Next Generation Data Center Security

vSEC for Azure Training Cookbook

Ver. 3.6

Table of Contents

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.

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.

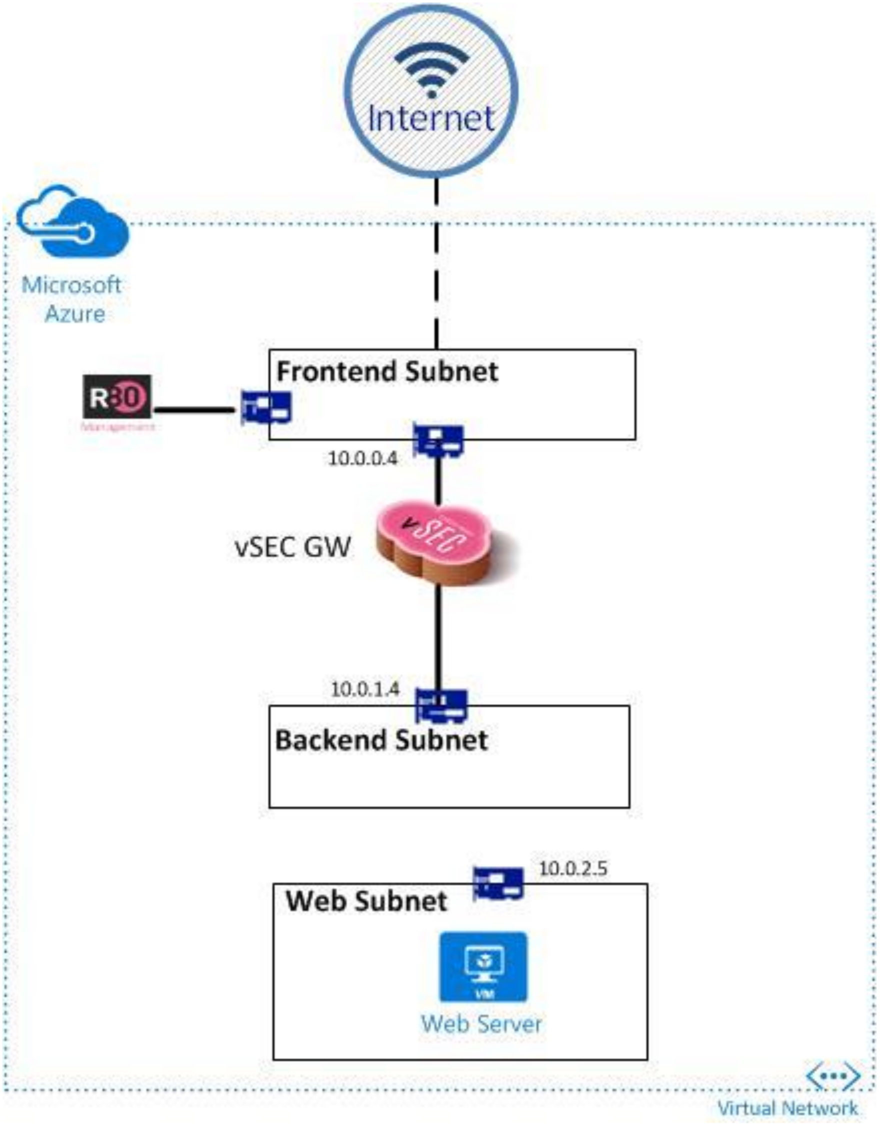
3. Deploy Check Point vSEC Gateway on Azure
   This exercise will demonstrate to you how to deploy a vSEC gateway into your Azure environment to improve transparency and enforcement of network traffic traversing through/from the environment.

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.

vSEC for Azure training environment:

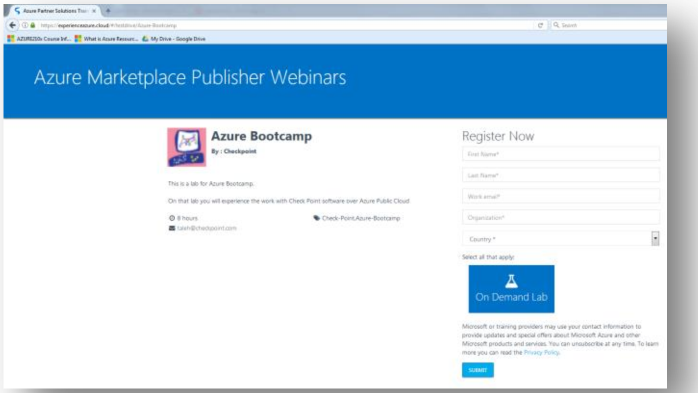
Getting to know your training environment



	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)

Connecting and setting up your work environment:

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



Azure Partner Solutions Trai

https://experienceazure.cloud/#/testdrive/Azure-Bootcamp

AZURE210x Course Inf... What is Azure Resourc... My Drive - Google Drive

Azure Marketplace Publisher Webinars

Azure Bootcamp

By : Checkpoint

This is a lab for Azure Bootcamp.

On that lab you will experience the work with Check Point software over Azure Public Cloud

8 hours

Check-Point.Azure-Bootcamp

taleh@checkpoint.com

Register Now

First Name*

Last Name*

Work email*

Organization*

Country *

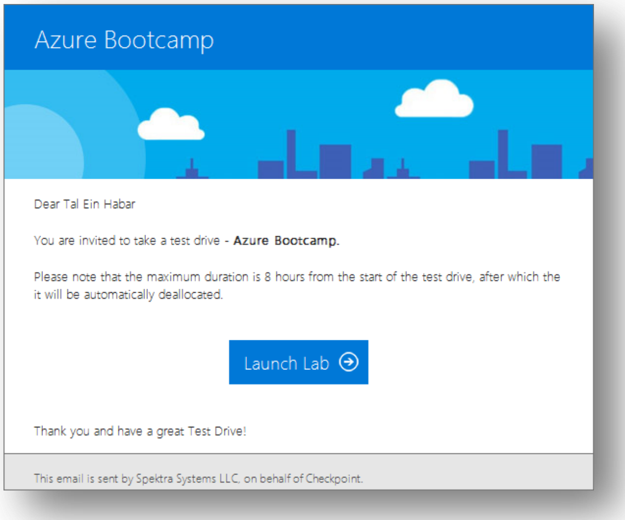
Select all that apply:

On Demand Lab

Microsoft or training providers may use your contact information to provide updates and special offers about Microsoft Azure and other Microsoft products and services. You can unsubscribe at any time. To learn more you can read the Privacy Policy.

SUBMIT

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**



Azure Bootcamp

Dear Tal Ein Habar

You are invited to take a test drive - **Azure Bootcamp**.

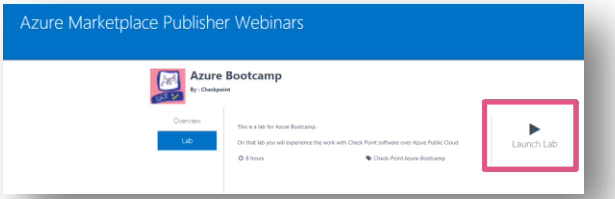
Please note that the maximum duration is 8 hours from the start of the test drive, after which the it will be automatically deallocated.

Launch Lab

Thank you and have a great Test Drive!

This email is sent by Spektra Systems LLC. on behalf of Checkpoint.

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"**



Azure Marketplace Publisher Webinars

Azure Bootcamp

By : Checkpoint

Overview

Lab

This is a lab for Azure Bootcamp.

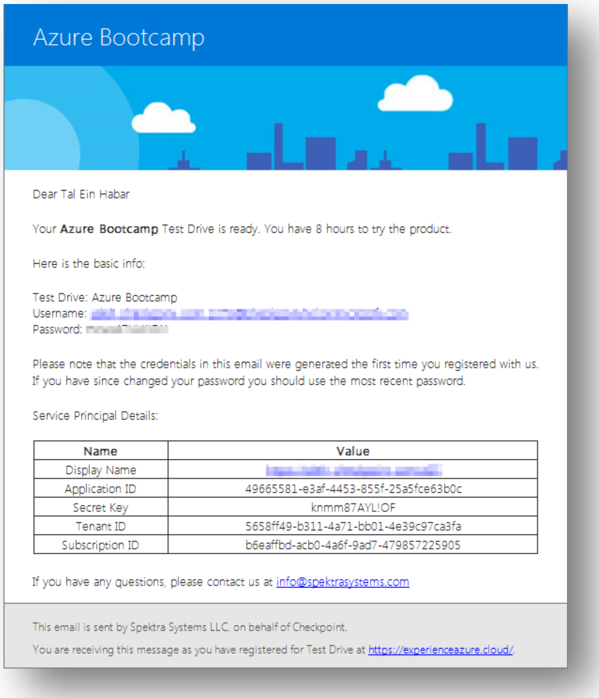
On that lab you will experience the work with Check Point software over Azure Public Cloud

8 hours

Check-Point.Azure-Bootcamp

Launch Lab

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



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:

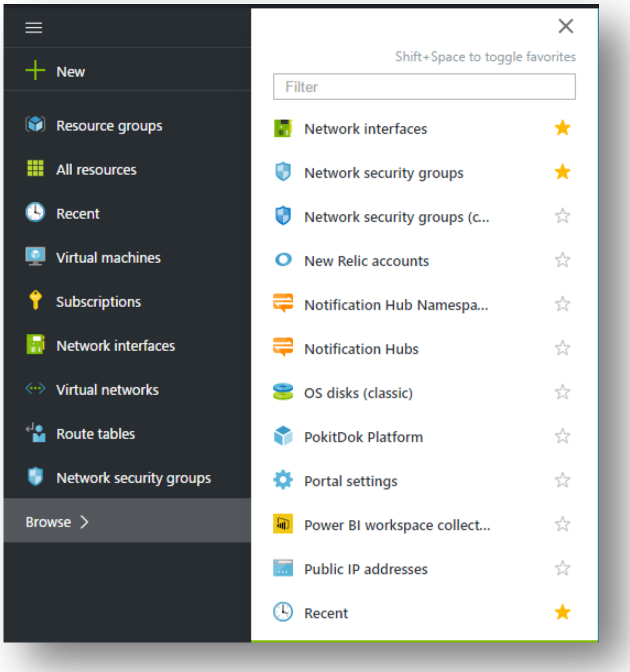
Name	Value
Display Name	[redacted]
Application ID	49665581-e3af-4453-855f-25a5fce63b0c
Secret Key	knmm87AYL!OF
Tenant ID	5658ff49-b311-4a71-bb01-4e39c97ca3fa
Subscription ID	b6eaffbd-acb0-4a6f-9ad7-479857225905

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

This email is sent by Spektra Systems LLC, on behalf of Checkpoint.

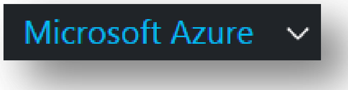
You are receiving this message as you have registered for Test Drive at https://experienceazure.cloud/.

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**



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.

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

Description

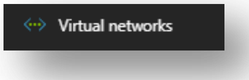
This exercise will guide you through the steps required to setup your own private Azure environment to which we will be deploying our virtual machines.

Method

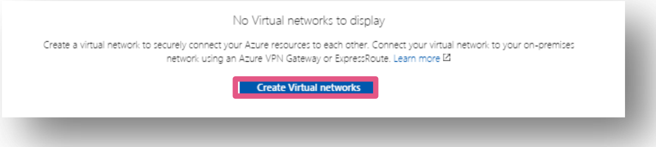
Using Azure portal you will create a new VNET (Virtual dedicated environment) in a designated region. You will then create subnets within that environment. This newly created environment will be used in later exercise as new virtual machines will be provisioned into the environment.

