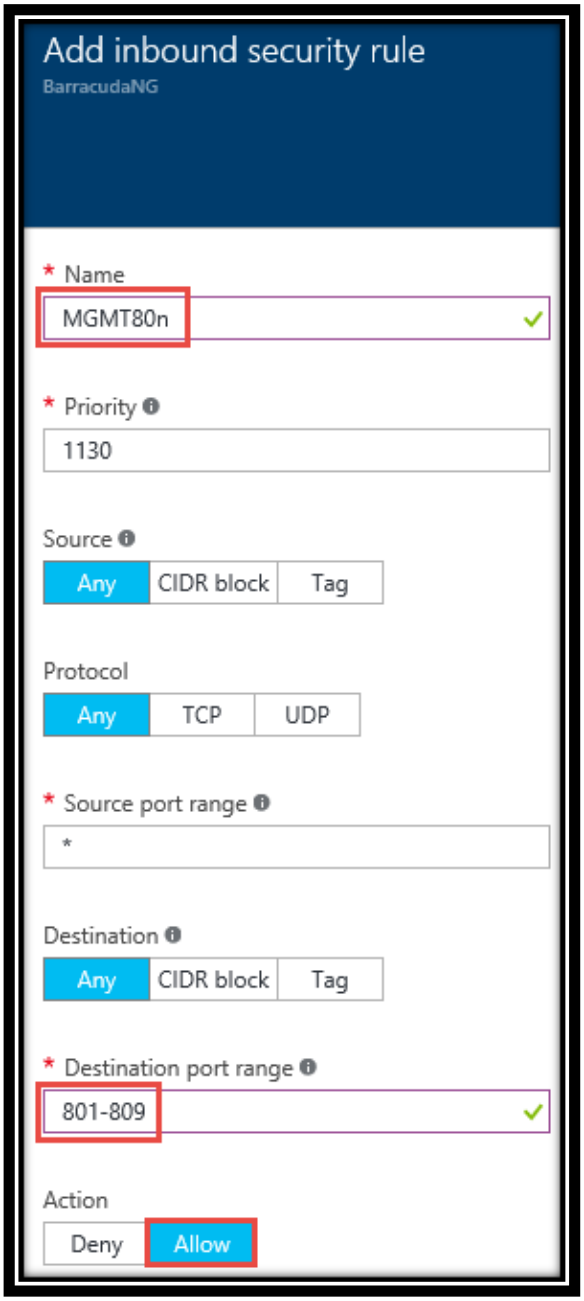
3. In the **Inbound security rules** blade, click **Add**.

©2016 Microsoft Corporation



4. In the **Add inbound security rule** blade, specify the following and click **OK**:
    - Name: *any unique name*
    - Priority: *accept the default (as long as it is unique)*
    - Source: **Any**
    - Protocol: **Any**
    - Source port range: *****
    - Destination: **Any**
    - Destination port range: **801-809**
    - Action: **Allow**

©2016 Microsoft Corporation

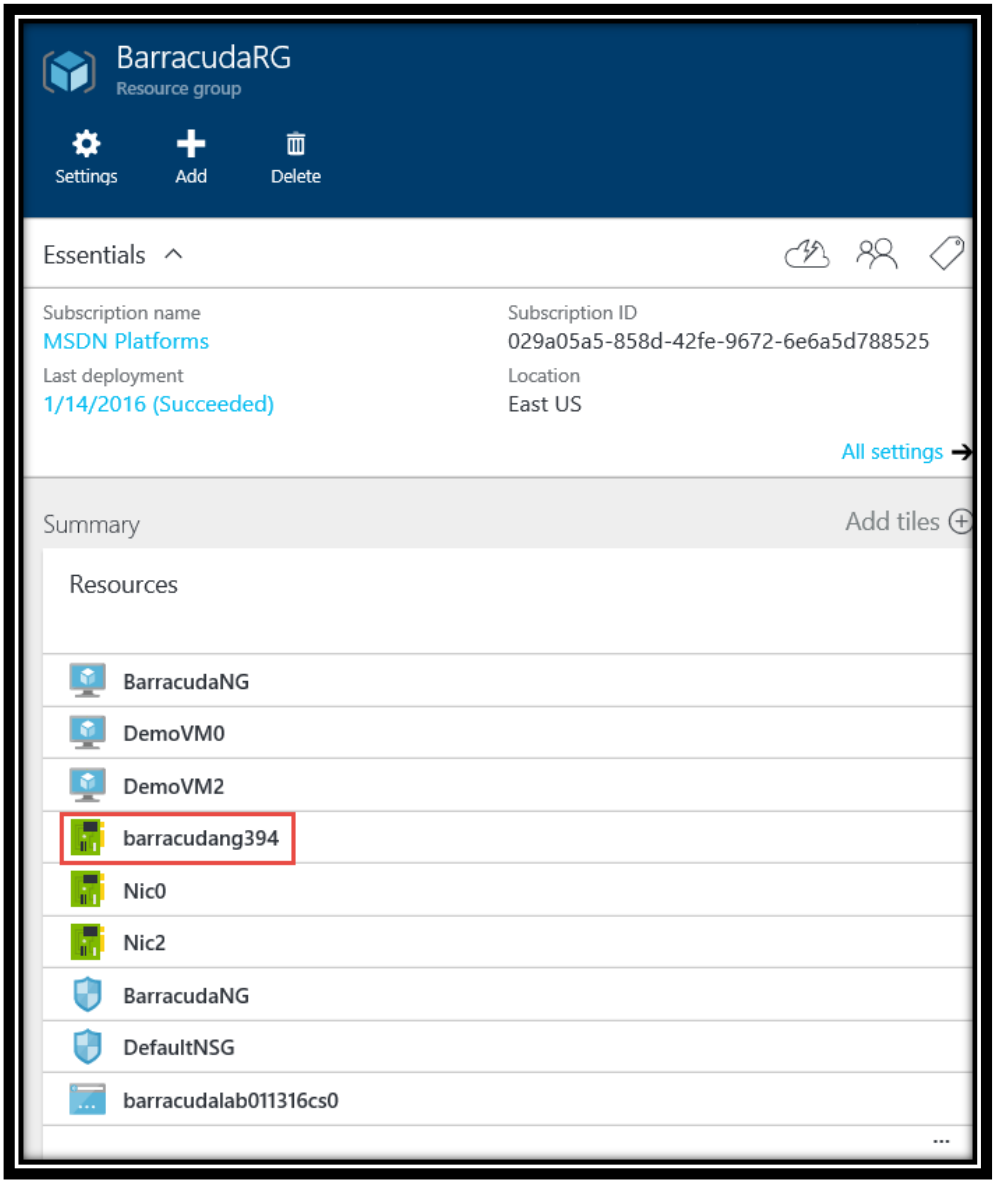


5. Verify that the rule has been successfully created.

©2016 Microsoft Corporation

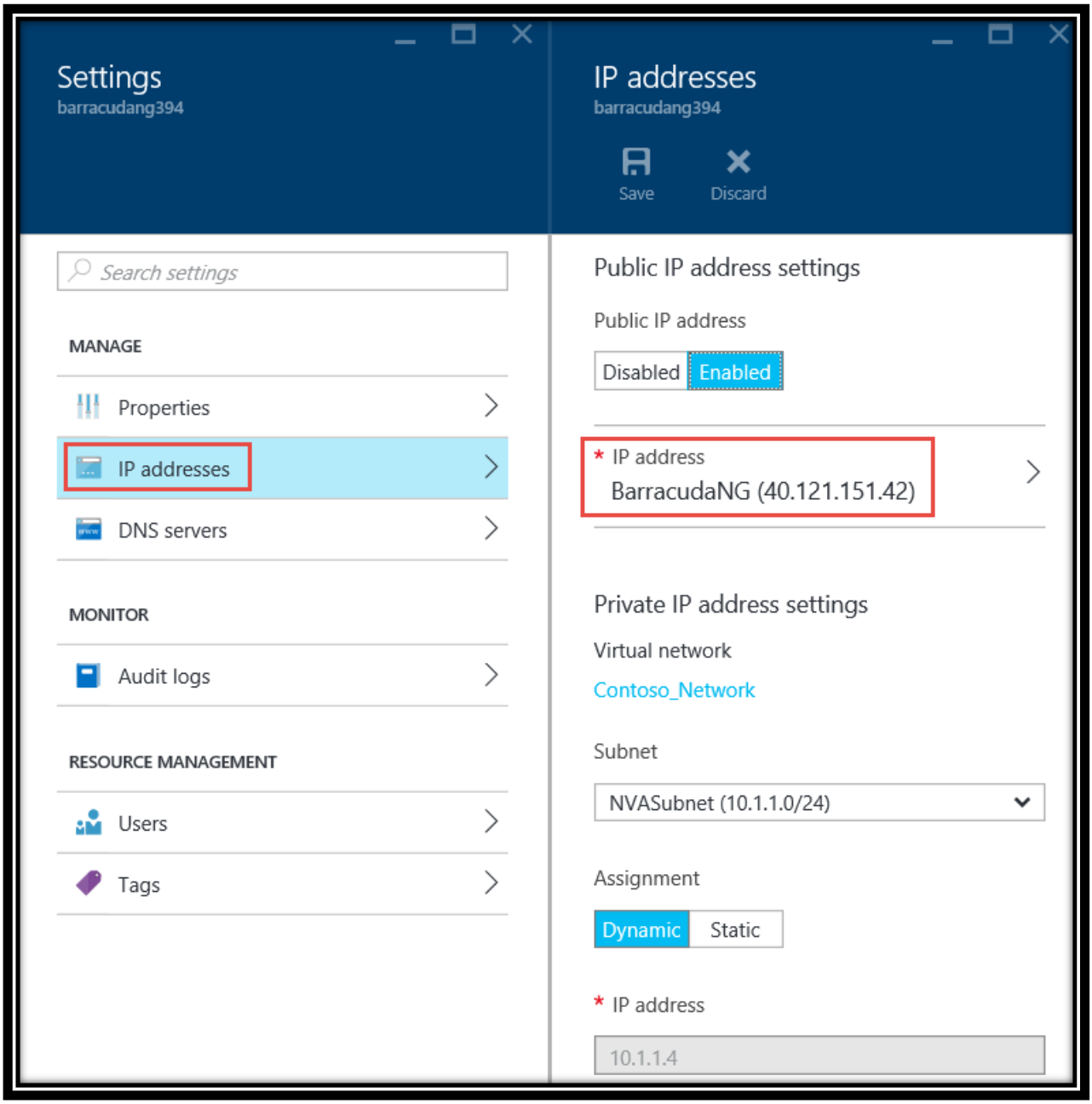
6. In order to identify the public IP address assigned to the network interface of the virtual machine hosting the Barracuda NG virtual appliance, navigate back to the **BarracudaRG** resource group.

