

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

Working with Barracuda F-Series Firewall.....	1
on Microsoft Azure.....	1
Overview.....	2
Exercise 1: Login to the Microsoft Azure Portal.....	3
Exercise 2: Deploy an Azure Resource Manager Template.....	4
Exercise 3: Review networking configuration of the new deployment.....	7
Exercise 4: Deploy Barracuda NG virtual appliance.....	17
Exercise 5: Configure Azure networking for the Barracuda NG virtual appliance.....	26
Exercise 6: Configure firewall component of the Barracuda NG virtual appliance.....	33
Validate Lab Completion.....	51
Lab Summary.....	53



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>

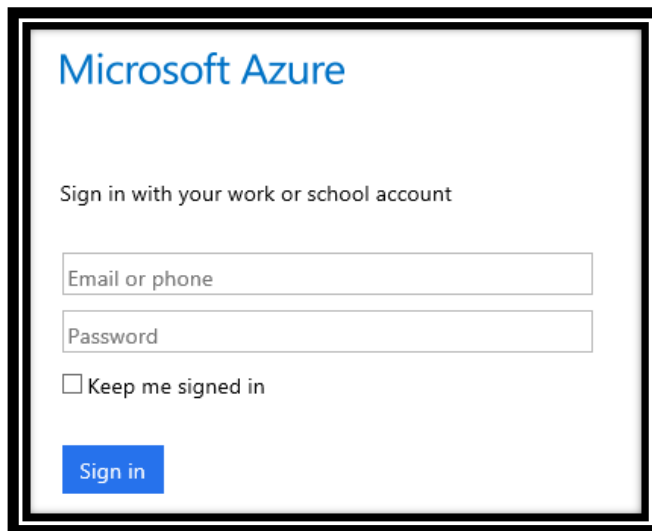
Technical Support

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

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.



Microsoft Azure

Sign in with your work or school account

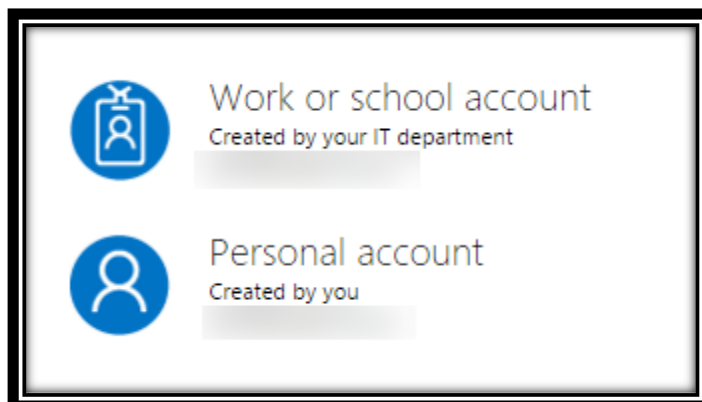
Email or phone

Password

☐ Keep me signed in

Sign in

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.



Work or school account
Created by your IT department

Personal account
Created by you

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

The screenshot shows the Azure portal interface for a custom deployment. The left pane, titled 'Custom deployment' (Deploy from a custom template), contains a sidebar with the following options: 'Template' (Edit template), 'Parameters' (Edit parameters), 'Subscription' (MSDN Platforms), 'Resource group' (Select a resource group), 'Or create new', 'Resource group location' (East US), 'Legal terms' (Review legal terms), and a 'Pin to dashboard' checkbox. The right pane, titled 'Parameters' (Customize your template parameters), displays several input fields: 'LOCATION (string)' (a dropdown menu), 'NEWSTORAGEACCOUNTNAME (string)', 'ADMINUSERNAME (string)', 'ADMINPASSWORD (securestring)', 'UNIQUEDNSPREFIXFORVM (string)', and 'VMNAMEPREFIX (string)' (set to 'Dynamic'). At the bottom of each pane are 'Create' and 'OK' buttons respectively.

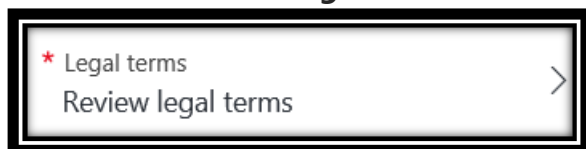
3. In the **Parameters** blade, specify the following and click **OK**:
 - LOCATION (string): *an available Azure region close to your location*
 - NEWSTORAGEACCOUNTNAME (string): *unique string consisting of 3-24 lower-case characters and digits.*
 - ADMINUSERNAME (string): **demouser**
 - ADMINPASSWORD (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.



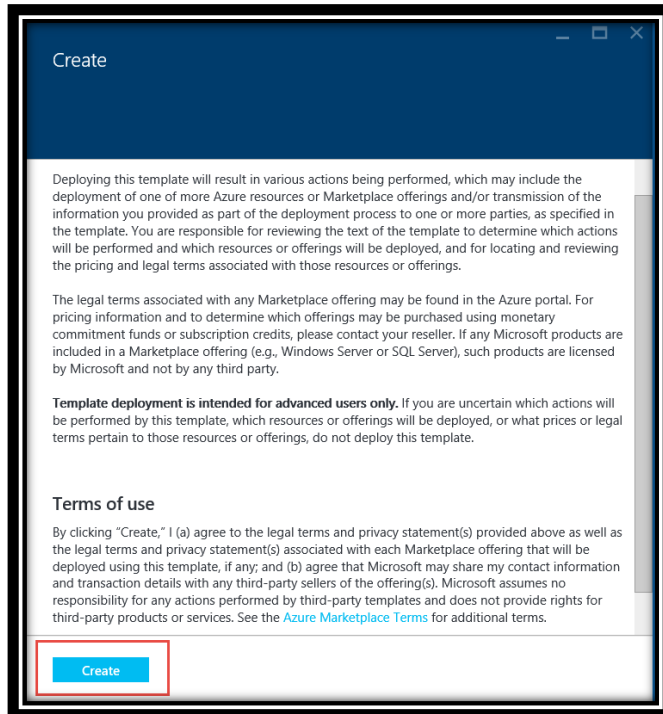
5. Type **BarracudaRG** in the textbox.



6. Click **Review legal terms**



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



Create

Deploying this template will result in various actions being performed, which may include the deployment of one or more Azure resources or Marketplace offerings and/or transmission of the information you provided as part of the deployment process to one or more parties, as specified in the template. You are responsible for reviewing the text of the template to determine which actions will be performed and which resources or offerings will be deployed, and for locating and reviewing the pricing and legal terms associated with those resources or offerings.

The legal terms associated with any Marketplace offering may be found in the Azure portal. For pricing information and to determine which offerings may be purchased using monetary commitment funds or subscription credits, please contact your reseller. If any Microsoft products are included in a Marketplace offering (e.g., Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

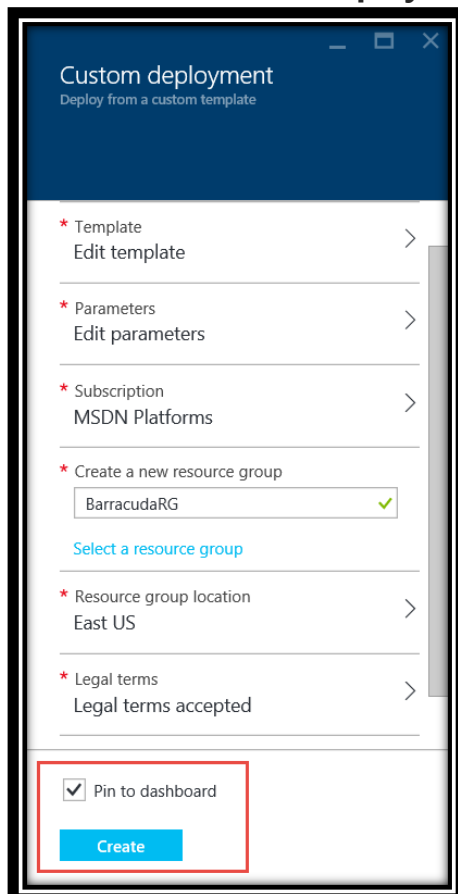
Template deployment is intended for advanced users only. If you are uncertain which actions will be performed by this template, which resources or offerings will be deployed, or what prices or legal terms pertain to those resources or offerings, do not deploy this template.

Terms of use

By clicking "Create," I (a) agree to the legal terms and privacy statement(s) provided above as well as the legal terms and privacy statement(s) associated with each Marketplace offering that will be deployed using this template, if any; and (b) agree that Microsoft may share my contact information and transaction details with any third-party sellers of the offering(s). Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

Create

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



Custom deployment
Deploy from a custom template

- * Template
Edit template
- * Parameters
Edit parameters
- * Subscription
MSDN Platforms
- * Create a new resource group
BarracudaRG ✓
[Select a resource group](#)
- * Resource group location
East US
- * Legal terms
Legal terms accepted

☒ Pin to dashboard

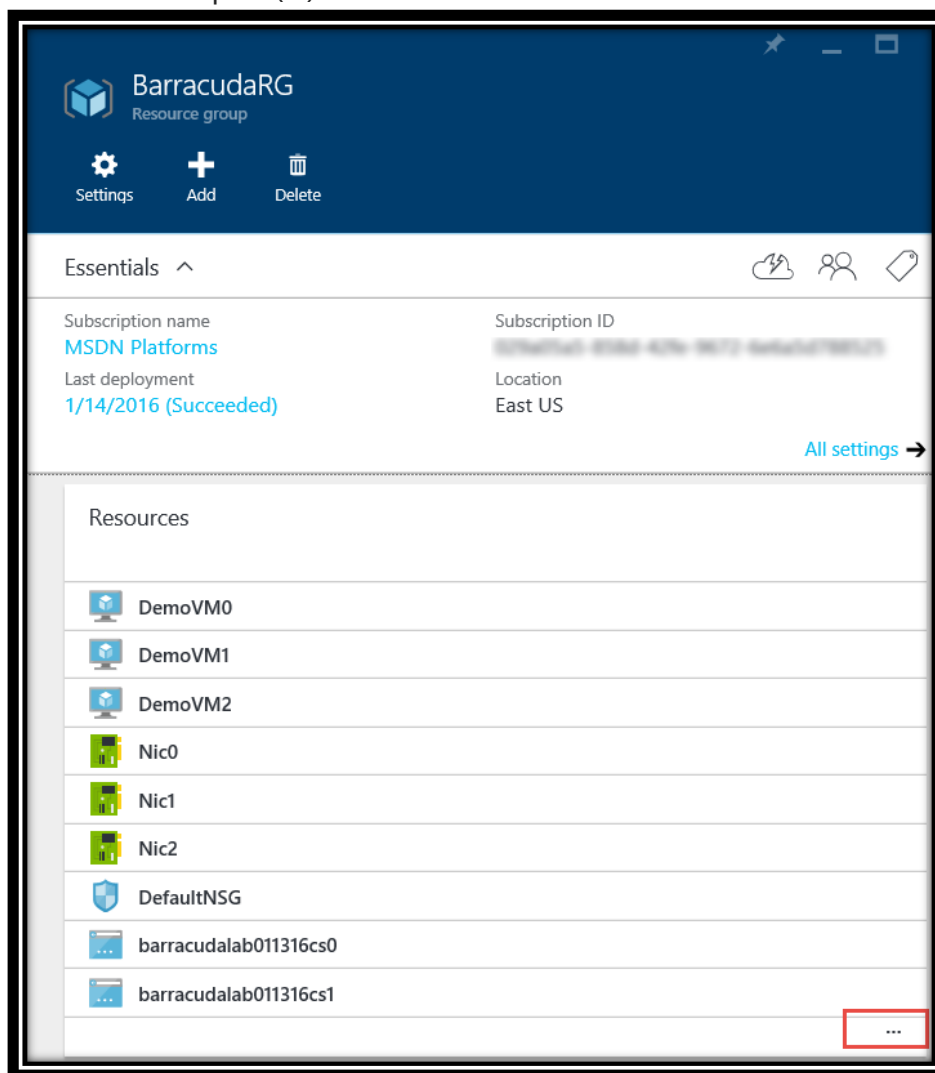
Create

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

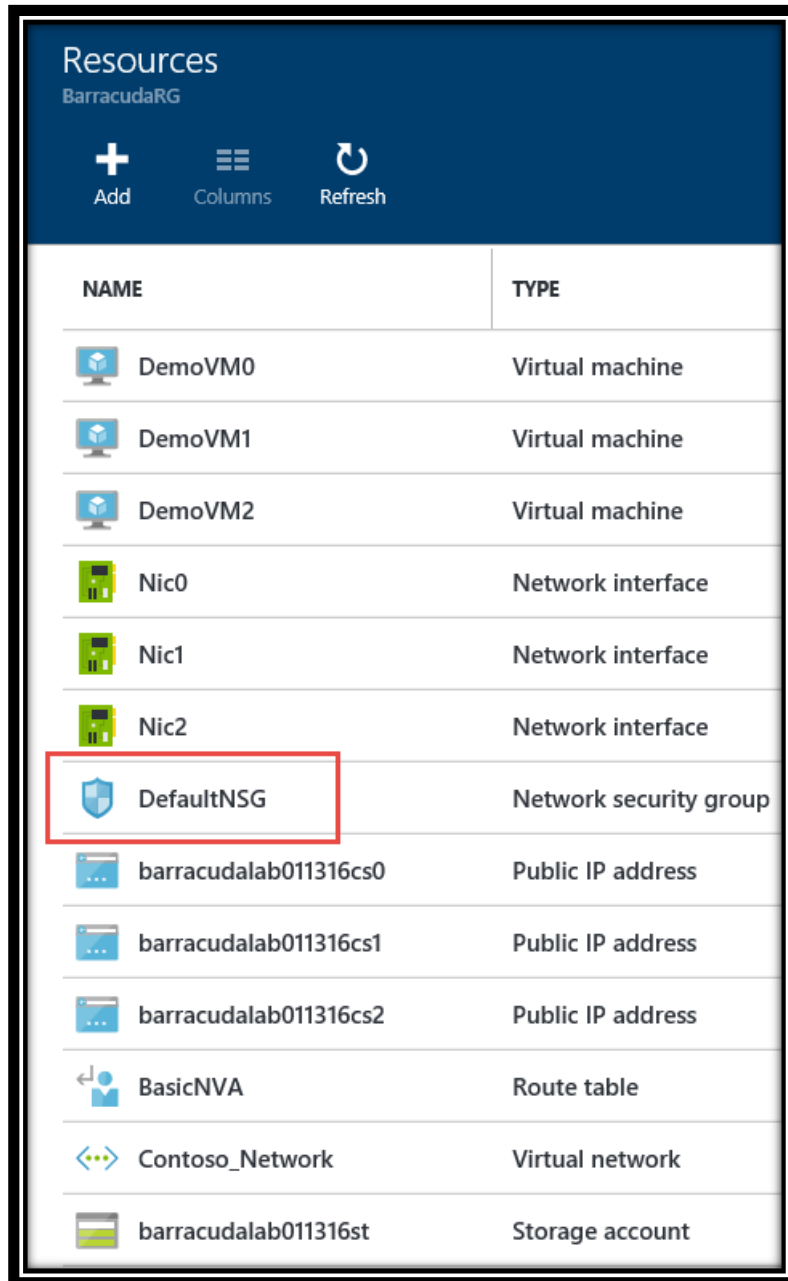
Exercise 3: Review networking configuration of the new deployment














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 (...).