How

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



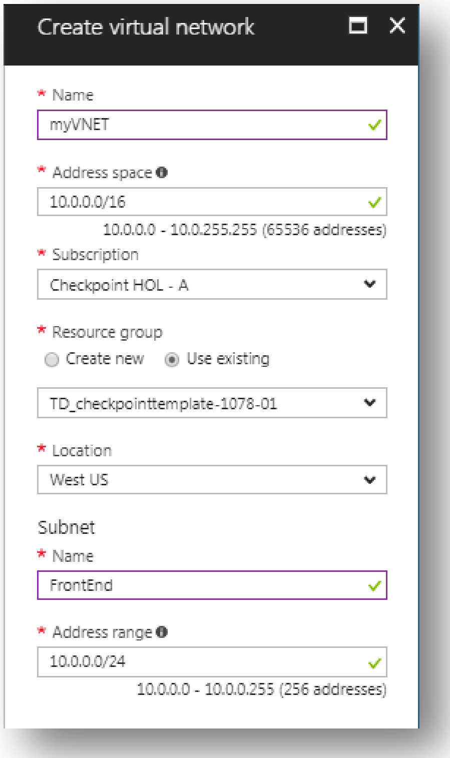
2. At the bottom of the window that appears, click “Create Virtual Networks”



No Virtual networks to display

Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute. Learn more

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



Create virtual network

* Name

myVNET ✓

* Address space

10.0.0.0/16 ✓

10.0.0.0 - 10.0.255.255 (65536 addresses)

* Subscription

Checkpoint HOL - A

* Resource group

○ Create new ● Use existing

TD_checkpointtemplate-1078-01

* Location

West US

Subnet

* Name

FrontEnd ✓

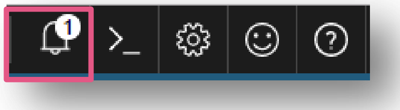
* Address range

10.0.0.0/24 ✓

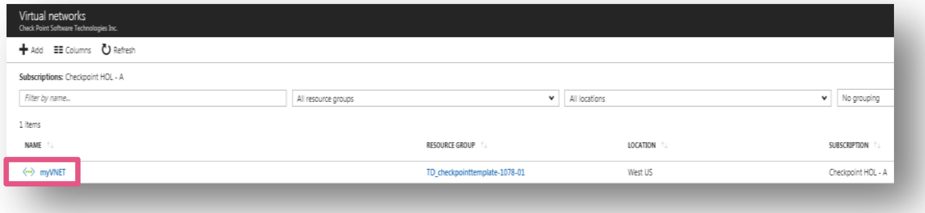
10.0.0.0 - 10.0.0.255 (256 addresses)

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)



Virtual networks

Check Point Software Technologies Inc.

Subscriptions: Checkpoint HOL - A

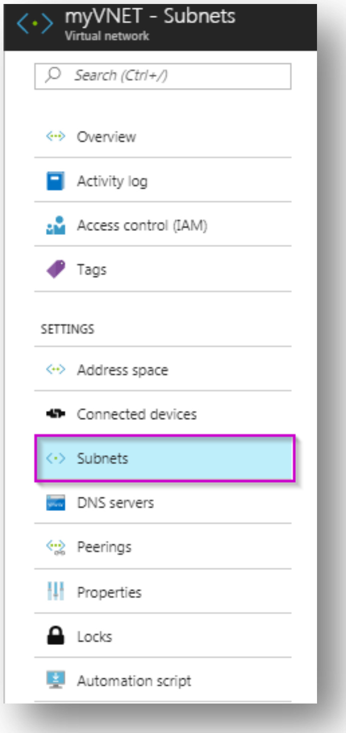
Filter by name... | All resource groups | All locations | No grouping

1 items

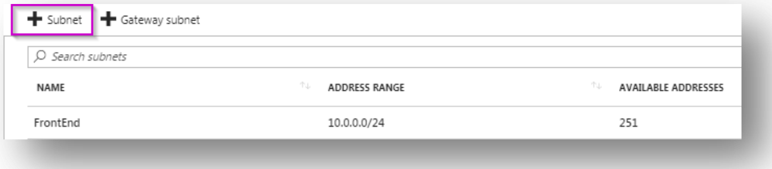
NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
myVNET	TD_checkpointtemplate-1078-01	West US	Checkpoint HOL - A

Click on the newly created VNET.

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

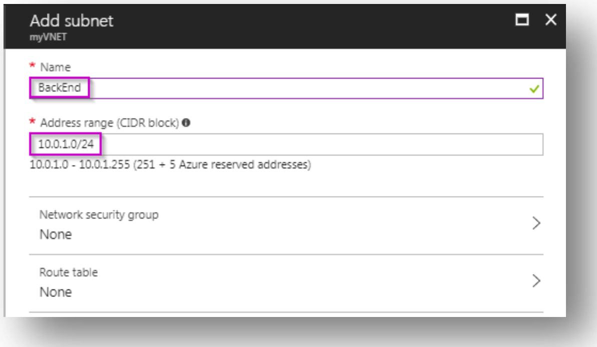


7. And then choose to add a new subnet by clicking on



NAME	ADDRESS RANGE	AVAILABLE ADDRESSES
FrontEnd	10.0.0.0/24	251

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.



* Name
BackEnd

* Address range (CIDR block)
10.0.1.0/24
10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

Network security group
None

Route table
None

Click “OK” to create the subnet.

You have finished exercise 1

Exercise #2 - Deploy Check Point Management on Azure

Description

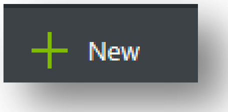
This exercise will guide you through the installation and configuration of Check Point's R80 SmartCenter Server in the environment you created on the former exercise.

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.

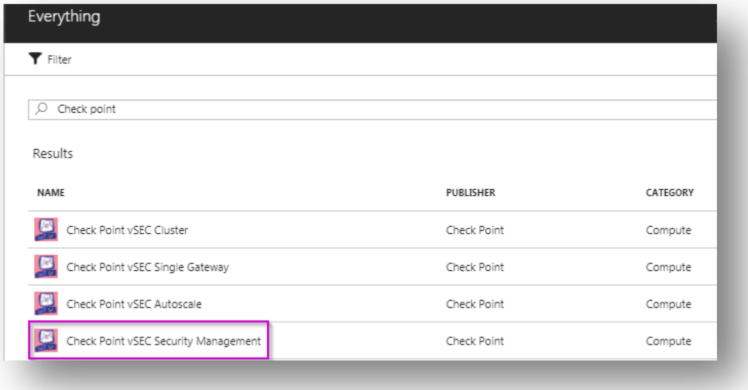
How

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)

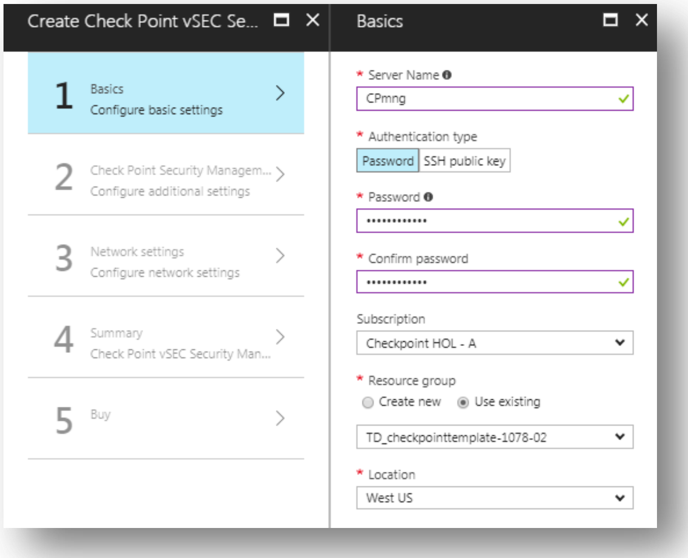


NAME	PUBLISHER	CATEGORY
Check Point vSEC Cluster	Check Point	Compute
Check Point vSEC Single Gateway	Check Point	Compute
Check Point vSEC Autoscale	Check Point	Compute
Check Point vSEC Security Management	Check Point	Compute

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

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



Create Check Point vSEC Se...

1 Basics
Configure basic settings

2 Check Point Security Managem...
Configure additional settings

3 Network settings
Configure network settings

4 Summary
Check Point vSEC Security Man...

5 Buy

Basics

* Server Name
CPmng

* Authentication type
Password | SSH public key

* Password
••••••••••••

* Confirm password
••••••••••••

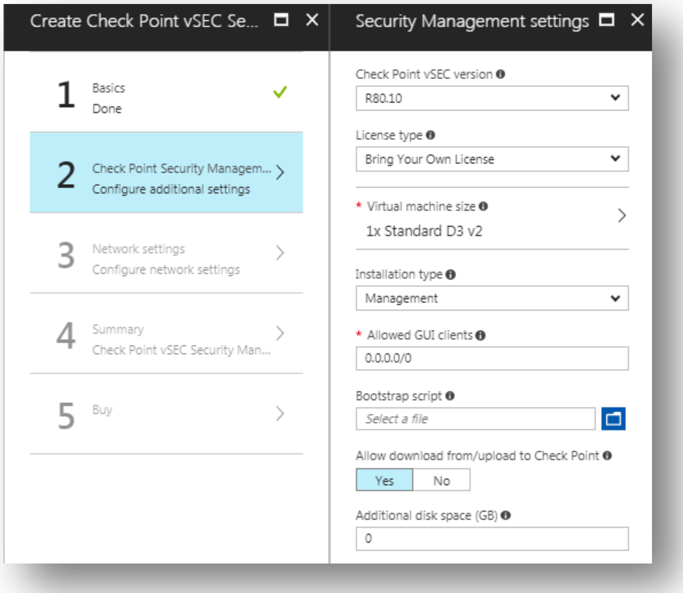
Subscription
Checkpoint HOL - A

* Resource group
○ Create new ● Use existing
TD_checkpointtemplate-1078-02

* Location
West US

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,



Create Check Point vSEC Se...

1 Basics
Done ✓

2 Check Point Security Managem...
Configure additional settings

3 Network settings
Configure network settings

4 Summary
Check Point vSEC Security Man...

5 Buy

Security Management settings

Check Point vSEC version
R80.10

License type
Bring Your Own License

* Virtual machine size
1x Standard D3 v2

Installation type
Management

* Allowed GUI clients
0.0.0.0/0

Bootstrap script
Select a file

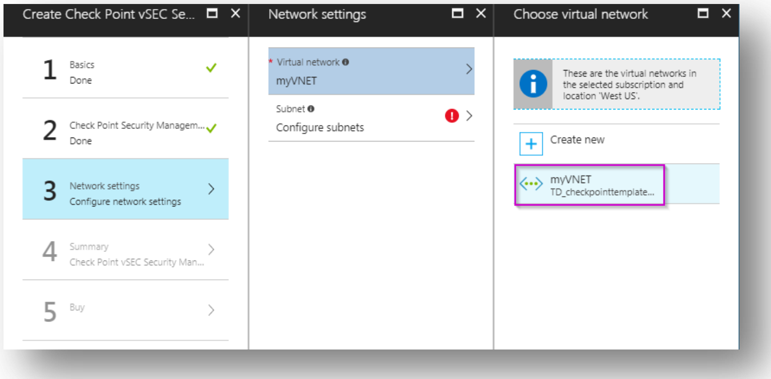
Allow download from/upload to Check Point
Yes | No

Additional disk space (GB)
0

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

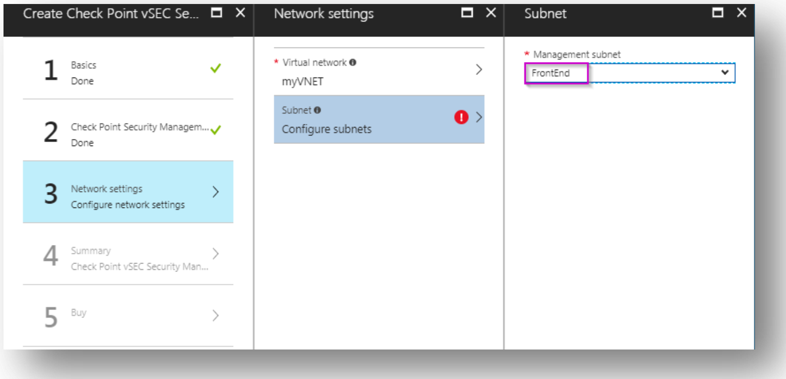
5. In the Network setting window (which appears),


Create Check Point vSEC Se...
1 Basics Done ✓
2 Check Point Security Managem... Done ✓
3 Network settings Configure network settings
4 Summary Check Point vSEC Security Man...
5 Buy
Network settings
Choose virtual network
These are the virtual networks in the selected subscription and location 'West US'.
Create new
myVNET
TD_checkpointtemplate...