7. In the **BarracudaRG** blade, click the entry representing the network interface associated with the **BarracudaNG** virtual machine (starting with the **barracuda** prefix).



©2016 Microsoft Corporation

8. In the network interface blade (**barracuda394** in our case), take a note of its Public IP address entry.

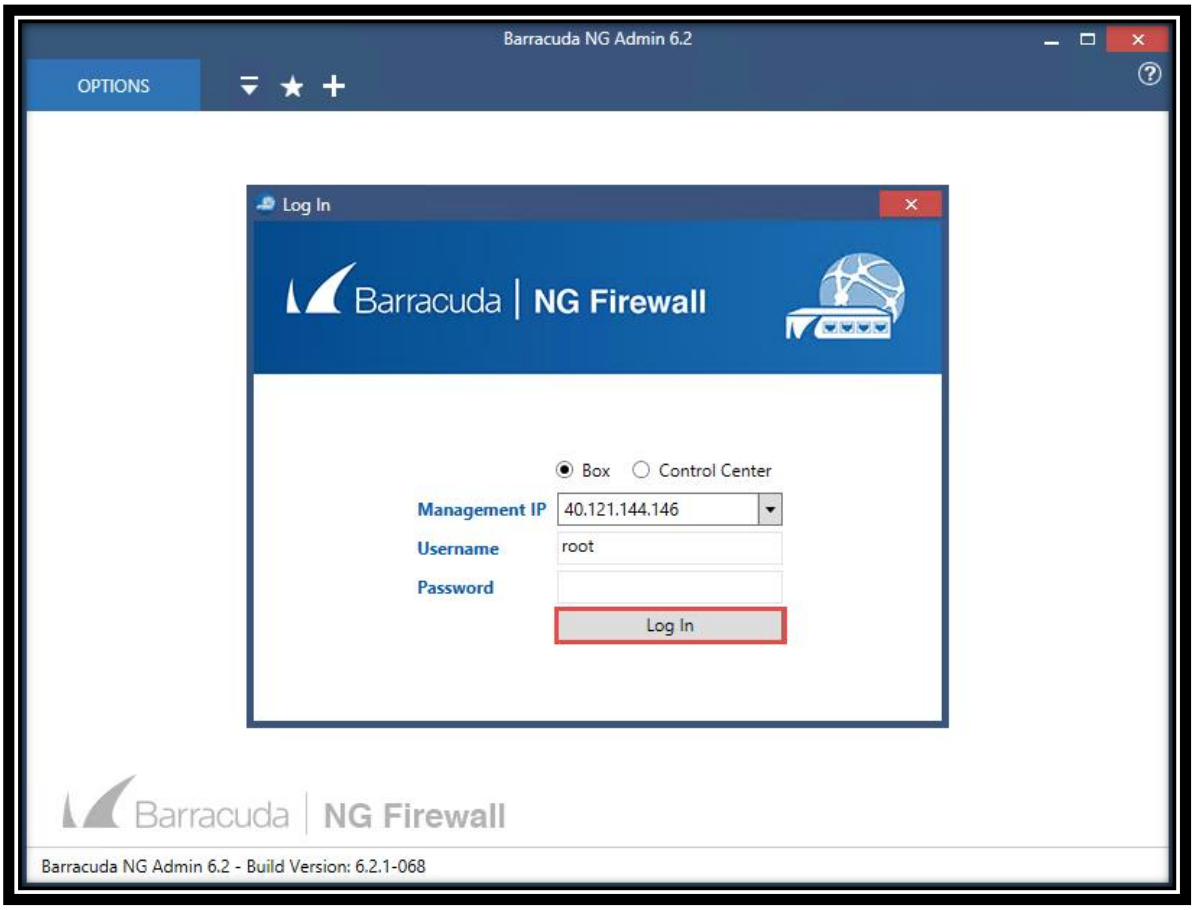


9. On your client machine launch the **ngadmin_6-2-1-068.exe** utility downloaded from https://copy.com/fG2FIvyHptjy9g7n

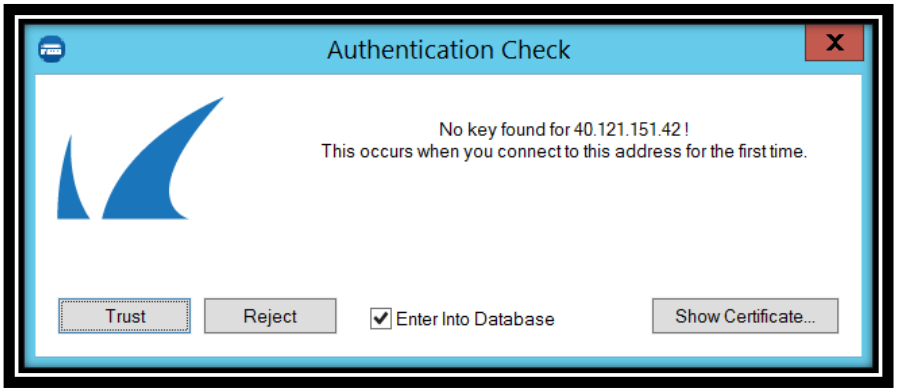
10. In the **Log in** dialog box of the **Barracuda NG Admin 6.2** utility, specify the following and click **Log in**:

©2016 Microsoft Corporation

- Management IP: *address you identified at the beginning of this exercise*
- Username: **root** *(note that this is **not** the username you specified when deploying the appliance from Azure Portal)*
- Password: **demo@pass1**

