Next Generation Data Center Security

vSEC for Azure Training Cookbook

Ver. 3.6

Table of Contents

Introduction: 2
vSEC for Azure training environment: 4
Exercise #1 – Build an Azure private environment (VNET) 8
Exercise #2 - Deploy Check Point Management on Azure 11
Exercise #3 - Deploy Check Point Gateway on Azure 18
Exercise #4 – Creating a web server 27
Exercise #5 – Connecting vSEC Controller 44
Exercise #6 – Advanced scenarios 49
Appendix #1 – SPN definitions 50

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

Introduction:

Organizations are starting to adopt public cloud environments as an extension of their internal Data Centers (DC) to gain operational flexibility and lower operational costs. The increasing number of applications in the DC has led to a dramatic increase in network traffic between the different servers / application inside the DC (east-west traffic).
However, when it comes to security, the focus has been on protecting the entrance to the DC, the perimeter, and there are few controls to secure east-west traffic inside the data center. That current security status presents a critical security risk where threats can traverse unimpeded once inside the data center. Furthermore, traditional security approaches to this problem are unable to keep pace with the dynamic network changes and rapid provisioning of applications in a cloud environment.

Check Point vSEC For Azure will allow you to deal with that security risk and minimize it to the minimum.

This document will provide you with getting started steps required to get familiar with the Azure environment & how to deploy a basic day to day scenario with vSEC in place. You will understand and simulate a real-life use case to grasp the ease of deploying automated advanced security protections within the Azure cloud.
We have prepared a few simple to follow exercises, to illustrate the benefits of having security integrated into a virtual networking platform. Those exercises are incremental; they start from basic setup and progress into more advanced scenarios.

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

Securing Next Generation Data Center Hands-on lab Objectives:

The target of this hands-on lab exercises is to provide you with practical real-life experience with Check Point's vSEC For Azure product.

The objectives of the hands-on training are:

1. Prepare your Public Cloud environment for deployment
   This exercise is meant to get you familiar with the Azure portal & concepts.

2. Deploy Check Point R80.10 management server on Azure
   The exercise will show you how to deploy R80.10 Management server & vSEC controller on your newly created environment on Azure. Also you will learn how to launch new web servers from the marketplace.

3. Deploy Check Point vSEC Gateway on Azure
   This exercise will demonstrate to you how to deploy a vSEC gateway into your Azure environment to improve transparency and enforcement of network traffic traversing through/from the environment.

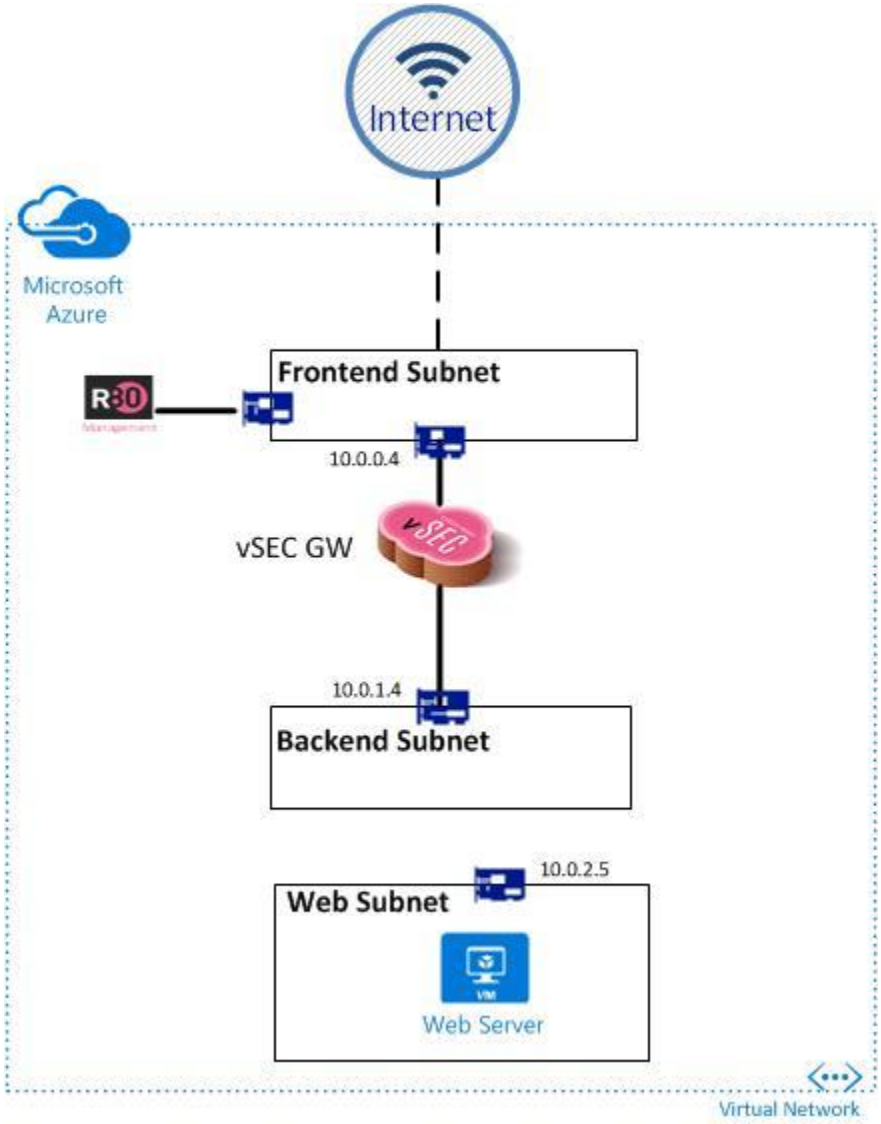
4. Configuring vSEC Controller
   In this exercise you will configure the controller to connect into your account in Azure.

5. Optional Advanced troubleshooting
   This optional exercise will teach you how to do basic debugging & validate that your gateway is running as designed.

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

vSEC for Azure training environment:

Getting to know your training environment

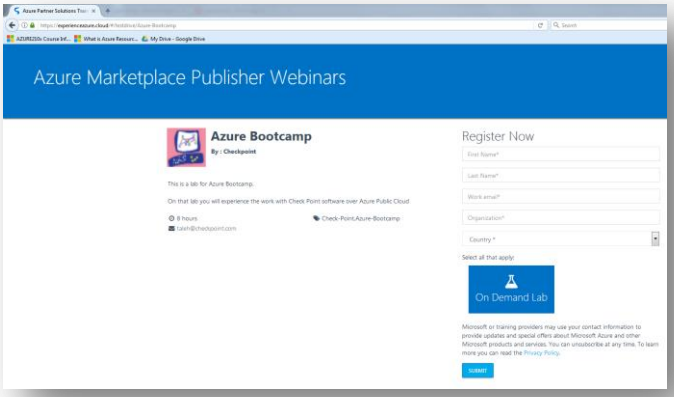


	IP address
vSEC GW – FrontEnd	10.0.0.5 (auto assigned by Azure)
vSEC GW - BackEnd	10.0.1.4 (auto assigned by Azure)
SmartCenter Server	10.0.0.4 (auto assigned by Azure)
Web Server	10.0.2.x (auto assigned by Azure)

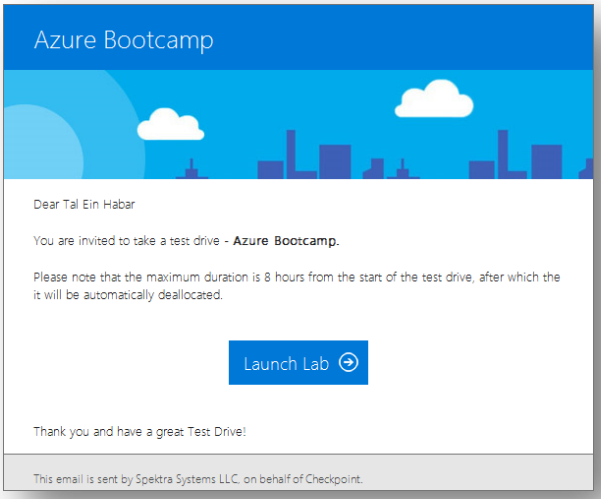
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

Connecting and setting up your work environment:

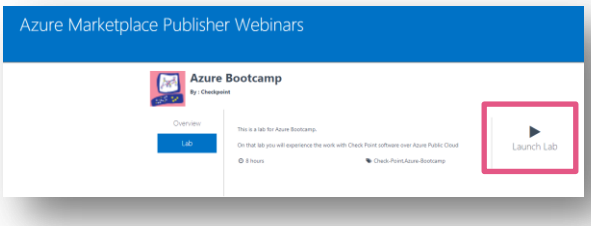
1. **Connect into the link that your trainer has provided for you.**



2. **Fill in your details for registration and click Submit.**
3. **You will see a message that approves your registration.**
4. **After 1 minute you will get an email that will start your lab**

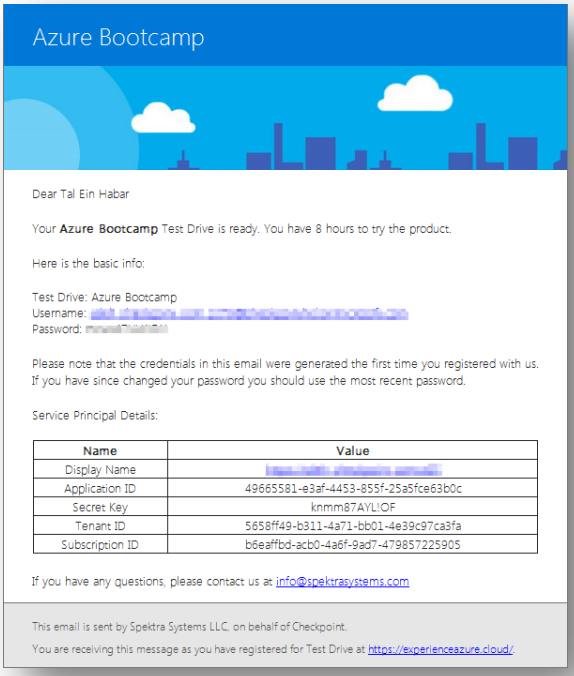


5. **Click on the "Launch Lab" button**
6. **An browser window will open automatically, Click on the "Lab" button at the left side and then "Launch Lab"**



7. **After 2 minutes you will get an email with your credentials for this session (the session is active for 12 hours)**

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



Azure Bootcamp

Dear Tal Ein Habar

Your **Azure Bootcamp** Test Drive is ready. You have 8 hours to try the product.

Here is the basic info:

Test Drive: Azure Bootcamp
Username: [redacted]
Password: [redacted]

Please note that the credentials in this email were generated the first time you registered with us.
If you have since changed your password you should use the most recent password.

Service Principal Details:

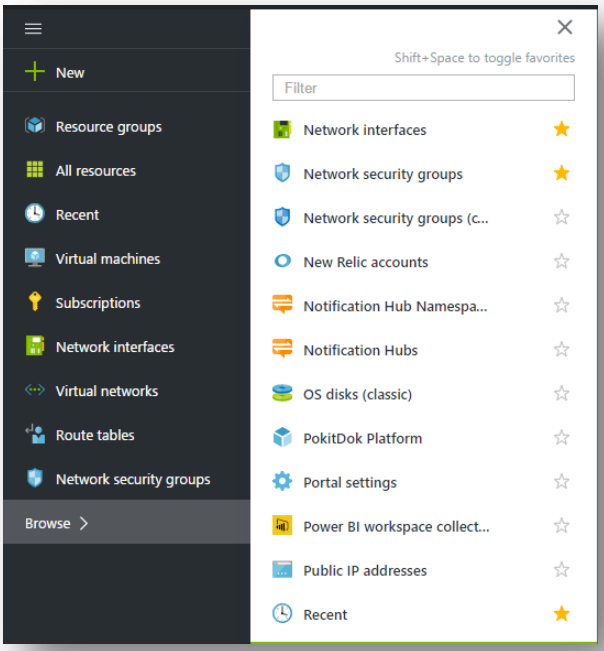
Name	Value
Display Name	[redacted]
Application ID	49665581-e3af-4453-855f-25a5fce63b0c
Secret Key	knmm87AYL!OF
Tenant ID	5658ff49-b311-4a71-bb01-4e39c97ca3fa
Subscription ID	b6eaffbd-acb0-4a6f-9ad7-479857225905

If you have any questions, please contact us at info@spektrasystems.com

This email is sent by Spektra Systems LLC, on behalf of Checkpoint.
You are receiving this message as you have registered for Test Drive at https://experienceazure.cloud/.

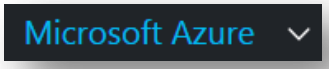
8. **Connect to Microsoft Azure portal using the following link https://portal.azure.com/ and using the credentials you got in the last email.**
9. **You will be asked to change your password.**
10. **Add shortcuts to dashboard main screen**
11. **On the left pane of the main portal window, click on Browse and search for the following services (one by one) and click on the star next to the service:**
    a. **Resource Groups**
    b. **All Resources**
    c. **Virtual Networks**
    d. **Virtual Machines**
    e. **Network Security Groups**
    f. **Network interfaces**
    g. **Route Tables**
    h. **Subscriptions**
    i. **Recent**

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



Naturally, you can add any desired service from that window and also set its location on the bar at your convenience (just drag and drop it).

12. **Take a few minutes to review Azure's different services (understanding the full breadth of the service offering).**
13. **Feel free to wander around those services (by clicking on them and reviewing their "landing page")**
14. **When you're done, go back to the portal home page by clicking on the blue "Microsoft Azure" text on the left top corner of the screen**



15. **Please progress to the next exercise where we will be preparing our environment for use.**

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

Exercise #1 – Build an Azure private environment (VNET)

Description

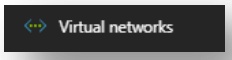
This exercise will guide you through the steps required to setup your own private Azure environment to which we will be deploying our virtual machines.

Method

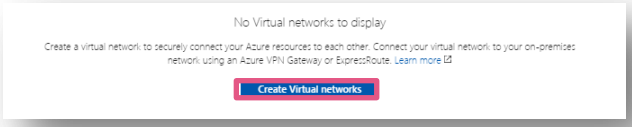
Using Azure portal you will create a new VNET (Virtual dedicated environment) in a designated region. You will then create subnets within that environment. This newly created environment will be used in later exercise as new virtual machines will be provisioned into the environment.