* Virtual network: myVNET
Subnet: Configure subnets

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

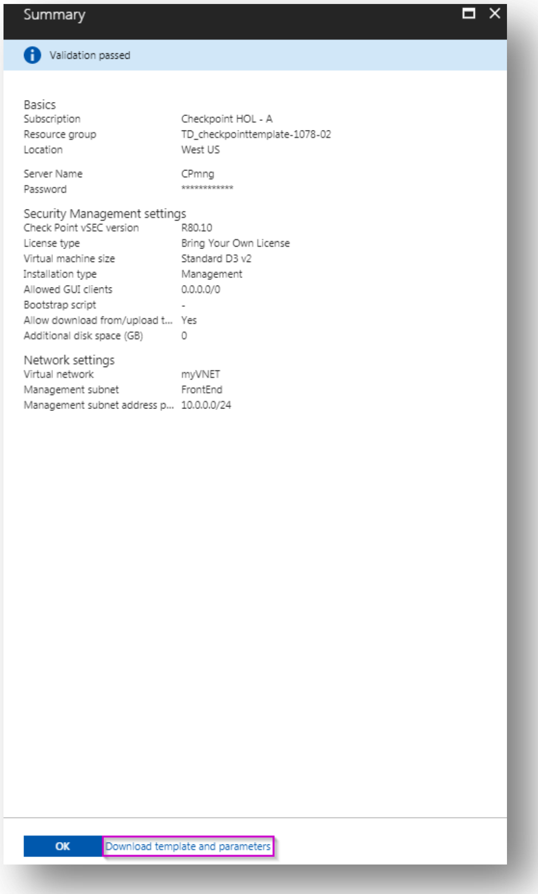
Next, click on subnets and choose the FrontEnd subnet we’ve created in previous exercise (as shown)


Create Check Point vSEC Se...
1 Basics Done ✓
2 Check Point Security Managem... Done ✓
3 Network settings Configure network settings
4 Summary Check Point vSEC Security Man...
5 Buy
Network settings
Subnet

* Virtual network: myVNET
Subnet: Configure subnets
* Management subnet: FrontEnd

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.



Summary

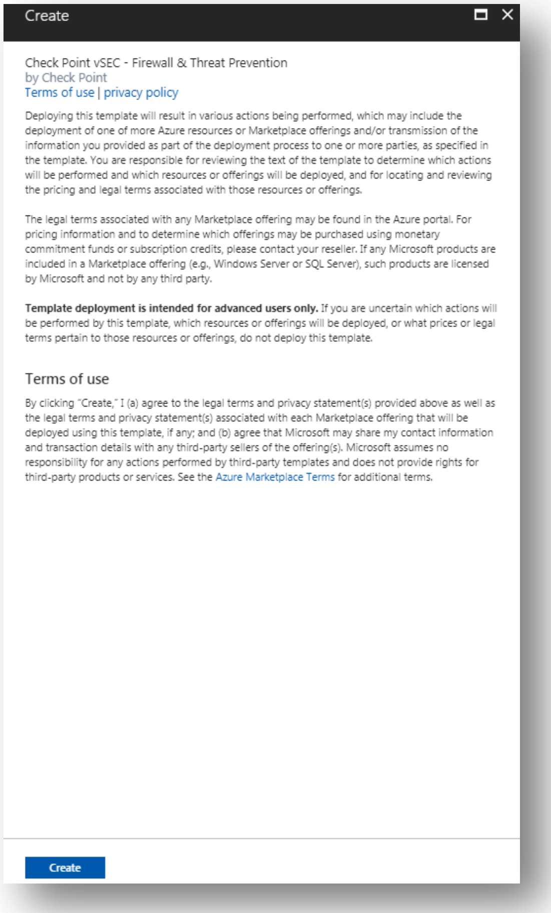
Validation passed

Basics	
Subscription	Checkpoint HOL - A
Resource group	TD_checkpointtemplate-1078-02
Location	West US
Server Name	CPmng
Password	************
Security Management settings	
Check Point vSEC version	R80.10
License type	Bring Your Own License
Virtual machine size	Standard D3 v2
Installation type	Management
Allowed GUI clients	0.0.0.0/0
Bootstrap script	-
Allow download from/upload t...	Yes
Additional disk space (GB)	0
Network settings	
Virtual network	myVNET
Management subnet	FrontEnd
Management subnet address p...	10.0.0.0/24

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)



Check Point vSEC - Firewall & Threat Prevention
by Check Point
Terms of use | privacy policy

Deploying this template will result in various actions being performed, which may include the deployment of one of 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.

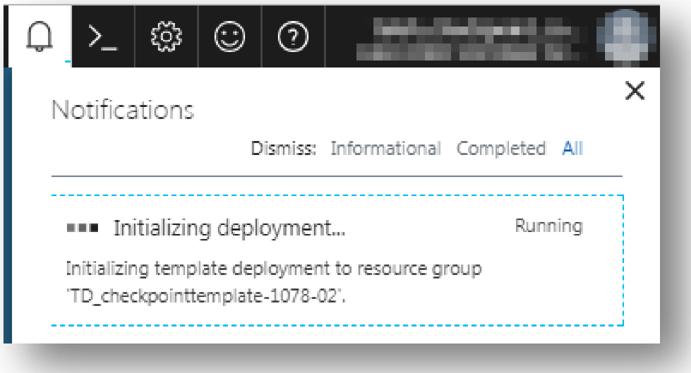
The legal terms associated with any Marketplace offering may be found in the Azure portal. For pricing information and to determine which offerings may be purchased using monetary commitment funds or subscription credits, please contact your reseller. If any Microsoft products are included in a Marketplace 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.

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

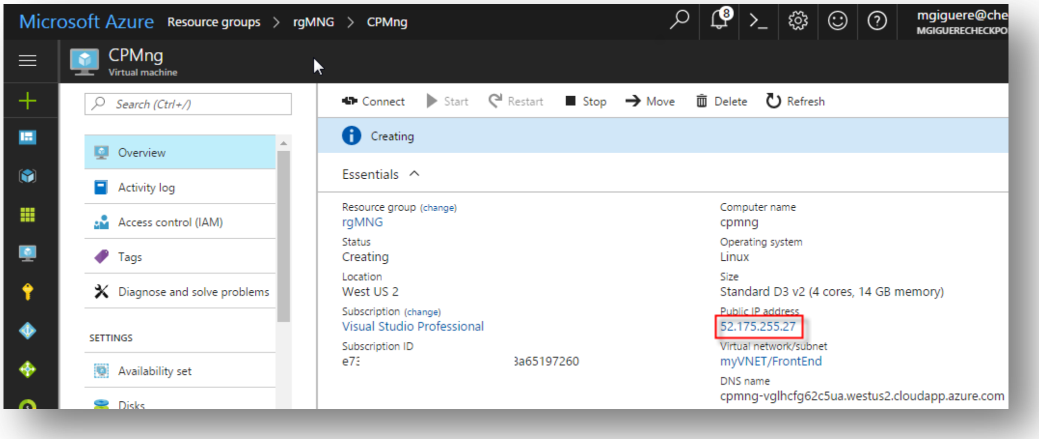


[redacted]

Initializing deployment... Running

Initializing template deployment to resource group 'TD_checkpointtemplate-1078-02'.

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):



Creating

Resource group (change)
rgMNG

Status
Creating

Location
West US 2

Subscription (change)
Visual Studio Professional

Subscription ID
e7: 3a65197260

Computer name
cpmng

Operating system
Linux

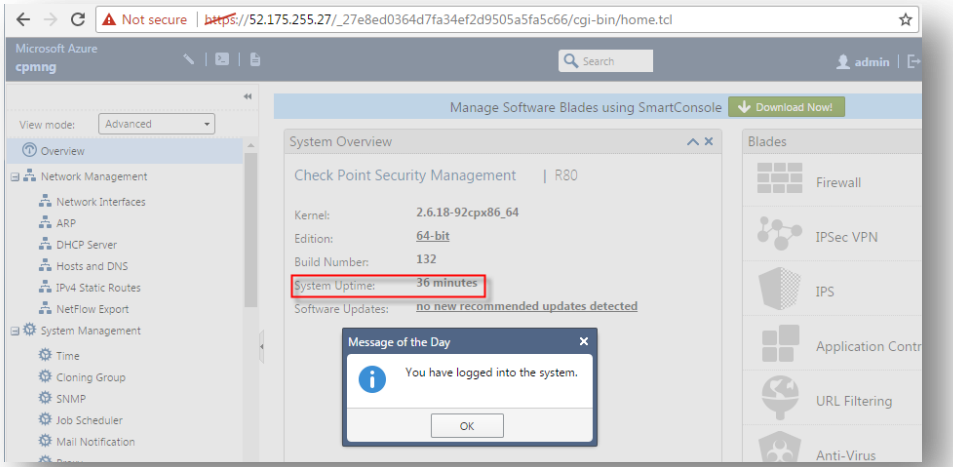
Size
Standard D3 v2 (4 cores, 14 GB memory)

Public IP address
52.175.255.27

Virtual network/subnet
myVNET/FrontEnd

DNS name
cpmng-vglhcfg62c5ua.westus2.cloudapp.azure.com

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.

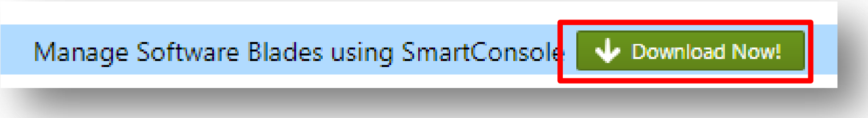


Check Point Security Management | R80

Kernel: 2.6.18-92cpx86_64
Edition: 64-bit
Build Number: 132
System Uptime: 36 minutes
Software Updates: no new recommended updates detected

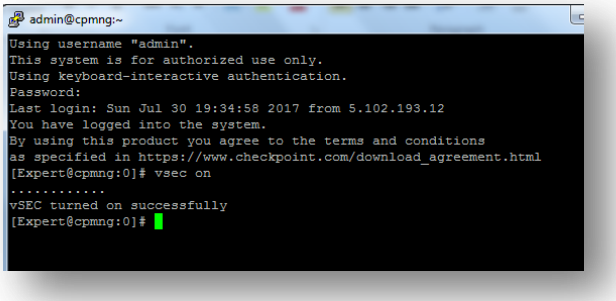
Message of the Day
You have logged into the system.
OK

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



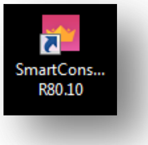
Install it with the default configuration (make sure it's R80.10 smart console).

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

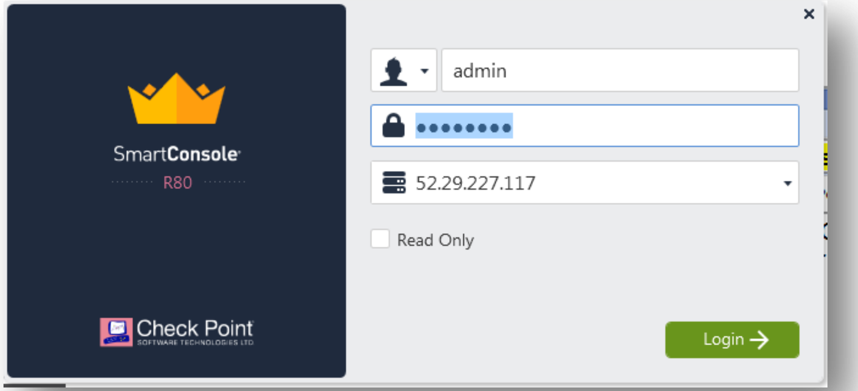


```
Using username "admin".
This system is for authorized use only.
Using keyboard-interactive authentication.
Password:
Last login: Sun Jul 30 19:34:58 2017 from 5.102.193.12
You have logged into the system.
By using this product you agree to the terms and conditions
as specified in https://www.checkpoint.com/download_agreement.html
[Expert@cpmng:0]# vsec on
...........
vSEC turned on successfully
[Expert@cpmng:0]#
```

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



admin

••••••••

52.29.227.117

□ Read Only

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

You have finished exercise 2

Exercise #3 - Deploy Check Point Gateway on Azure

Description

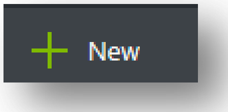
This exercise will guide you through the installation and configuration of Check Point's vSEC gateway on the environment created in Azure.