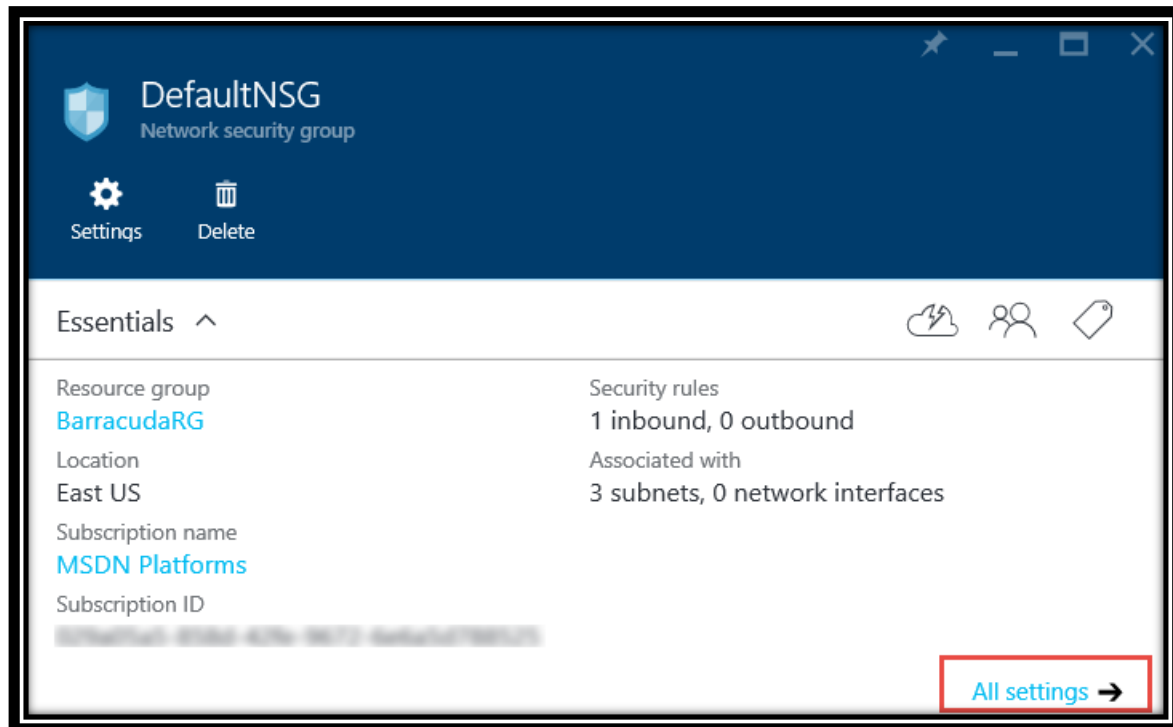


- In the **Resources** blade, note that the resource group contains three virtual machines, three network interfaces (one per each VM), one default network security group, one route table, virtual network, and a storage account. Click **DefaultNSG**.

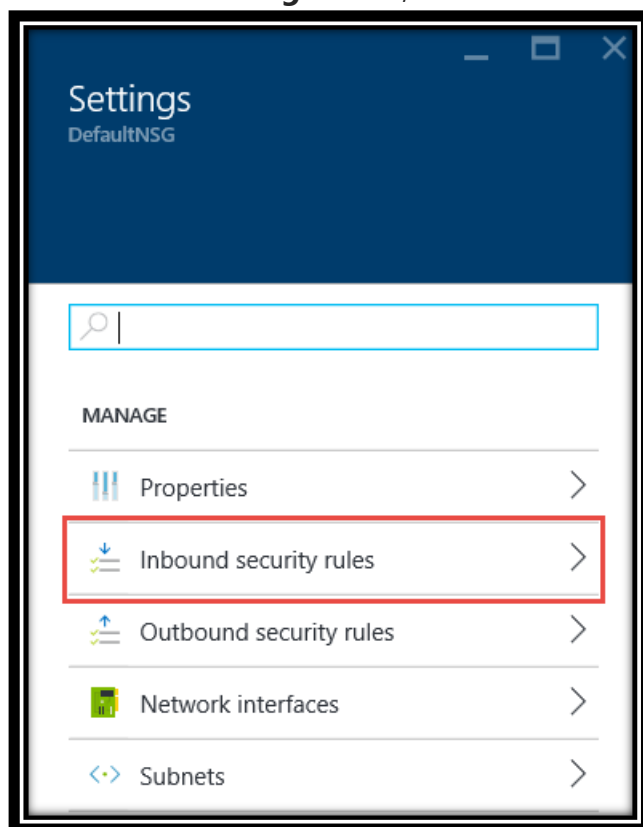


NAME	TYPE
 DemoVM0	Virtual machine
 DemoVM1	Virtual machine
 DemoVM2	Virtual machine
 Nic0	Network interface
 Nic1	Network interface
 Nic2	Network interface
 DefaultNSG	Network security group
 barracudalab011316cs0	Public IP address
 barracudalab011316cs1	Public IP address
 barracudalab011316cs2	Public IP address
 BasicNVA	Route table
 Contoso_Network	Virtual network
 barracudalab011316st	Storage account

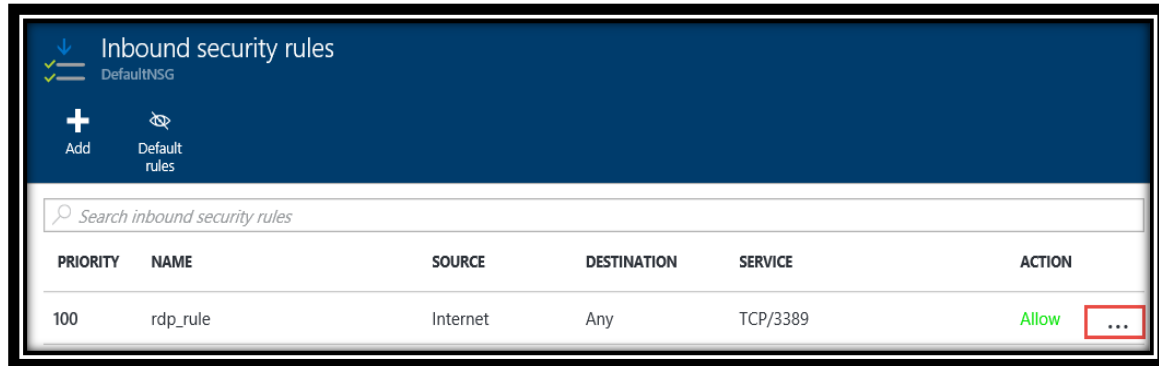
- In the **DefaultNSG** blade, click **All settings**.



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



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.

rdp_rule
BarracudaRG

Save Discard Delete

* Name
rdp_rule

* Priority ⓘ
100

Source ⓘ
Any CIDR block Tag

Protocol
Any TCP UDP

* Source port range ⓘ
*

Destination ⓘ
Any CIDR block Tag

* Destination port range ⓘ
3389

Action
Deny Allow

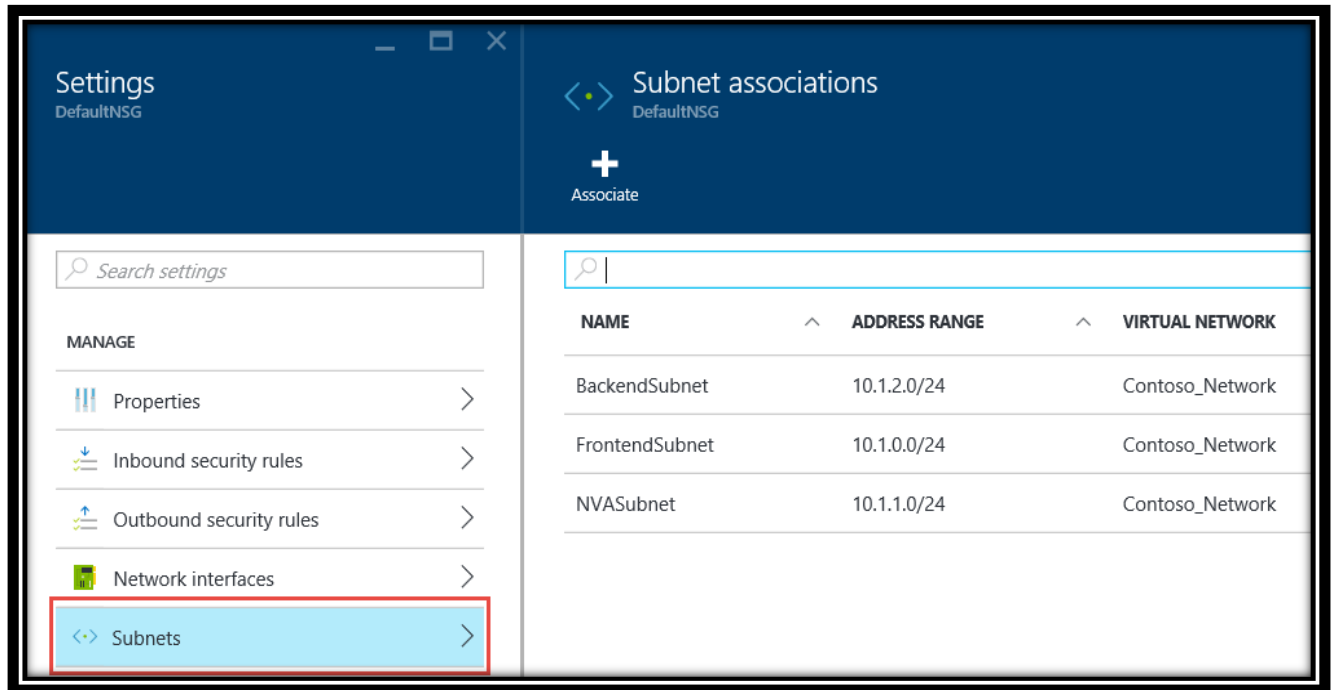
7. Wait for the rule to be successfully saved.



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



- 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.



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



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



- 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.

Routes		
NAME	ADDRESS PREFIX	NEXT HOP
VirtualApplianceRouteToSubnet3	10.1.2.0/24	10.1.1.4




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

Subnets		
NAME	ADDRESS RANGE	VIRTUAL NETWORK
FrontendSubnet	10.1.0.0/24	Contoso_Network

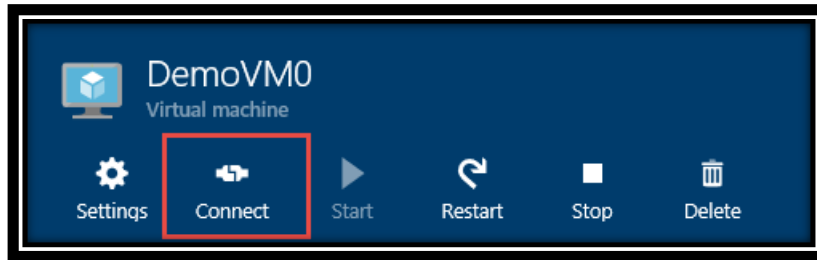
14. Click **Resources** at the top of the Azure Portal page.

BarracudaRG	>	Resources	>	DefaultNSG	>	Settings	>	Inbound security rules
-------------	---	-----------	---	------------	---	----------	---	------------------------

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

Resources	
	DemoVM0
	DemoVM1
	DemoVM2

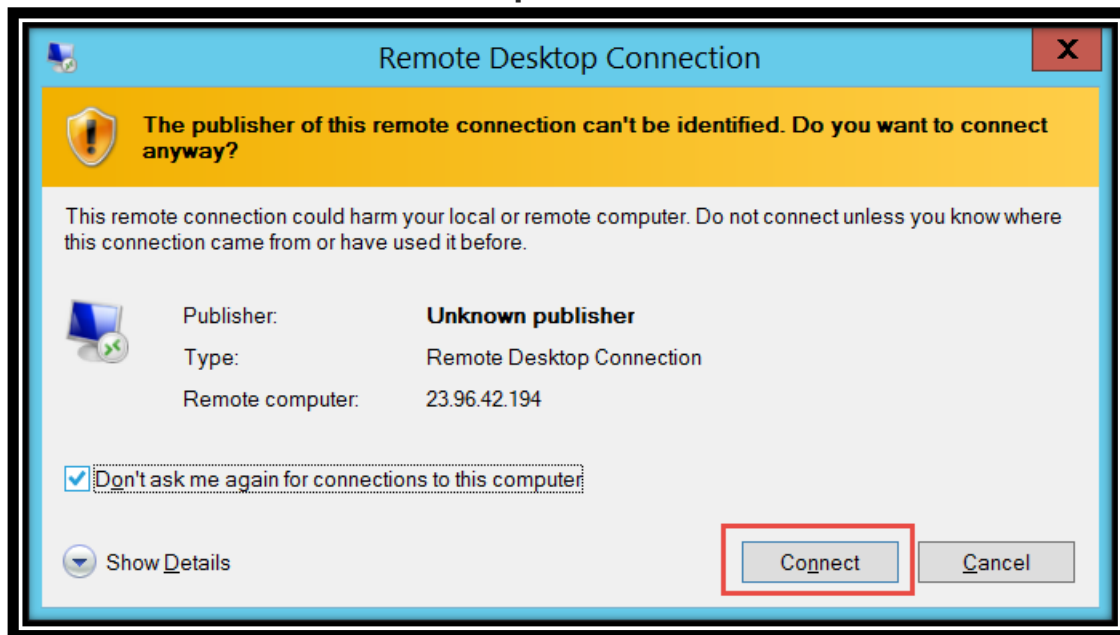
16. In the **DemoVM0** blade, click **Connect**.



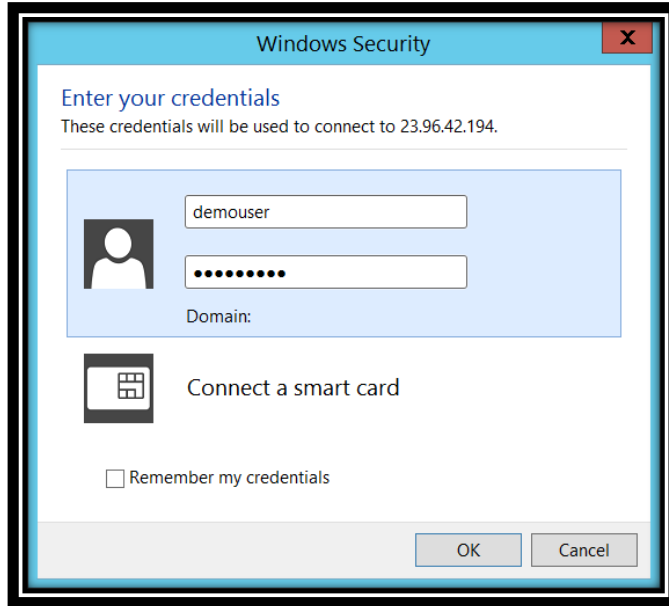
17. When prompted, click **Open**.



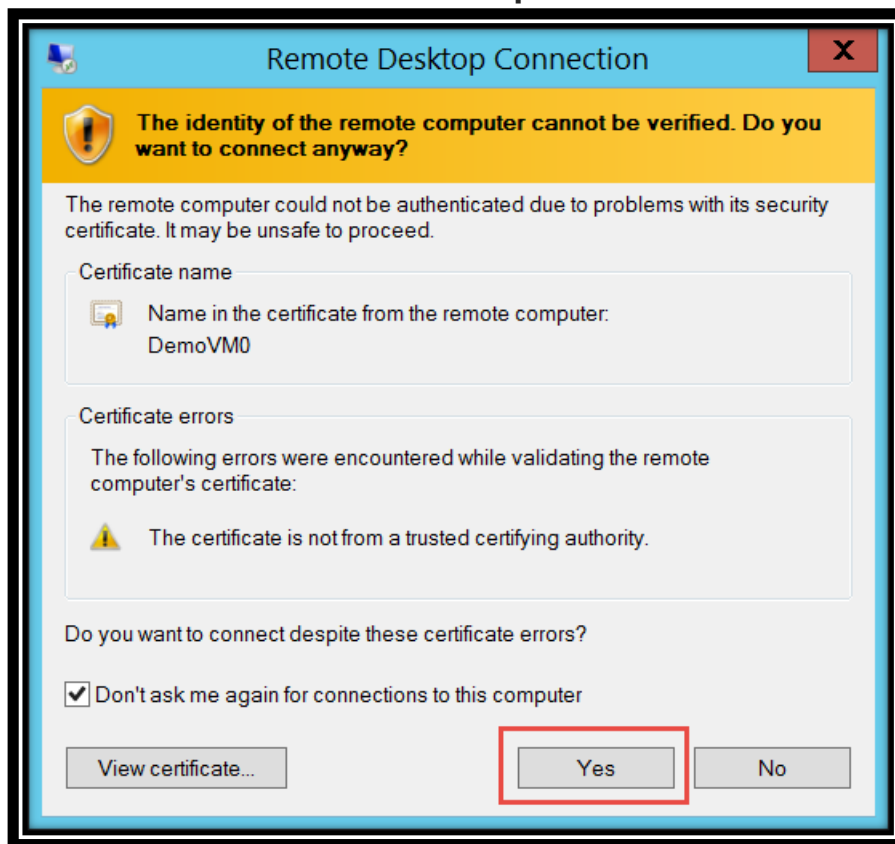
18. In the **Remote Desktop Connection** dialog box, enable the **Don't ask me again for connections to this computer** checkbox and click **Connect**.