How

1. On the left side bar choose “virtual networks”

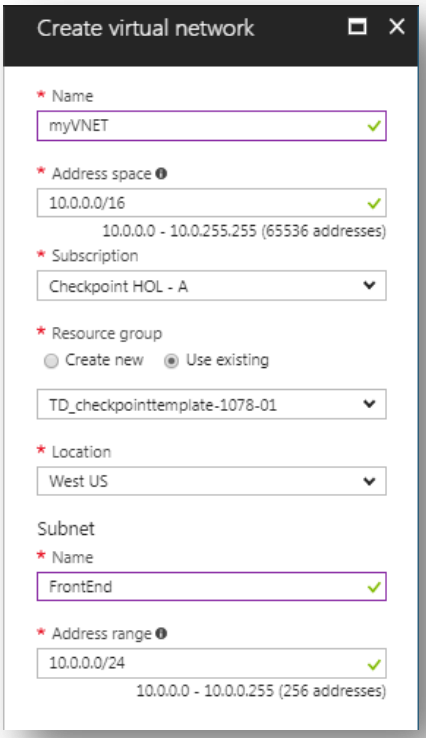


2. At the bottom of the window that appears, click “Create Virtual Networks”



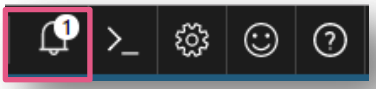
3. In the window that appear fill in the fields as describe below,

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

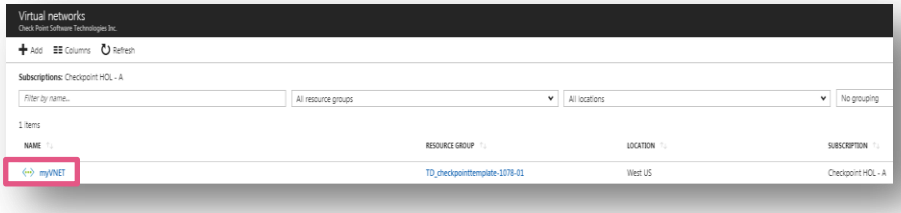


a. Pick a name for the newly created VNET (e.g. myVNET)
b. Set the VNET address space (make sure to change the mask to /16)
c. Leave subscription as is
d. Change Resource Group to “use existing” and choose the first one.
e. Pick the location where the VNET is to be created (any Europe or US will do)
f. Pick a name for the subnet that will be created inside the VNET (e.g. FrontEnd)
g. Pick an address range for the above subnet (leave its default value for our exercise)
h. Click on “Create”

4. The deployment process will now run, you can track its running status by clicking the bell icon on the upper right corner of the screen (as shown)



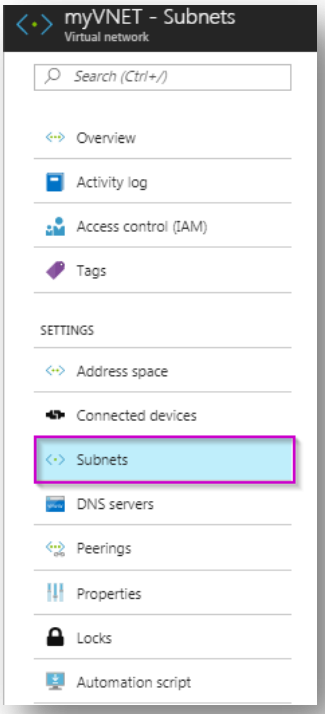
5. Once deployment is successful, lets add another subnet which will represent our “BackEnd” network (where our web server will be provisioned)



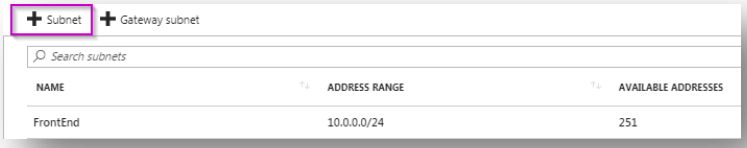
Click on the newly created VNET.

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

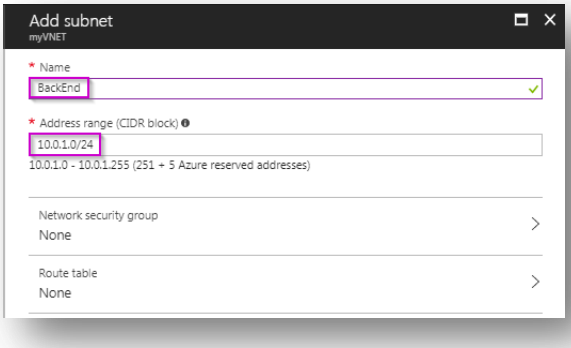
6. Click on “subnets” on the window that appears



7. And then choose to add a new subnet by clicking on



8. Choose a name for the new subnet (e.g. BackEnd) and specify its address range (10.0.1.0/24), leave the rest as is.



Click “OK” to create the subnet.

You have finished exercise 1

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

Exercise #2 - Deploy Check Point Management on Azure

Description

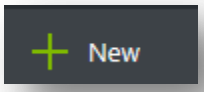
This exercise will guide you through the installation and configuration of Check Point's R80 SmartCenter Server in the environment you created on the former exercise.

Method

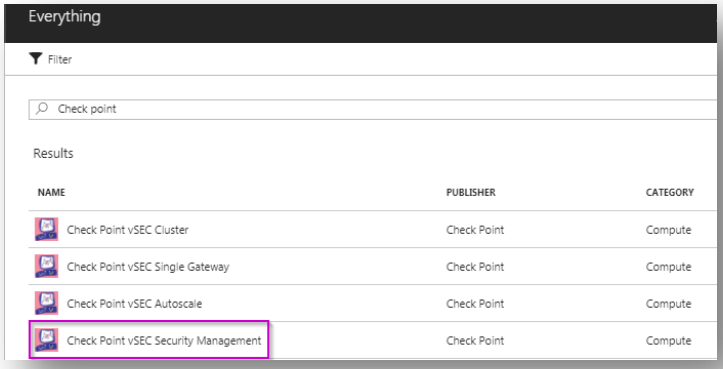
Using Azure portal and the preconfigured templates, you will provision the latest R80 management server to manage the GW's that will control the traffic in your Azure public cloud environment.

How

1. From the Azure portal, click on "New" on the left pane



   In the window that appears, write "check point" in the search box and press enter
2. Choose "Check Point vSEC Security Management" (as shown)

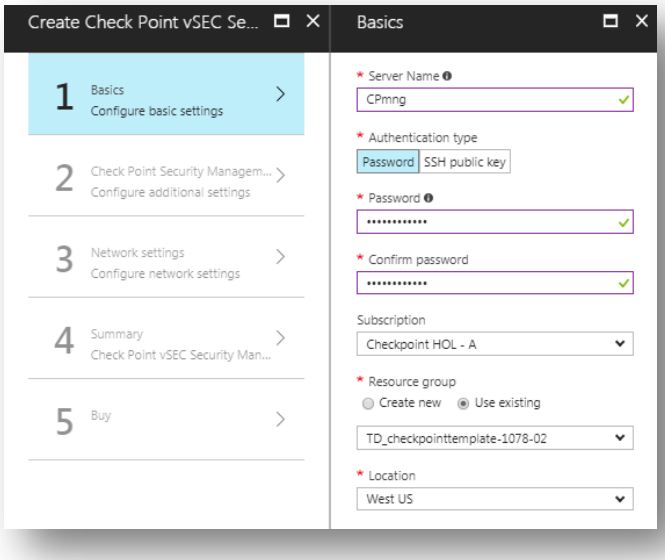


   And in the new window that opens, click on "Create".

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

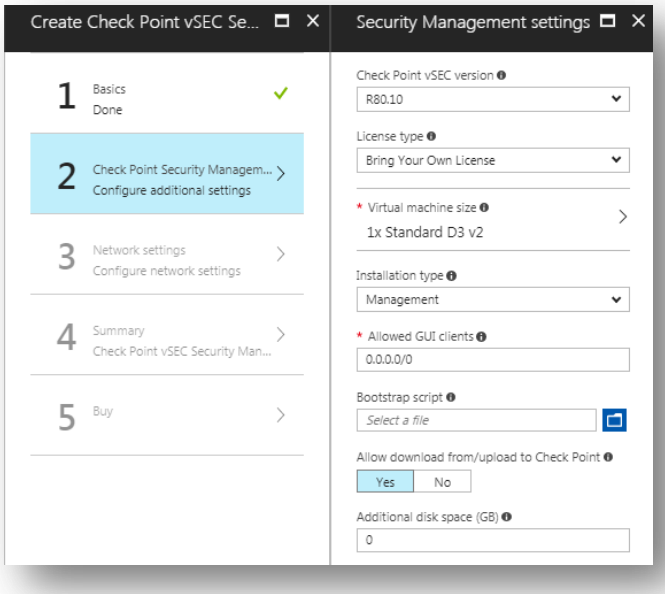
On the next section, we will fill in the details for the management server in the solution template

3. In the next window, fill in the management



Name: CPMng
Password: Choose your own
Subscription: Leave as is
Resource Group: use existing base (the second in the list)
Location: Use the same location as the previous exercise (VNET creation).
When you are done, please click on “ok”.

4. The next window, fill in the fields,

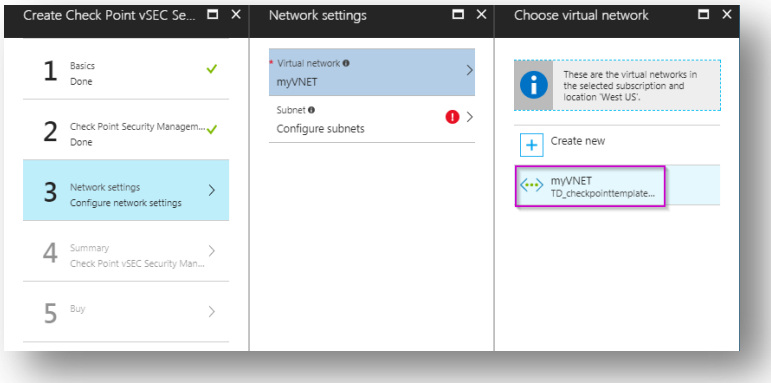


©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

Check Point vSEC version: R80.10
Virtual Machine size: Leave virtual machine size as is (or choose smaller one if instructed to do so).
Installation Type: Management
Leave all the rest as is

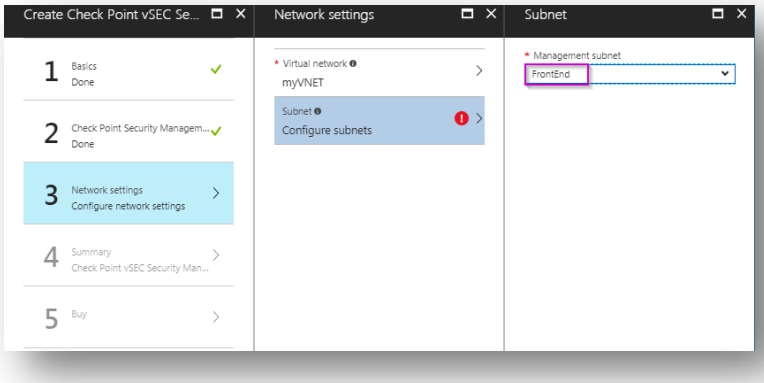
Click OK

5. In the Network setting window (which appears),



Virtual Network: choose virtual network and pick the VNET that we've created in exercise #1.

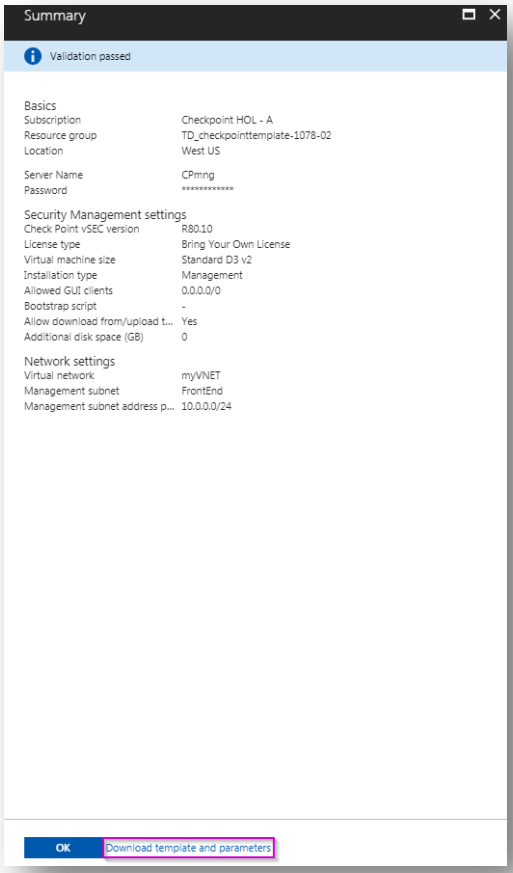
Next, click on subnets and choose the FrontEnd subnet we've created in previous exercise (as shown)



When you're done, click on "ok" and then another "ok" to move to the next stage.

6. Make sure that Azure has verified your settings.

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

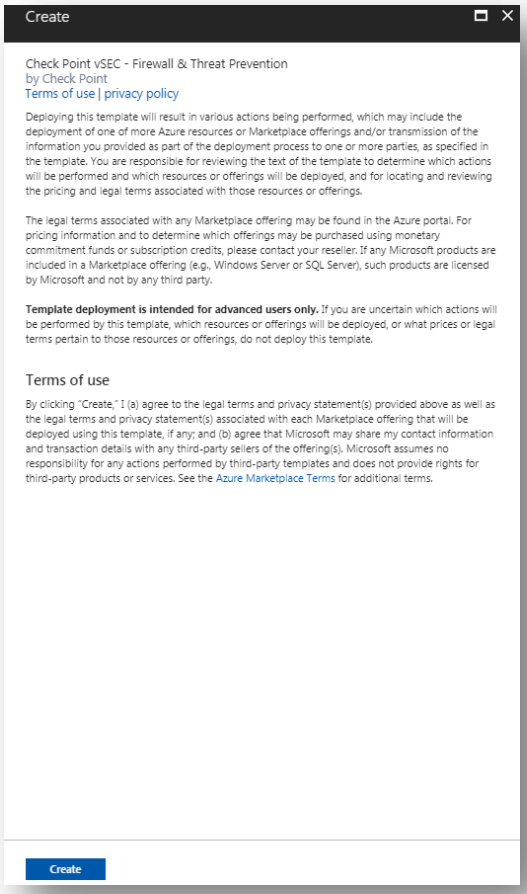


On that stage you can save the template and information as a backup for later use in your account.