Method

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

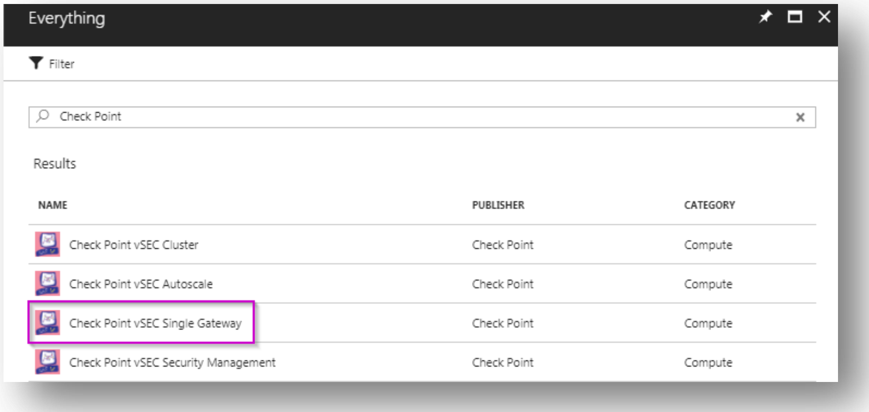
How

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)



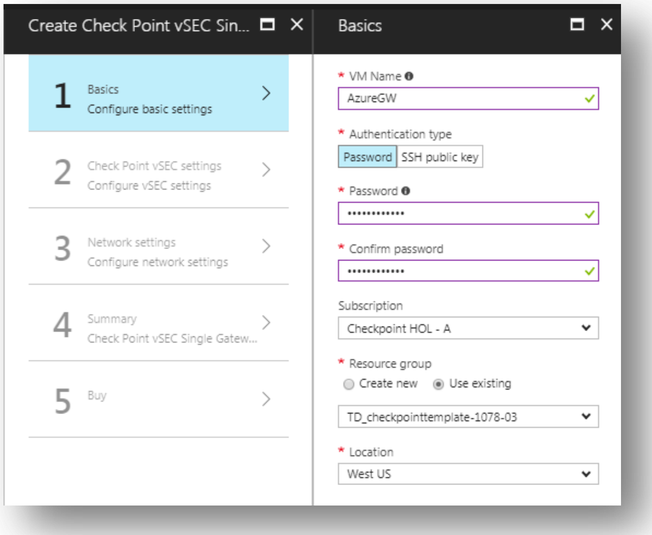
Check Point

Results

NAME	PUBLISHER	CATEGORY
Check Point vSEC Cluster	Check Point	Compute
Check Point vSEC Autoscale	Check Point	Compute
Check Point vSEC Single Gateway	Check Point	Compute
Check Point vSEC Security Management	Check Point	Compute

And then click on "create"

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



Create Check Point vSEC Sin...

1 Basics
Configure basic settings

2 Check Point vSEC settings
Configure vSEC settings

3 Network settings
Configure network settings

4 Summary
Check Point vSEC Single Gatew...

5 Buy

Basics

* VM Name
AzureGW ✓

* Authentication type
Password | SSH public key

* Password
•••••••••••• ✓

* Confirm password
•••••••••••• ✓

Subscription
Checkpoint HOL - A

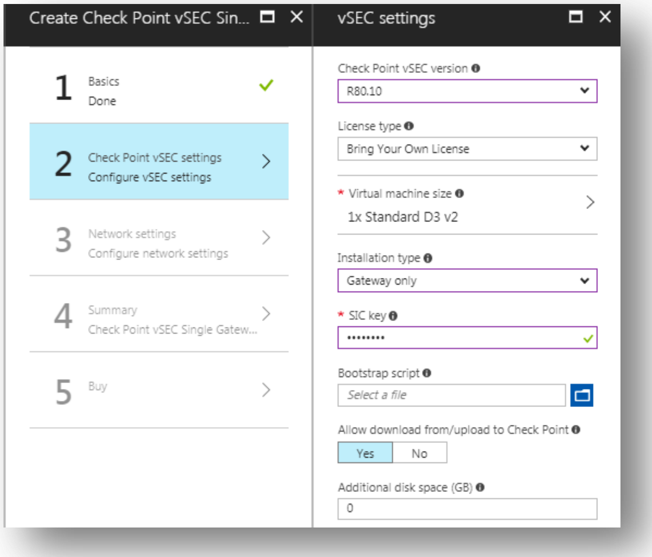
* Resource group
○ Create new ● Use existing

TD_checkpointtemplate-1078-03

* Location
West US

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.



Create Check Point vSEC Sin...

1 Basics
Done ✓

2 Check Point vSEC settings
Configure vSEC settings

3 Network settings
Configure network settings

4 Summary
Check Point vSEC Single Gatew...

5 Buy

vSEC settings

Check Point vSEC version
R80.10

License type
Bring Your Own License

* Virtual machine size
1x Standard D3 v2

Installation type
Gateway only

* SIC key
•••••••• ✓

Bootstrap script
Select a file

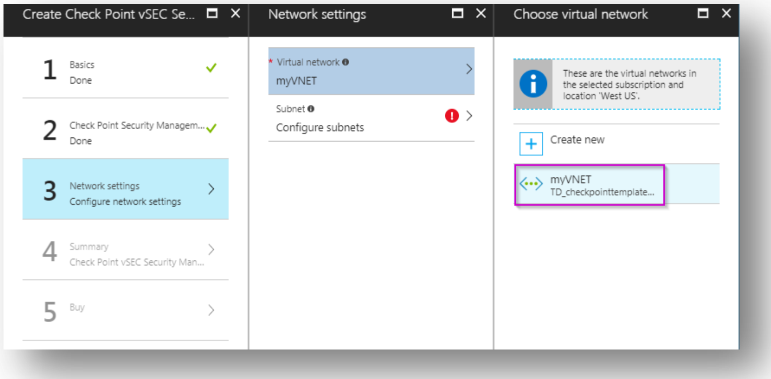
Allow download from/upload to Check Point
Yes | No

Additional disk space (GB)
0

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

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



Create Check Point vSEC Se...

1 Basics
Done ✓

2 Check Point Security Managem... ✓
Done

3 Network settings
Configure network settings

4 Summary
Check Point vSEC Security Man...

5 Buy

Network settings

* Virtual network
myVNET

Subnet
Configure subnets

Choose virtual network

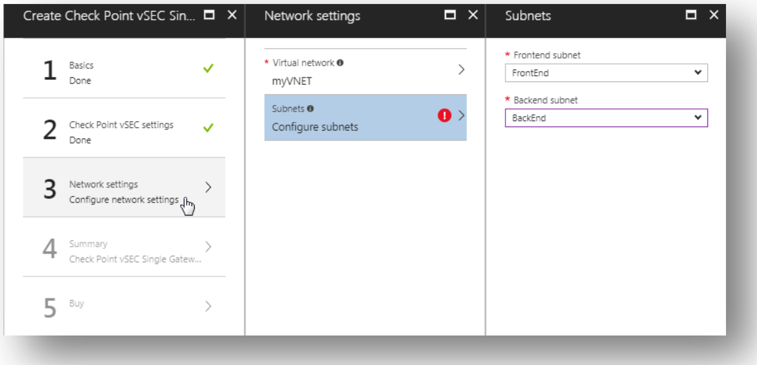
These are the virtual networks in the selected subscription and location 'West US'.

Create new

myVNET
TD_checkpointtemplate...

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)



Create Check Point vSEC Sin...

1 Basics
Done ✓

2 Check Point vSEC settings ✓
Done

3 Network settings
Configure network settings

4 Summary
Check Point vSEC Single Gatew...

5 Buy

Network settings

* Virtual network
myVNET

Subnets
Configure subnets

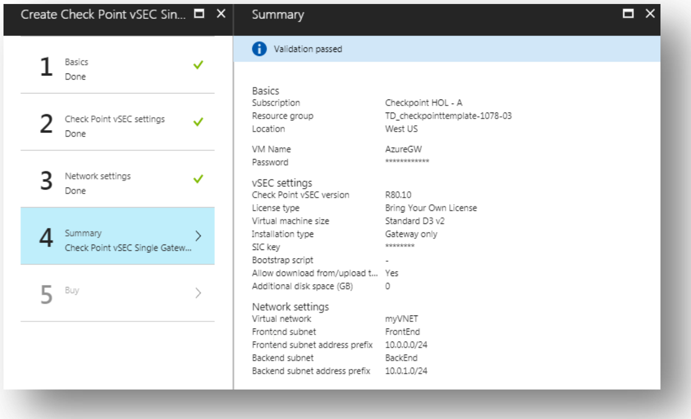
Subnets

* Frontend subnet: FrontEnd

* Backend subnet: 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".



Create Check Point vSEC Sin...

1 Basics
Done ✓

2 Check Point vSEC settings ✓
Done

3 Network settings ✓
Done

4 Summary
Check Point vSEC Single Gatew...

5 Buy

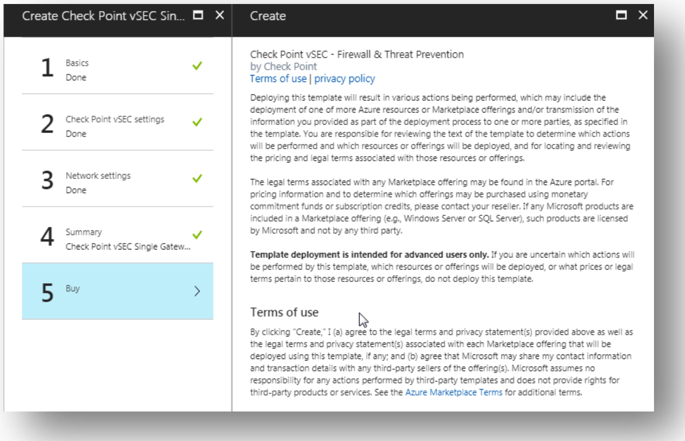
Summary

Validation passed

Basics	
Subscription	Checkpoint HOL - A
Resource group	TD_checkpointtemplate-1078-03
Location	West US
VM Name	AzureGW
Password	************
vSEC settings	
Check Point vSEC version	R80.10
License type	Bring Your Own License
Virtual machine size	Standard D3 v2
Installation type	Gateway only
SIC key	********
Bootstrap script	-
Allow download from/upload t...	Yes
Additional disk space (GB)	0
Network settings	
Virtual network	myVNET
Frontend subnet	FrontEnd
Frontend subnet address prefix	10.0.0.0/24
Backend subnet	BackEnd
Backend subnet address prefix	10.0.1.0/24

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)


Create Check Point vSEC Sin...
1 Basics Done
2 Check Point vSEC settings Done
3 Network settings Done
4 Summary Check Point vSEC Single Gatew...
5 Buy
Create

Check Point vSEC - Firewall & Threat Prevention
by Check Point
Terms of use | privacy policy

Deploying this template will result in various actions being performed, which may include the deployment of one of 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.

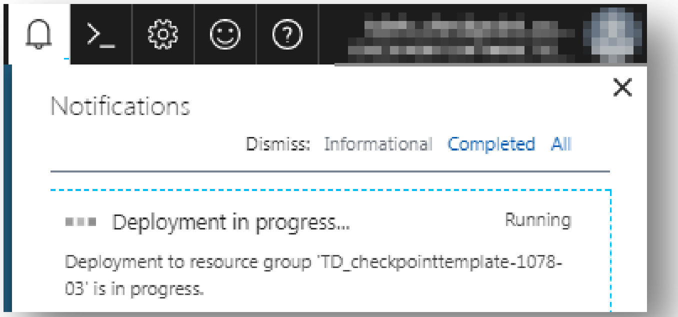
The legal terms associated with any Marketplace offering may be found in the Azure portal. For pricing information and to determine which offerings may be purchased using monetary commitment funds or subscription credits, please contact your reseller. If any Microsoft products are included in a Marketplace 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.

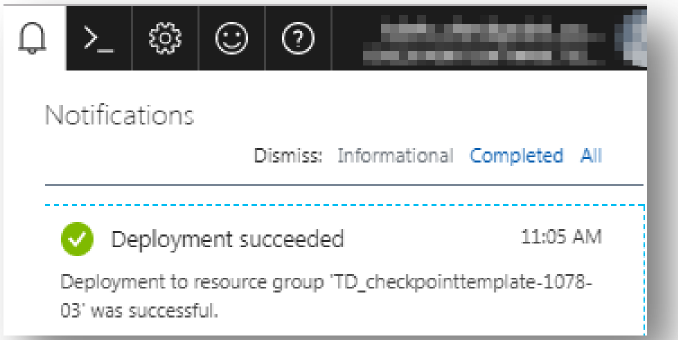
6. The gateway will now be created. You should be able to see creation progress by clicking on the bell icon on the top right corner of the screen (as shown)



Deployment in progress... Running

Deployment to resource group 'TD_checkpointtemplate-1078-03' is in progress.