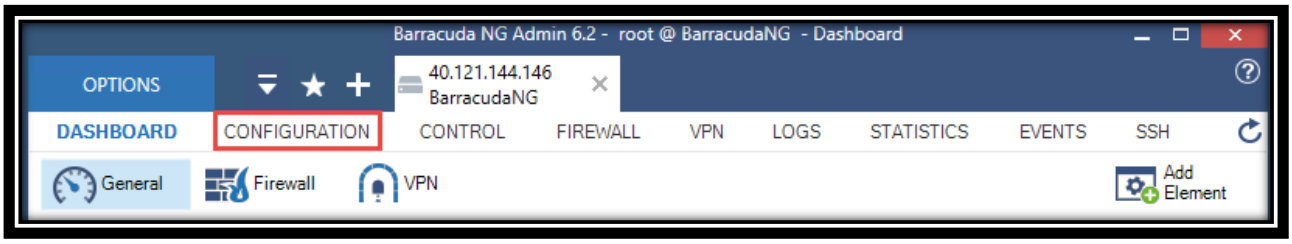


11. When prompted, in the **Authentication Check** dialog box, click **Trust**.

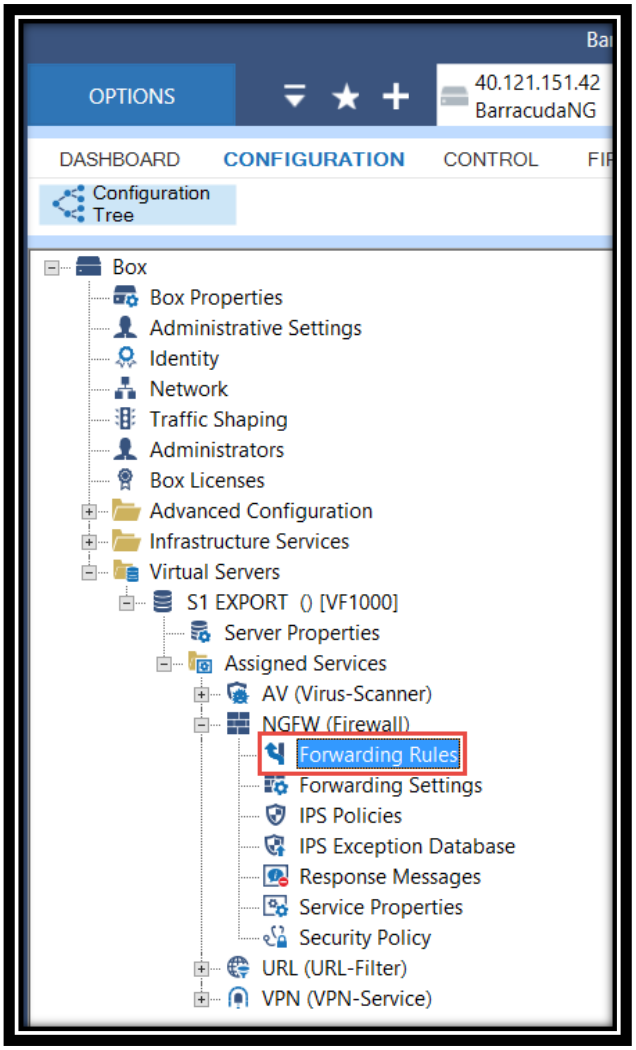


©2016 Microsoft Corporation

12. Once successfully connected, in the **Barracuda NG Admin 6.2** console, click **CONFIGURATION**.

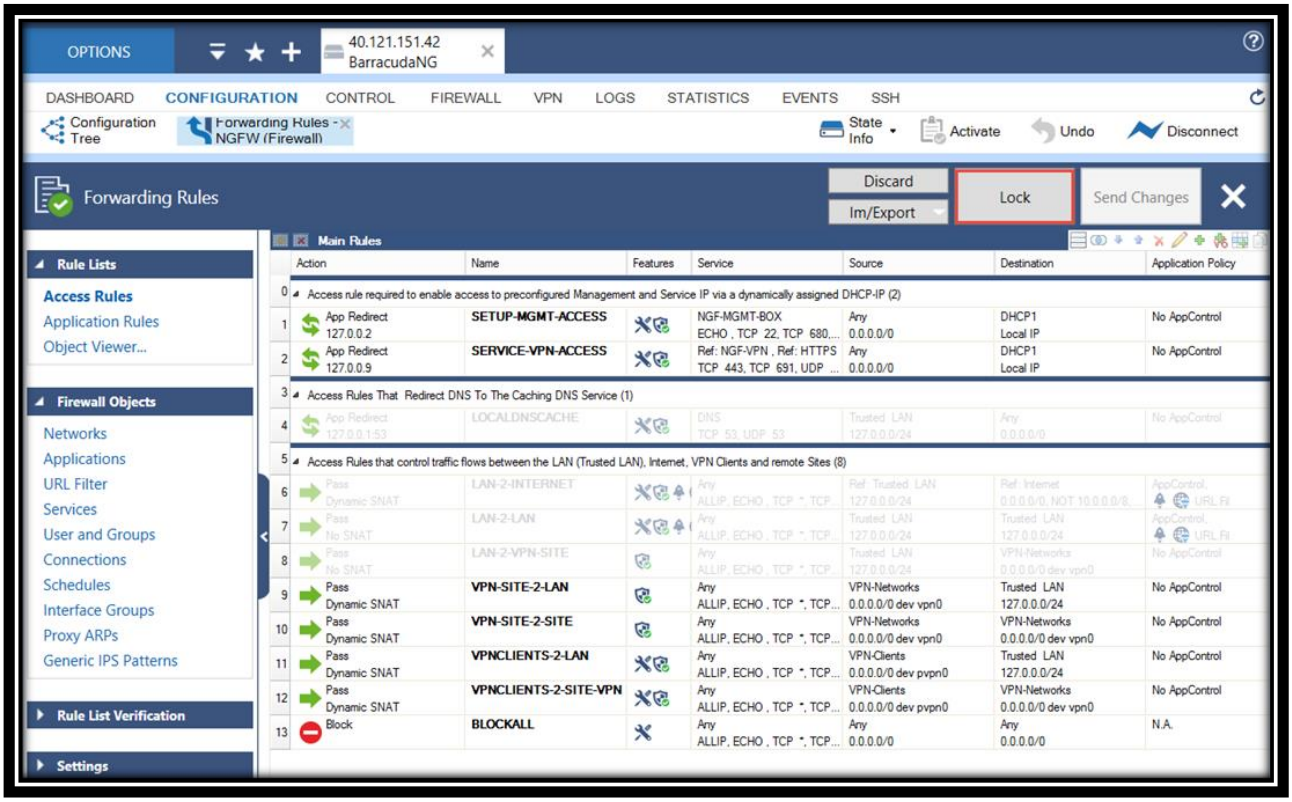


13. In the **Configuration Tree,** expand the **Virtual Servers → S1 Export () [VF1000] → Assigned Services → NGFW (Firewall)** and double-click **Forwarding Rules**.