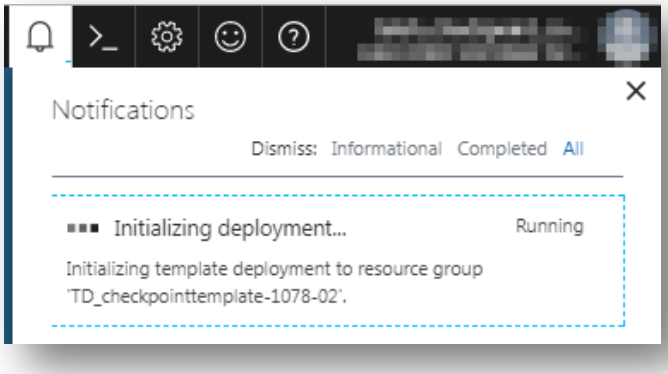
Click OK

7. The last stage, before the management server will actually be installed, you will be presented with Terms of use and license agreement. Review and press “create” (assuming you agree with the terms of course)

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

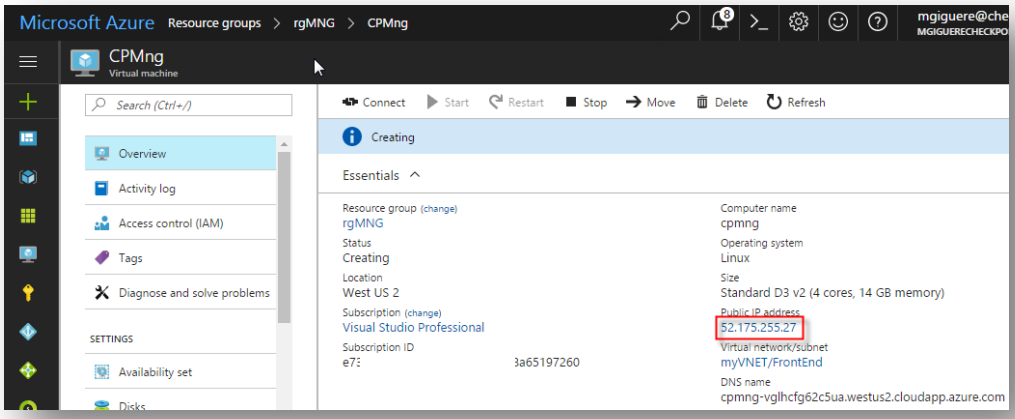


8. The management server will now be created. You should be able to see creation progress by clicking on the bell icon on the top right corner of the screen

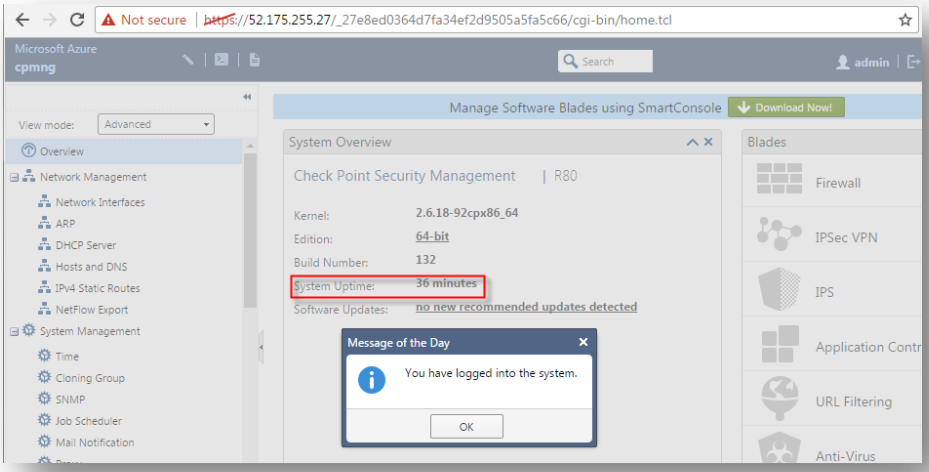


9. This process takes about 30 minutes, jump to exercise 3 and return afterword.
10. After the deployment is finished, connect via https to the IP address of the new machine (can be found under the created Resource group name and Virtual Machine CPmng):

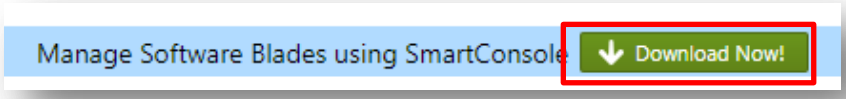
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



11. Confirm the first time wizard is completed before continuing with the next step by insuring the System Uptime in the GAiA web ui is over 5 minutes.



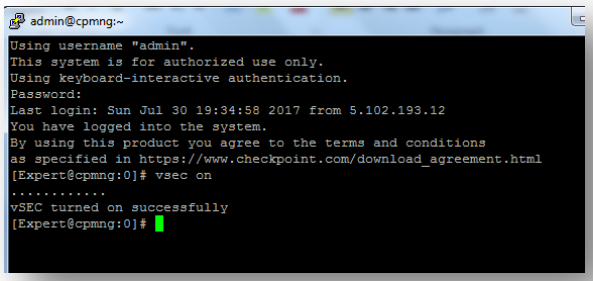
12. If you don't already have Check Point R80.10 SmartConsole, download it from the link on the upper central screen:



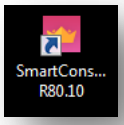
Install it with the default configuration (make sure it's R80.10 smart console).

13. Open a SSH session to the Management server (same address as the web GUI)
14. Run command "vsec on"

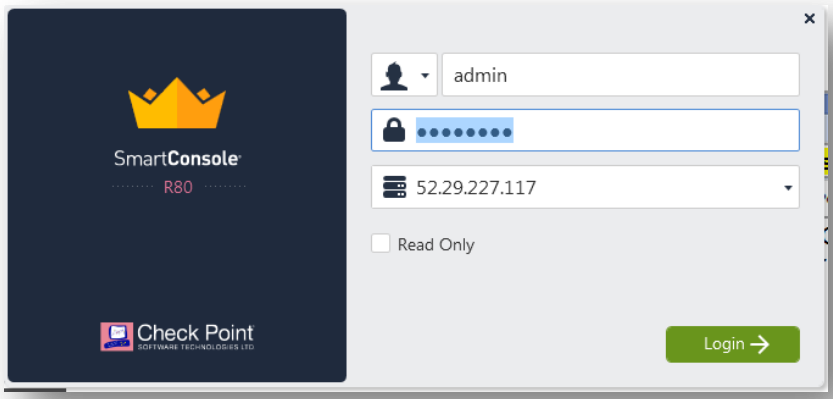
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



15. Connect to the SmartCenter server using R80.10 SmartConcole GUI client on your laptop (use the admin credentials you created during the setup)



16. Fill in the relevant information (e.g. username/password and the same public IP) and click on login



17. Wander around and inspect the GUI and make yourself familiar with its options.

You have finished exercise 2

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

Exercise #3 - Deploy Check Point Gateway on Azure

Description

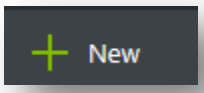
This exercise will guide you through the installation and configuration of Check Point's vSEC gateway on the environment created in Azure.

Method

Using Azure portal preconfigured templates, you will provision the latest vSEC gateway to protect workloads deployed on your Azure public cloud environment

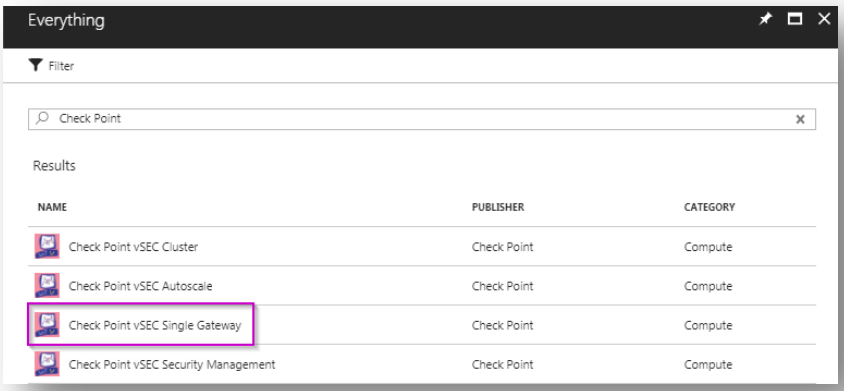
How

1. From the Azure portal, click on "New" on the left pane



In the window that appears, write "check point" in the search box and press enter

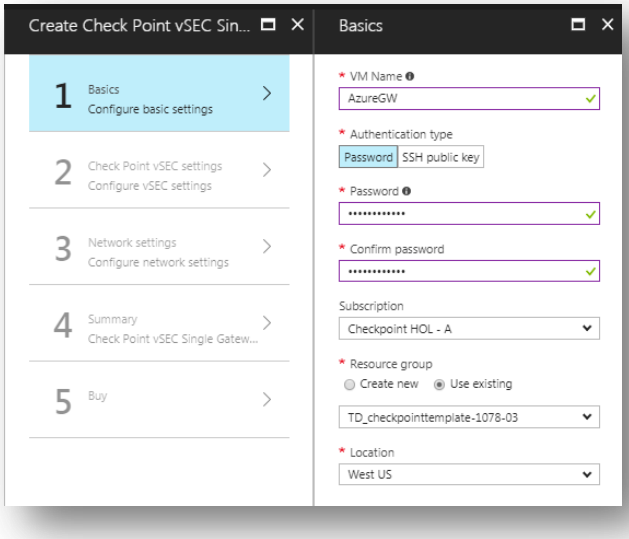
2. Choose "Check Point vSEC Single Gateway" (as shown)



And then click on "create"

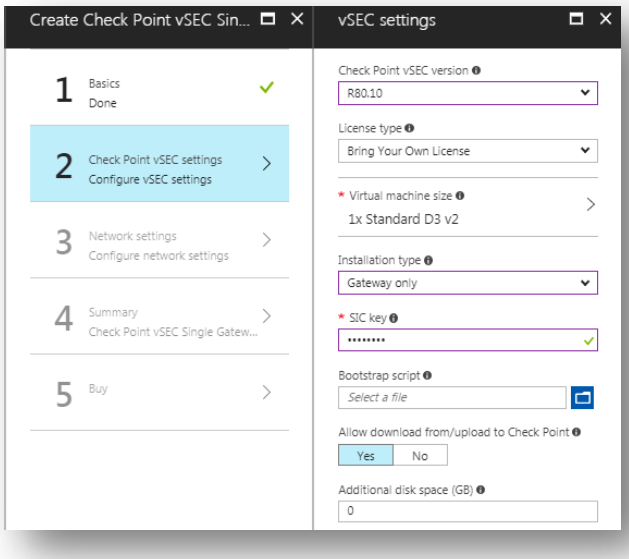
1. In the next window, fill in the gateway details as described below.

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



VM Name: AzureGW
Password: Choose your own
Subscription: Leave as is
Resource Group: use existing, choose the third one on the list
Location: use the same Location as in exercise 1
When you are done, please click on “ok”

3. In the Network setting window (which appears), fill in the details as listed below.

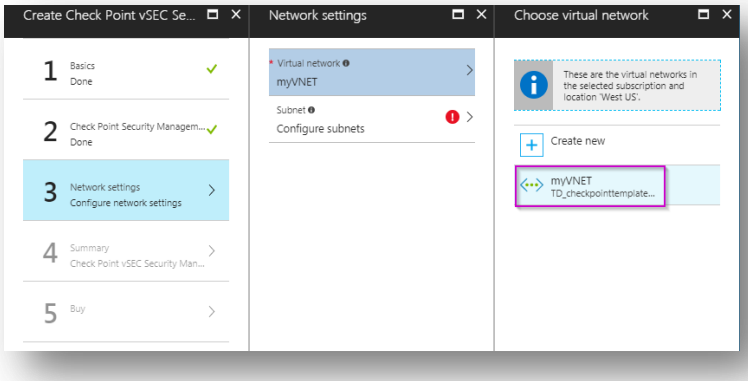


Check Point vSEC version: R80.10
License Type: Bring Your Own License
Virtual Machine: change to D3 v2 size (find out how)
Installation type: Gateway Only
SIC Key: Choose your own
Don’t change the bootstrap script or the disk size.

Click OK

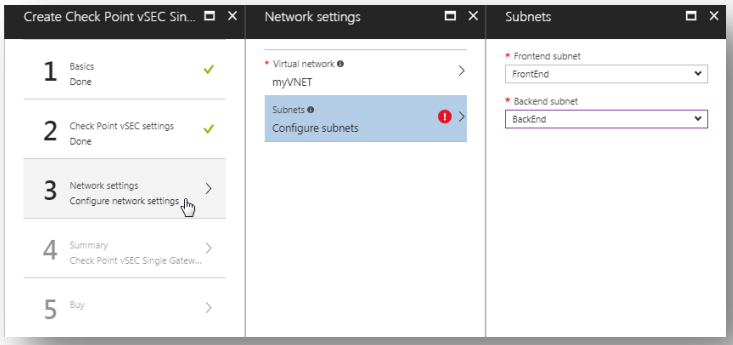
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

18. In the Network setting window (which appears),



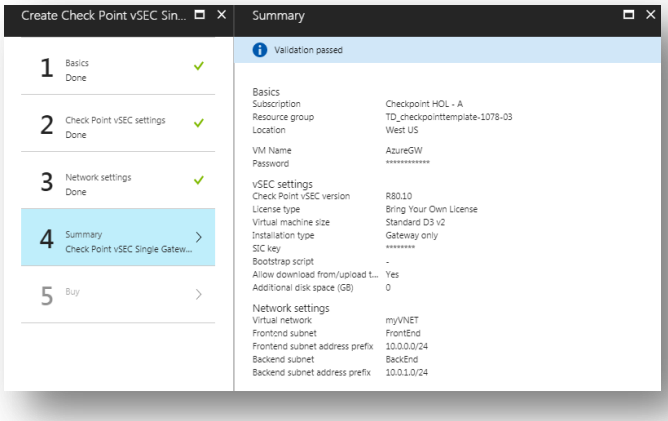
Virtual Network: choose virtual network and pick the VNET that we've created in exercise #1.