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

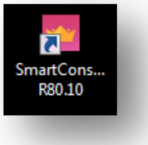


Deployment succeeded 11:05 AM

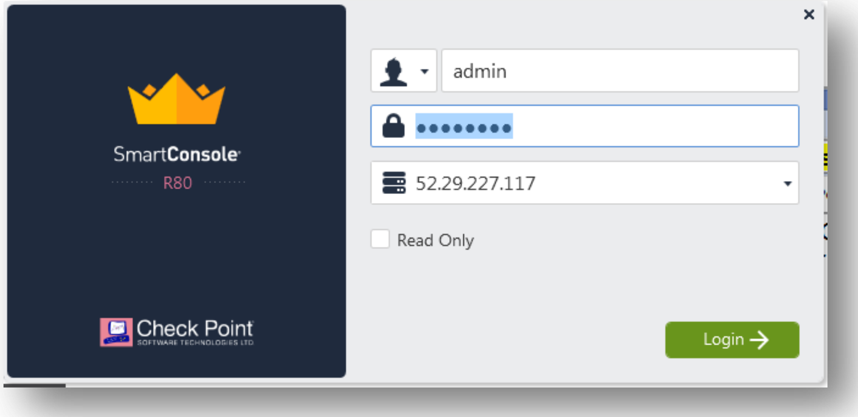
Deployment to resource group 'TD_checkpointtemplate-1078-03' was successful.

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

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



admin

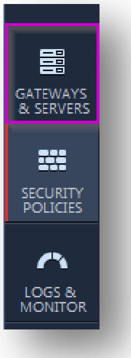
●●●●●●●●

52.29.227.117

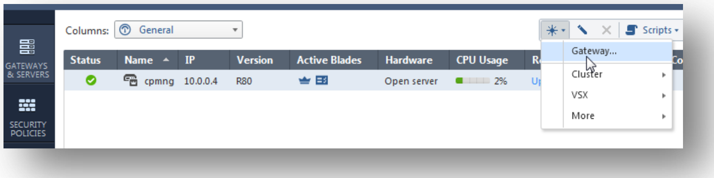
□ Read Only

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



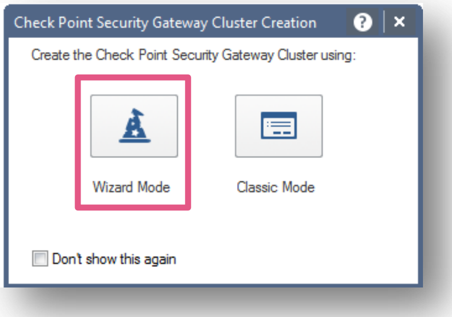
   b. In the upper middle of the screen choose to add new Gateway object



Columns: General

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	R	Co
✓	cpmng	10.0.0.4	R80		Open server	2%	Up	

c. On the box that opened choose wizard mode

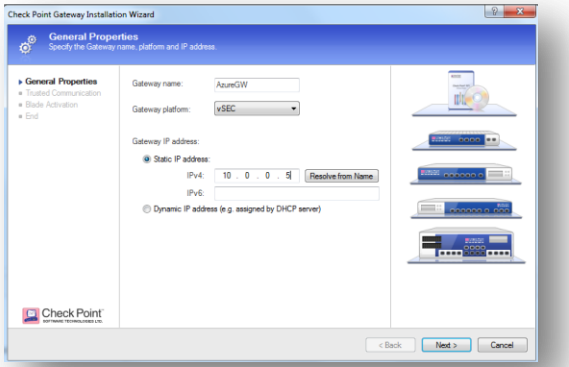


Check Point Security Gateway Cluster Creation

Create the Check Point Security Gateway Cluster using:

□ Don't show this again

d. Fill in the details as listed below:



Check Point Gateway Installation Wizard

General Properties

Specify the Gateway name, platform and IP address.

Gateway name: AzureGW

Gateway platform: vSEC

Gateway IP address:

● Static IP address:

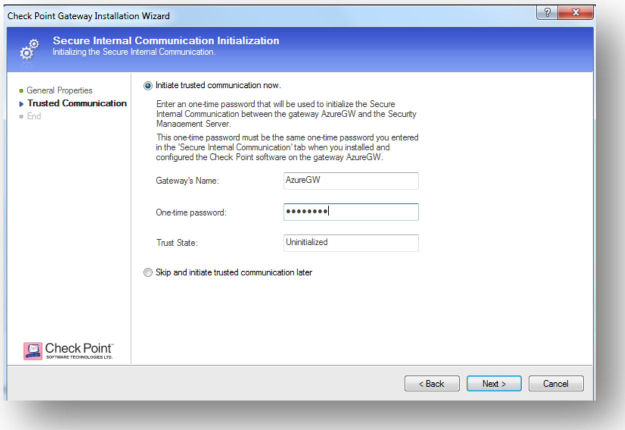
IPv4: 10 . 0 . 0 . 5

IPv6:

○ Dynamic IP address (e.g. assigned by DHCP server)

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:



Check Point Gateway Installation Wizard

Secure Internal Communication Initialization
Initializing the Secure Internal Communication.

- General Properties
- **Trusted Communication**
- End

● Initiate trusted communication now.

Enter an one-time password that will be used to initialize the Secure Internal Communication between the gateway AzureGW and the Security Management Server.

This one-time password must be the same one-time password you entered in the 'Secure Internal Communication' tab when you installed and configured the Check Point software on the gateway AzureGW.

Gateway's Name: AzureGW

One-time password: ••••••••

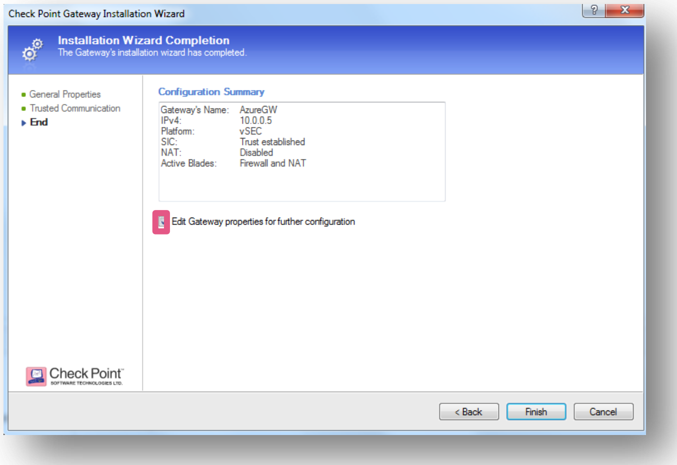
Trust State: Uninitialized

○ Skip and initiate trusted communication later

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



Check Point Gateway Installation Wizard

Installation Wizard Completion
The Gateway's installation wizard has completed.

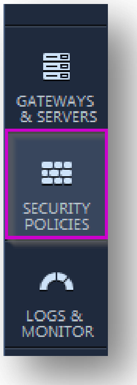
- General Properties
- Trusted Communication
- **End**

Configuration Summary

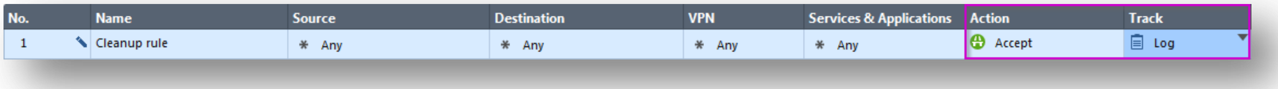
```
Gateway's Name:   AzureGW
IPv4:             10.0.0.5
Platform:         vSEC
SIC:              Trust established
NAT:              Disabled
Active Blades:    Firewall and NAT
```

Edit Gateway properties for further configuration

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

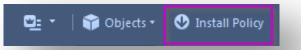


10. Change the existing rule to allow all traffic by changing the action to accept and adding Log

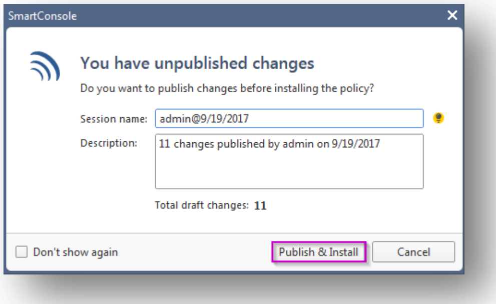


No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Cleanup rule	Any	Any	Any	Any	Accept	Log

11. On the upper left side click Install policy



a. Click the Publish & Install



SmartConsole

You have unpublished changes

Do you want to publish changes before installing the policy?

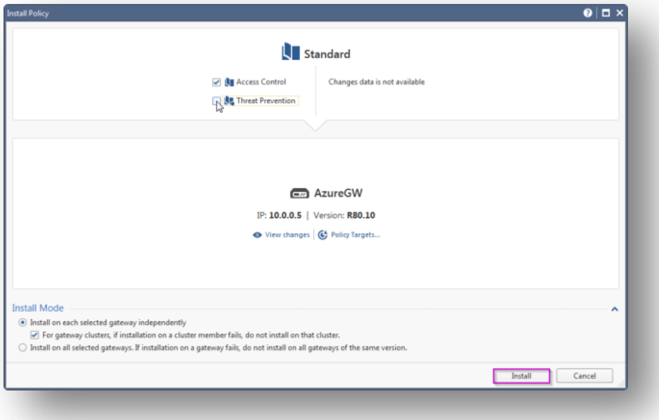
Session name: admin@9/19/2017

Description: 11 changes published by admin on 9/19/2017

Total draft changes: 11

□ Don't show again

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



Install Policy

Standard

☑ Access Control

□ Threat Prevention

Changes data is not available

AzureGW

IP: 10.0.0.5 | Version: R80.10

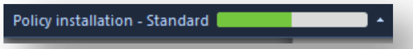
Install Mode

● Install on each selected gateway independently

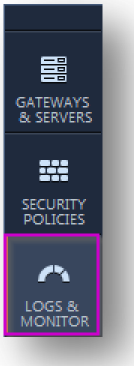
☑ For gateway clusters, if installation on a cluster member fails, do not install on that cluster.

○ Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.

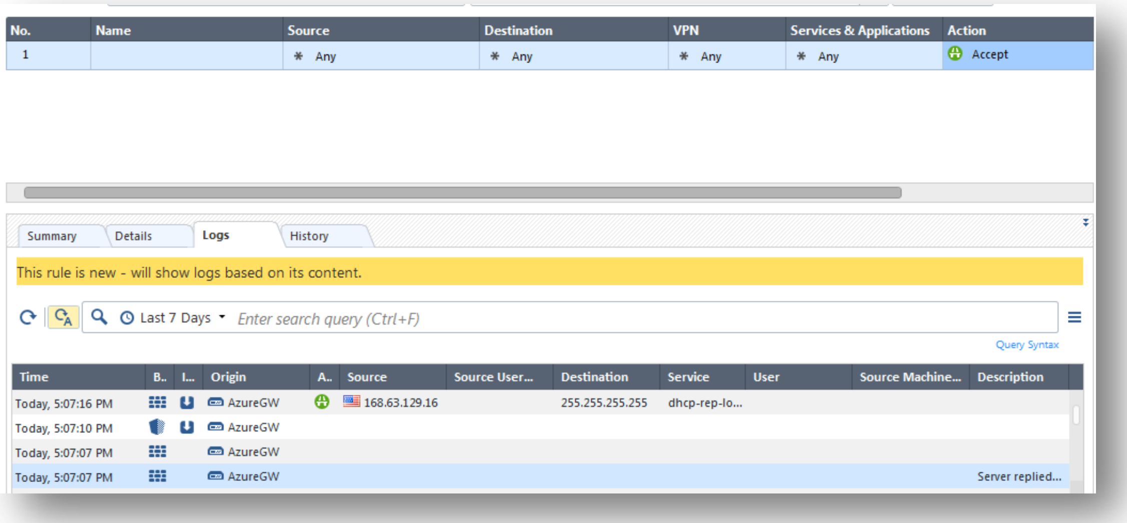
c. You can see the progress on the bottom left side



12. on the left bar choose security Policies



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



No.	Name	Source	Destination	VPN	Services & Applications	Action
1		Any	Any	Any	Any	Accept

This rule is new - will show logs based on its content.

Time	B..	I...	Origin	A..	Source	Source User...	Destination	Service	User	Source Machine...	Description
Today, 5:07:16 PM			AzureGW		168.63.129.16		255.255.255.255	dhcp-rep-lo...			
Today, 5:07:10 PM			AzureGW								
Today, 5:07:07 PM			AzureGW								
Today, 5:07:07 PM			AzureGW								Server replied...