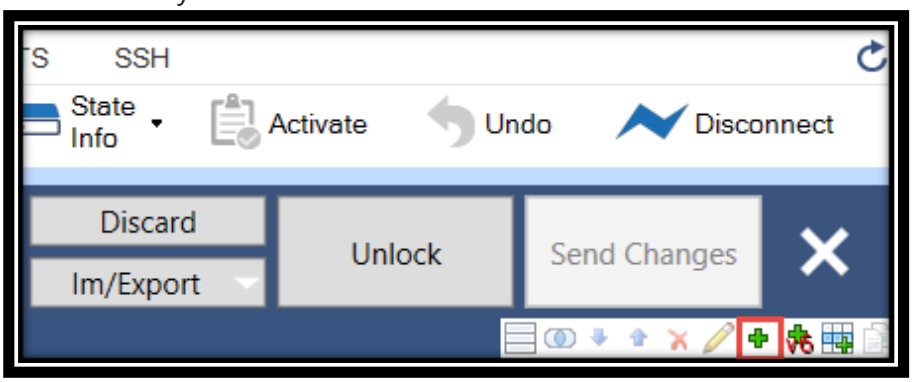


14. In the **Forwarding Rules** window, click **Lock** in the upper right corner (the label will change to **Unlock**):

©2016 Microsoft Corporation

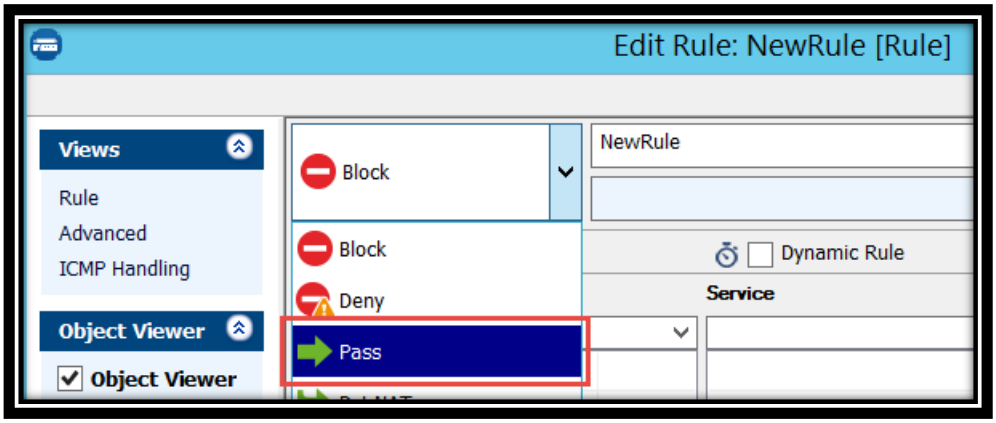


15. In the **Forwarding Rules** window, click the plus sign (**Insert rule**) in the toolbar directly underneath:

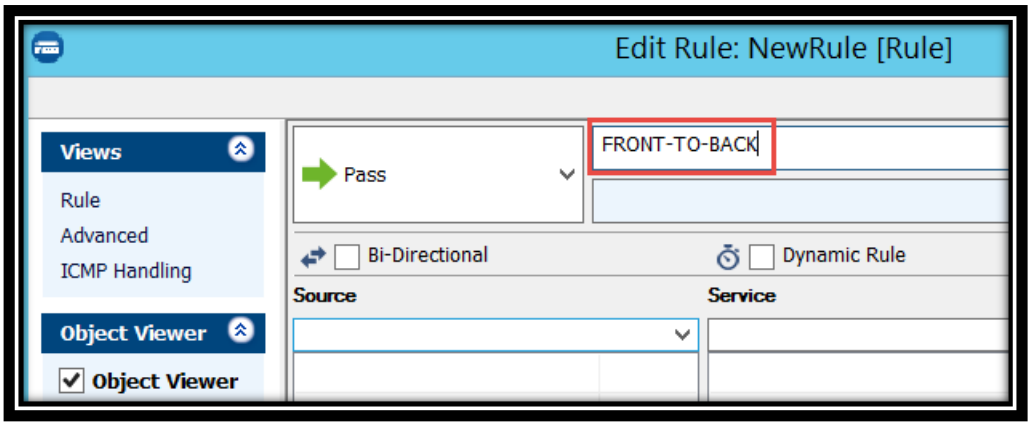


16. In the **Edit Rule: New Rule** dialog box, change **Block** to **Pass**.

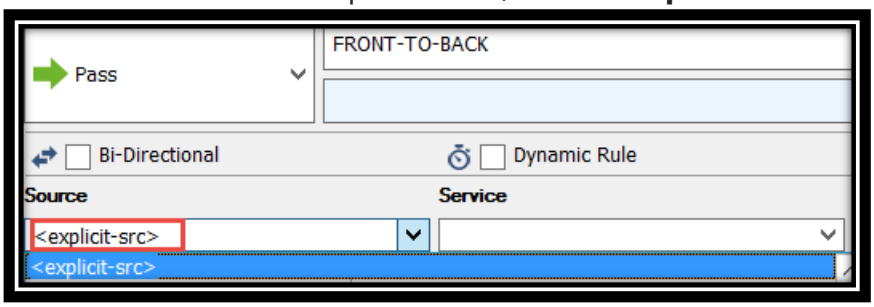
©2016 Microsoft Corporation



17. Replace **NewRule** entry at the top of the dialog box with a more descriptive name (we will use **FRONT-TO-BACK**).

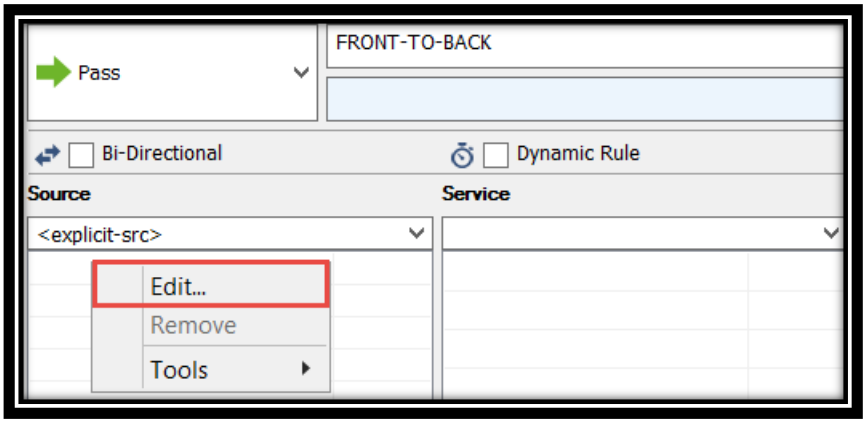


18. In the **Source** drop down list, select **<explicit-src>**

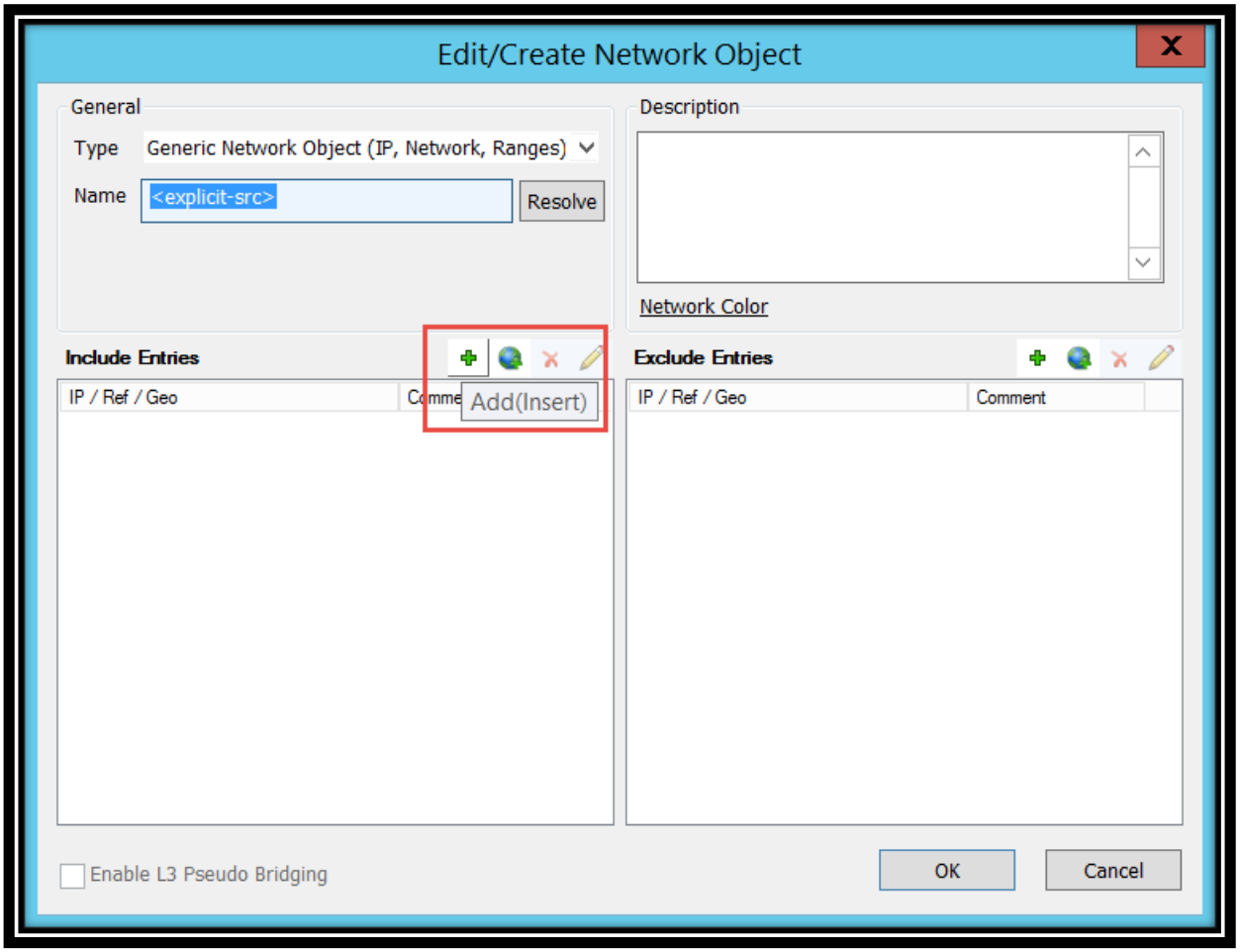


19. Right-click the empty grid in the **Source** section and select **Edit** from the context-sensitive menu

©2016 Microsoft Corporation

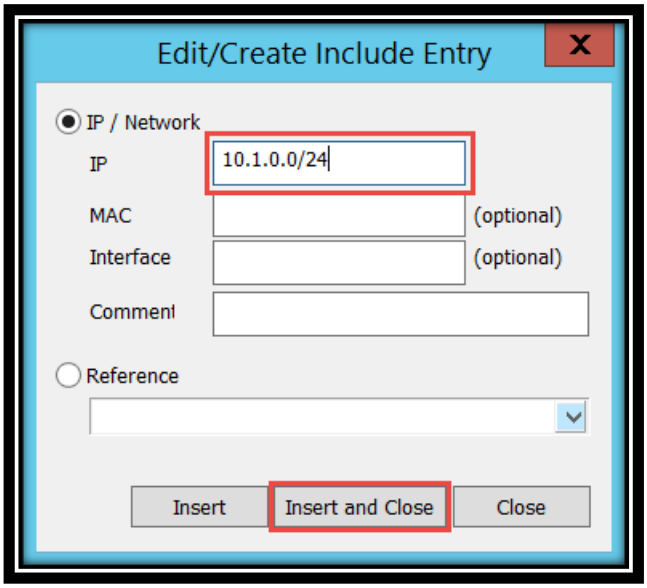


20. In the **Edit/Create Network Object**, click the plus sign (**Add**) in the toolbar.

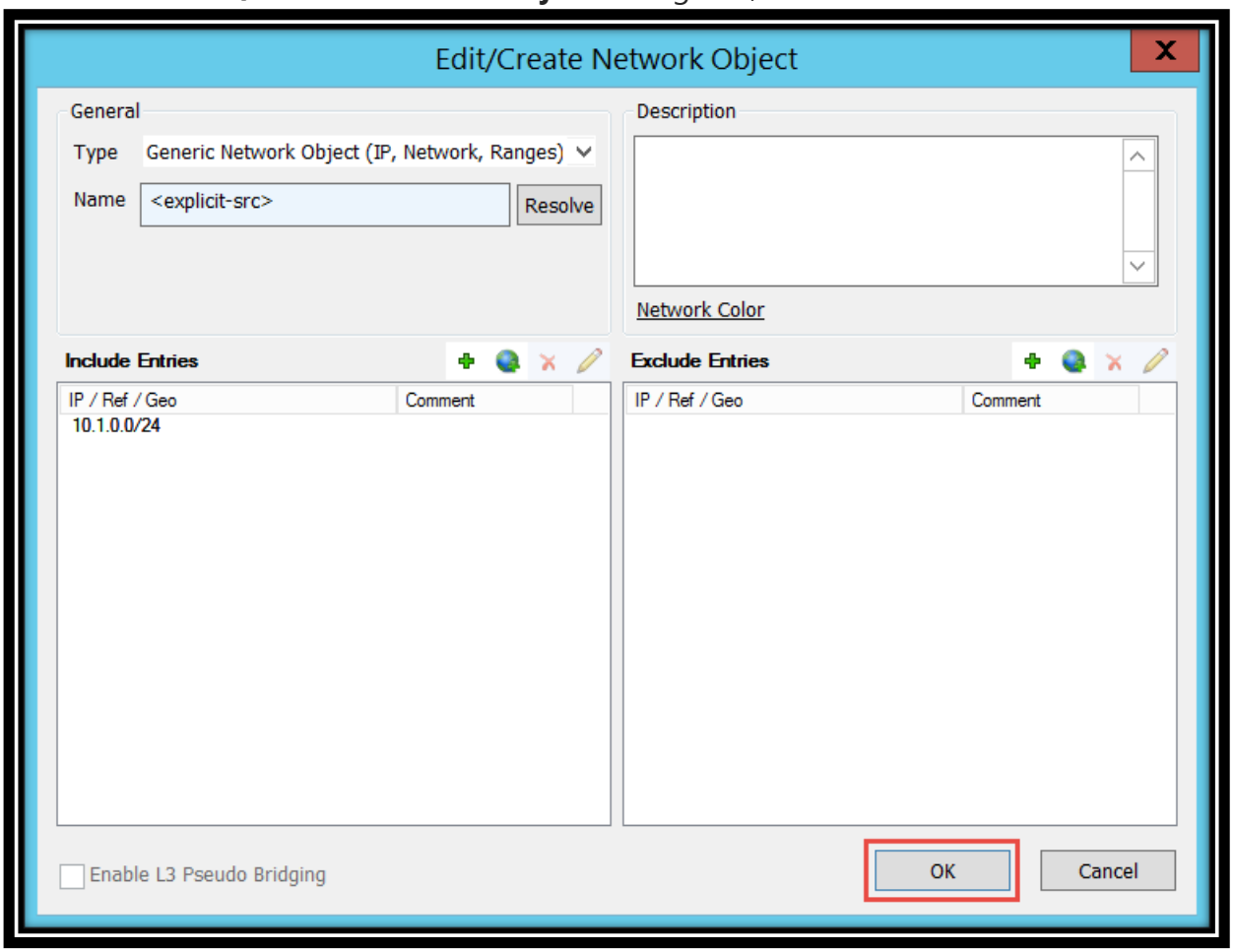


21. In the **Edit/Create Include Entry**, in the **IP** textbox, type **10.1.0.0/24** (representing the front-end subnet) and click **Insert and Close**.