Next, click on subnets and pick the right subnets accordingly (Change the backend subnet to backend)



When you're done, click on "ok" and then another "OK" to move to the next stage.

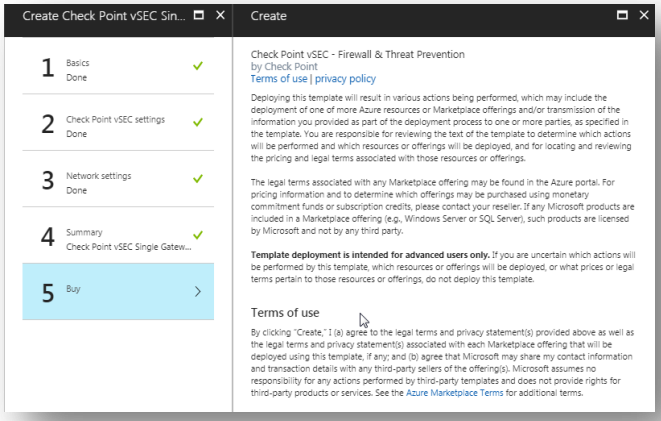
4. The gateway configuration validation window appears, review the configuration and then press on "ok".



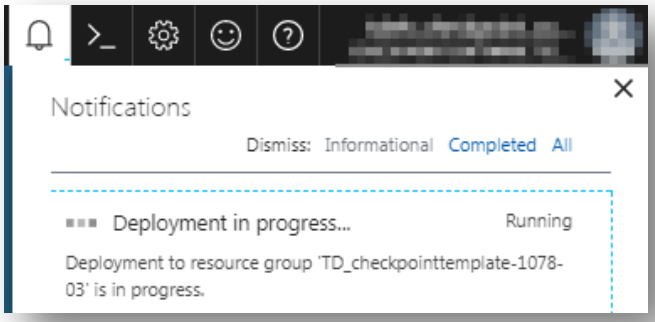
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

On that stage you can save the template and information as a backup for later use in your account.

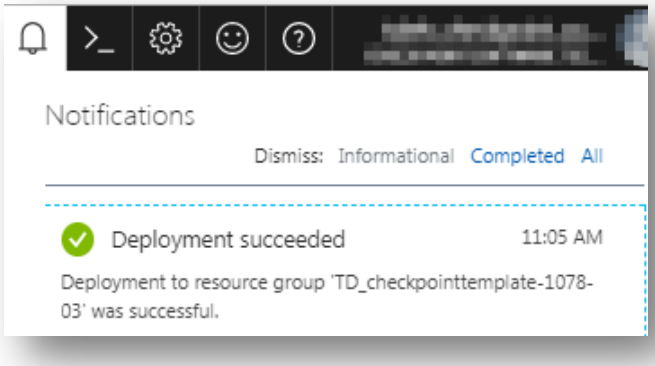
5. The last stage, before the vSEC gateway is actually being installed, you will be presented with Terms of use and license agreement. Review and press “Create” (assuming you agree with the terms of course)



6. The gateway will now be created. You should be able to see creation progress by clicking on the bell icon on the top right corner of the screen (as shown)



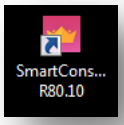
7. When deployment is done, you should see the following message (by clicking on the bell icon on the top right corner)



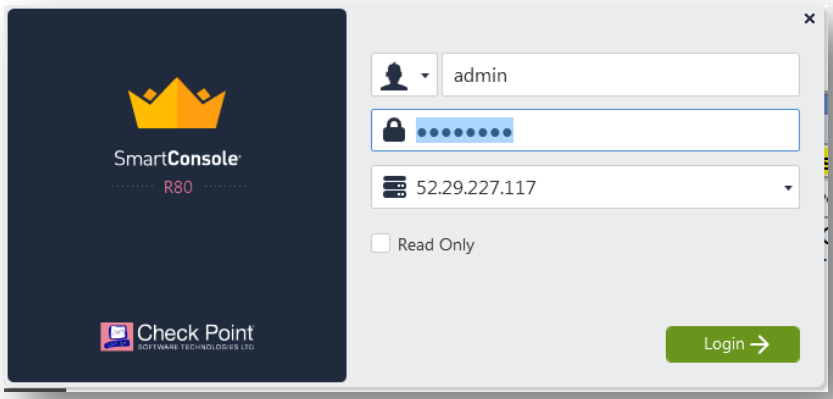
19. Go back to exercise 2 section 10 to finish the exercise before you continue.

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

20. Connect to the SmartCenter server using R80.10 SmartConcole GUI client on your laptop (use the admin credentials you created during the setup)

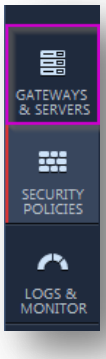


21. Fill in the relevant information (e.g. username/password and the same public IP) and click on login



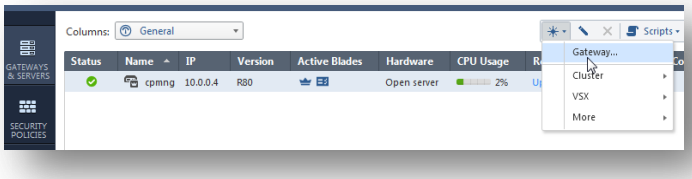
8. Create the gateway object on SmartConsole and follow the wizard to add the gateway nodes and create trust connectivity between them.
   Note: you can use sk109360 for help configuring that stage.

   a. Click on the gateway & services on the left side of the screen

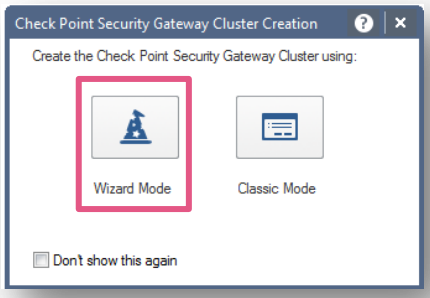


   b. In the upper middle of the screen choose to add new Gateway object

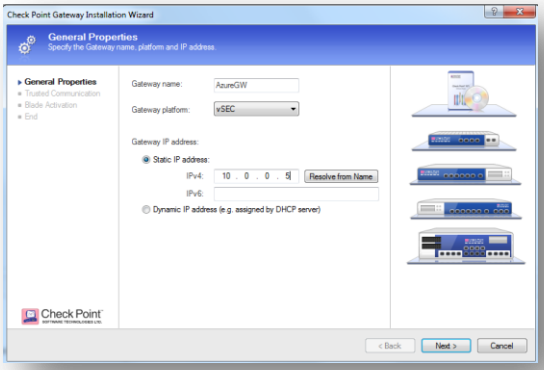
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



c. On the box that opened choose wizard mode



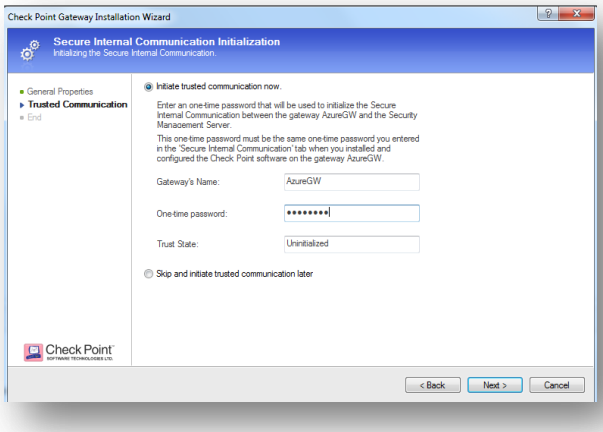
d. Fill in the details as listed below:



Gateway name: AzureGW
Gateway Platform: vSEC
Static IP address: 10.0.0.5
Click Next

e. Fill in the connection details between the management server and the gateway:

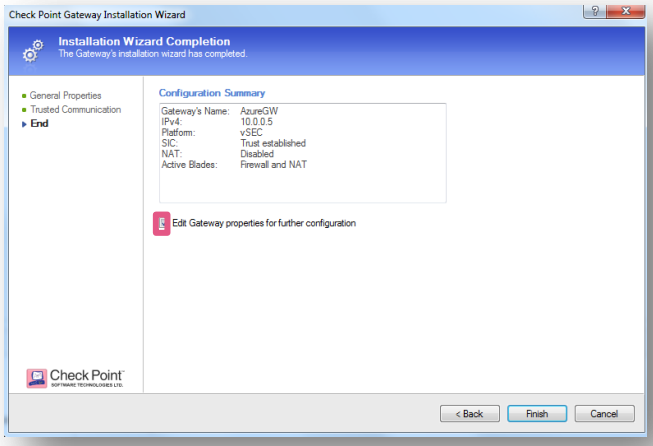
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



Gateway name: AzureGW
One-Time password: the one that you defined on step 3

Click Next

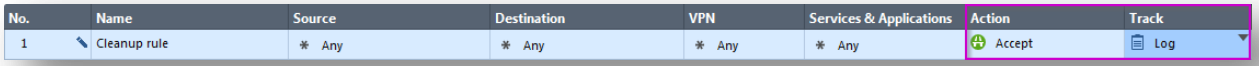
f. Make sure the gateway has the 2 nic's and Click Close
g. Review configuration, uncheck the tag and click Finish



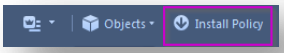
9. Once gateway configuration is done, on the left bar choose security Policies

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

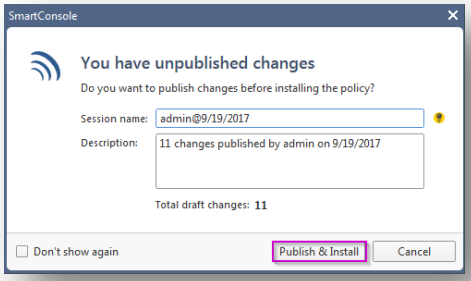
10. Change the existing rule to allow all traffic by changing the action to accept and adding Log



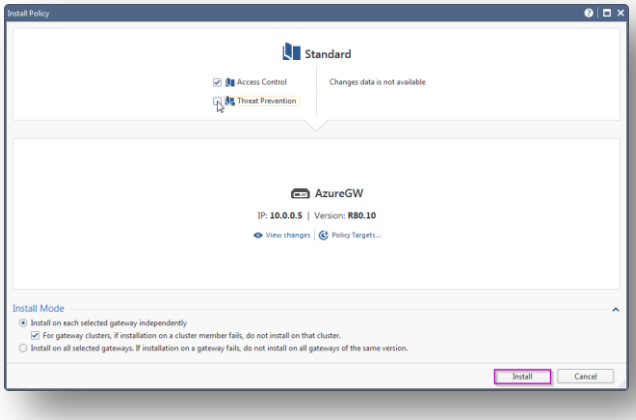
11. On the upper left side click Install policy



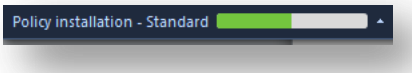
a. Click the Publish & Install



b. In the opened screen uncheck the Threat prevention and click Install

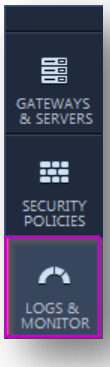


c. You can see the progress on the bottom left side

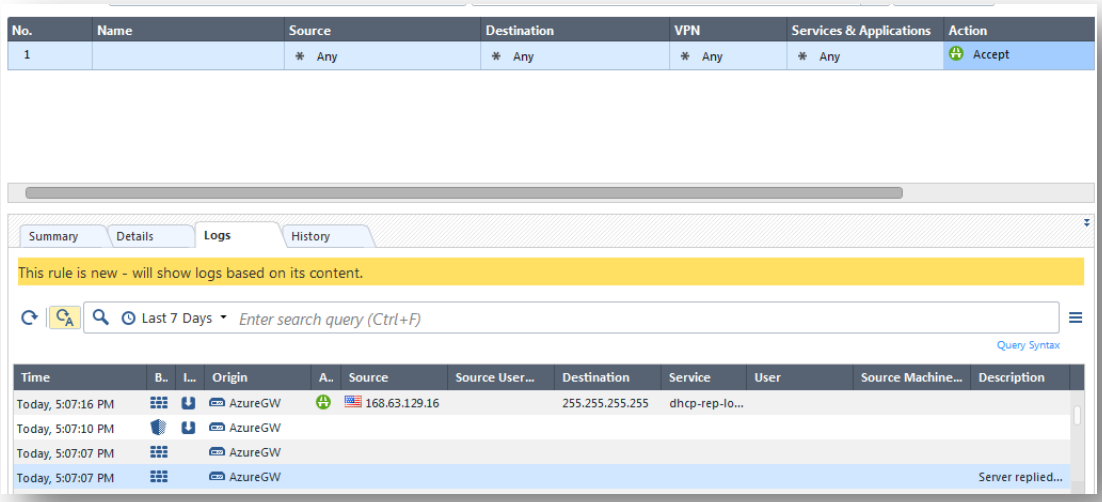


12. on the left bar choose security Policies

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



13. Verify that security policy is installed correctly and make sure you see logs originating for the gateway.



You have finished exercise 3

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

Exercise #4 – Creating a web server

Description

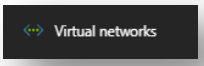
This exercise will guide you through the installation and configuration of a simple web server into the environment we created in previous exercises. This web server will then be protected by the firewall gateway (controlling traffic to/from it)