You have finished exercise 3

Exercise #4 – Creating a web server

Description

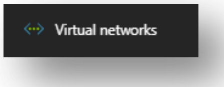
This exercise will guide you through the installation and configuration of a simple web server into the environment we created in previous exercises. This web server will then be protected by the firewall gateway (controlling traffic to/from it)

Method

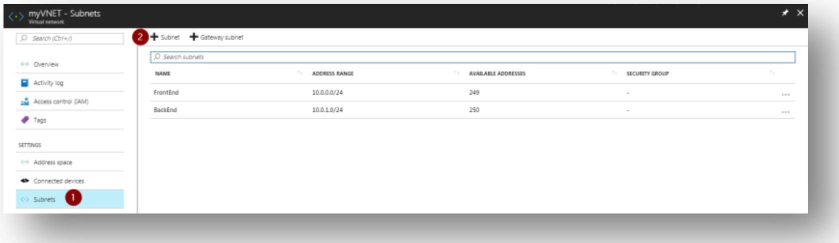
Using Azure portal, you will provision a web server and place it inside the environment (behind the firewall)

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

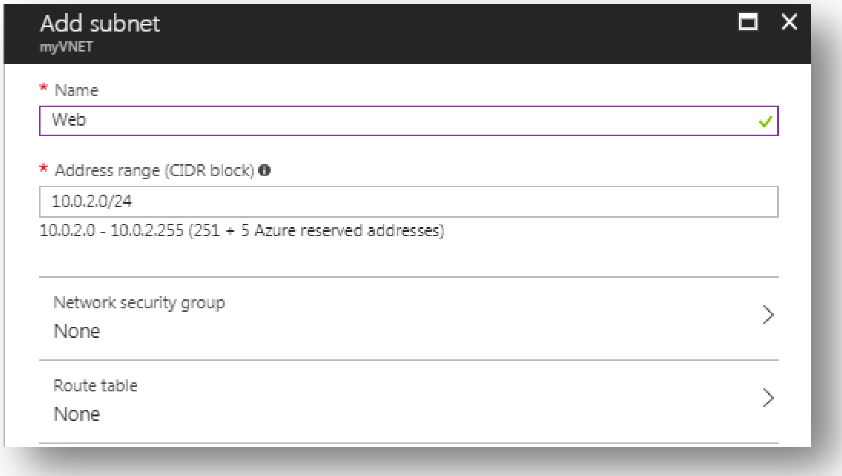


3. Choose myVNET (1) then click on "+ Subnets" (2) to add a new subnet



NAME	ADDRESS RANGE	AVAILABLE ADDRESSES	SECURITY GROUP
FrontEnd	10.0.0.0/24	249	-
BackEnd	10.0.1.0/24	250	-

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



* Name
Web

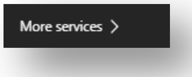
* Address range (CIDR block)
10.0.2.0/24
10.0.2.0 - 10.0.2.255 (251 + 5 Azure reserved addresses)

Network security group
None

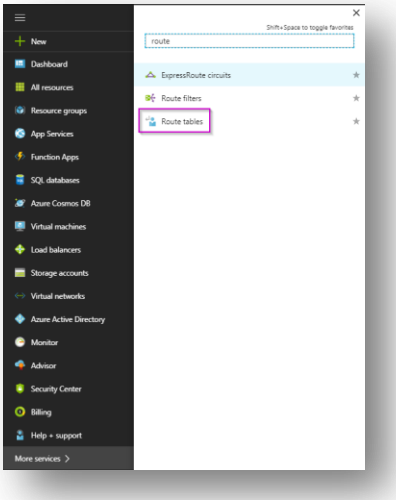
Route table
None

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"

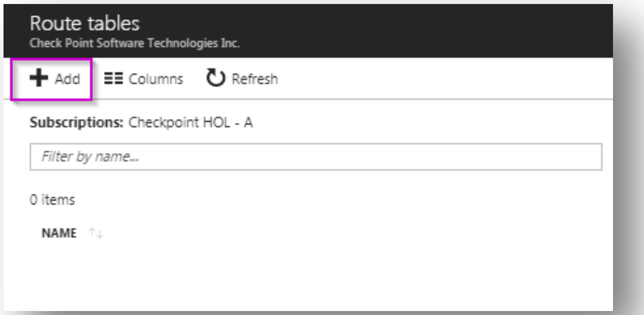


6. In the new windows search for "route" and choose the "Route Table"



route

7. Once inside, click on "+ add".



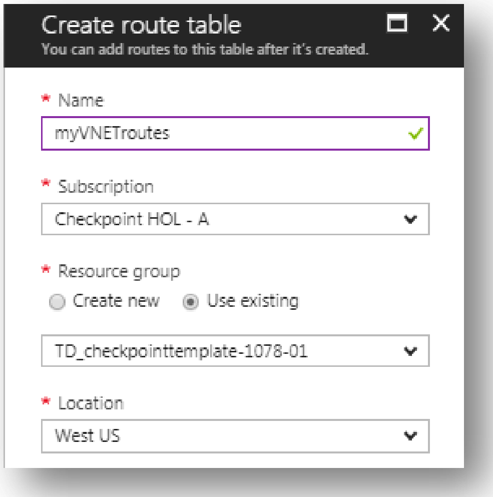
Route tables
Check Point Software Technologies Inc.

Subscriptions: Checkpoint HOL - A

Filter by name...

0 items

8. The first item is to create a route table



Create route table

You can add routes to this table after it's created.

* Name

myVNETroutes ✓

* Subscription

Checkpoint HOL - A

* Resource group

○ Create new ● Use existing

TD_checkpointtemplate-1078-01

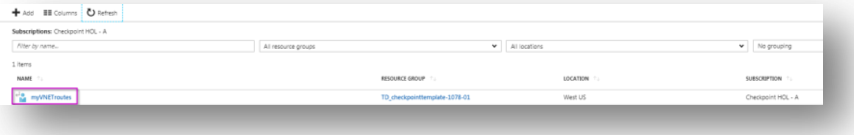
* Location

West US

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



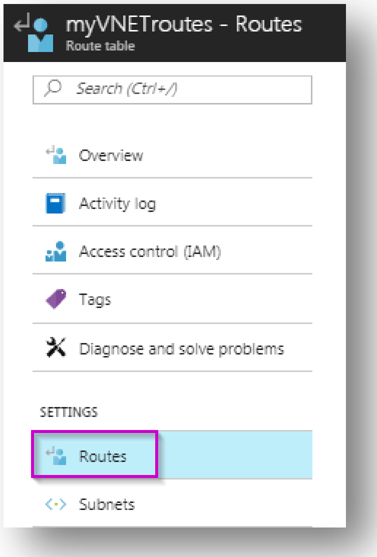
Subscriptions: Checkpoint HOL - A

Filter by name... | All resource groups | All locations | No grouping

1 items

NAME	RESOURCE GROUP	LOCATION	SUBSCRIPTION
myVNETroutes	TD_checkpointtemplate-1078-01	West US	Checkpoint HOL - A

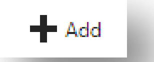
10. On the open bar click on routes



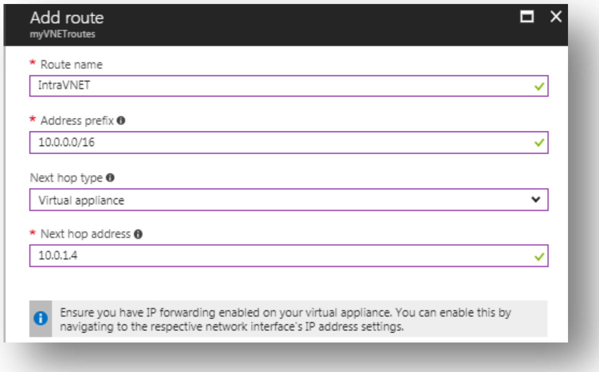
myVNETroutes - Routes

Route table

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



12. Fill in the following information


Add route
myVNETroutes

* Route name
IntraVNET

* Address prefix
10.0.0.0/16

Next hop type
Virtual appliance

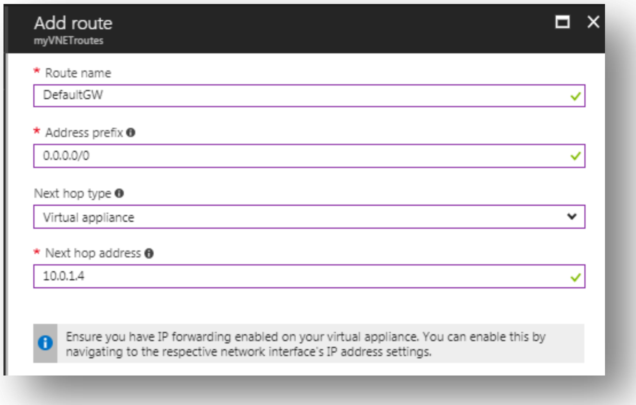
* Next hop address
10.0.1.4

Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

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)


Add route
myVNETroutes

* Route name
DefaultGW

* Address prefix
0.0.0.0/0

Next hop type
Virtual appliance

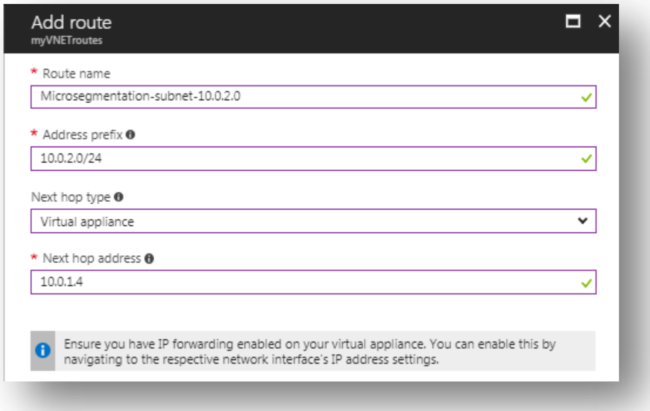
* Next hop address
10.0.1.4

Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

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

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).



Add route
myVNETroutes

* Route name
Microsegmentation-subnet-10.0.2.0

* Address prefix
10.0.2.0/24

Next hop type
Virtual appliance

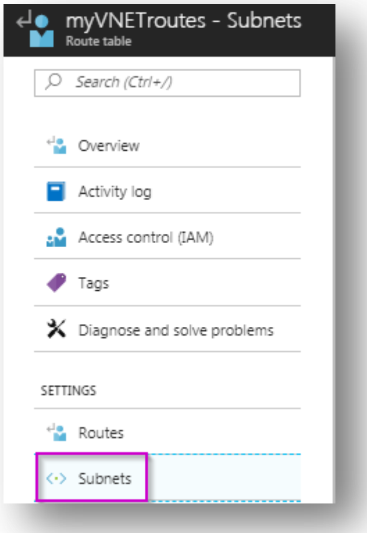
* Next hop address
10.0.1.4

Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

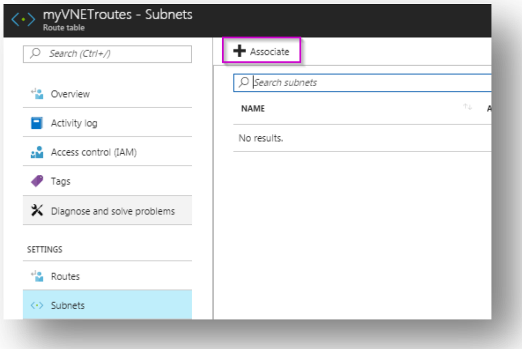
Route name: Micorsegmentation-subnet-10.0.2.0
Address prefix: 10.0.2.0/24
Next hop type: virtual appliance
Next hop address: pay attention that the "Next hop address" should be filled with the Gateway Internal IP.
Click on "ok" when done

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

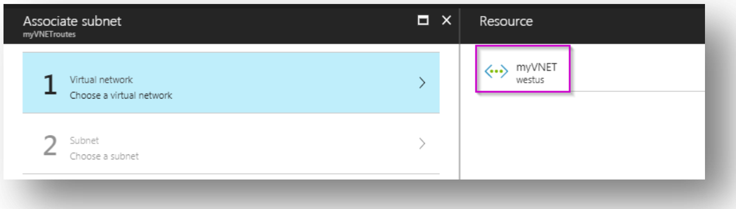
15. After adding the route, we need to associate the subnet will use with that route table, on the route table list on the left side click on the "subnets"



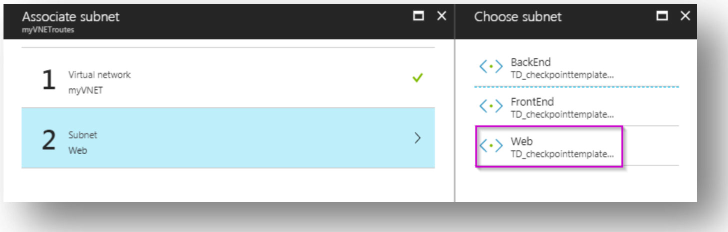
16. Click on Associate.