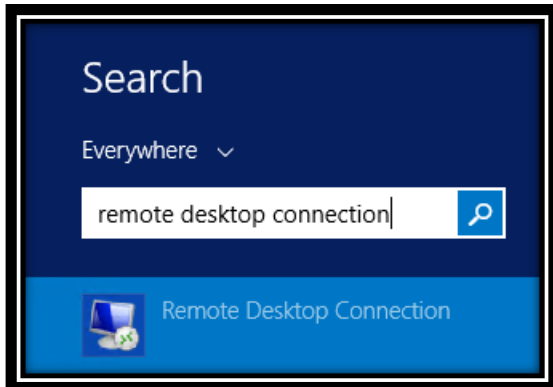
19. In the **Windows Security** dialog box, sign in with the **demouser** username and **demo@pass1** password credentials.



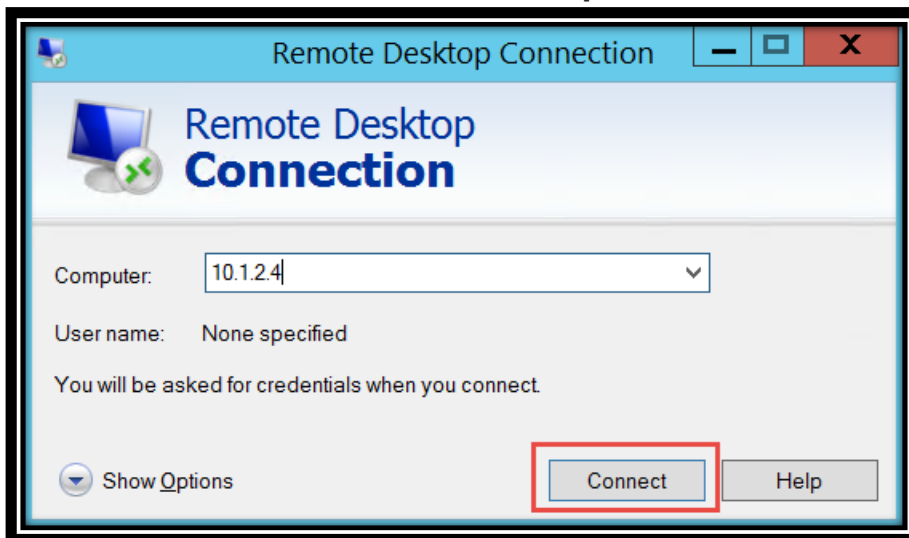
20. In the **Remote Desktop Connection** dialog box, enable the **Don't ask me again for connections to this computer** checkbox and click **Yes**.



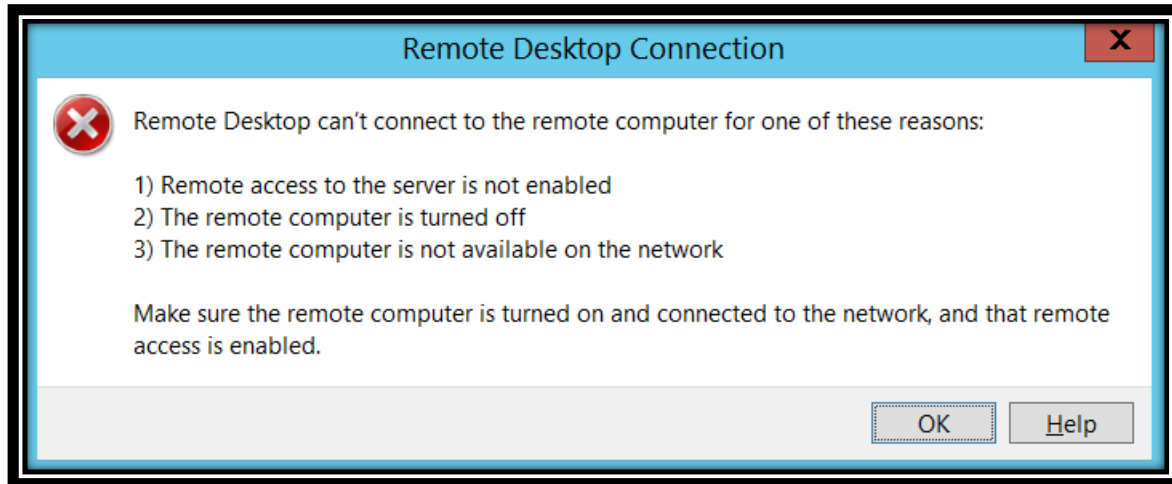
21. Once you log on to **DemoVM0**, from within the RDP session, from the **Start** screen, launch Remote Desktop Connection



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.



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

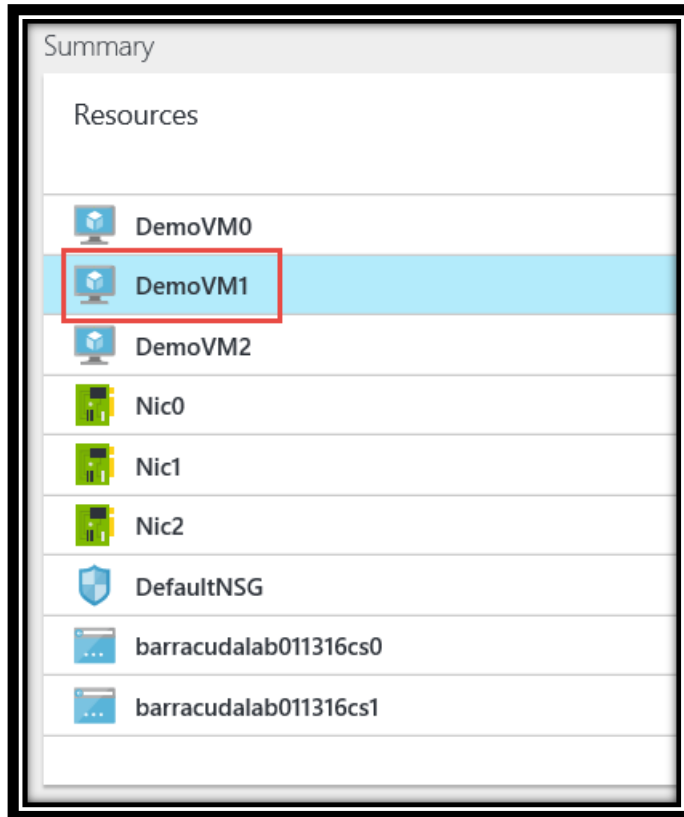
Exercise 4: Deploy Barracuda NG virtual appliance

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

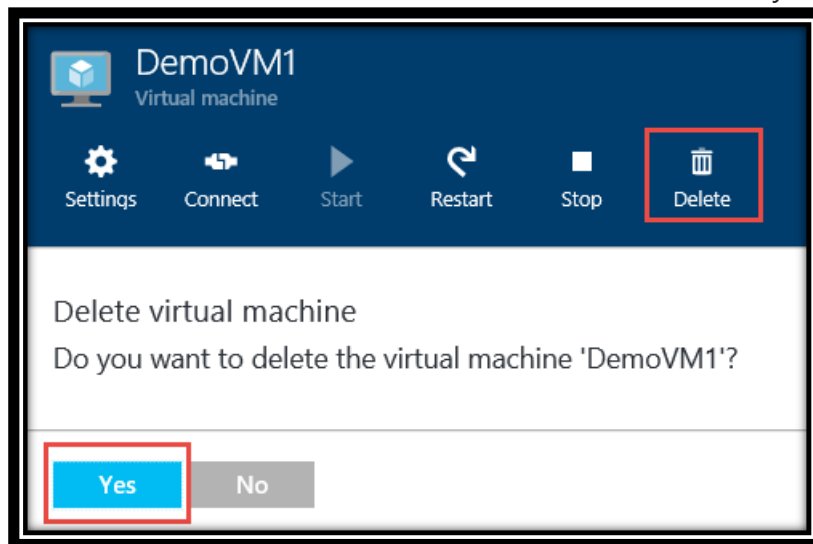
1. Return to the Azure Portal page on your lab computer. Click **BarracudaRG** at the top of the page.



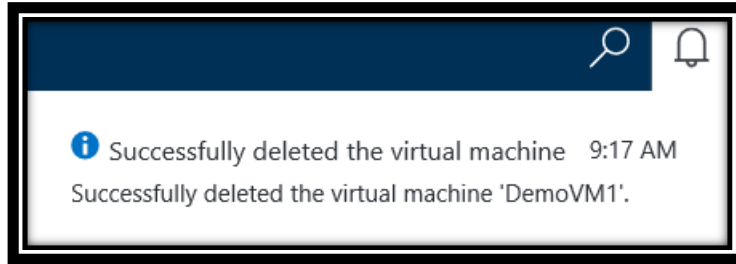
2. In the **Summary** lens of the **BarracudaRG** blade, click **DemoVM1**.



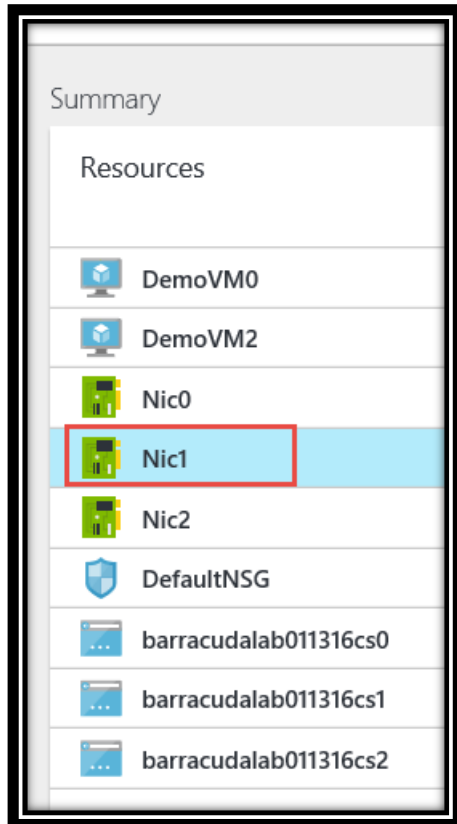
3. In the **DemoVM1** blade, click **Delete** followed by **Yes** when prompted to confirm.



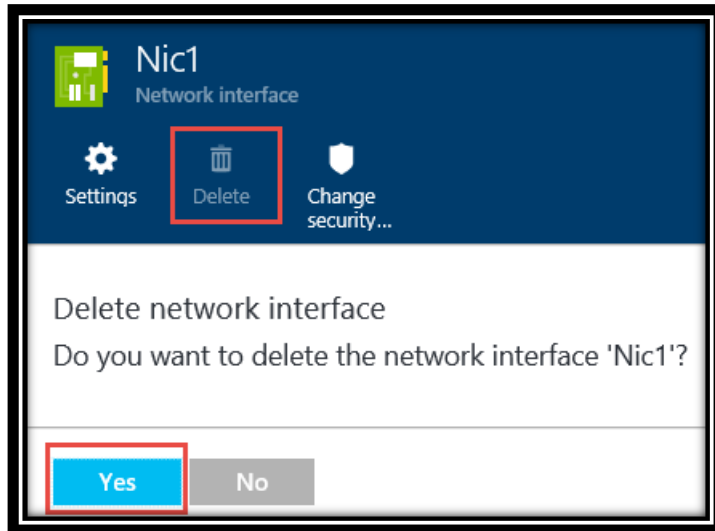
4. Wait for the confirmation that the **DemoVM1** has been successfully deleted.



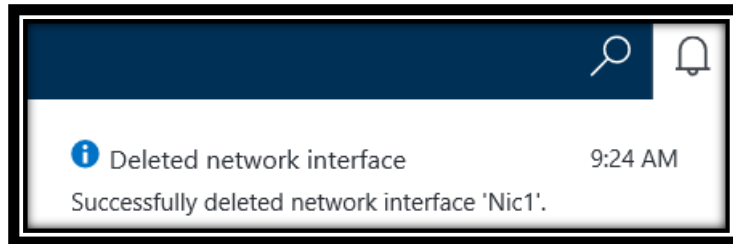
5. In the **Summary** lens of the **BarracudaRG** blade, click **Nic1**.



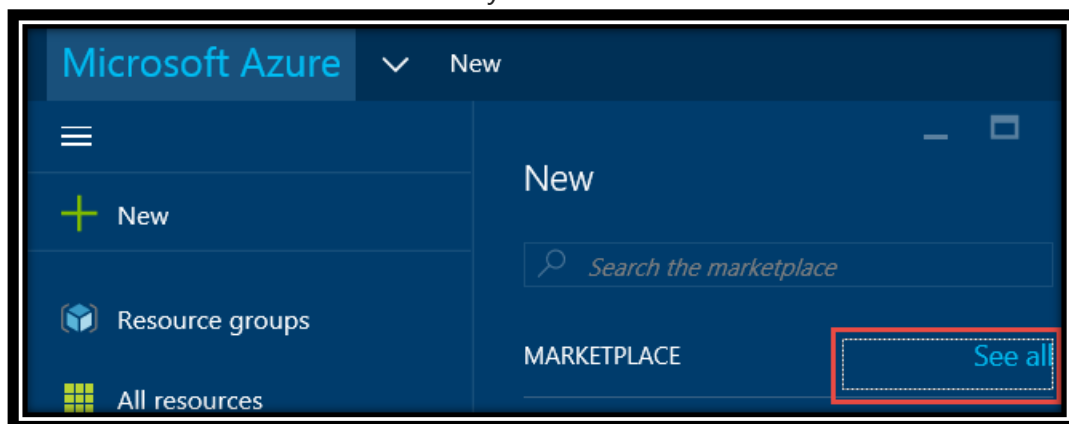
6. In the **Nic1** blade, click **Delete** followed by **Yes** when prompted to confirm.



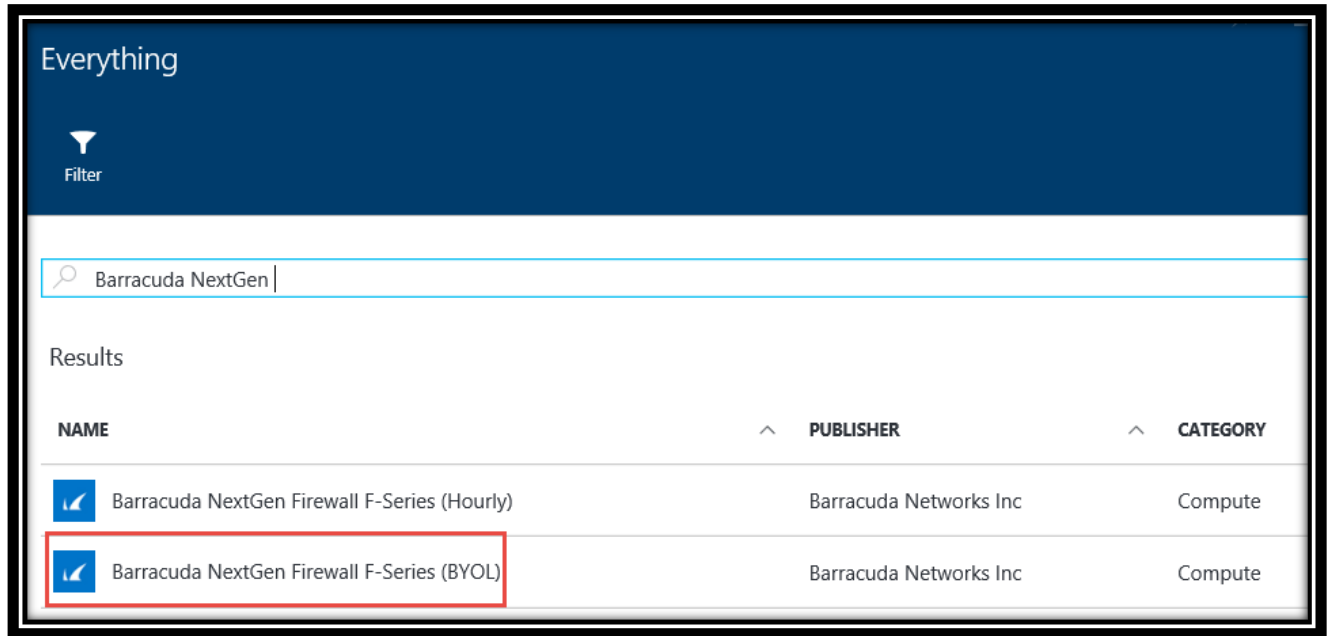
7. Wait for the confirmation that the **Nic1** is successfully deleted.