©2016 Microsoft Corporation

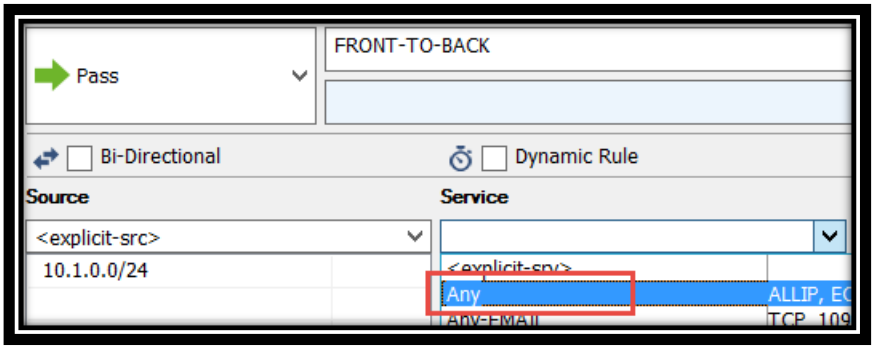


22. In the **Edit/Create Network Object** dialog box, click **OK**.

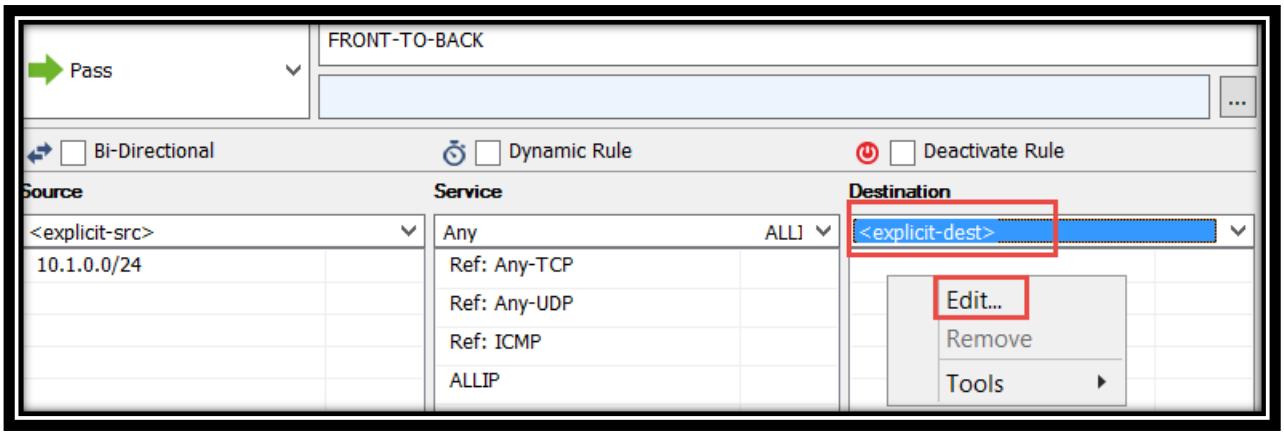


©2016 Microsoft Corporation

23. In the **Service** drop-down list, select **Any**.

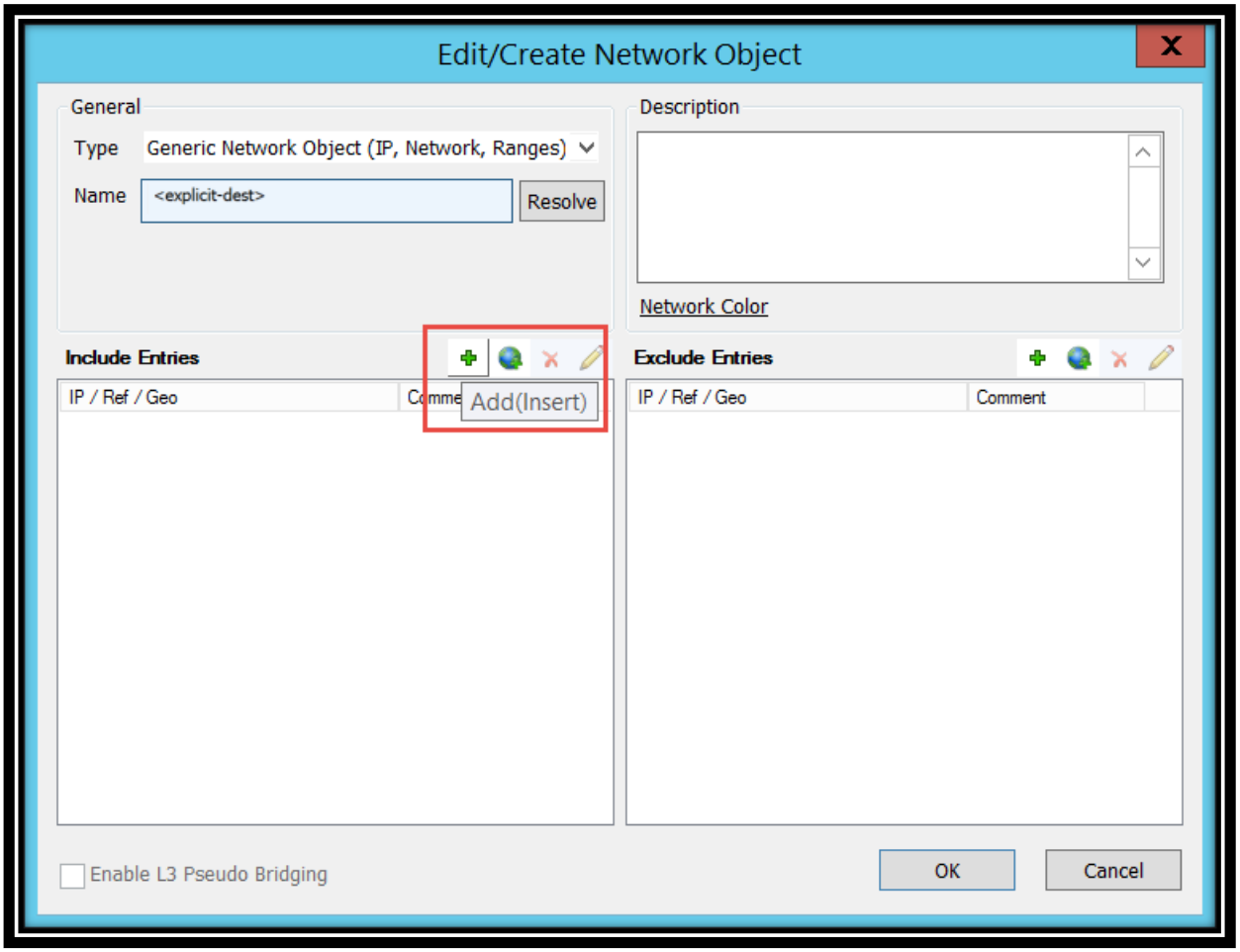


24. In the **Destination** drop-down list, select **<explicit-dest>**, right-click the empty grid in the **Source** section and select **Edit** from the context-sensitive menu