Method

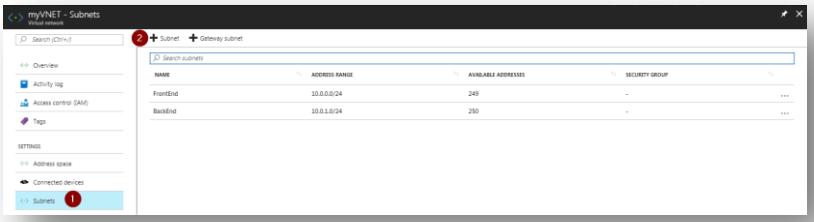
Using Azure portal, you will provision a web server and place it inside the environment (behind the firewall)

How

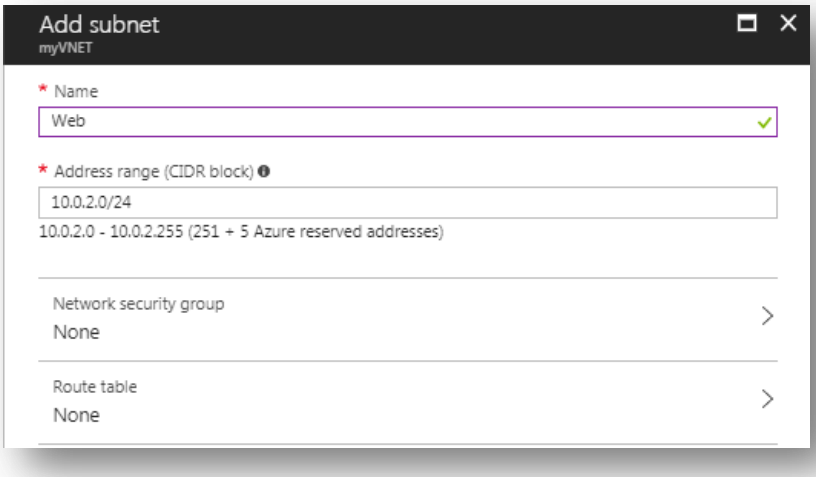
1. We will now create a new subnet which will be used for the Web server (call it “web”). This is done (we can also use an existing subnet although it is not recommended for our purpose) to demonstrate the use of UDR inside the environment
2. From the VNET page



3. Choose myVNET (1) then click on “+ Subnets” (2) to add a new subnet



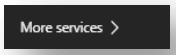
4. Name the subnet “web” and allocate the following IP range to is (10.0.2.0/24)



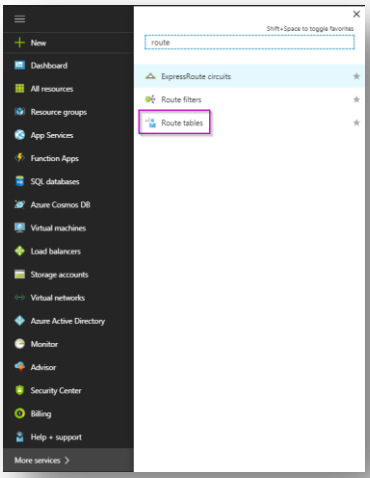
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

Now let’s add a route which will force all traffic originating from that new subnet to go through our firewall.

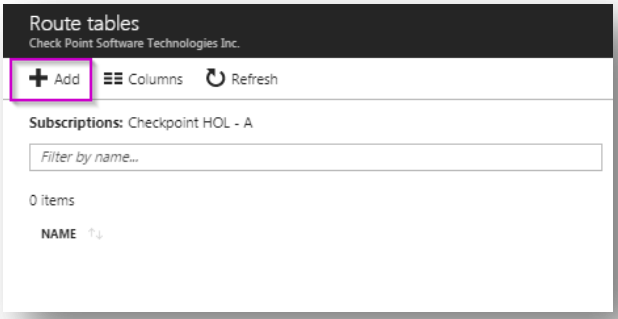
5. From the left pane choose “more services”



6. In the new windows search for “route” and choose the “Route Table”

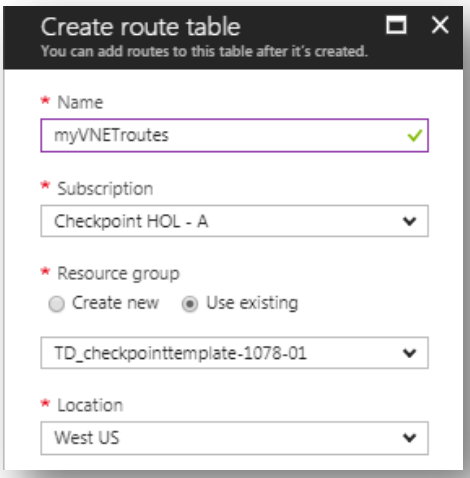


7. Once inside, click on “+ add”.



8. The first item is to create a route table

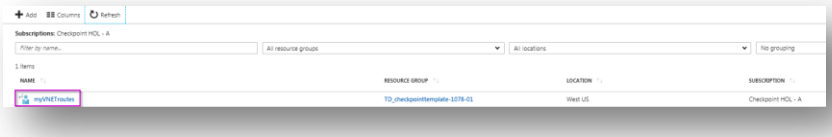
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



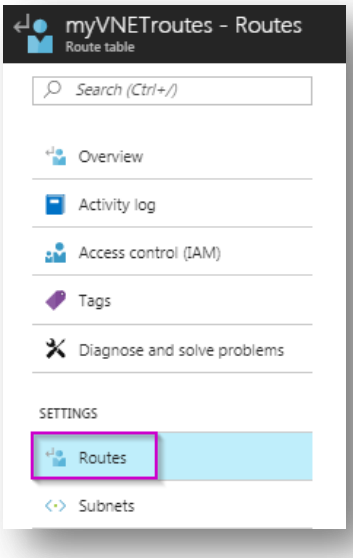
Name: myVNETroutes
Subscription: Leave as is
Resource Group: Use existing (the first on the list)
Location: use the same Location as in exercise 1

Click Create

9. Next, click on the newly created route table

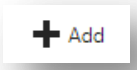


10. On the open bar click on routes

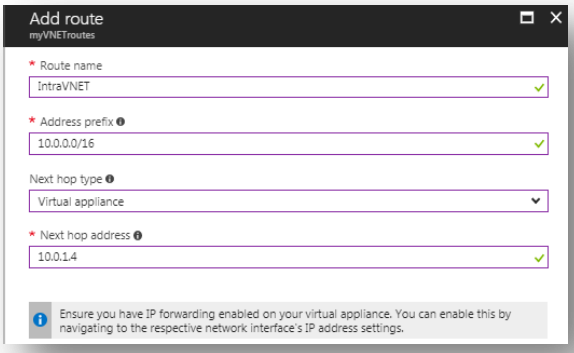


11. Click on the Add button at the upper side of the screen

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



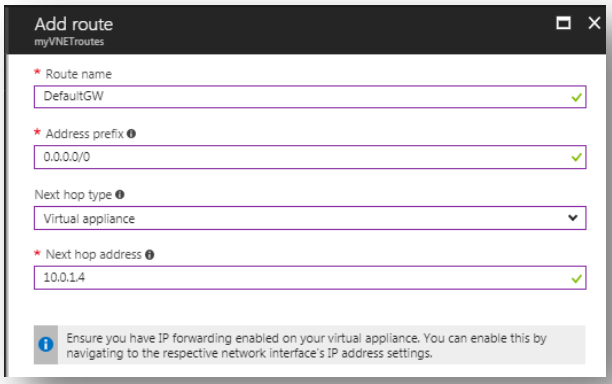
12. Fill in the following information



Route name: IntraVNET
Address prefix: 10.0.0.0/16
Next hop type: virtual appliance
Next hop address: pay attention that the “Next hop address” should be filled with the Gateway Internal IP.
Click on “ok” when done

This will create a route entry which will direct all VNET related traffic to vSEC

13. Now, let’s add another route that will be served as the default (to the internet)

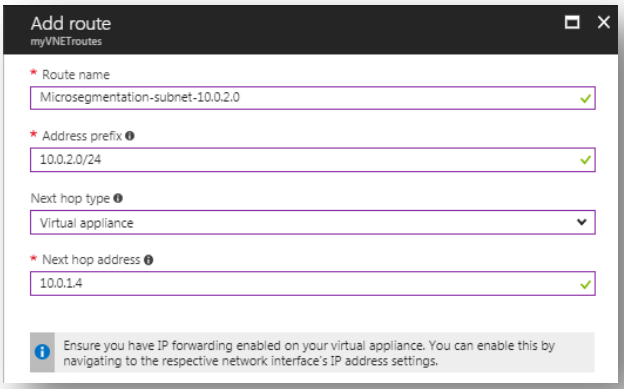


Route name: DefaultGW
Address prefix: 0.0.0.0/0
Next hop type: virtual appliance
Next hop address: pay attention that the “Next hop address” should be filled with the Gateway Internal IP.
Click on “ok” when done

This will create a route entry which will direct all Internet related traffic to vSEC

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

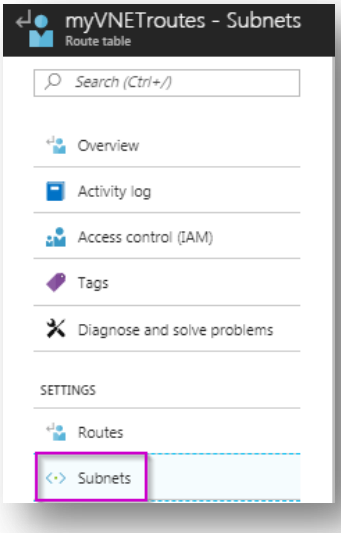
14. And another route which will force all traffic within the subnet to also go through our gateway (this is need only in the case you wish to control that traffic otherwise it's irrelevant).



Route name: Micorsegmentation-subnet-10.0.2.0
Address prefix: 10.0.2.0/24
Next hop type: virtual appliance
Next hop address: pay attention that the "Next hop address" should be filled with the Gateway Internal IP.
Click on "ok" when done

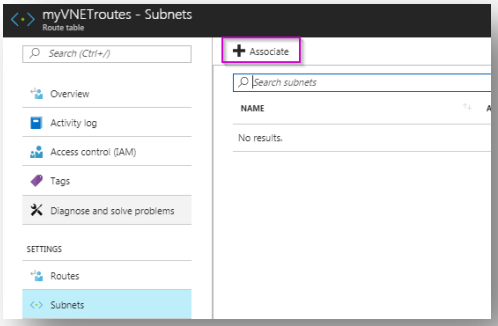
This will create a route entry which will direct all internal subnet 10.0.2.0 traffic to vSEC

15. After adding the route, we need to associate the subnet will use with that route table, on the route table list on the left side click on the "subnets"

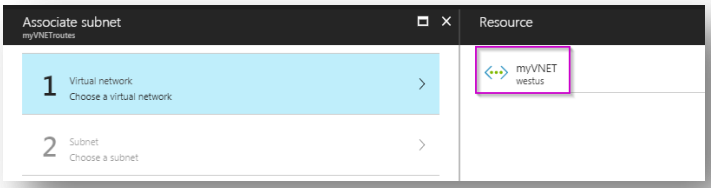


16. Click on Associate.

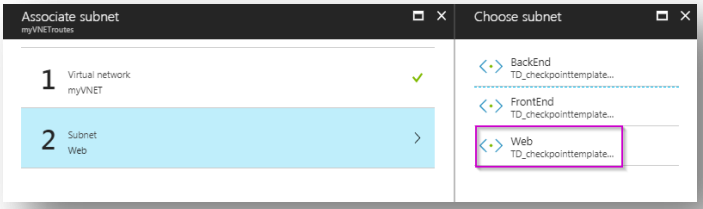
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



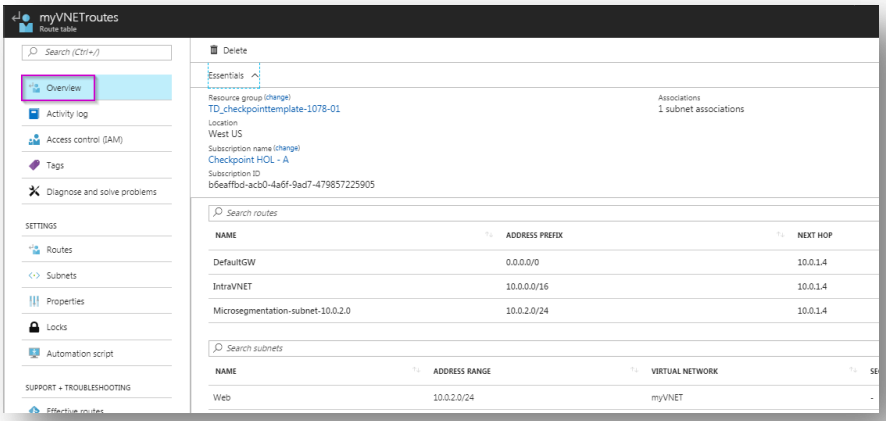
17. Choose your VNET



18. Click on Subnet top add your web subnet

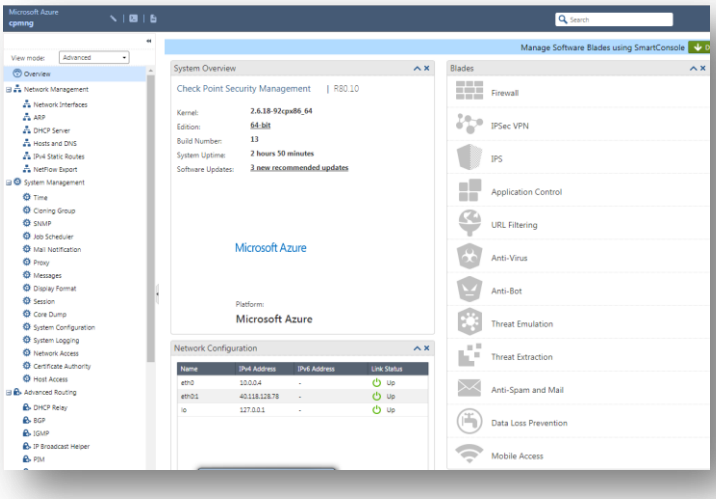


19. Click OK and review the configuration by clicking on the overview at the left side bar

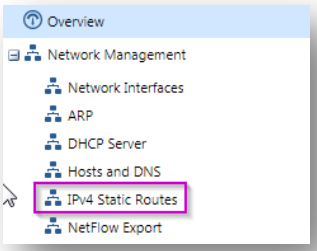


20. For our firewall gateway to be able to route traffic into the new subnet, a new route is to be added on the Gaia portal, first connect via HTTPS into your Gateway using its Public IP.