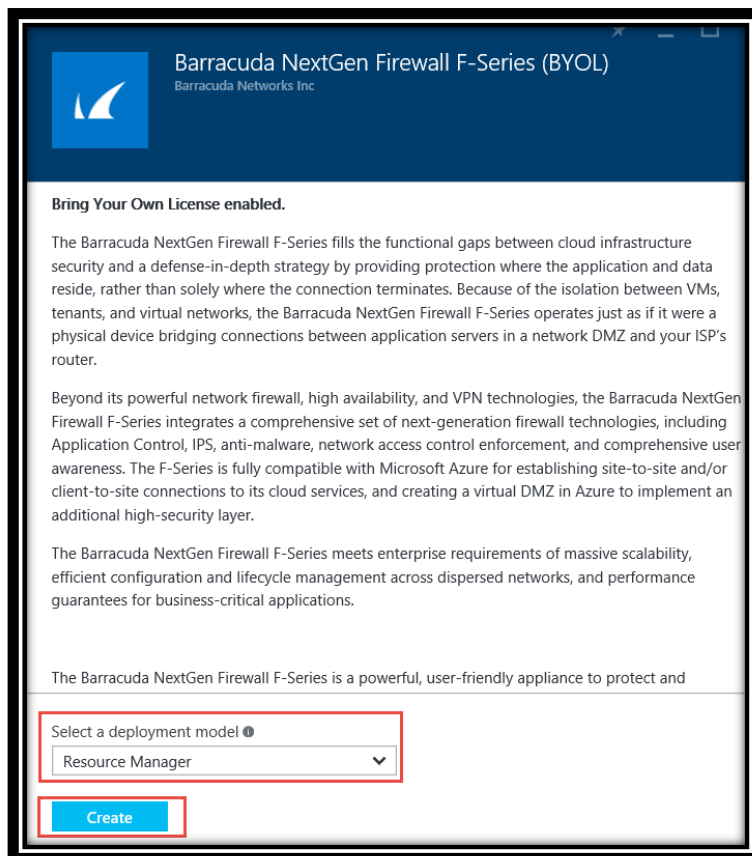
8. In the upper left corner of the Azure Portal, click **+New** followed by **See all** next to the **MARKETPLACE** entry



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)**



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**.



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*

The screenshot shows the 'Create virtual machine' wizard in the 'Basics' blade. The left sidebar contains five steps: 1 Basics (selected), 2 Size, 3 Settings, 4 Summary, and 5 Buy. The main area displays the following fields:

- Name:** BarracudaNG (with a green checkmark)
- User name:** demouser (with a green checkmark)
- Authentication type:** Password (selected from a dropdown with 'SSH public key' as an alternative)
- Password:** masked with dots (with a green checkmark)
- Subscription:** MSDN Platforms (with a right arrow)
- Resource group:** BarracudaRG (with a right arrow and a 'Create new' link below it)
- Location:** East US (with a right arrow)

An **OK** button is located at the bottom right of the form.

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

Create virtual machine

Choose a size
Browse the available sizes and their features

Prices presented below are estimated retail prices that include both Azure infrastructure and applicable third-party software costs. Prices do not reflect applicable discounts for your subscription and may include currency conversions.

★ Recommended | [View all](#)

A1 Standard ★		A2 Standard ★		A3 Standard ★	
1	Core	2	Cores	4	Cores
1.75	GB	3.5	GB	7	GB
2 Data disks		4 Data disks		8 Data disks	
2x500 Max IOPS		4x500 Max IOPS		8x500 Max IOPS	
Load balancing		Load balancing		Load balancing	
Auto scale		Auto scale		Auto scale	
44.64		89.28		178.56	
USD/MONTH (ESTIMATED)		USD/MONTH (ESTIMATED)		USD/MONTH (ESTIMATED)	

Select

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**

Create virtual machine

1 Basics Done ✓

2 Size Done ✓

3 Settings Configure optional features >

4 Summary Barracuda NextGen Firewall F-S... >

5 Buy >

Settings

Storage

Disk type ⓘ

Standard Premium (SSD)

* Storage account ⓘ (new) barracudalab011616 >

Network

* Virtual network ⓘ Contoso_Network >

* Subnet ⓘ NVASubnet (10.1.1.0/24) >

* Public IP address ⓘ (new) BarracudaNG >

* Network security group ⓘ (new) BarracudaNG >

Monitoring

Diagnostics ⓘ

Disabled Enabled

OK

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

Create virtual machine

1 Basics Done ✓

2 Size Done ✓

3 Settings Done ✓

4 Summary Barracuda NextGen Firewall F-S... >

5 Buy >

Summary

Basics

Subscription MSDN Platforms

Resource group BarracudaRG

Location East US

Settings

Computer name BarracudaNG

User name demouser

Size Standard A1

Disk type Standard

Storage account (new) barracudalab011616

Virtual network Contoso_Network

Subnet NVASubnet (10.1.1.0/24)

Public IP address (new) BarracudaNG

Network security group (new) BarracudaNG

Availability set None

Diagnostics Disabled

OK

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

Create virtual machine

1 Basics Done ✓

2 Size Done ✓

3 Settings Done ✓

4 Summary Barracuda NextGen Firewall F-S... ✓

5 Buy >

Purchase

Offer details

Barracuda NextGen Firewall F-Series by Barracuda Networks Inc 0.0000 USD/hr *

[Terms of use](#) and [privacy policy](#)

Standard A1 by Microsoft 0.0600 USD/hr +

[Terms of use](#) and [privacy policy](#)

[Pricing for other VM sizes](#)

* **Marketplace Offering:** May not be purchased using Microsoft subscription credits or monetary commitment funds and does not participate in discounts. These purchases are billed separately.

+ **Azure Resource:** May be purchased using Microsoft subscription credits or monetary commitment funds and participates in discounts. Prices presented are retail prices and may not reflect discounts associated with your subscription.

Terms of use

By clicking "Purchase", I (a) agree to the legal terms and privacy statement(s) associated with each Marketplace offering above, (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s), and (c) agree that Microsoft may share my contact information and transaction details with the seller(s) of the offering (s). Microsoft does not provide rights for third-party products or services. See the [Azure Marketplace Terms](#) for additional terms.

Purchase

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

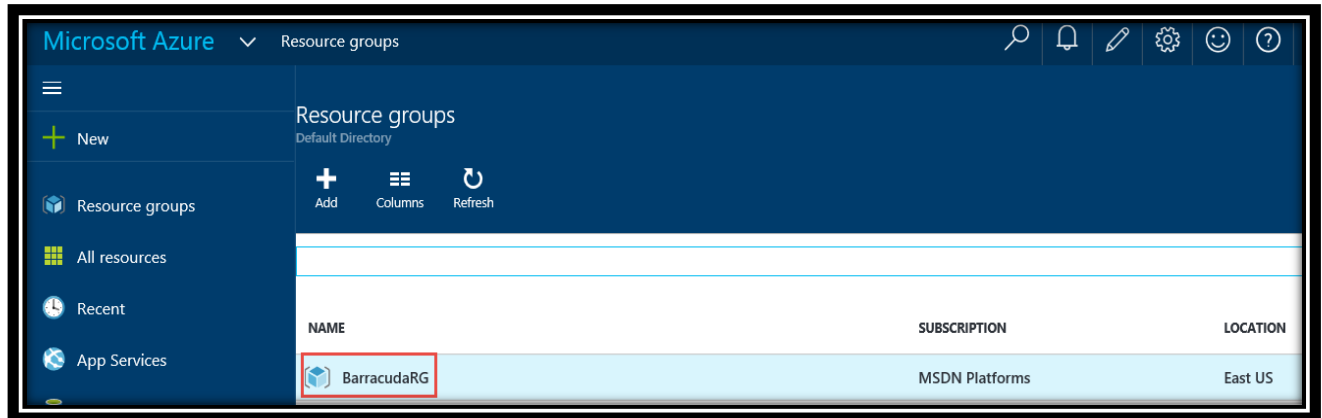
Exercise 5: Configure Azure networking for the Barracuda NG virtual appliance

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.

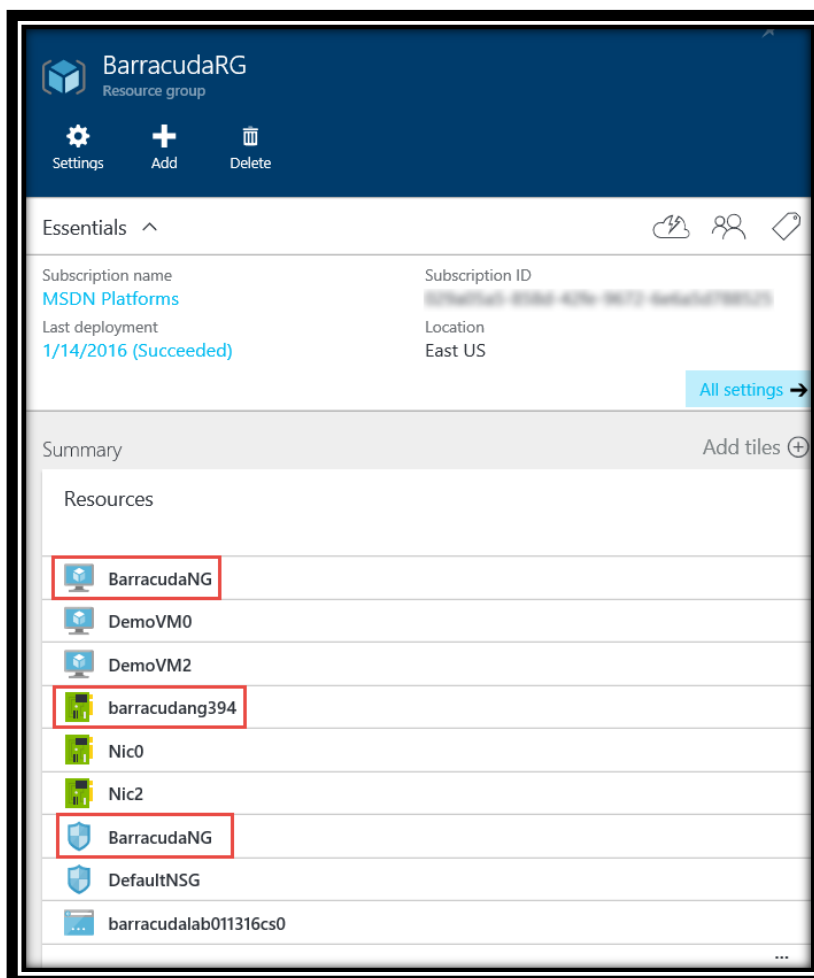
1. In the Microsoft Azure portal, in the Hub menu on the left hand side of the page, click **Resource groups**. Then in the **Resource groups** page, click **BarracudaRG**.

©2016 Microsoft Corporation

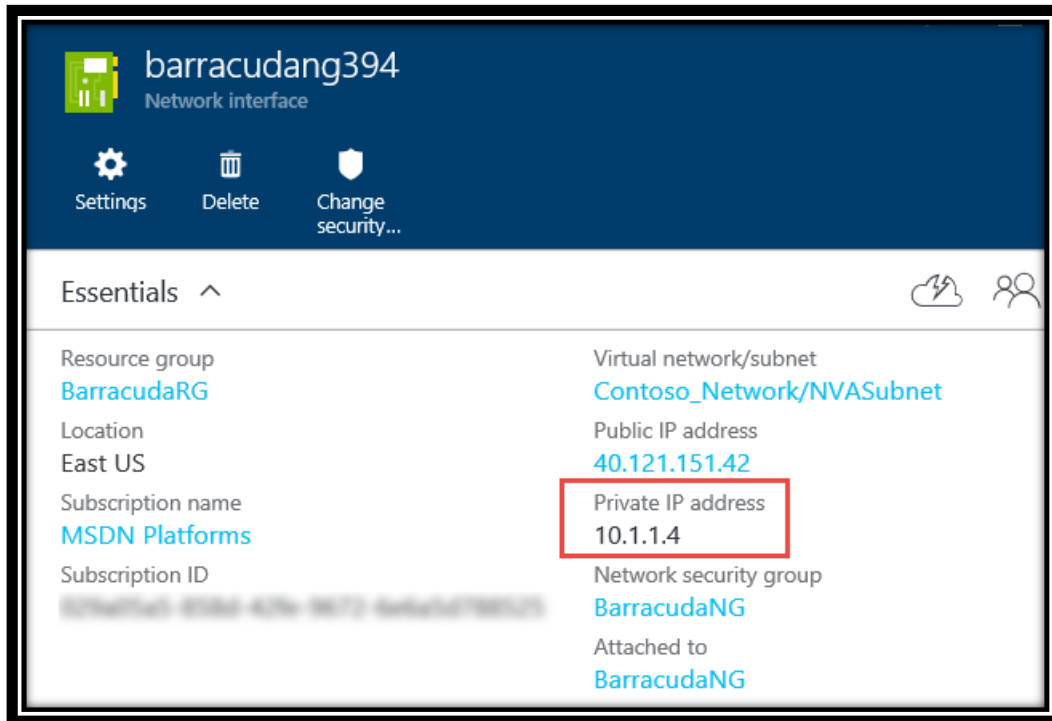
26



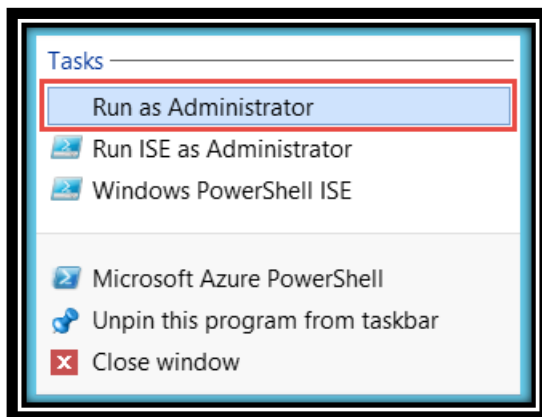
- Note that the resource group contains a number of additional resources, including the **BarracudaNG** virtual machine, the corresponding network interface (starting with the **barracudang** prefix) and a separate network security group **BarracudaNG**.



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.



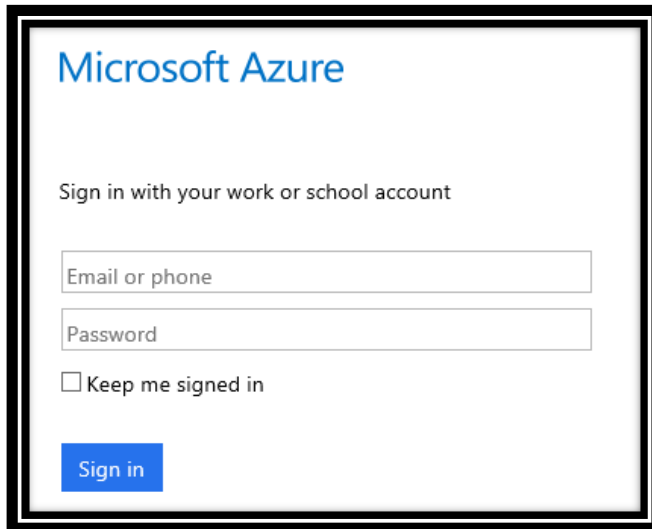
4. From your lab computer, launch Microsoft Azure PowerShell as Administrator from the taskbar shortcut.