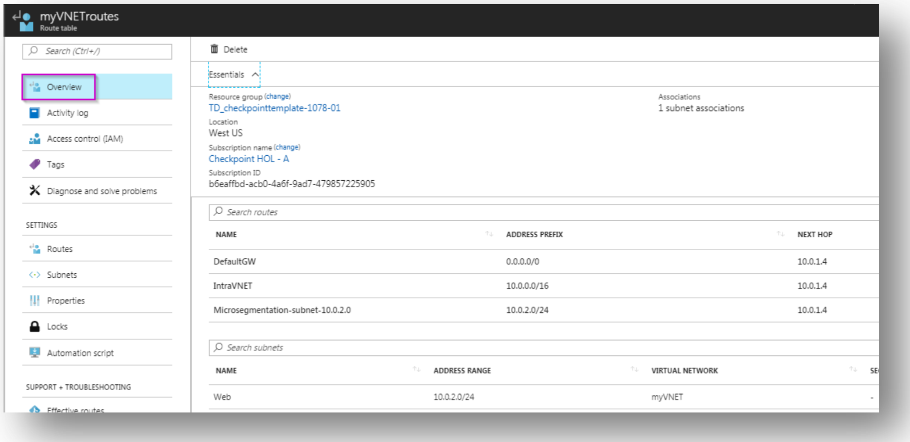
17. Choose your VNET



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



Resource group (change)
TD_checkpointtemplate-1078-01

Location
West US

Subscription name (change)
Checkpoint HOL - A

Subscription ID
b6eaffbd-acb0-4a6f-9ad7-479857225905

Associations
1 subnet associations

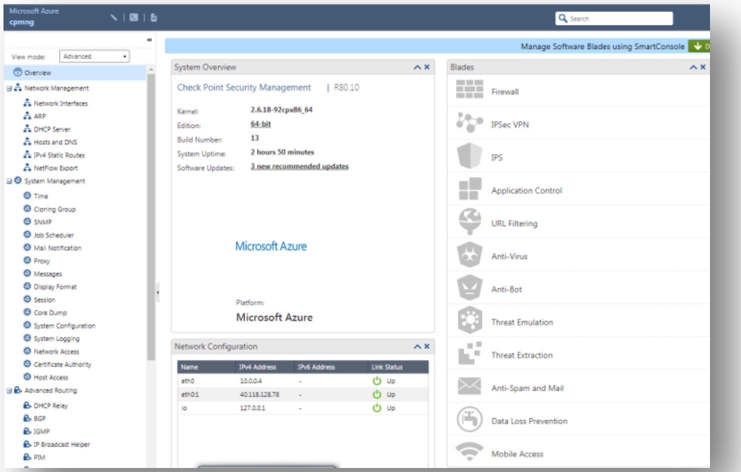
Search routes

NAME	ADDRESS PREFIX	NEXT HOP
DefaultGW	0.0.0.0/0	10.0.1.4
IntraVNET	10.0.0.0/16	10.0.1.4
Microsegmentation-subnet-10.0.2.0	10.0.2.0/24	10.0.1.4

Search subnets

NAME	ADDRESS RANGE	VIRTUAL NETWORK	SE
Web	10.0.2.0/24	myVNET	-

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.



System Overview

Check Point Security Management | R80.10

Kernel: 2.6.18-92cpx86_64
Edition: 64-bit
Build Number: 13
System Uptime: 2 hours 50 minutes
Software Updates: 3 new recommended updates

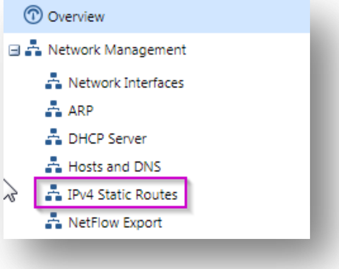
Microsoft Azure

Platform: Microsoft Azure

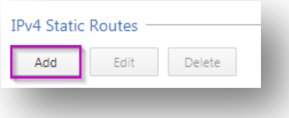
Network Configuration

Name	IPv4 Address	IPv6 Address	Link Status
eth0	10.0.0.4	-	Up
eth0:1	40.118.128.78	-	Up
lo	127.0.0.1	-	Up

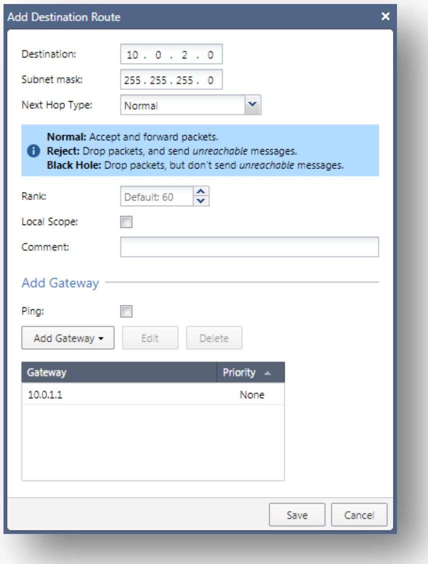
21. Navigate to Network Management, on the bar at the left side and click on IPv4 Static Routes.



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



23. Fill in the relevant fields as described below:



Add Destination Route

Destination: 10 . 0 . 2 . 0

Subnet mask: 255 . 255 . 255 . 0

Next Hop Type: Normal

Normal: Accept and forward packets.
Reject: Drop packets, and send *unreachable* messages.
Black Hole: Drop packets, but don't send *unreachable* messages.

Rank: Default: 60

Local Scope: □

Comment:

Add Gateway

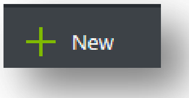
Ping: □

Gateway	Priority
10.0.1.1	None

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)

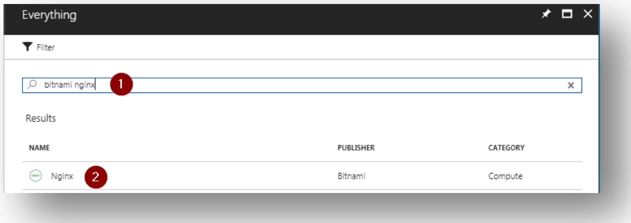
Creating a Web server

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)



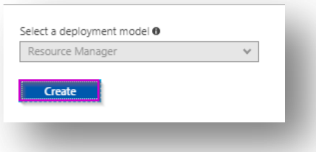
Everything

bitnami nginx

Results

NAME	PUBLISHER	CATEGORY
Nginx	Bitnami	Compute

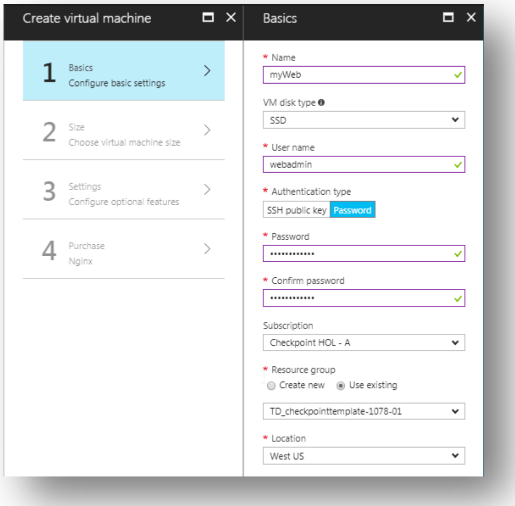
And then click on "create"



Select a deployment model

Resource Manager

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



Create virtual machine

1 Basics
Configure basic settings

2 Size
Choose virtual machine size

3 Settings
Configure optional features

4 Purchase
Nginx

Basics

* Name: myWeb

VM disk type: SSD

* User name: webadmin

* Authentication type: SSH public key | Password

* Password: ••••••••••••

* Confirm password: ••••••••••••

Subscription: Checkpoint HOL - A

* Resource group: ○ Create new ● Use existing

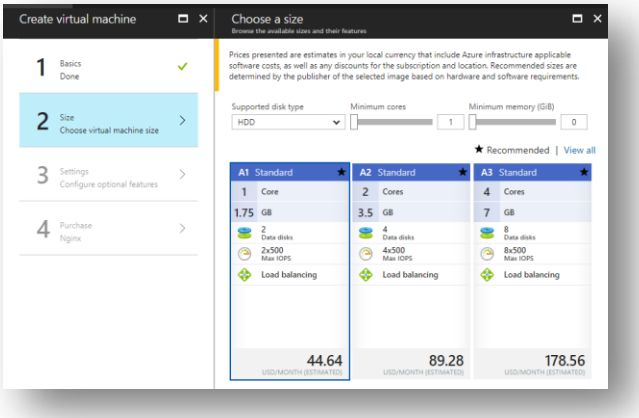
TD_checkpointtemplate-1078-01

* Location: West US

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)



Create virtual machine

1 Basics
Done ✓

2 Size
Choose virtual machine size

3 Settings
Configure optional features

4 Purchase
Nginx

Choose a size
Browse the available sizes and their features

Prices presented are estimates in your local currency that include Azure infrastructure applicable software costs, as well as any discounts for the subscription and location. Recommended sizes are determined by the publisher of the selected image based on hardware and software requirements.

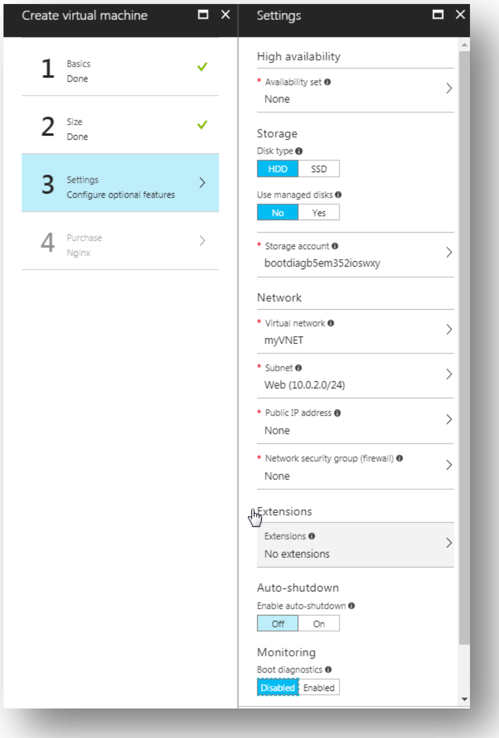
Supported disk type: HDD
Minimum cores: 1
Minimum memory (GiB): 0

★ 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
44.64 USD/MONTH (ESTIMATED)	89.28 USD/MONTH (ESTIMATED)	178.56 USD/MONTH (ESTIMATED)

And click on “select”

29. Choose the characteristics of your new virtual machine:



Create virtual machine

1 Basics
Done

2 Size
Done

3 Settings
Configure optional features

4 Purchase
Nginx

Settings

High availability

* Availability set
None

Storage

Disk type
HDD | SSD

Use managed disks
No | Yes

* Storage account
bootdiagb5em352ioswxy

Network

* Virtual network
myVNET

* Subnet
Web (10.0.2.0/24)

* Public IP address
None

* Network security group (firewall)
None

Extensions

Extensions
No extensions

Auto-shutdown

Enable auto-shutdown
Off | On

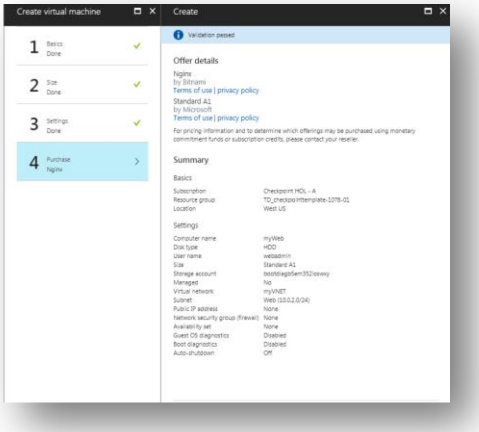
Monitoring

Boot diagnostics
Disabled | Enabled

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.



Create virtual machine

1 Basics
Done

2 Size
Done

3 Settings
Done

4 Purchase
Nginx

Create

Validation passed

Offer details

Nginx
by Bitnami
Terms of use | privacy policy

Standard A1
by Microsoft
Terms of use | privacy policy

For pricing information and to determine which offerings may be purchased using monetary commitment funds or subscription credits, please contact your reseller.