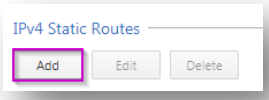
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



21. Navigate to Network Management, on the bar at the left side and click on IPv4 Static Routes.

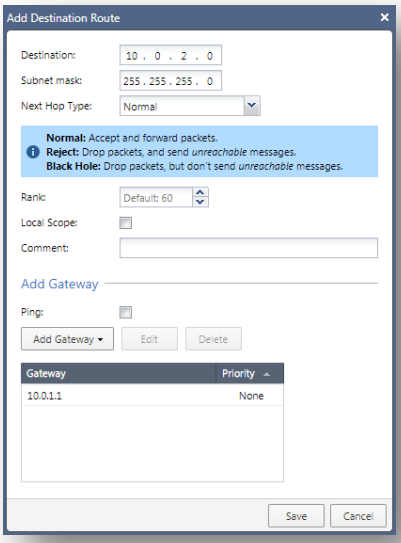


22. Add a route by clicking on the Add button.



23. Fill in the relevant fields as described below:

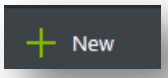
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



Destination: 10.0.2.0
Subnet mask: 255.255.255.0
Next hop type: Normal
Add gateway: IP address
Gateway IP: 10.0.1.1 (Azure router on internal subnet)

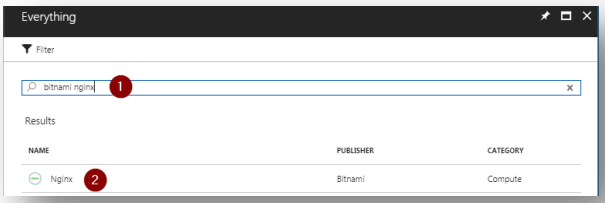
Creating a Web server

24. Now, let's create the new web server.
25. From the Azure portal, click on "New" on the left pane

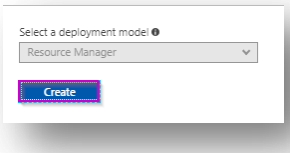


In the window that appears, write "bitnami nginx" in the search box and press enter

26. Choose "Nginx" (as shown)

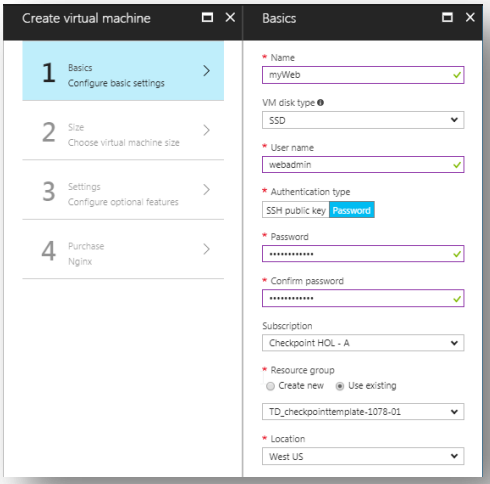


And then click on "create"



©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

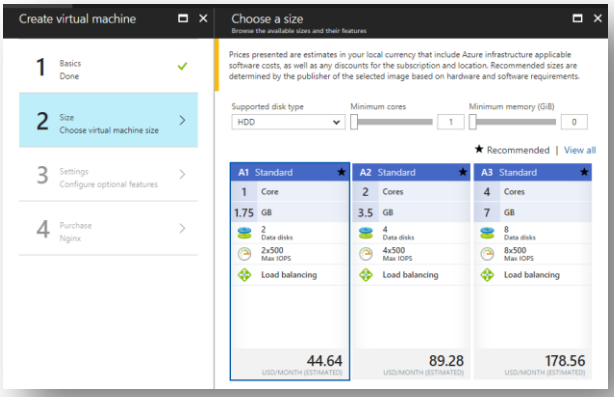
27. Choose the web server's properties (as describe below)



Name: myWeb
User name: webadmin
Authentication type: Password
Password: Choose your own
Subscription: leave as is
Resource Group: Use existing , the first on the list
Location: use the same Location as in exercise 1

When done, click on "ok"

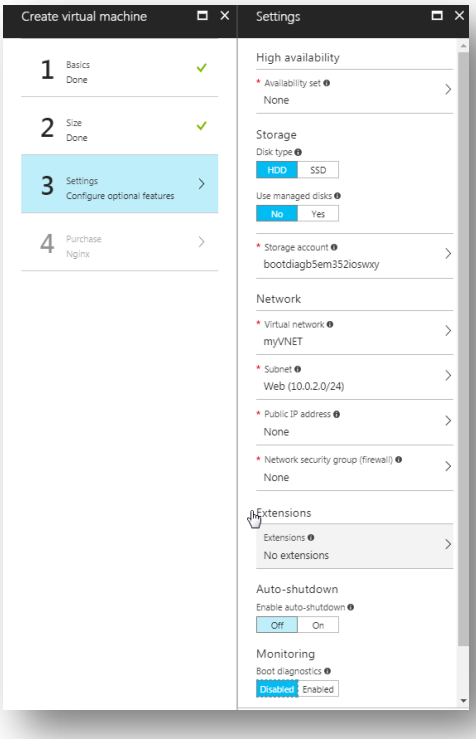
28. Next, choose the virtual machine size (A1)



And click on "select"

29. Choose the characteristics of your new virtual machine:

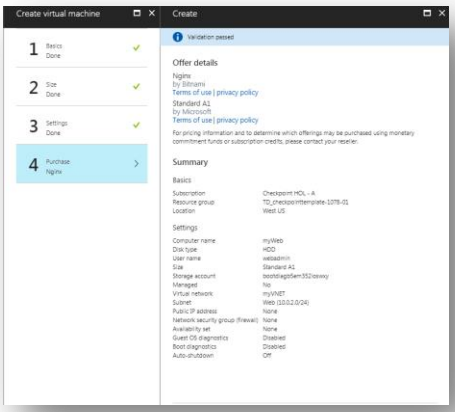
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



Disk Type: HDD
Use Managed disk: No
Virtual Network: myVNET
Subnet: Web (10.0.2.0/24)
Public IP address: None
Network security group: None
Boot monitoring: Disabled

All the rest should stay at the default.
Click OK

30. Validate the virtual machine details and click “create” to start deployment.

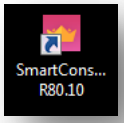


©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

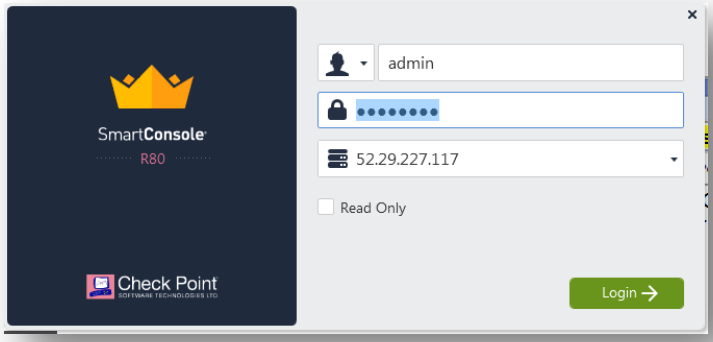
Note: there is no way to set the virtual machine private IP address at that stage, so the virtual machine actually gets auto-assigned with an IP (DHCP) and you are able to change it later on (after deployment)

Configuring the Check Point SmartConsole policy

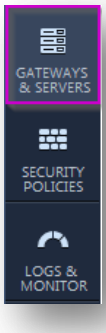
29. Connect to the SmartCenter server using R80.10 SmartConcole GUI client on your laptop (use the admin credentials you created during the setup)



30. Fill in the relevant information (e.g. username/password and the same public IP) and click on login

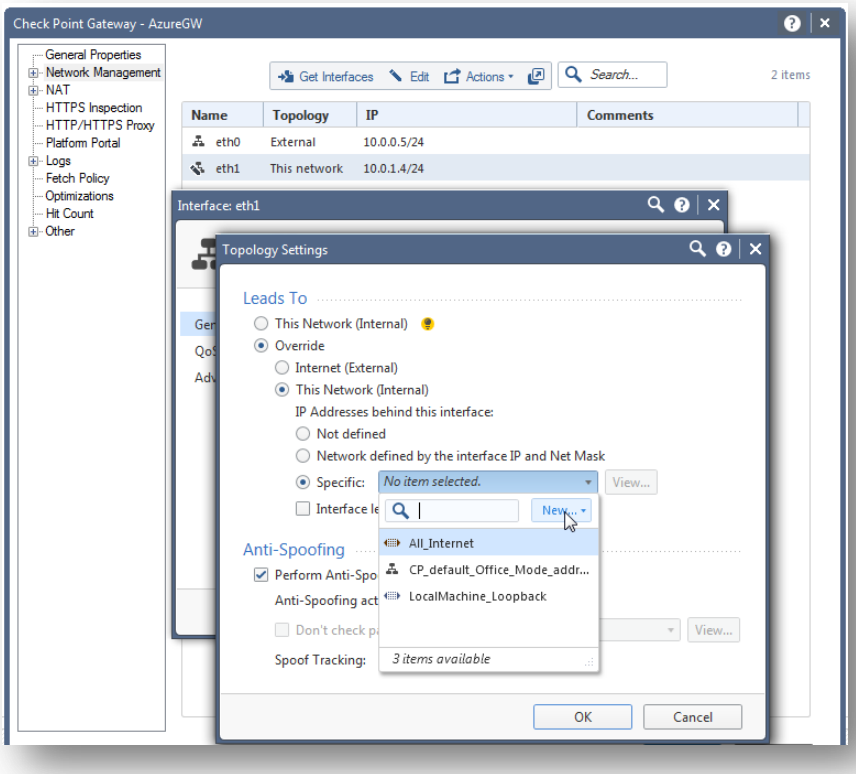


31. on the left bar choose Gateways & Services

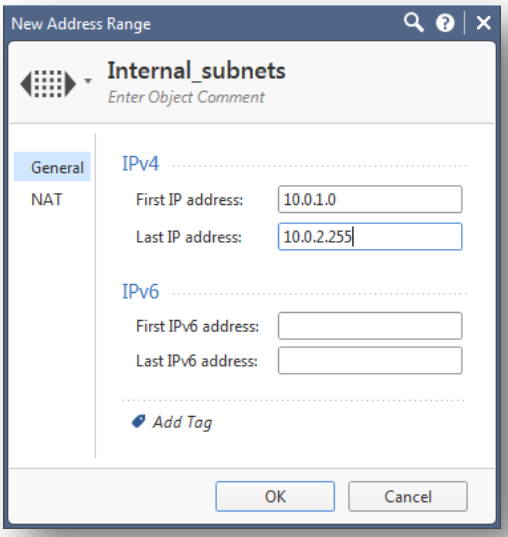


34. Open the AzureGW properties by DoubleClick.
35. Go into the Network Management section and DoubleClick interface ETH1 and then choose modify.
36. Remove the ant spoofing tag (on public clouds it is done by the platform itself).
37. Include the web subnet in that interface protected network

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



Change to “Override”
Pick “This network” and move to Specific.
Click on “New” and create an address range called:
Name: Internal_subnets
IP: 10.0.1.0 to 10.0.2.255

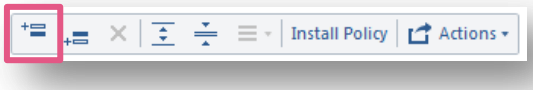


Click OK and than OK and another time.

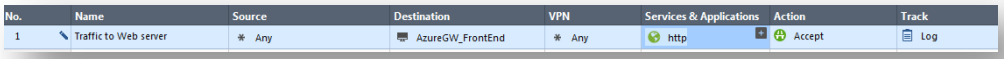
32. on the left bar choose Security Policies

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

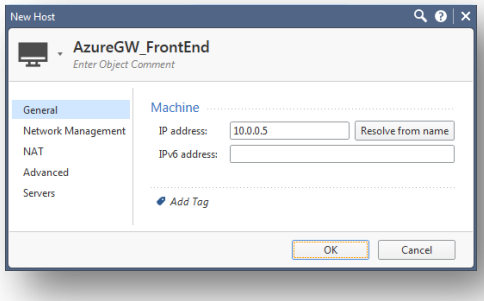
38. create a new rule by choosing the Add rule above from the upper middle bar



39. This rule will allow http traffic to the Web server from the internet, fill in the relevant fields:



a. Name: Traffic to Web server
b. Source: Any
c. Destination: (click on the + sign, choose new -> Host)

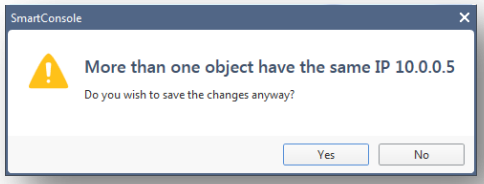


Name: AzureGW_FrontEnd
IPv4 Address: 10.0.0.5

Click OK.