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

```
Login-AzureRmAccount
```

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. **You will need to change the Name parameter to match the name of your Network interface:**

```
$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**

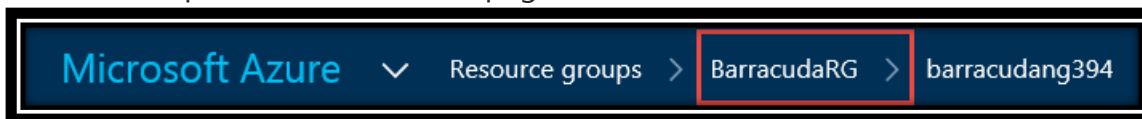
```
Set-AzureRmNetworkInterface -NetworkInterface $BarracudaNIC
```

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

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

BarracudaRG
Resource group

Settings Add Delete

Essentials ^

Subscription name: **MSDN Platforms**
Subscription ID: [REDACTED]
Last deployment: **1/14/2016 (Succeeded)**
Location: **East US**

[All settings](#) →

Summary Add tiles +

Resources

- BarracudaNG
- DemoVM0
- DemoVM2
- barracudang394
- Nic0
- Nic2
- BarracudaNG
- DefaultNSG**
- barracudalab011316cs0

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

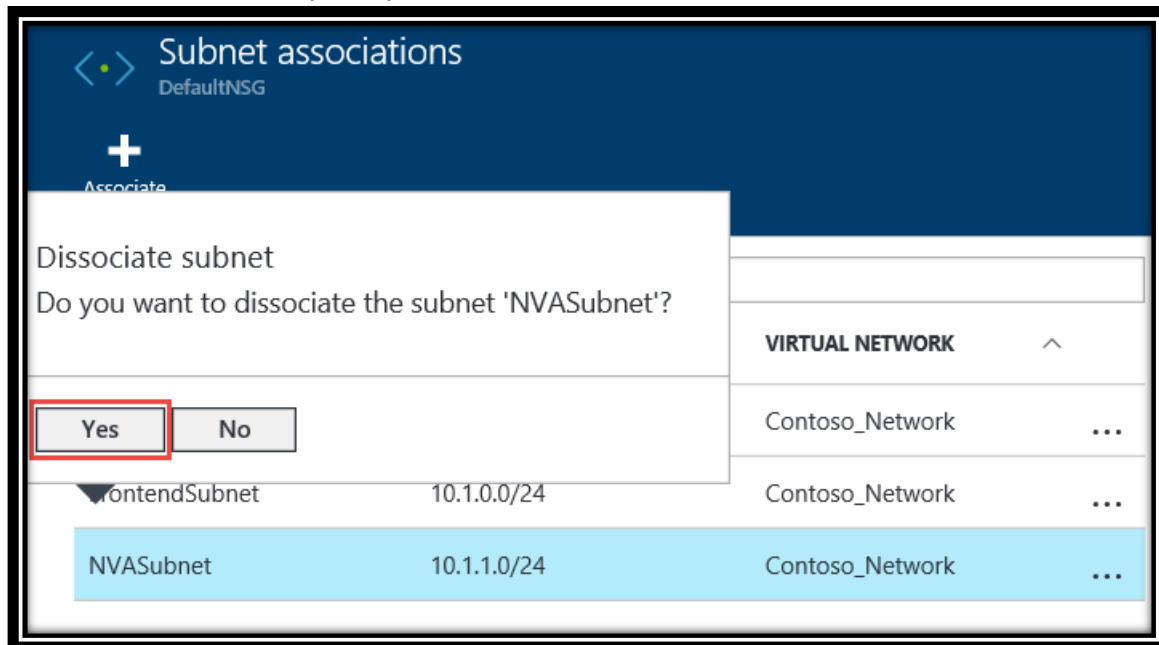
The screenshot shows the 'DefaultNSG' settings page in the Azure portal. The left-hand navigation pane is expanded, showing the 'Subnets' link highlighted with a red box. The main content area displays the 'Essentials' section with details about the resource group, location, and security rules. The right-hand pane shows the 'Settings' section with a search bar and a list of settings categories: MANAGE, MONITOR, and RESOURCE MANAGEMENT. The 'Subnets' link is highlighted with a red box.

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

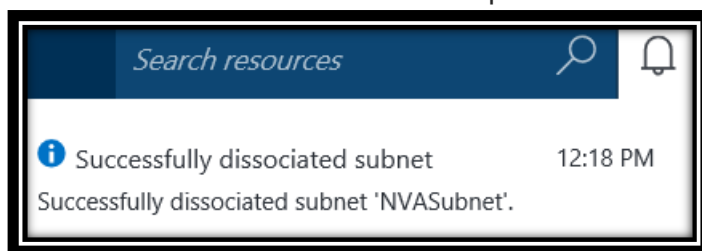
The screenshot shows the 'Subnet associations' blade in the Azure portal. The blade displays a table with columns: NAME, ADDRESS RANGE, and VIRTUAL NETWORK. The table lists three subnets: BackendSubnet, FrontendSubnet, and NVASubnet. The 'Dissociate' button in the NVASubnet row is highlighted with a red box.

NAME	ADDRESS RANGE	VIRTUAL NETWORK
BackendSubnet	10.1.2.0/24	Contoso_Network
FrontendSubnet	10.1.0.0/24	Contoso_Network
NVASubnet	10.1.1.0/24	Contoso_Network

14. Confirm when prompted



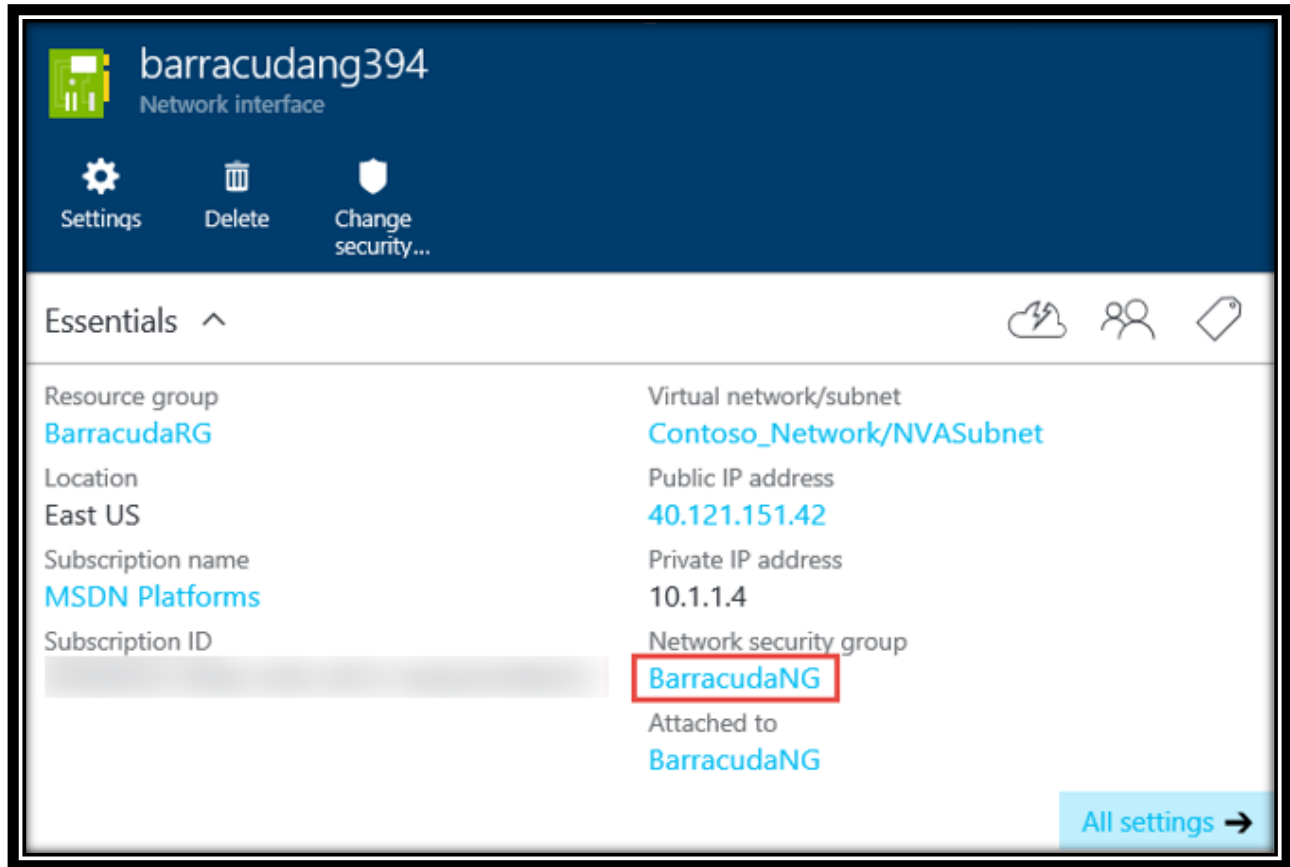
15. Wait until the action is completed.



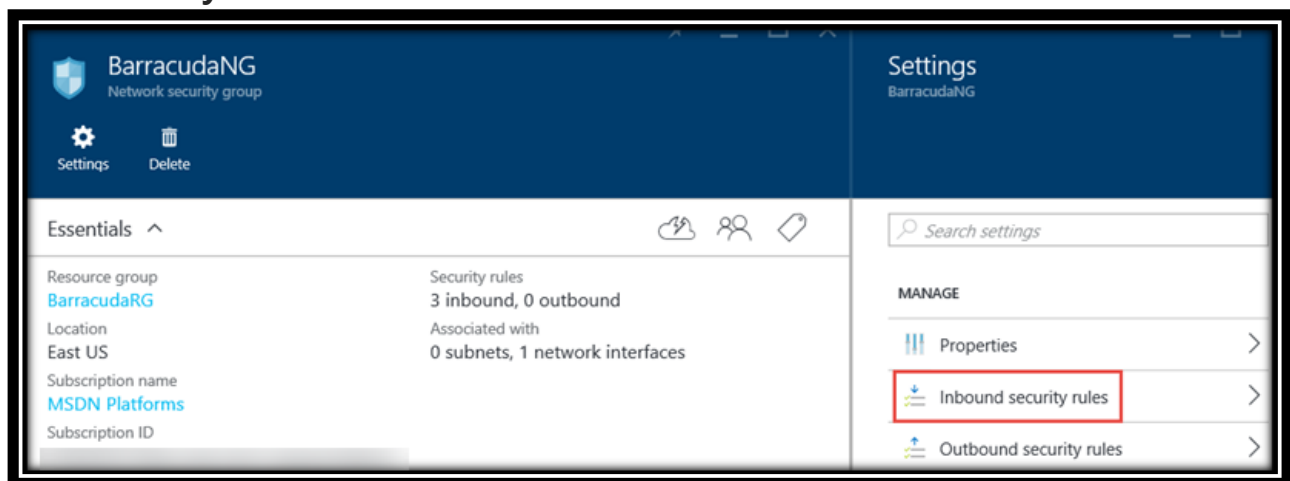
Exercise 6: Configure firewall component of the Barracuda NG virtual appliance

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.



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



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

Inbound security rules
BarracudaNG

Add Default rules

PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
1010	MGMT	Any	Any	TCP/807	Allow ...
1020	TINA_VPN	Any	Any	Any/691	Allow ...
1030	default-allow-ssh	Any	Any	TCP/22	Allow ...

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**

Add inbound security rule

BarracudaNG

* Name
 ✓

* Priority ⓘ

Source ⓘ

Protocol

* Source port range ⓘ

Destination ⓘ

* Destination port range ⓘ