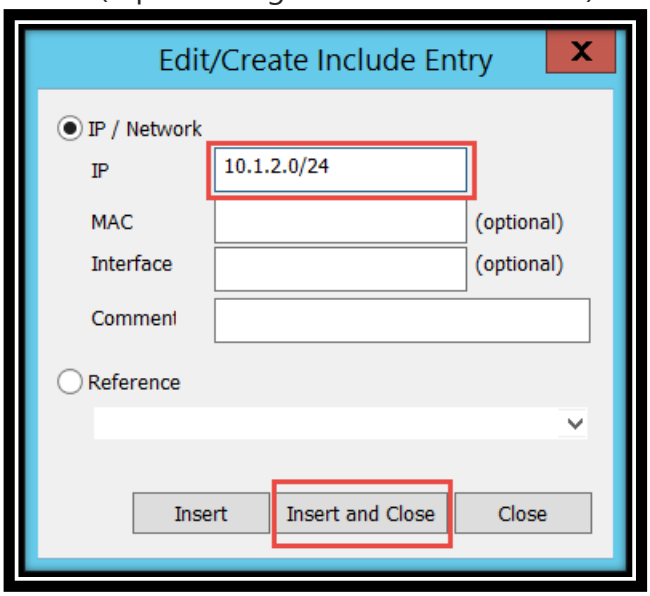


25. In the **Edit/Create Network Object**, click the plus sign (**Add**) in the toolbar.

©2016 Microsoft Corporation

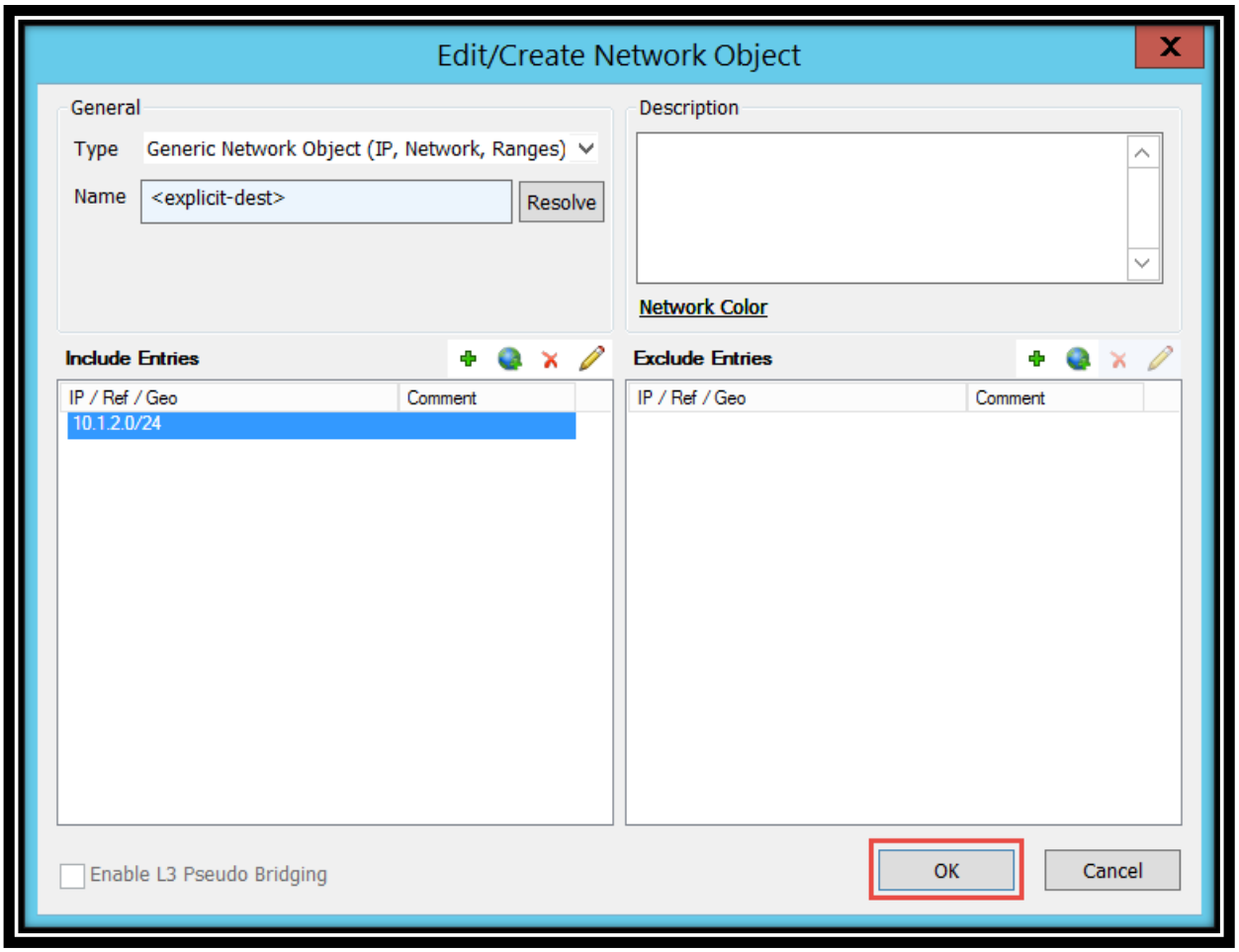


26. In the **Edit/Create Include Entry**, in the **IP** textbox, type **10.1.2.0/24** (representing the back-end subnet) and click **Insert and Close**.



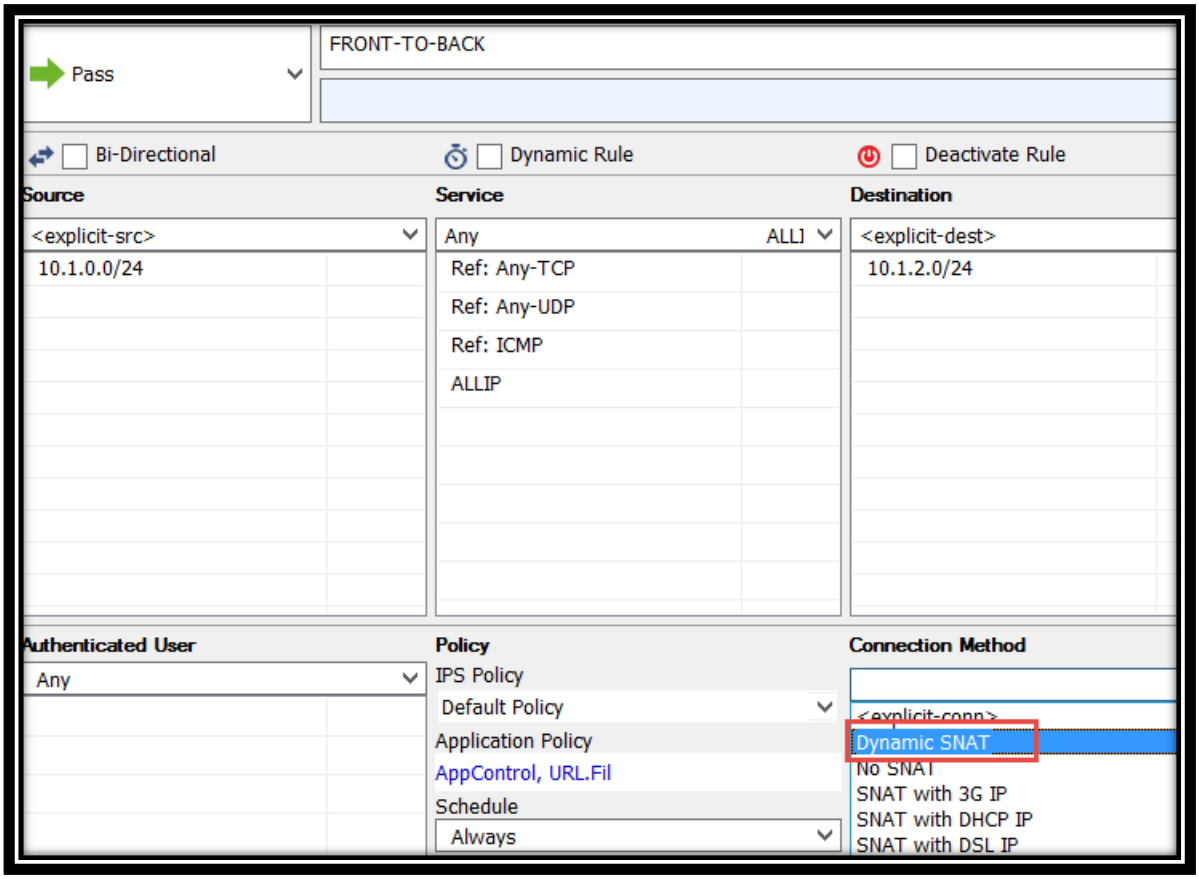
©2016 Microsoft Corporation

27. In the **Edit/Create Network Object** dialog box, click **OK**.



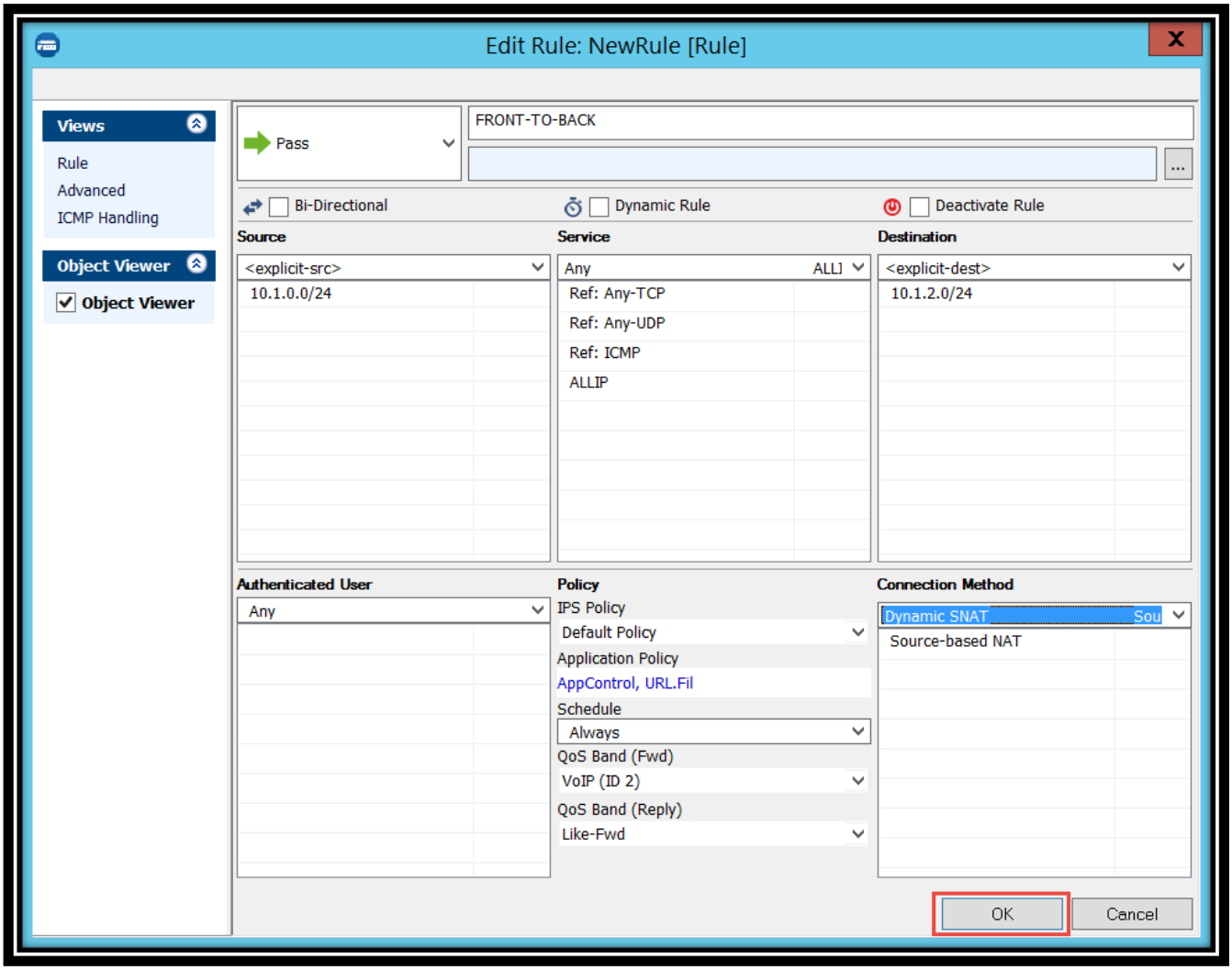
28. In the **Connection Method** drop-down list, select **Dynamic SNAT**