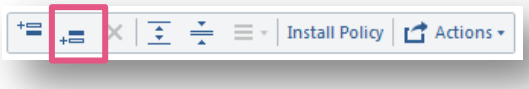
Acknowledge the warning as it is expected:

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

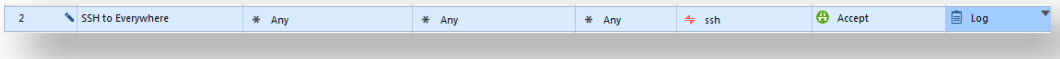


d. Services & Applications: (click on the + sign) search for HTTP
e. Action: Allow
f. Track: Log

40. Mark the rule you have just created and create a new rule by choosing the Add rule below from the upper middle bar



41. Create another rule for administration and troubleshooting of the lab

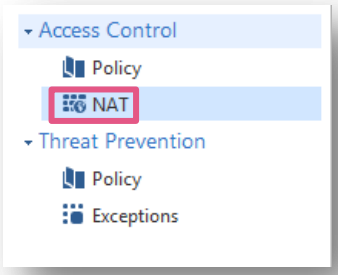


a. Name: SSH to Everywhere
b. Source: Any
c. Destination: Any
d. Services & Applications: (click on the + sign) search for SSH
e. Action: Allow
f. Track: Log

42. Your security rulesets should look like that:

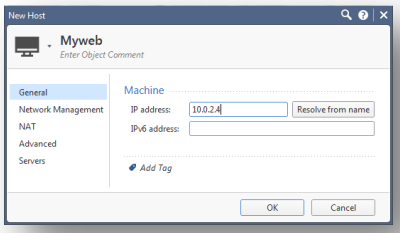
43. At the left bar choose the NAT policy

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



44. On the upper central bar choose add rule above

45. Next create the following NAT rule to protect the connections to the web server
    Original Source – All_Internet
    Original Destination: AzureGW_FrontEnd
    Original Service: HTTP
    Translated Source: Original
    Translated Destination: Myweb
        Click on the + sign, choose new -> Host)



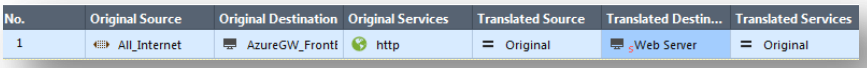
Name: Myweb
IPv4 Address: 10.0.2.4 (make sure this is the address of the web)

Click OK.

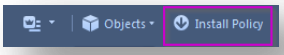
Translated Service: Original

NAT Rule:

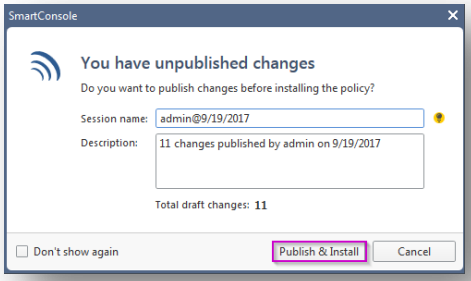
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



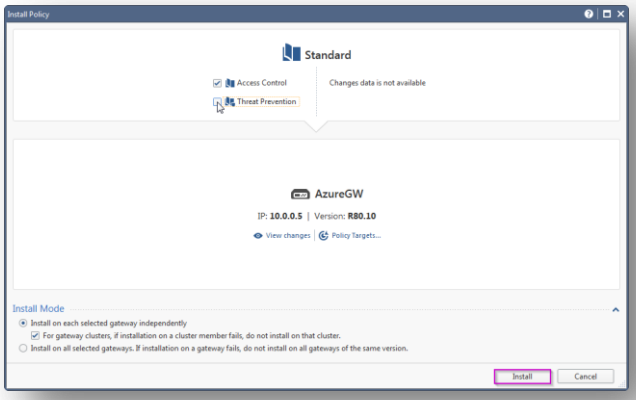
14. On the upper left side click Install policy



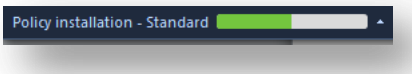
d. Click the Publish & Install



e. In the opened screen uncheck the Threat prevention and click Install

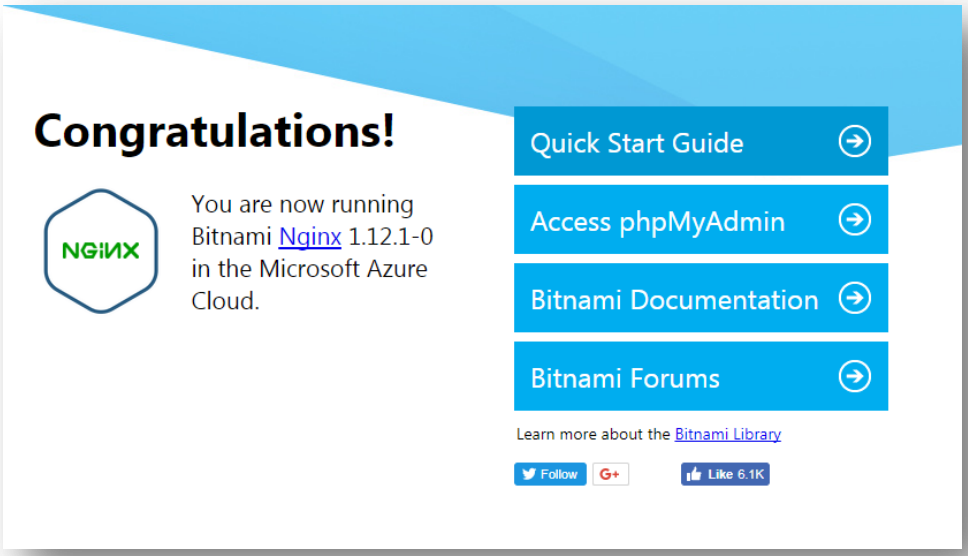


f. You can see the progress on the bottom left side



46. Verify connectivity to the web server using a browser. Type the vSEC gateway public IP address and verifying access in the logs, If configuration is successful, you will be able to see the below web site.

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



You have finished exercise 4

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

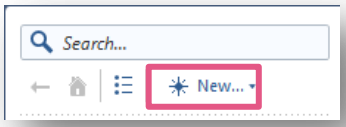
Exercise #5 – Connecting vSEC Controller

Now we need to allow the management server access to the Azure API to enable the vSEC controller.

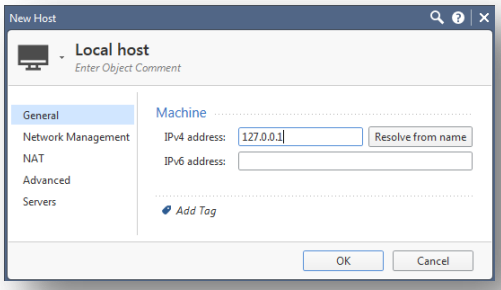
The suggested way of assigning those permissions is using Service Principal (SPN), you can find on appendix 1 the instructions on how to configure SPN.

For this lab you already have the SPN defined and received the definitions on your email

1. On the Check Point SmartConsole, on the upper right section choose New object



2. Pick the host type
3. Create new host object by the following parameters

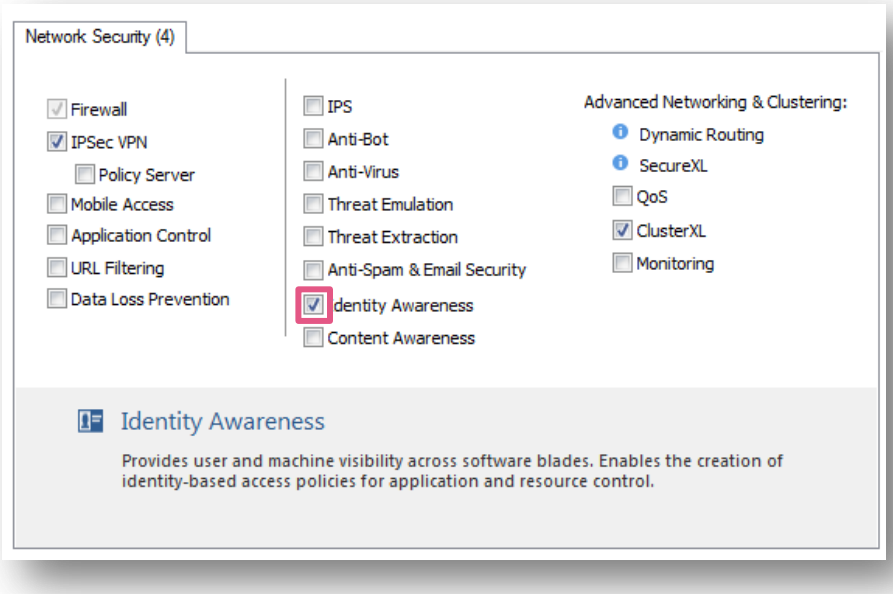


Name: Local Host
IPv4 address: 127.0.0.1
Click OK

4. At the left bar choose Gateways & Servers

5. DoubleClick the gateway object, move into the General Properties tab, and check the Identity Awareness Blade.

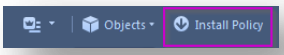
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



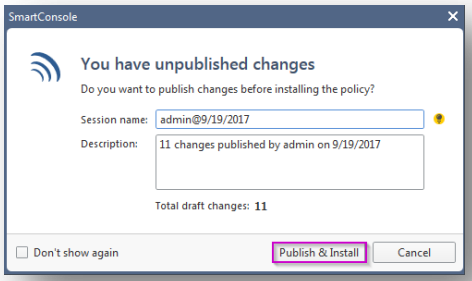
6. A window will be open, select the Terminal Servers & uncheck the AD query, Click next.

7. Select the option: “I don’t want to configure Active Directory at this time” & than click: Next -> Finish -> OK.

8. DoubleClick the gateway object, move into the Identity awareness section
9. Choose Identity Web API and click the Settings button
10. On the new window, click the green + sign on the right
11. Choose the Local Host object
12. Click OK and another OK
13. A massage will popup, accept.
15. On the upper left side click Install policy

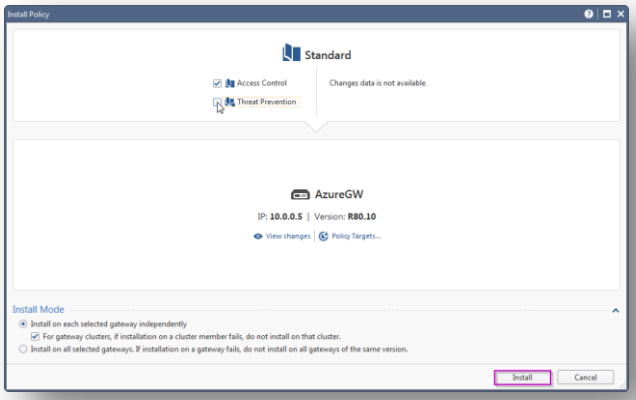


g. Click the Publish & Install

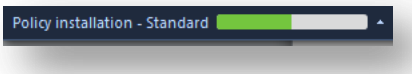


h. In the opened screen uncheck the Threat prevention and click Install

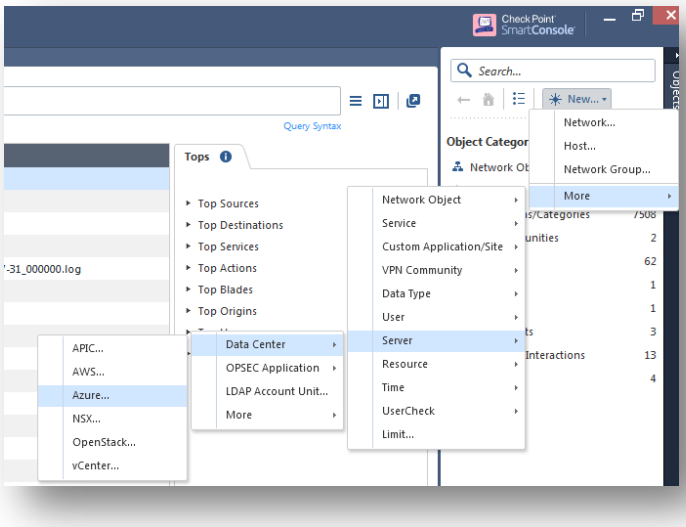
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



i. You can see the progress on the bottom left side

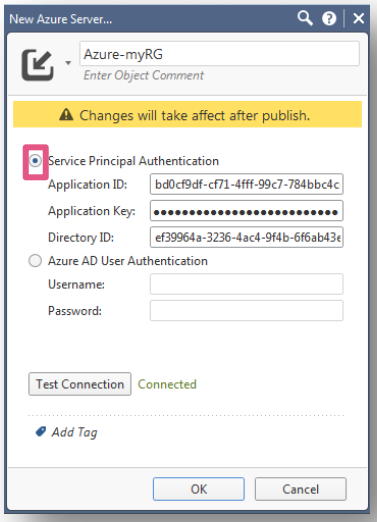


14. Now we will create the connection between the SMS & the Azure account, on the SmartConsole, create a new server object -> Data Center - > Azure

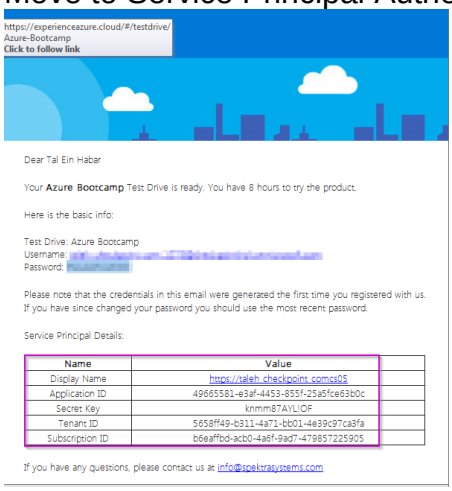


15. On the new Azure Datacenter object fill in the details (as shown in the email):

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

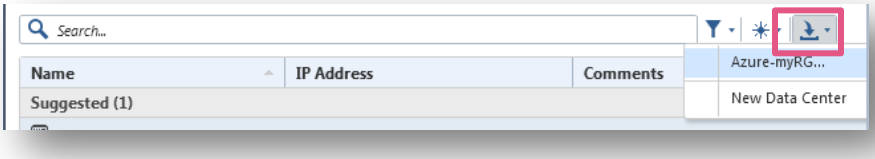


Move to Service Principal Authentication

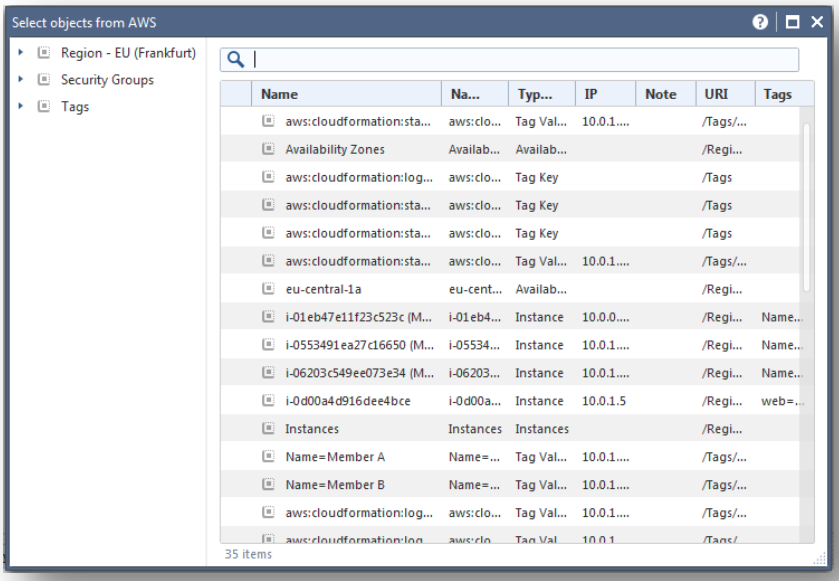


Test Connection to see that the system is connected.