 ✓

Action

5. Verify that the rule has been successfully created.

Search resources

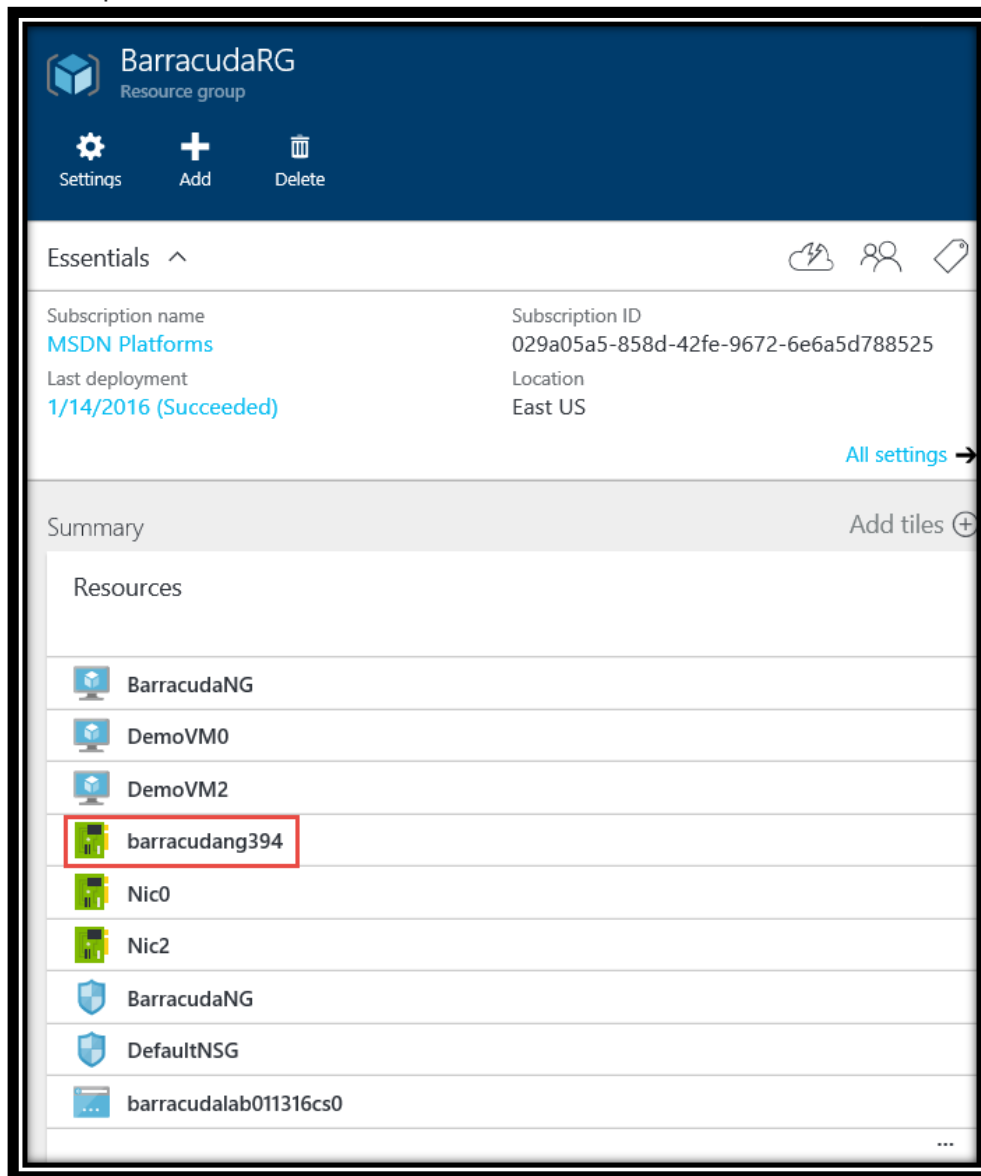
i Created security rule 12:41 PM

Successfully created security rule 'MGMT801'.

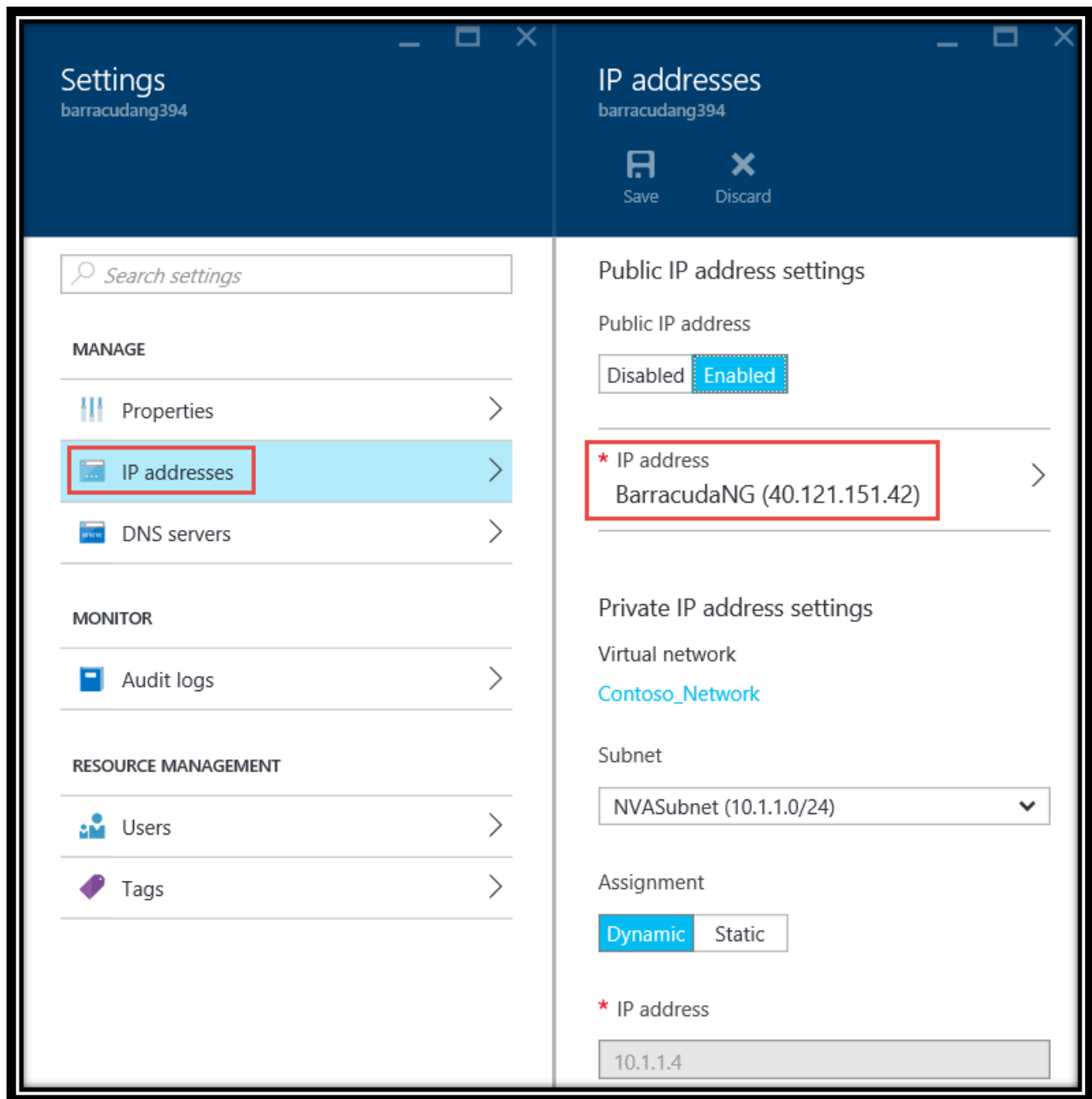
- In order to identify the public IP address assigned to the network interface of the virtual machine hosting the Barracuda NG virtual appliance, navigate back to the **BarracudaRG** resource group.



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

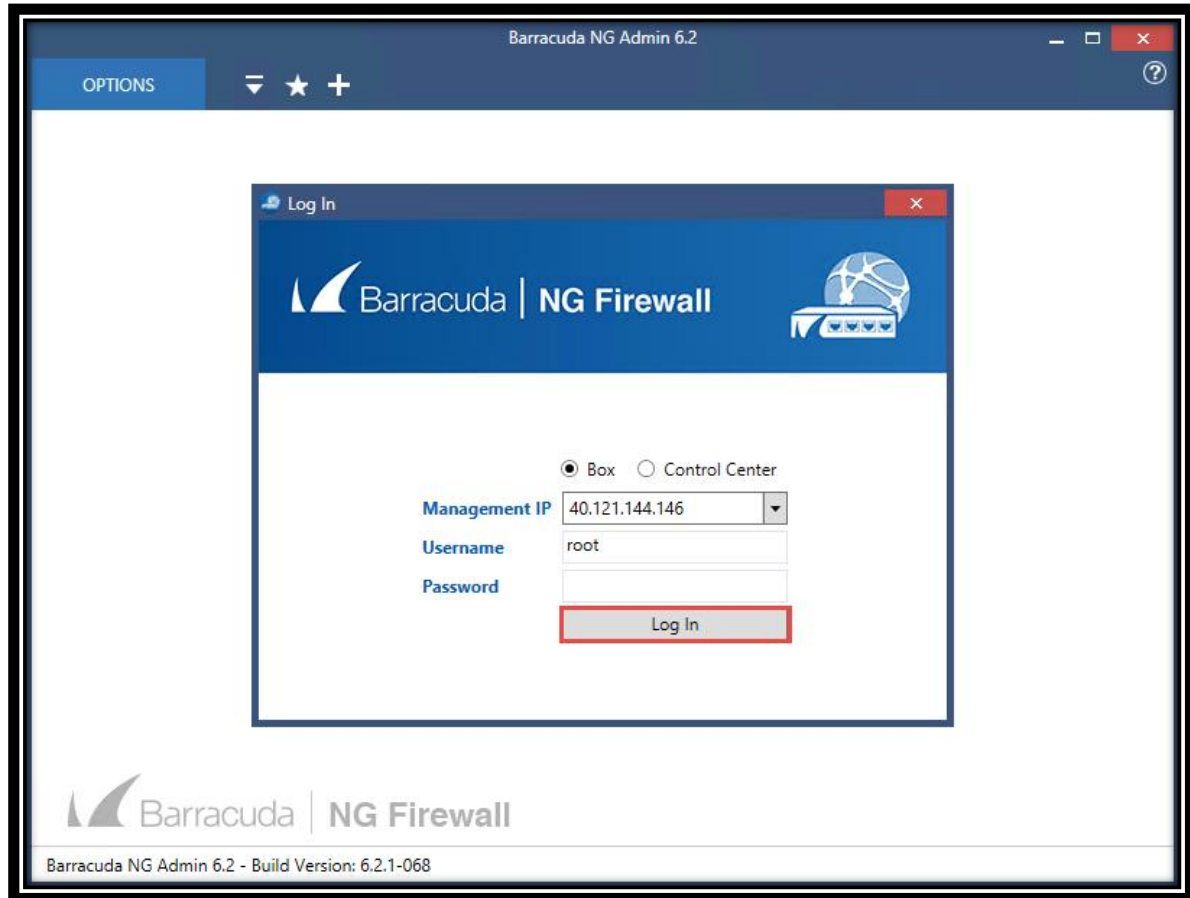


8. In the network interface blade (**barracuda394** in our case), take a note of its Public IP address entry.

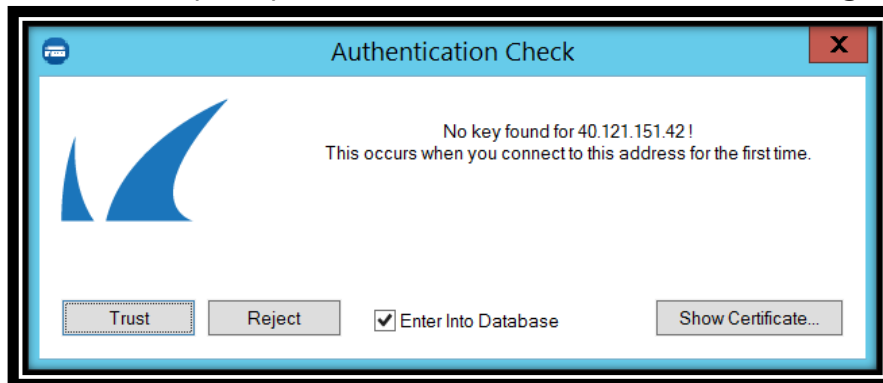


9. On your client machine launch the **ngadmin_6-2-1-068.exe** utility downloaded from <https://copy.com/fG2FIvyHptjy9g7n>
10. In the **Log in** dialog box of the **Barracuda NG Admin 6.2** utility, specify the following and click **Log in**:

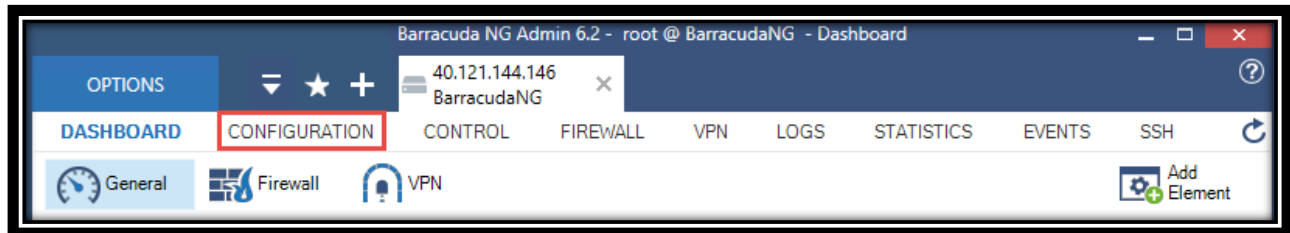
- Management IP: *address you identified at the beginning of this exercise*
- Username: **root** (note that this is **not** the username you specified when deploying the appliance from Azure Portal)
- Password: **demo@pass1**



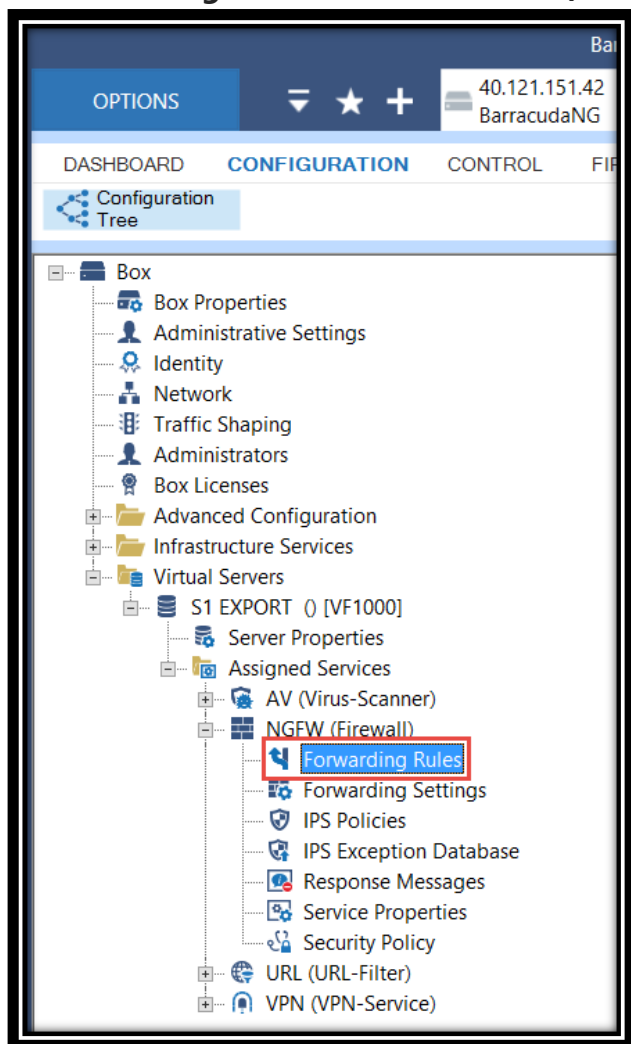
11. When prompted, in the **Authentication Check** dialog box, click **Trust**.



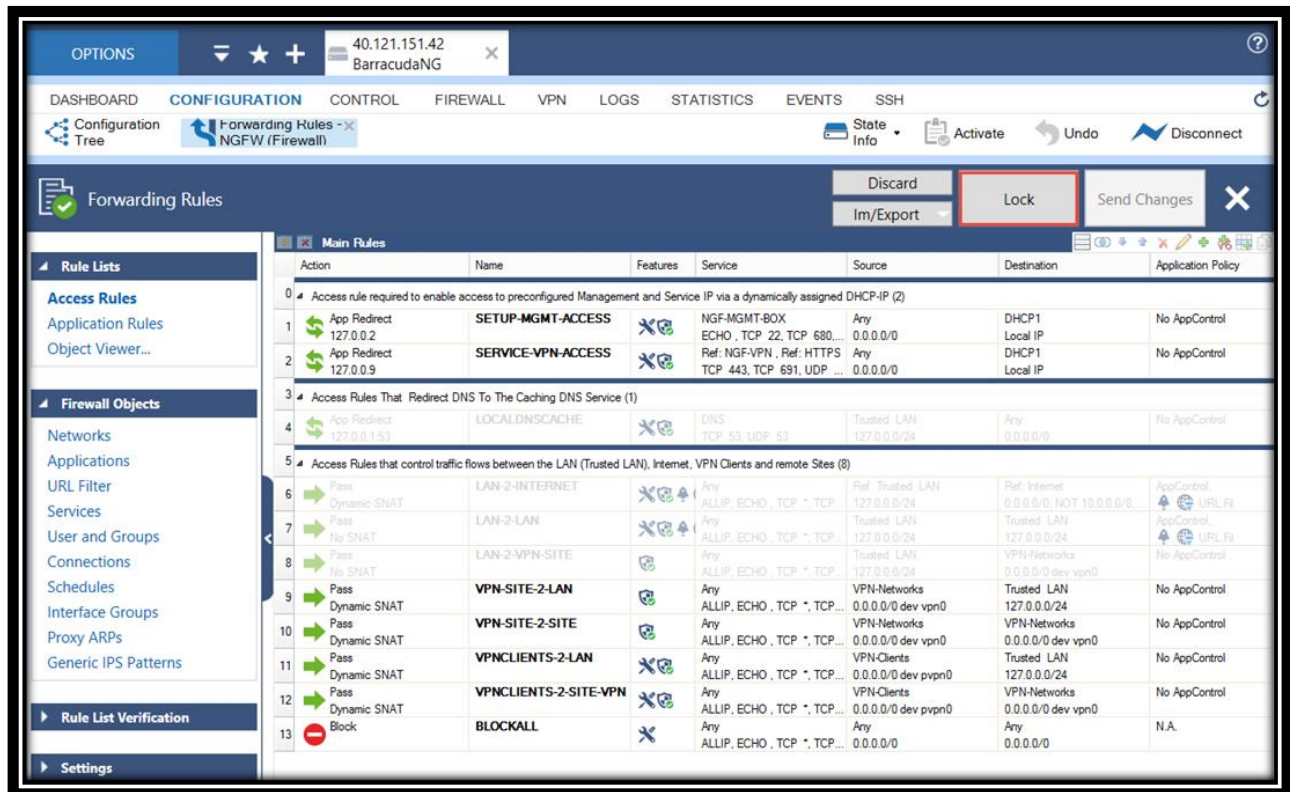
12. Once successfully connected, in the **Barracuda NG Admin 6.2** console, click **CONFIGURATION**.



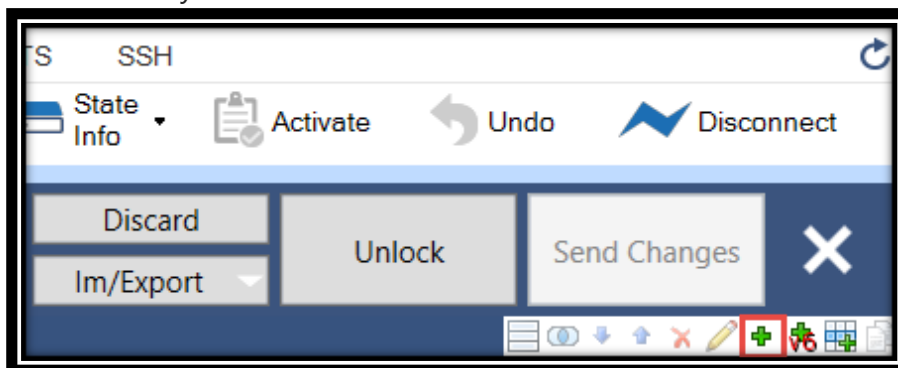
13. In the **Configuration Tree**, expand the **Virtual Servers** → **S1 Export () [VF1000]** → **Assigned Services** → **NGFW (Firewall)** and double-click **Forwarding Rules**.



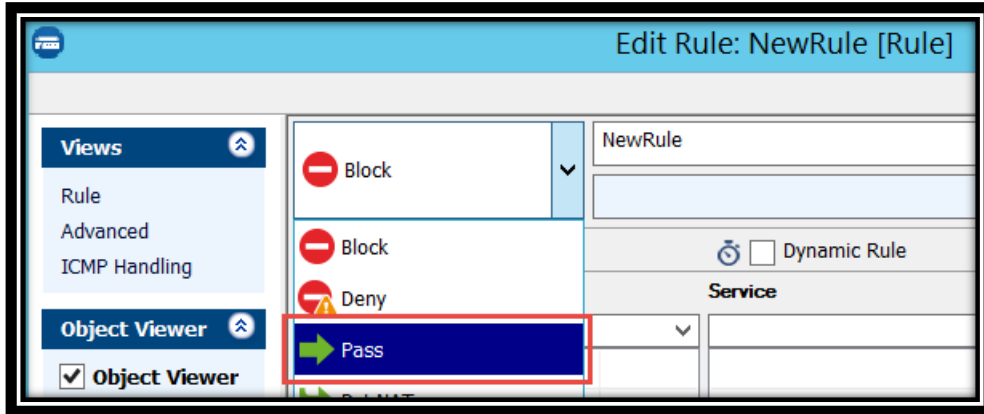
14. In the **Forwarding Rules** window, click **Lock** in the upper right corner (the label will change to **Unlock**):



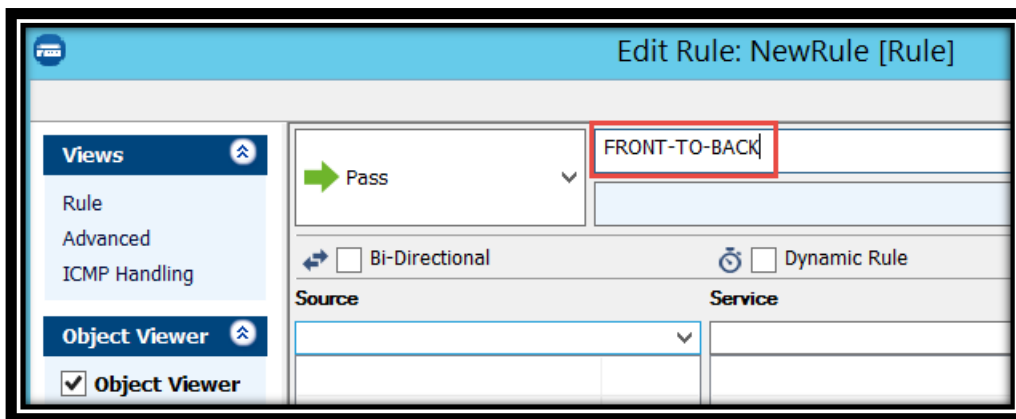
15. In the **Forwarding Rules** window, click the plus sign (**Insert rule**) in the toolbar directly underneath:



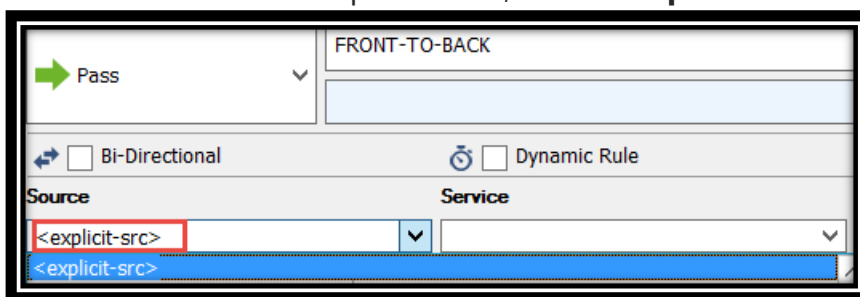
16. In the **Edit Rule: New Rule** dialog box, change **Block** to **Pass**.



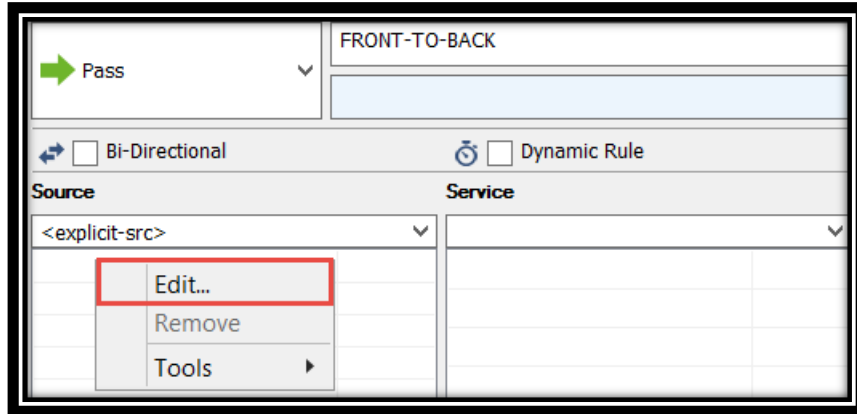
17. Replace **NewRule** entry at the top of the dialog box with a more descriptive name (we will use **FRONT-TO-BACK**).



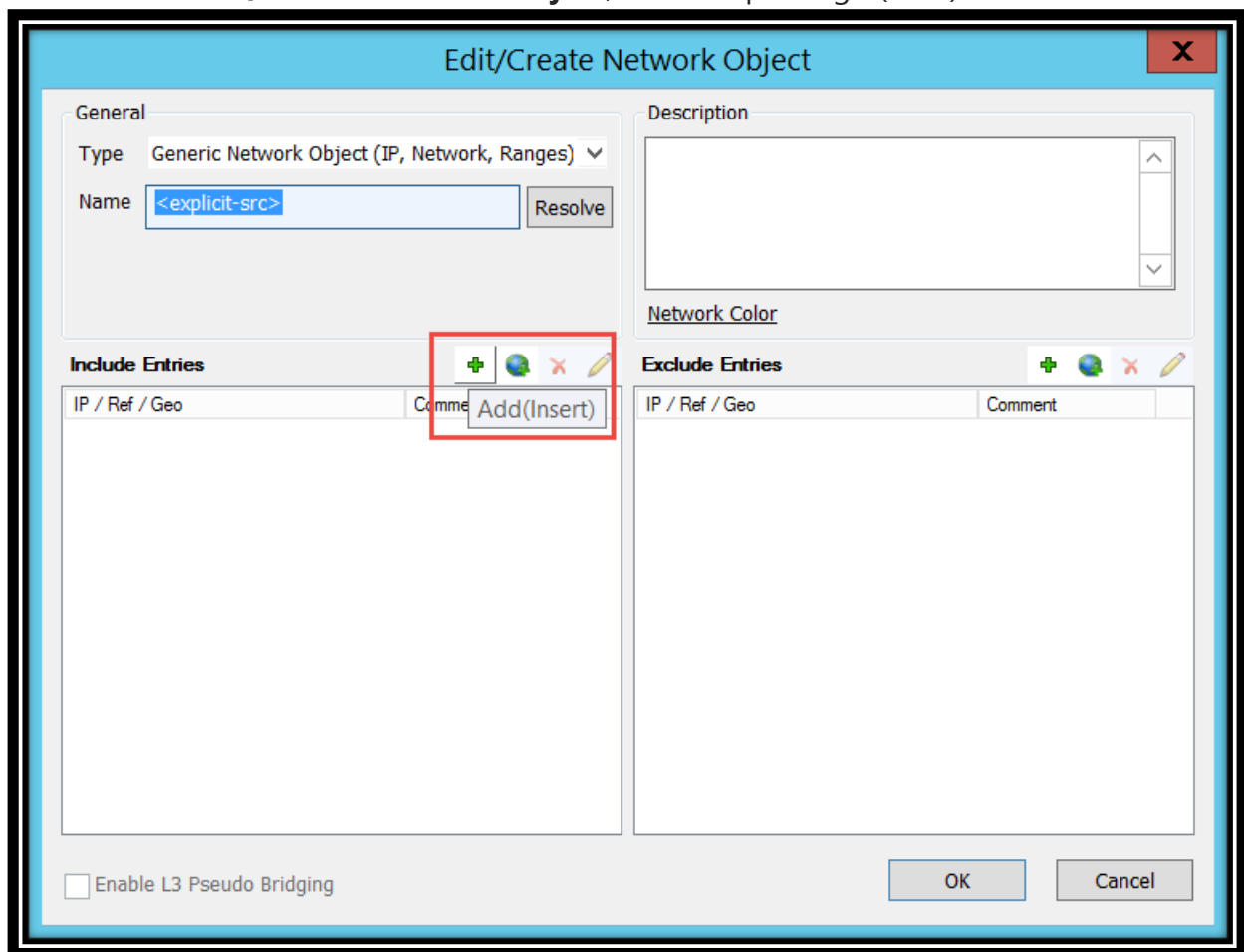
18. In the **Source** drop down list, select **<explicit-src>**



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



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**.

Edit/Create Include Entry [X]

☒ IP / Network

IP:

MAC: (optional)

Interface: (optional)

Comment:

☐ Reference

Buttons: Insert, **Insert and Close**, Close

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

Edit/Create Network Object [X]

General

Type: Generic Network Object (IP, Network, Ranges) ▼

Name: [Resolve]