©2016 Microsoft Corporation



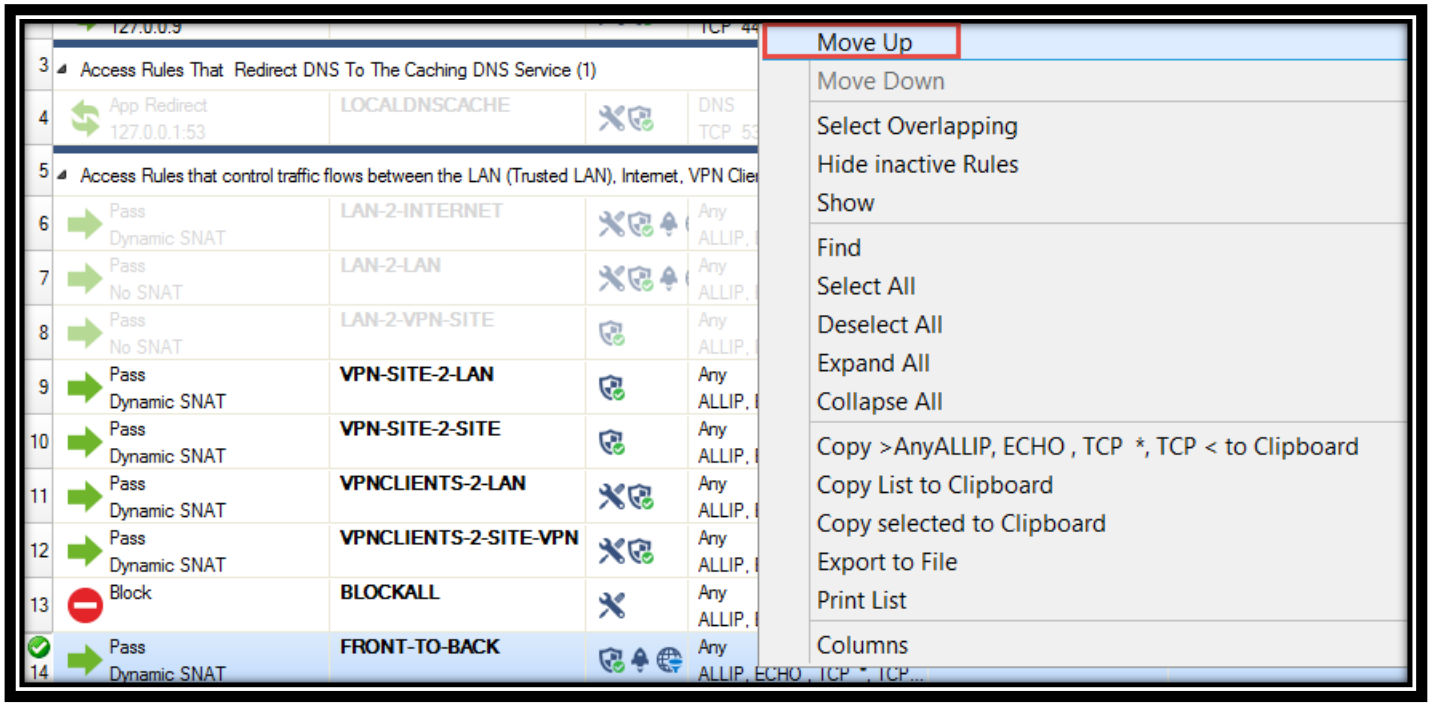
29. In the **Edit Rule: NewRule [Rule]** dialog box, click **OK**.

©2016 Microsoft Corporation

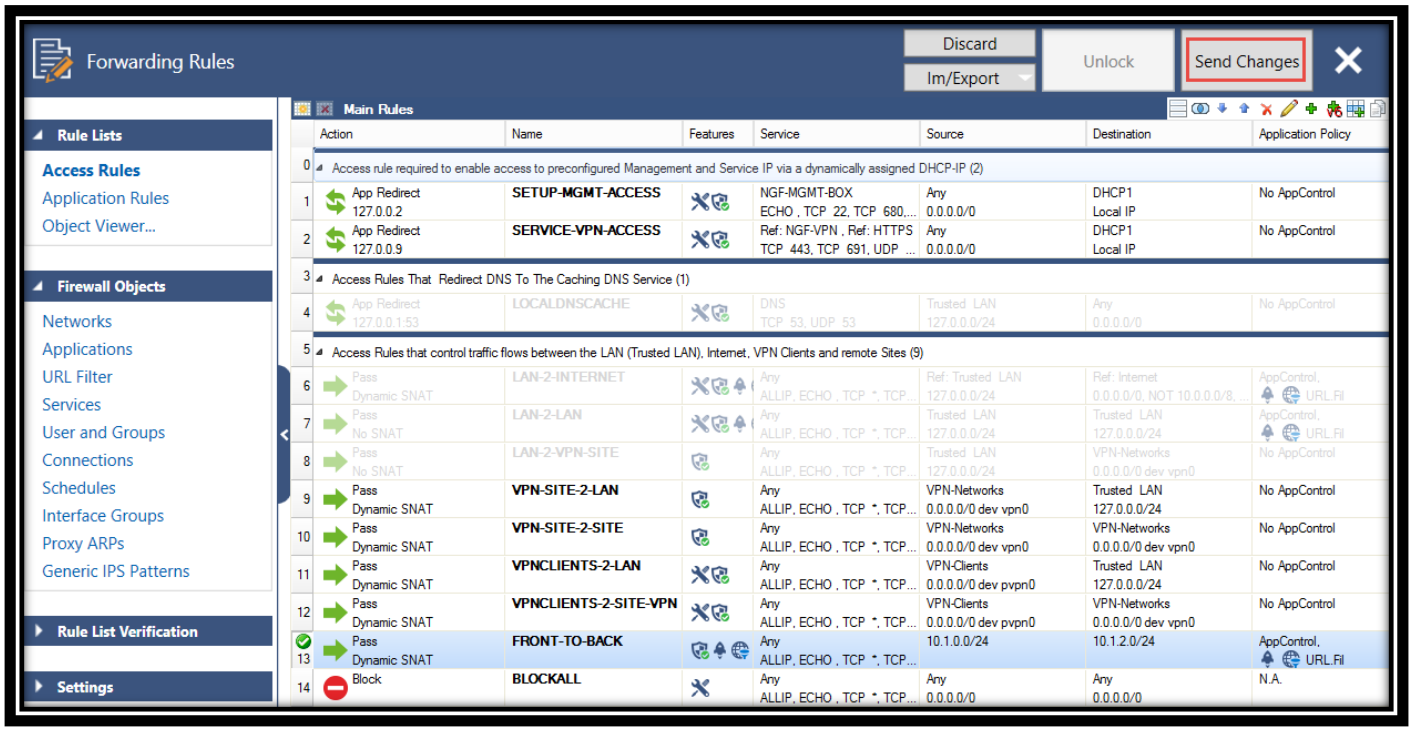


30. By default, the new rule will appear below the **BLOCKALL** rule. In order for it to take effect, you need to right click on the main area of the **Forwarding Rules** pane and select **Move Up** from the context-sensitive menu.

©2016 Microsoft Corporation



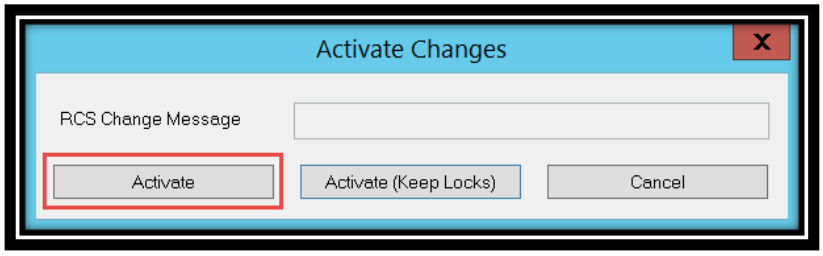
31. In the **Forwarding Rules** pane, click **Send Changes** button in the upper right corner.



32. Click **Activation Pending.**

©2016 Microsoft Corporation

33. In the **Activate Changes** dialog box, click **Activate**.

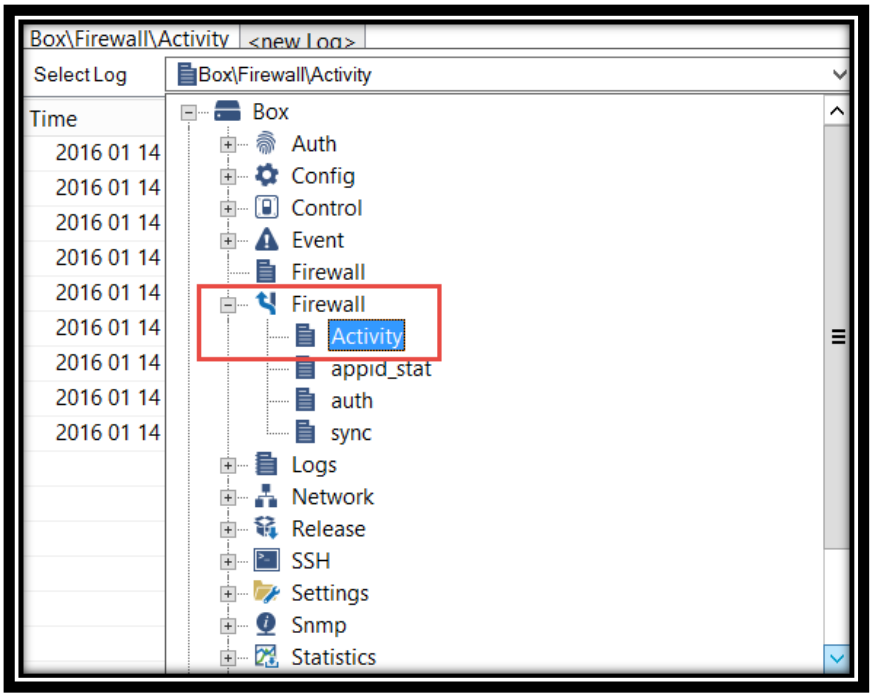


Validate Lab Completion

In this task, you will create a Remote Desktop Connection from **DemoVM0** to **DemoVM2** through the Barracuda appliance and capture the Log Files containing entries representing a successful RDP session as proof you completed this lab.