16. Try to create new rule & import objects from the Azure portal in 3 different ways.



©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



You can import the object via:

a) **Region view** to import Azure vNETs, Subnets or virtual machines to your Security Policy.
b) **Tags view** to import all virtual machine that have specific Tag Key or to import all virtual machines that have specific Tag Key with a specific value.
c) Search view to import the object directly.

You have finished exercise 5

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

Exercise #6 – Advanced scenarios

If you are done with the rest of the exercises, (well done) you are welcome to dive deeper with the following scenarios

Test Scenarios:

1. Initiate “fw monitor” on the gateway and inspect traffic traversing the gateway

2. Activate Threat Protection blades (Anti-Virus, Anti-Bot, URL filtering, Application control) on the gateway and inspect the logs and check which traffic is hitting our environment (are you able to identify malicious traffic targeting our environment)?

3. Add another server on the Web subnet and verify that traffic between two servers on the subnets are actually traversing through the firewall (micro-segmentation or AKA East - west protection)

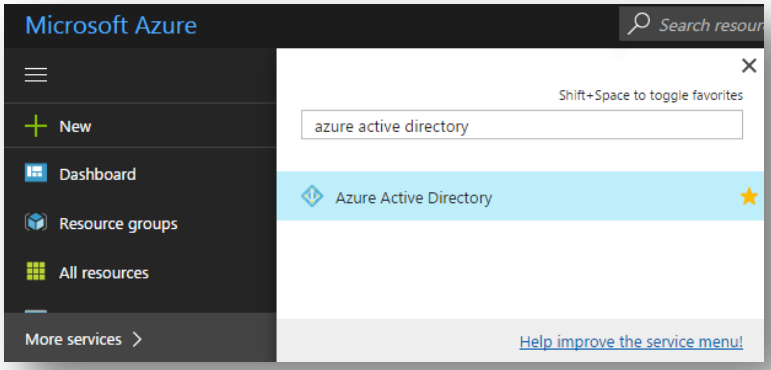
You have finished exercise 6

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

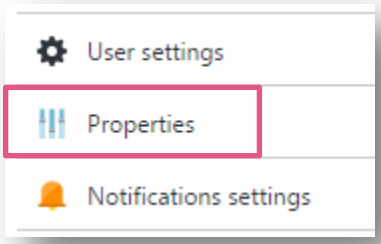
Appendix #1 – SPN definitions

Please follow the below to create a service principal and assign it with the relevant permissions.

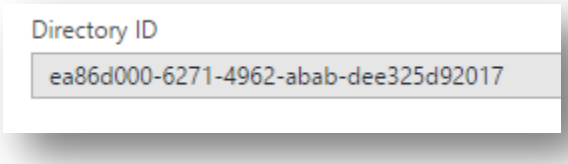
17. Click the Azure Active directory section on the right side



18. Click on properties

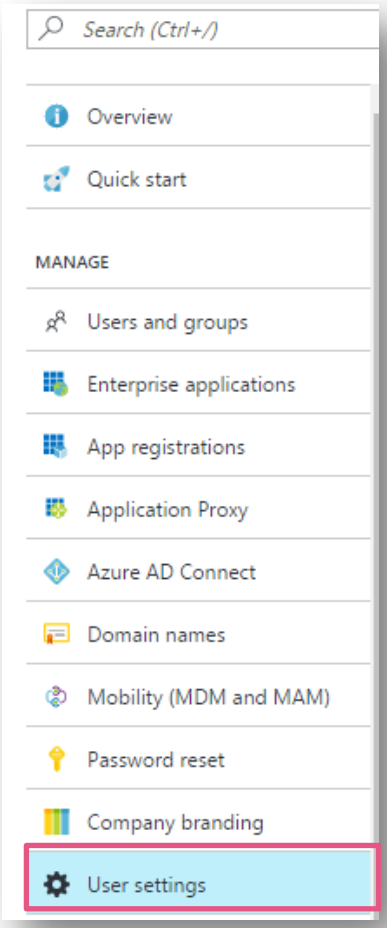


19. Copy aside the directory ID for later use

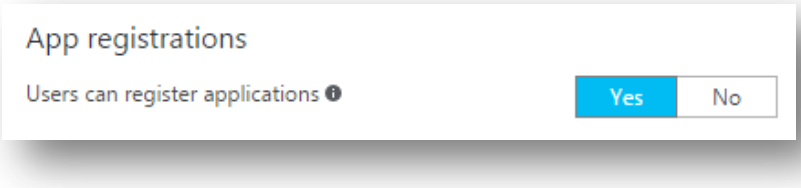


©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals

20. Now, enter the “user settings” section

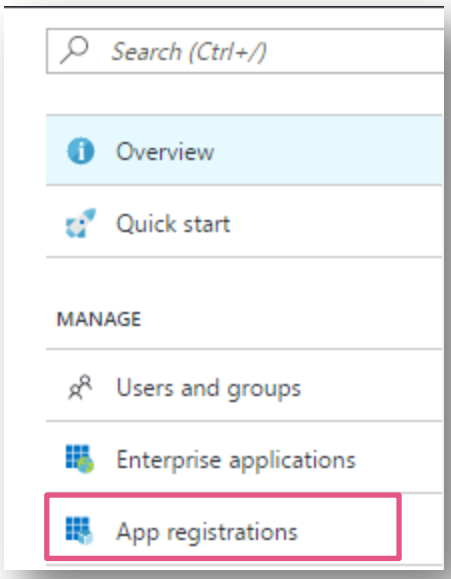


21. Check the App registrations setting. It should set to Yes.

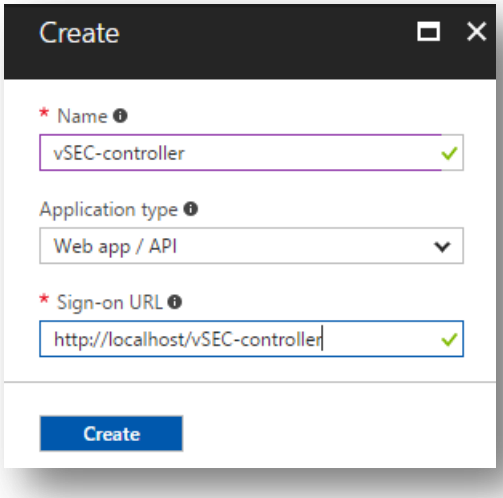


22. Click App registrations, and then select New application registration

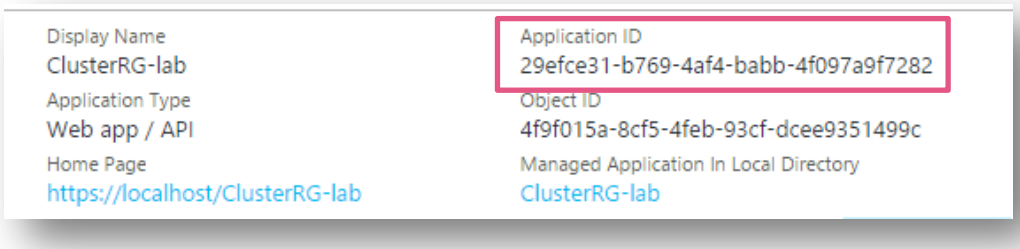
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



23. Fill in the relevant info (as shown in the pic):

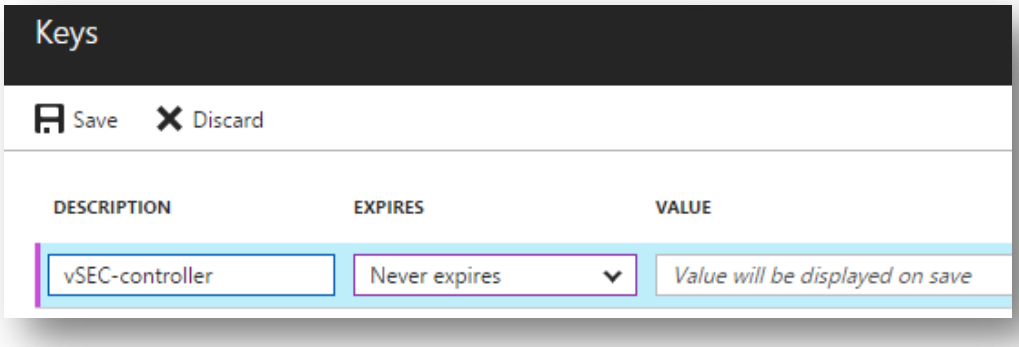


24. Select the newly created application, copy the application ID to a safe place

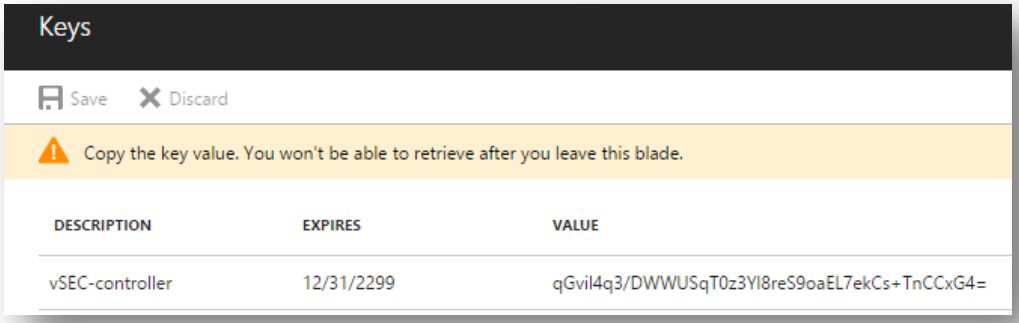


25. Now on the menu on the right under all settings. Select Keys, and create key as shown:

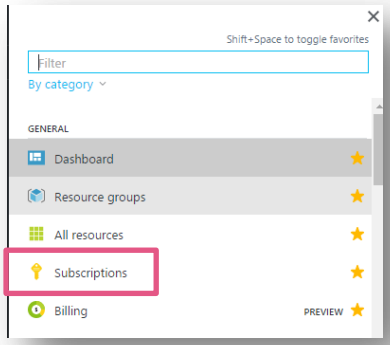
©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



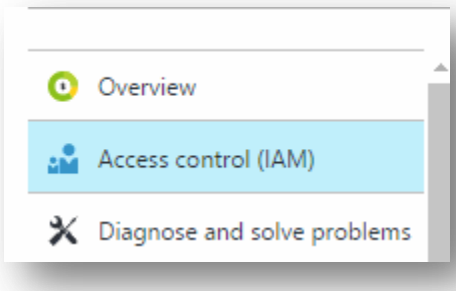
After you click, save the key value appears, copy it to a safe place as you cannot retrieve it later (In this lab and after).



26. In the left Azure menu bar on the left choose “Subscriptions”

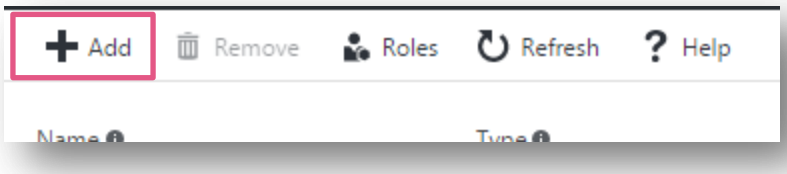


27. Choose your subscriptions and click on Access Control (IAM)

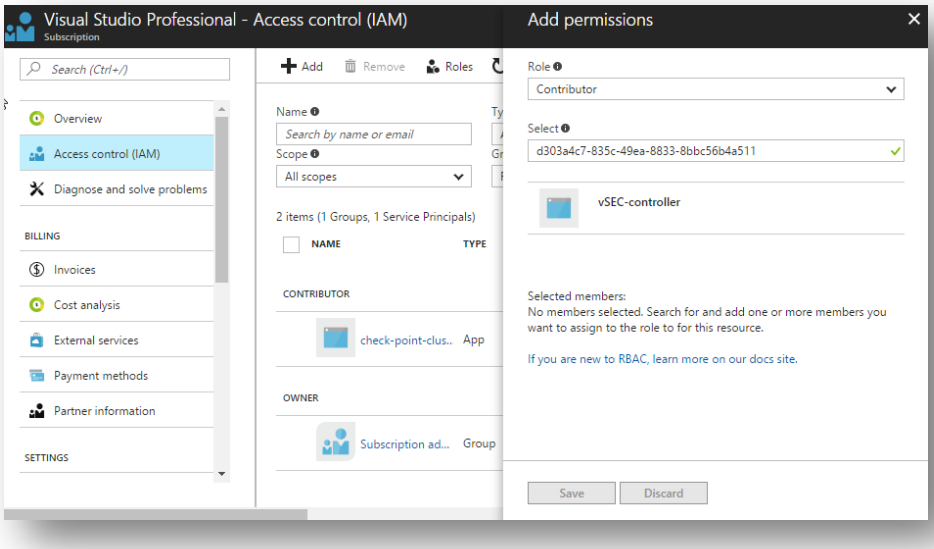


28. Click on the Add to create a new role for our application

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals



29. On the next windows choose a contributor role and then search for your new application using its application id.



30. Click “Save

©2015 Check Point Software Technologies Ltd. All rights reserved
[Restricted] ONLY for designated groups and individuals