Description

Network Color

Include Entries [Add] [Edit] [Delete] [New]

IP / Ref / Geo	Comment
10.1.0.0/24	

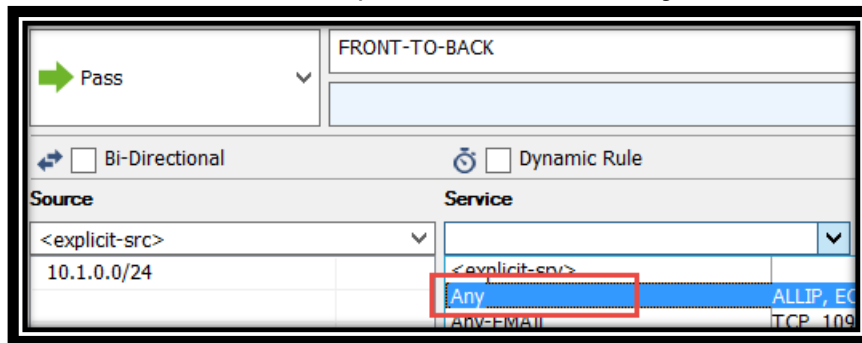
Exclude Entries [Add] [Edit] [Delete] [New]

IP / Ref / Geo	Comment
----------------	---------

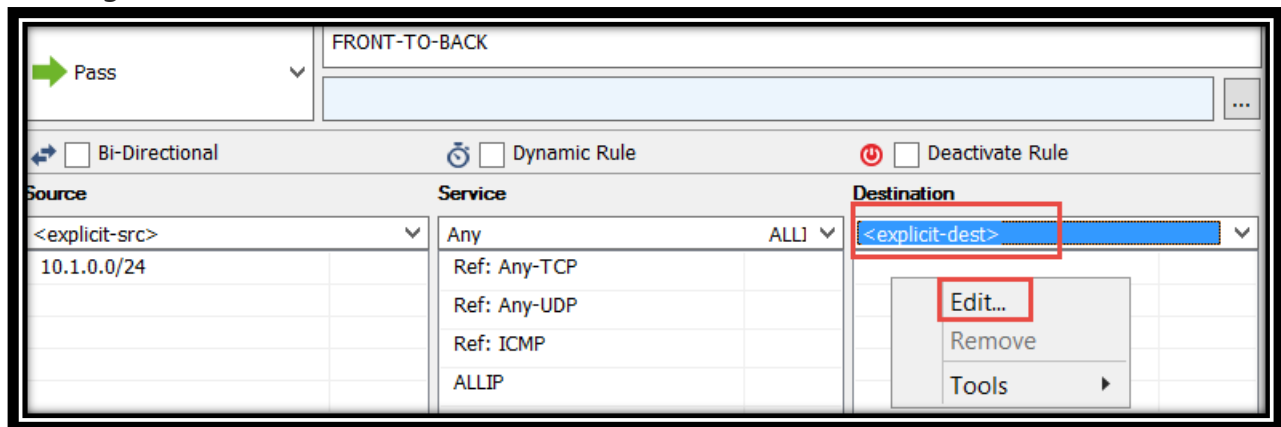
☐ Enable L3 Pseudo Bridging

Buttons: **OK**, Cancel

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.

Edit/Create Network Object

General

Type: Generic Network Object (IP, Network, Ranges) ▼

Name: <explicit-dest> Resolve

Description

Network Color

Include Entries

IP / Ref / Geo Comment + 🌐 - ✎ Add(Insert)

Exclude Entries

IP / Ref / Geo Comment + 🌐 - ✎

☐ Enable L3 Pseudo Bridging

OK Cancel

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**.

Edit/Create Include Entry

☒ IP / Network

IP: 10.1.2.0/24

MAC: (optional)

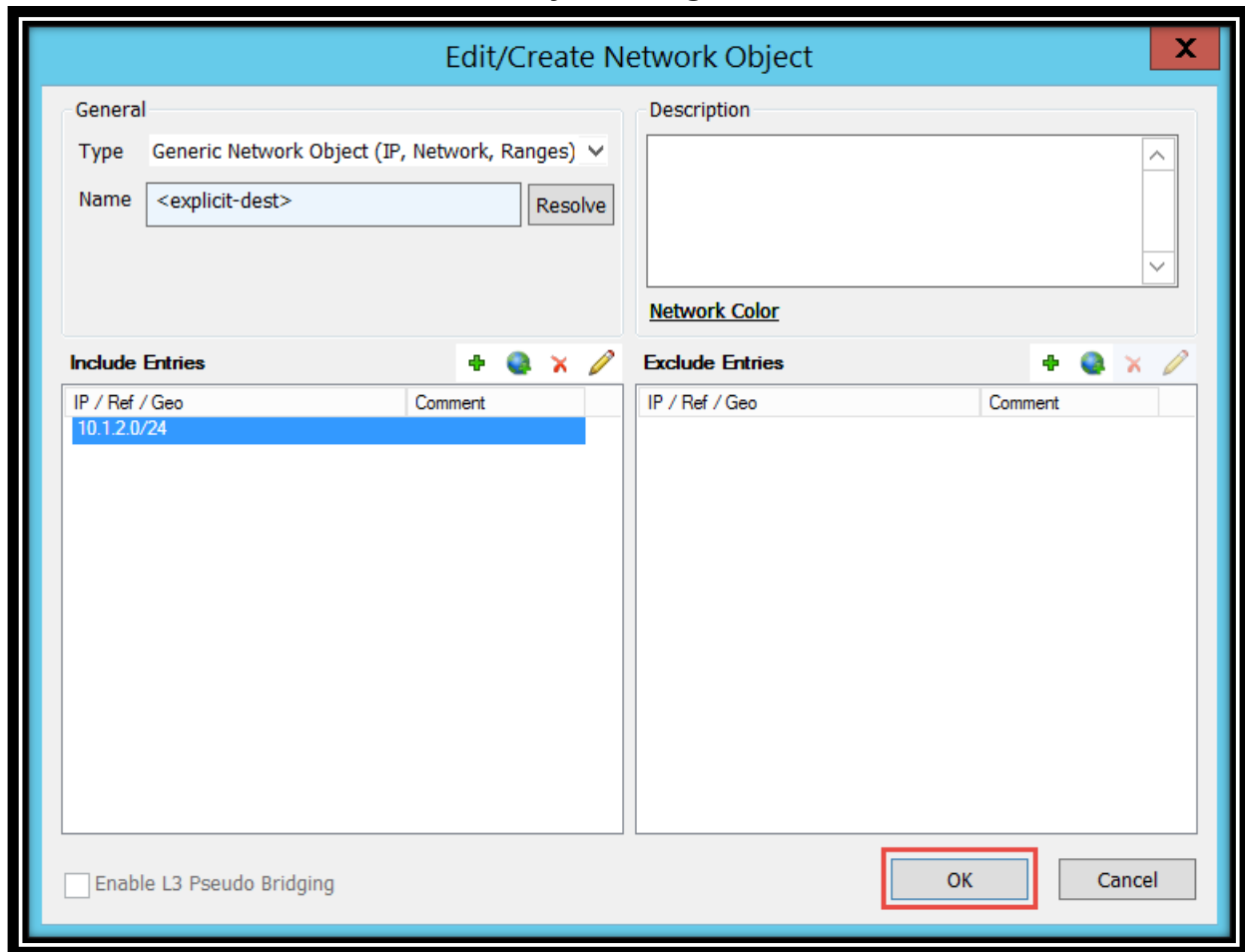
Interface: (optional)

Comment:

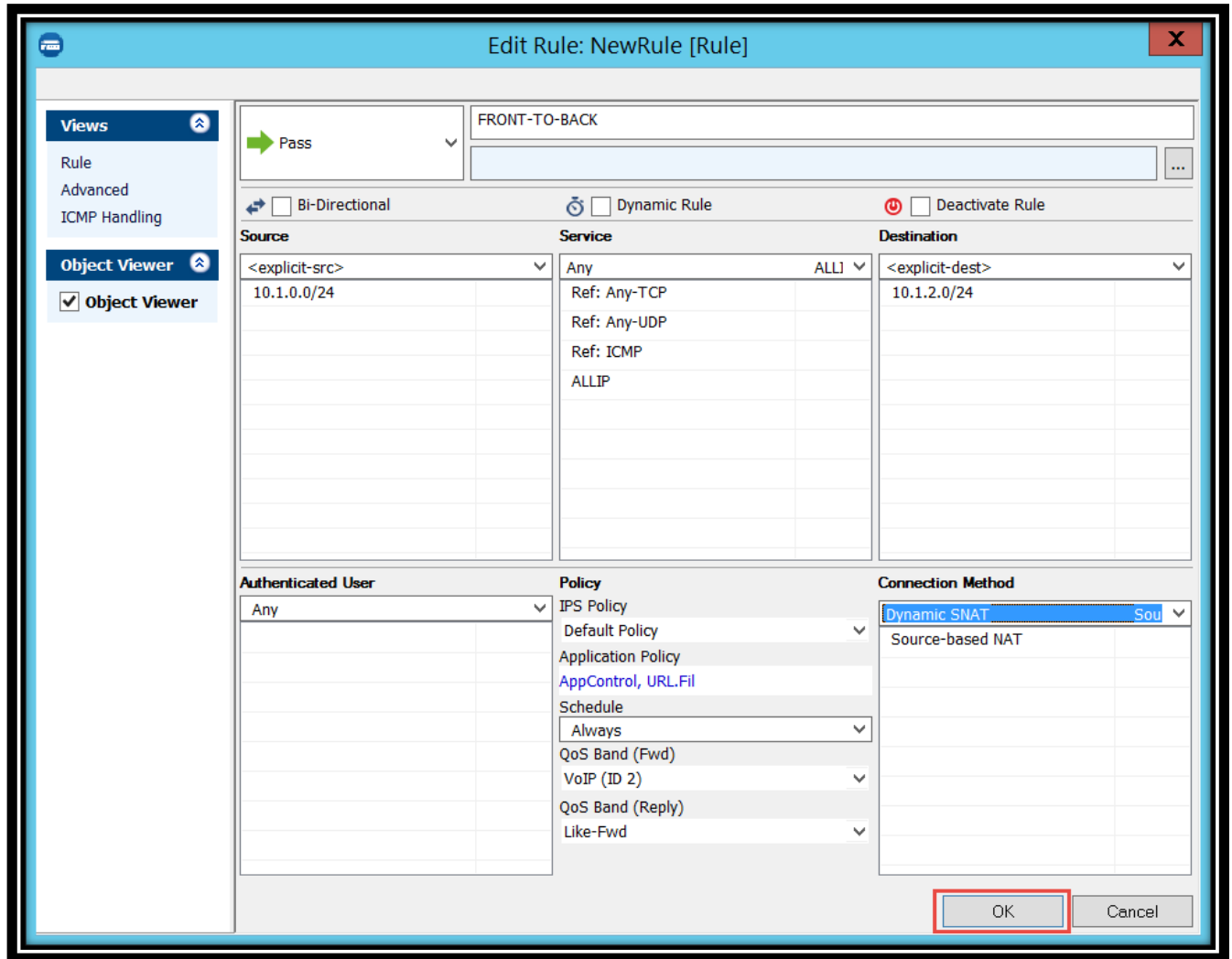
☐ Reference

Insert Insert and Close Close

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



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



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.

The screenshot shows the 'Forwarding Rules' pane in a network management interface. A list of rules is displayed, including 'Access Rules That Redirect DNS To The Caching DNS Service (1)', 'Access Rules that control traffic flows between the LAN (Trusted LAN), Internet, VPN Clients', and 'Access Rules that control traffic flows between the LAN (Trusted LAN), Internet, VPN Clients and remote Sites (9)'. A context menu is open over the rules, showing options like 'Move Up', 'Move Down', 'Select Overlapping', 'Hide inactive Rules', 'Show', 'Find', 'Select All', 'Deselect All', 'Expand All', 'Collapse All', 'Copy >AnyALLIP, ECHO, TCP *, TCP < to Clipboard', 'Copy List to Clipboard', 'Copy selected to Clipboard', 'Export to File', 'Print List', and 'Columns'.

Action	Name	Features	Service	Source	Destination	Application Policy
App Redirect	SETUP-MGMT-ACCESS	NGF-MGMT-BOX	Any	DHCP1	No AppControl	
App Redirect	SERVICE-VPN-ACCESS	Ref: NGF-VPN, Ref: HTTPS	Any	DHCP1	No AppControl	
Access Rules That Redirect DNS To The Caching DNS Service (1)	LOCALDNSCACHE	DNS	Trusted LAN	Any	No AppControl	
Access Rules that control traffic flows between the LAN (Trusted LAN), Internet, VPN Clients and remote Sites (9)	LAN-2-INTERNET	Any ALLIP, ECHO, TCP *, TCP...	Ref: Trusted LAN	Ref: Internet	AppControl, URL FI	
Pass	LAN-2-LAN	Any	Trusted LAN	Trusted LAN	AppControl, URL FI	
Pass	LAN-2-VPN-SITE	Any	Trusted LAN	VPN-Networks	No AppControl	
Pass	VPN-SITE-2-LAN	Any	VPN-Networks	Trusted LAN	No AppControl	
Pass	VPN-SITE-2-SITE	Any	VPN-Networks	VPN-Networks	No AppControl	
Pass	VPNCLIENTS-2-LAN	Any	VPN-Clients	Trusted LAN	No AppControl	
Pass	VPNCLIENTS-2-SITE-VPN	Any	VPN-Clients	VPN-Networks	No AppControl	