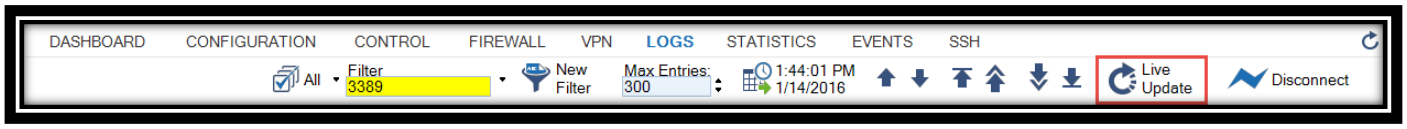
Please save your lab screenshots as either a .jpeg or .png. Upload your screenshots in one .zip file here.

1. In the **Barracuda NG Admin 6.2** interface, click **LOGS**, and, in the **Select Log File** select **Box\Firewall\Activity**.

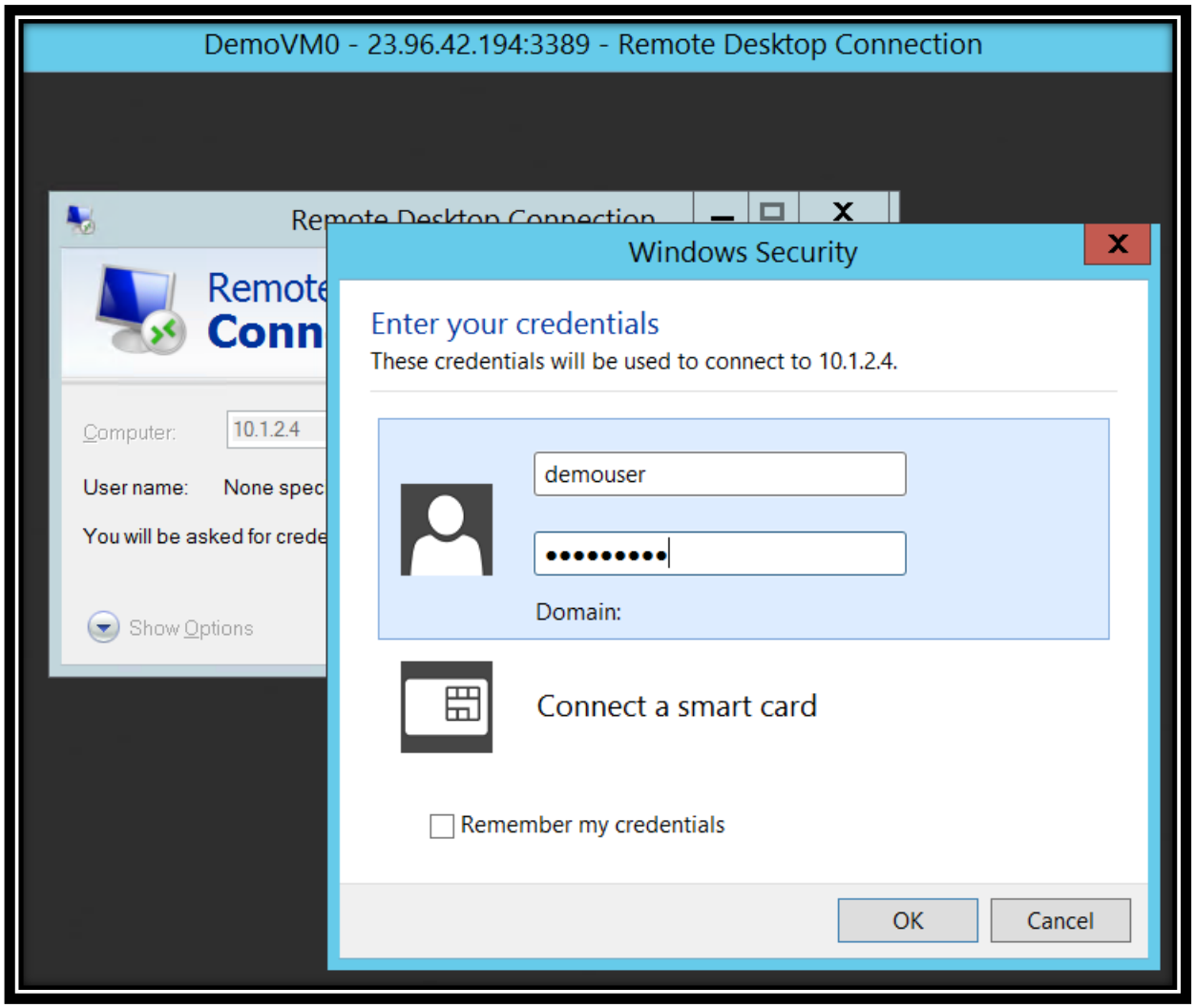


©2016 Microsoft Corporation

2. In the toolbar of the **LOGS** window, in the **Filter** text box, type in **3389** and click **Live Update**.

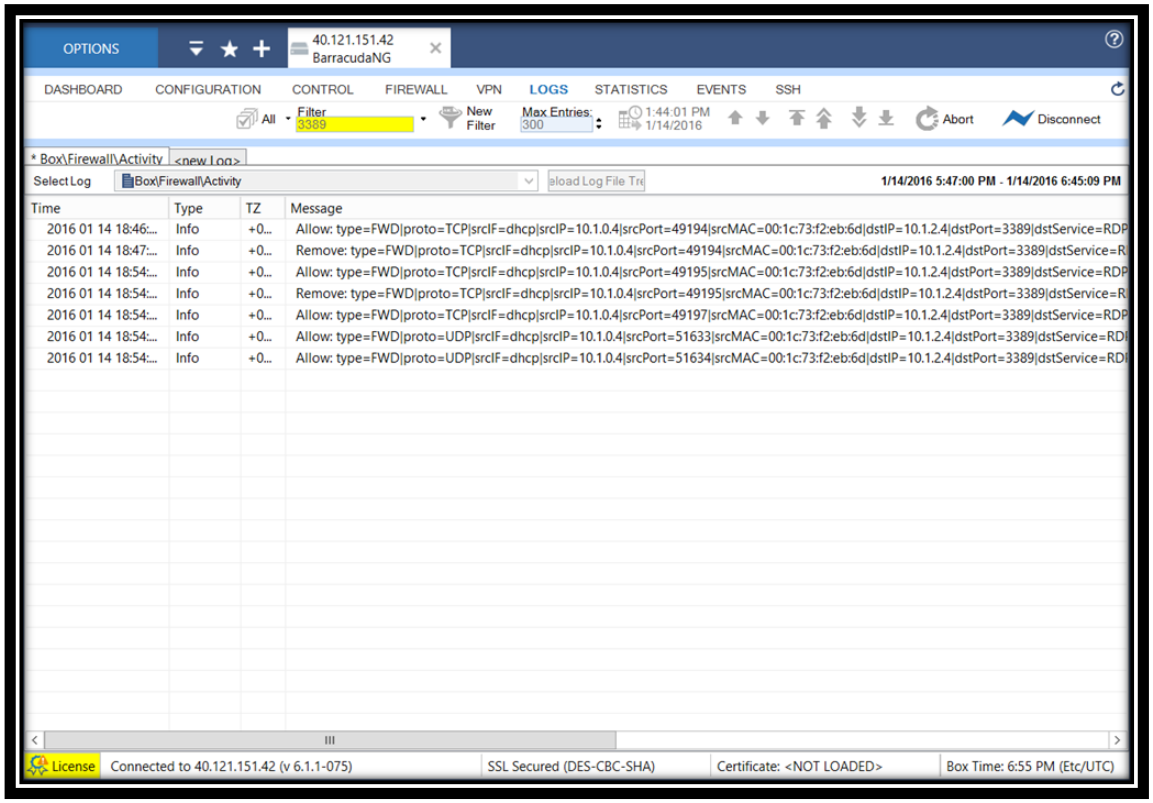


3. Next, switch back to the Remote Desktop session to **DemoVM0** you established earlier from your lab computer and, from it, initiate a new Remote Desktop session to **10.1.2.4** (the private IP address of **DemoVM2**).



4. Switch back to the **Barracuda NG Admin 6.2 interface,** and you should see entries representing the new RDP session in the firewall log.

©2016 Microsoft Corporation



5. Take a screen capture of this connection as proof that you have completed the Barracuda Lab.

Lab Summary

In this lab, you started by deploying an Azure Resource Manager template that consisted of three Windows Server 2012 R2 virtual machines, each of them residing on a separate subnet within the same virtual network. The deployment implemented User Defined Route and IP forwarding, enforcing routing of the traffic originating from the first virtual machine and destined for the third virtual machine via the second one. Next, you replaced the second virtual machine with a virtual machine hosting Barracuda NextGen Firewall F-Series virtual appliance from Azure Marketplace. By modifying existing network security groups, configuring the network interface of the new virtual machine, and defining firewall rules of the Barracuda appliance, you allowed for a controlled traffic flow between the two remaining virtual machines.

©2016 Microsoft Corporation