Pass	FRONT-TO-BACK	Any	10.1.0.0/24	10.1.2.0/24	AppControl, URL FI	
Block	BLOCKALL	Any	Any	Any	N.A.	

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

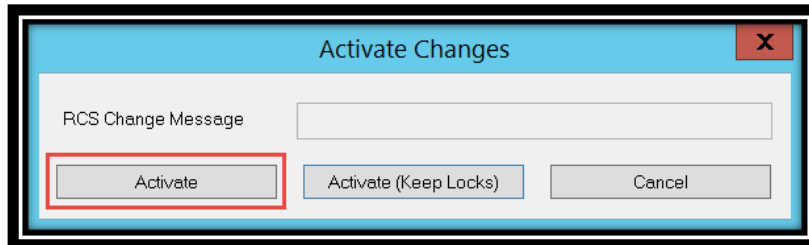
The screenshot shows the 'Forwarding Rules' pane with the 'Send Changes' button highlighted in the upper right corner. The pane displays a list of rules, including 'Access Rules That Redirect DNS To The Caching DNS Service (1)', 'Access Rules that control traffic flows between the LAN (Trusted LAN), Internet, VPN Clients and remote Sites (9)', and 'Access Rules that control traffic flows between the LAN (Trusted LAN), Internet, VPN Clients and remote Sites (9)'. The 'Send Changes' button is located in the top right corner of the pane.

Action	Name	Features	Service	Source	Destination	Application Policy
Access rule required to enable access to preconfigured Management and Service IP via a dynamically assigned DHCP-IP (2)	SETUP-MGMT-ACCESS	NGF-MGMT-BOX	Any	DHCP1	No AppControl	
App Redirect	SERVICE-VPN-ACCESS	Ref: NGF-VPN, Ref: HTTPS	Any	DHCP1	No AppControl	
Access Rules That Redirect DNS To The Caching DNS Service (1)	LOCALDNSCACHE	DNS	Trusted LAN	Any	No AppControl	
Access Rules that control traffic flows between the LAN (Trusted LAN), Internet, VPN Clients and remote Sites (9)	LAN-2-INTERNET	Any ALLIP, ECHO, TCP *, TCP...	Ref: Trusted LAN	Ref: Internet	AppControl, URL FI	
Pass	LAN-2-LAN	Any	Trusted LAN	Trusted LAN	AppControl, URL FI	
Pass	LAN-2-VPN-SITE	Any	Trusted LAN	VPN-Networks	No AppControl	
Pass	VPN-SITE-2-LAN	Any	VPN-Networks	Trusted LAN	No AppControl	
Pass	VPN-SITE-2-SITE	Any	VPN-Networks	VPN-Networks	No AppControl	
Pass	VPNCLIENTS-2-LAN	Any	VPN-Clients	Trusted LAN	No AppControl	
Pass	VPNCLIENTS-2-SITE-VPN	Any	VPN-Clients	VPN-Networks	No AppControl	
Pass	FRONT-TO-BACK	Any	10.1.0.0/24	10.1.2.0/24	AppControl, URL FI	
Block	BLOCKALL	Any	Any	Any	N.A.	

32. Click **Activation Pending**.



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

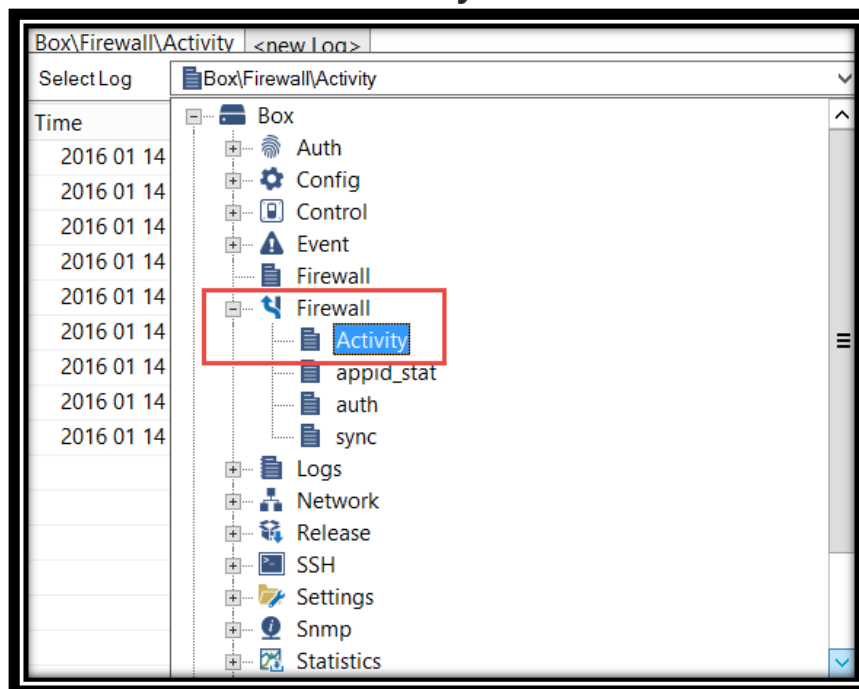


Validate Lab Completion

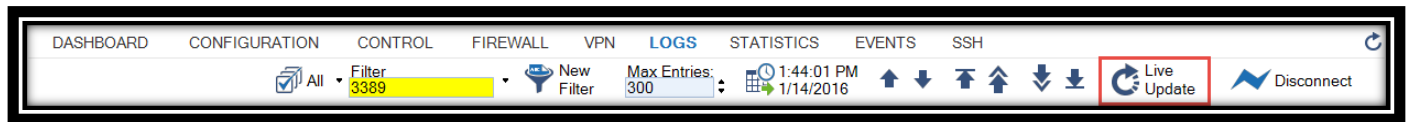
In this task, you will create a Remote Desktop Connection from **DemoVM0** to **DemoVM2** through the Barracuda appliance and capture the Log Files containing entries representing a successful RDP session as proof you completed this lab.

Please save your lab screenshots as either a .jpeg or .png. Upload your screenshots in one .zip file [here](#).

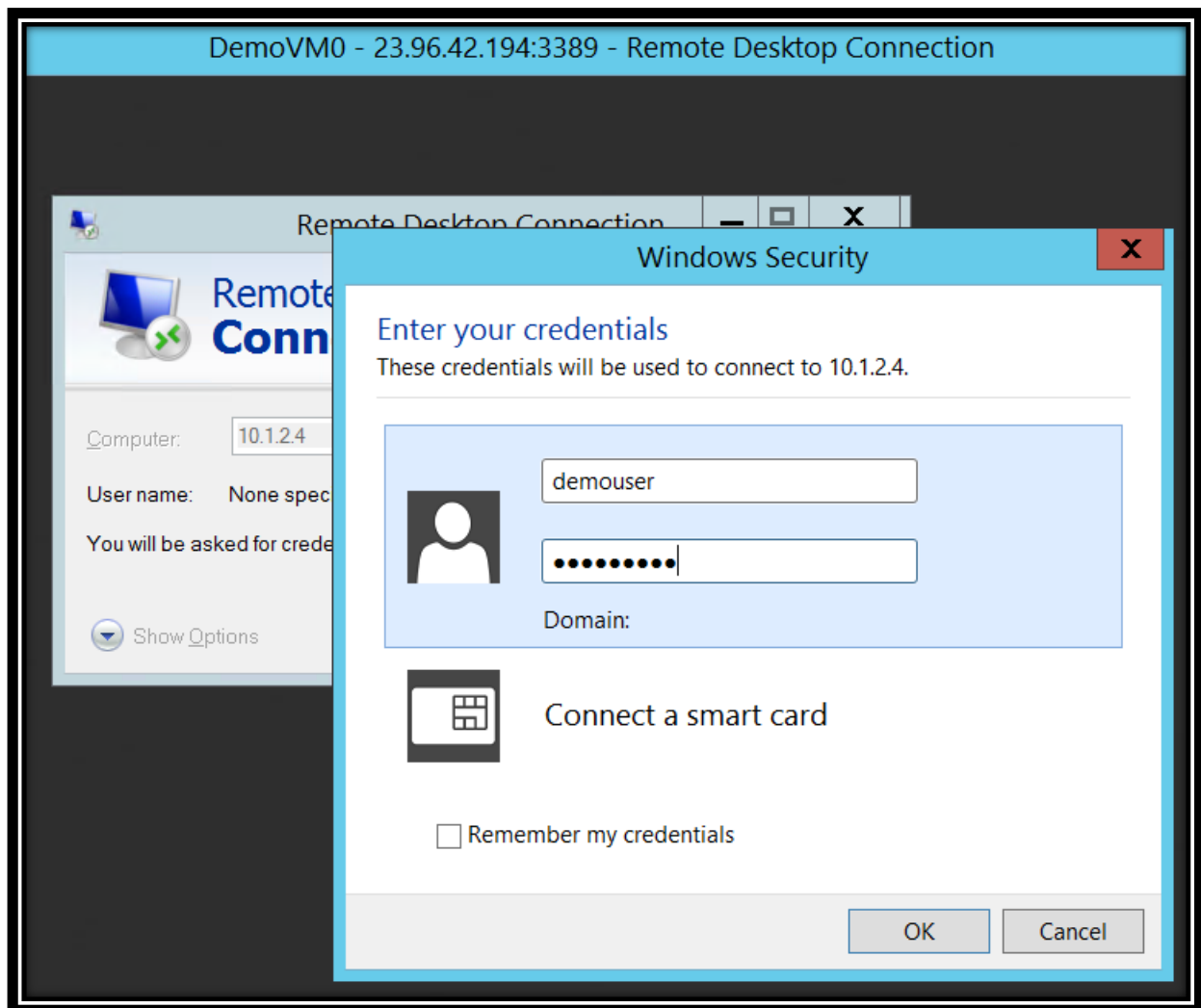
1. In the **Barracuda NG Admin 6.2** interface, click **LOGS**, and, in the **Select Log File** select **Box\Firewall\Activity**.



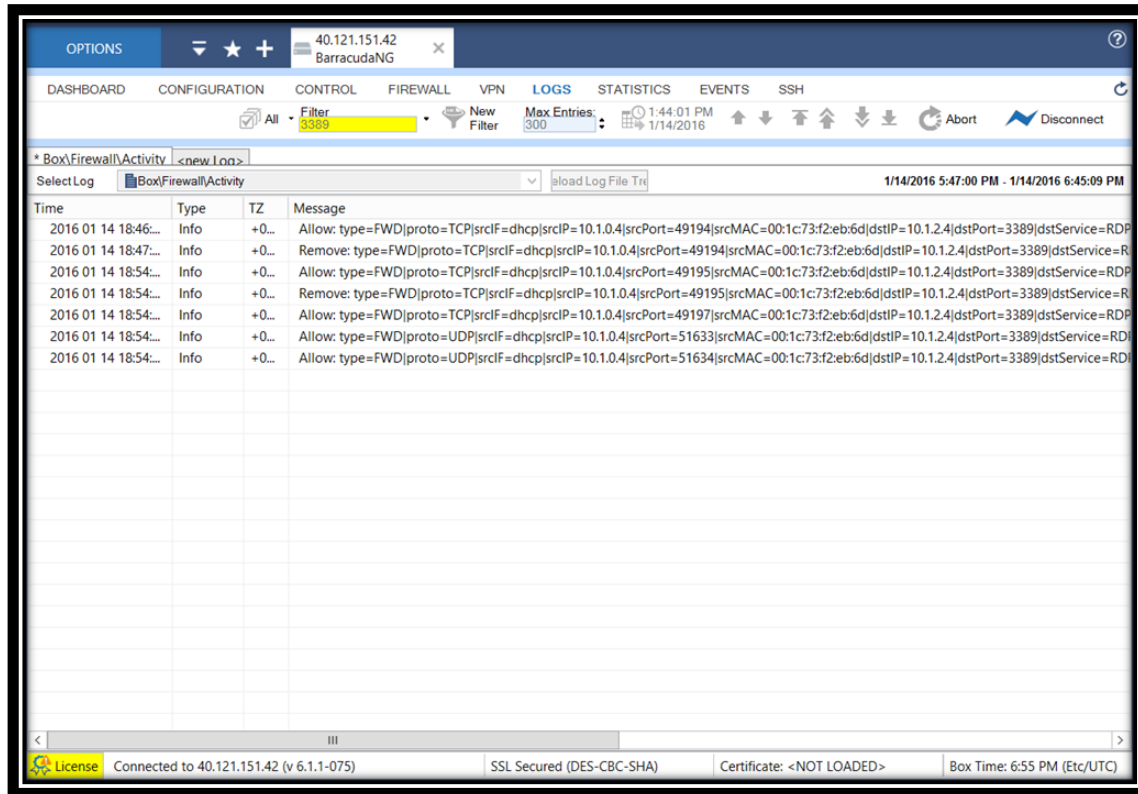
2. In the toolbar of the **LOGS** window, in the **Filter** text box, type in **3389** and click **Live Update**.



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.



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.