Summary

Basics

Subscription	Checkpoint HOL - A
Resource group	TD_checkpointtemplate-1078-01
Location	West US

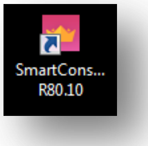
Settings

Computer name	myWeb
Disk type	HDD
User name	webadmin
Size	Standard A1
Storage account	bootdiagb5em352ioswxy
Managed	No
Virtual network	myVNET
Subnet	Web (10.0.2.0/24)
Public IP address	None
Network security group (firewall)	None
Availability set	None
Guest OS diagnostics	Disabled
Boot diagnostics	Disabled
Auto-shutdown	Off

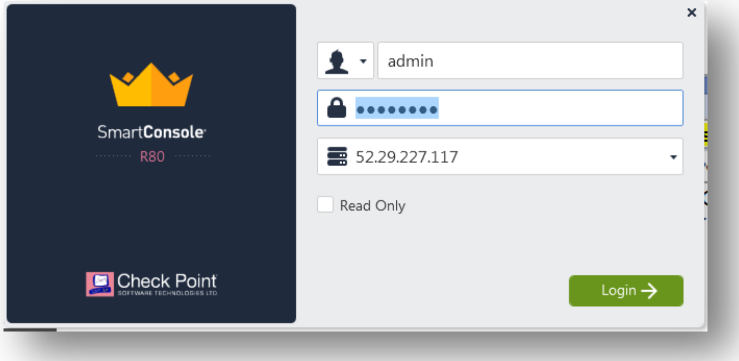
Note: there is no way to set the virtual machine private IP address at that stage, so the virtual machine actually gets auto-assigned with an IP (DHCP) and you are able to change it later on (after deployment)

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



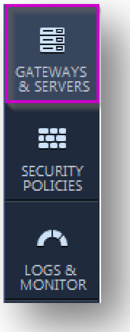
admin

••••••••

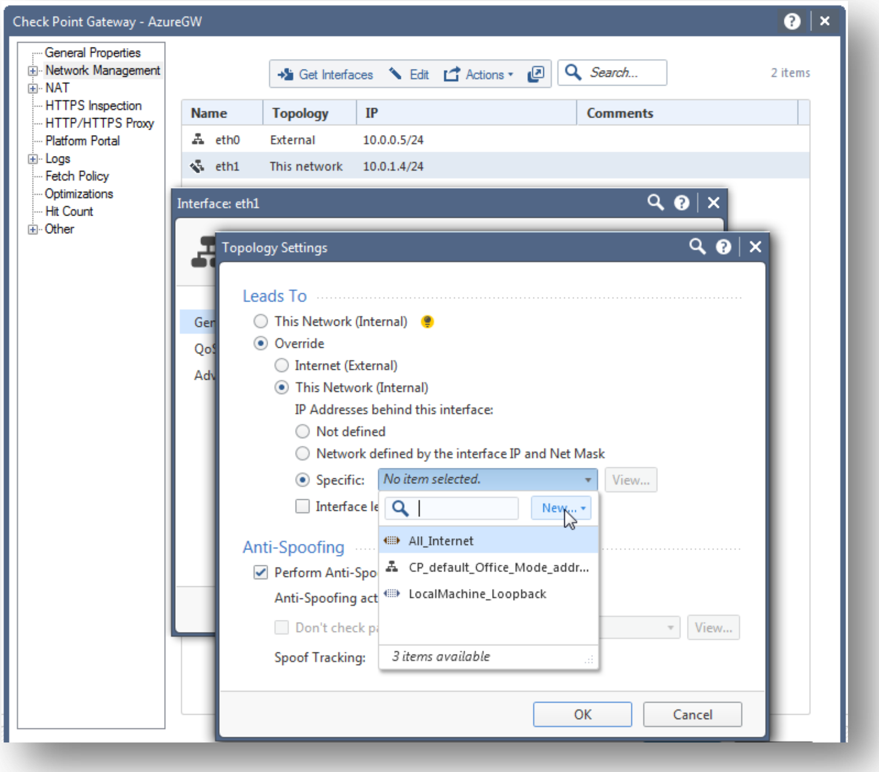
52.29.227.117

□ Read Only

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


Check Point Gateway - AzureGW

- General Properties
- Network Management
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- Platform Portal
- Logs
- Fetch Policy
- Optimizations
- Hit Count
- Other

2 items

Name	Topology	IP	Comments
eth0	External	10.0.0.5/24	
eth1	This network	10.0.1.4/24	

Interface: eth1

Topology Settings

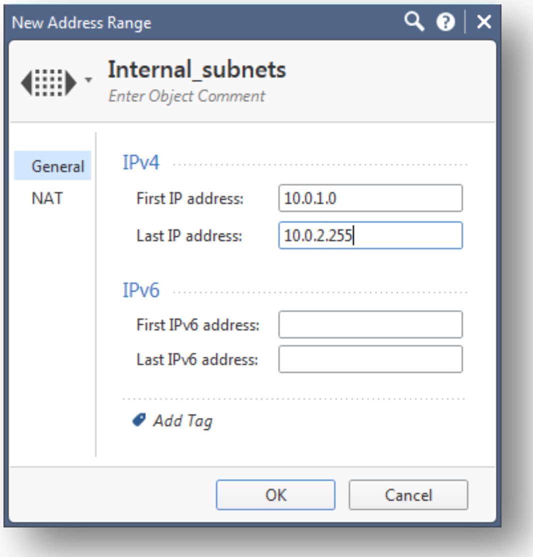
Leads To
- ○ This Network (Internal)
- ● Override
  - ○ Internet (External)
  - ● This Network (Internal)
    - IP Addresses behind this interface:
    - ○ Not defined
    - ○ Network defined by the interface IP and Net Mask
    - ● Specific: No item selected.
    - □ Interface le

- All_Internet
- CP_default_Office_Mode_addr...
- LocalMachine_Loopback

3 items available

Anti-Spoofing
- ☑ Perform Anti-Spo
- Anti-Spoofing act
- □ Don't check p
- Spoof Tracking:

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


New Address Range

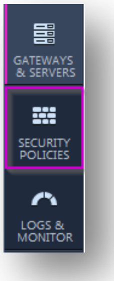
Internal_subnets
Enter Object Comment

IPv4
First IP address: 10.0.1.0
Last IP address: 10.0.2.255

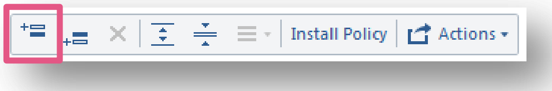
IPv6
First IPv6 address:
Last IPv6 address:

Click OK and than OK and another time.

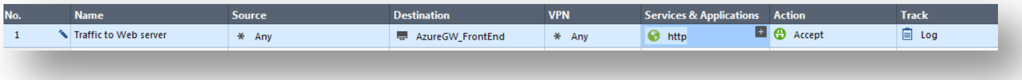
32. on the left bar choose Security Policies



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

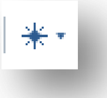


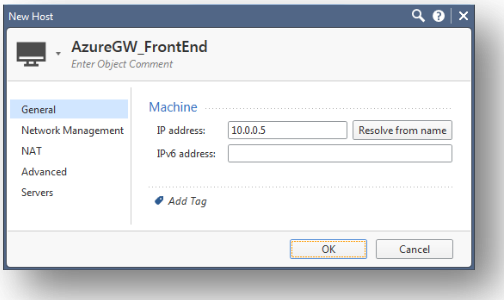
39. This rule will allow http traffic to the Web server from the internet, fill in the relevant fields:



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Traffic to Web server	Any	AzureGW_FrontEnd	Any	http	Accept	Log

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





AzureGW_FrontEnd

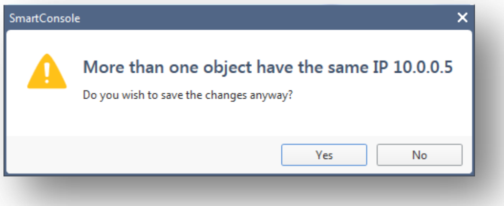
IP address: 10.0.0.5

IPv6 address:

Name: AzureGW_FrontEnd
IPv4 Address: 10.0.0.5

Click OK.

Acknowledge the warning as it is expected:

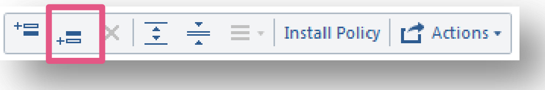


More than one object have the same IP 10.0.0.5

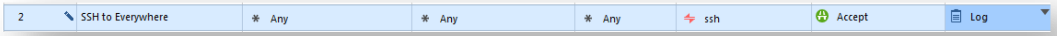
Do you wish to save the changes anyway?

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



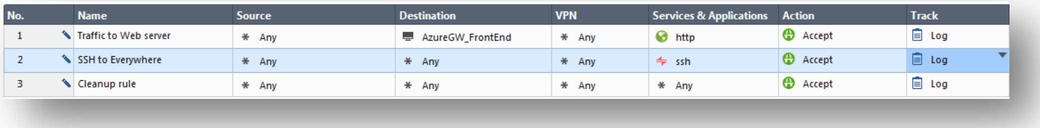
41. Create another rule for administration and troubleshooting of the lab



2	SSH to Everywhere	Any	Any	Any	ssh	Accept	Log

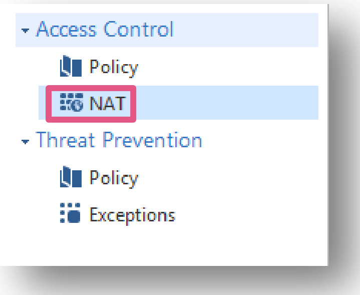
a. Name: SSH to Everywhere
b. Source: Any
c. Destination: Any
d. Services & Applications: (click on the + sign) search for SSH
e. Action: Allow
f. Track: Log

42. Your security rulesets should look like that:

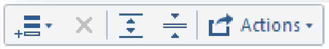


No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Traffic to Web server	Any	AzureGW_FrontEnd	Any	http	Accept	Log
2	SSH to Everywhere	Any	Any	Any	ssh	Accept	Log
3	Cleanup rule	Any	Any	Any	Any	Accept	Log

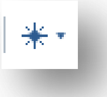
43. At the left bar choose the NAT policy

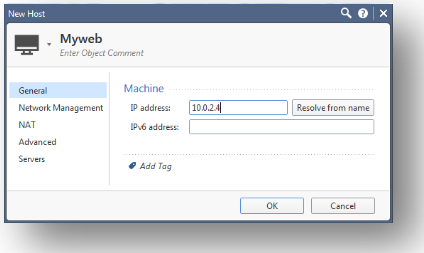


44. On the upper central bar choose add rule above



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)





Myweb

IP address: 10.0.2.4

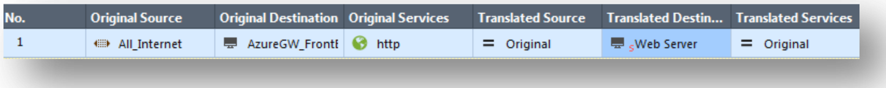
IPv6 address:

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

Click OK.

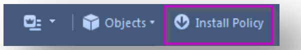
Translated Service: Original

NAT Rule:

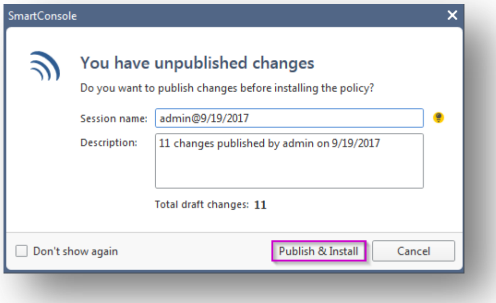


No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services
1	All_Internet	AzureGW_Frontl	http	= Original	Web Server	= Original

14. On the upper left side click Install policy



d. Click the Publish & Install



SmartConsole

You have unpublished changes

Do you want to publish changes before installing the policy?

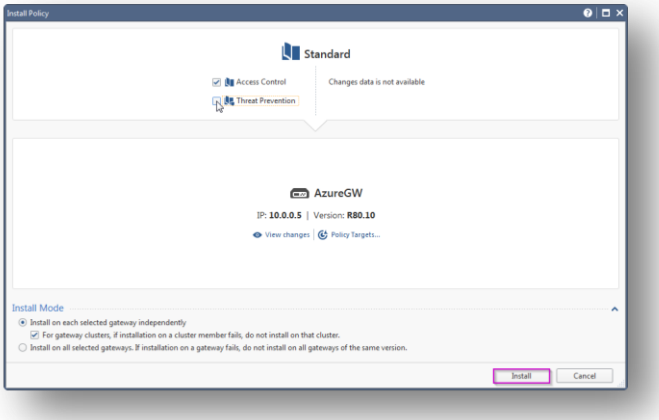
Session name: admin@9/19/2017

Description: 11 changes published by admin on 9/19/2017

Total draft changes: **11**

□ Don't show again

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



Install Policy

Standard

☑ Access Control

□ Threat Prevention

Changes data is not available

AzureGW

IP: **10.0.0.5** | Version: **R80.10**

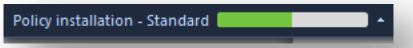
Install Mode

● Install on each selected gateway independently

☑ For gateway clusters, if installation on a cluster member fails, do not install on that cluster.

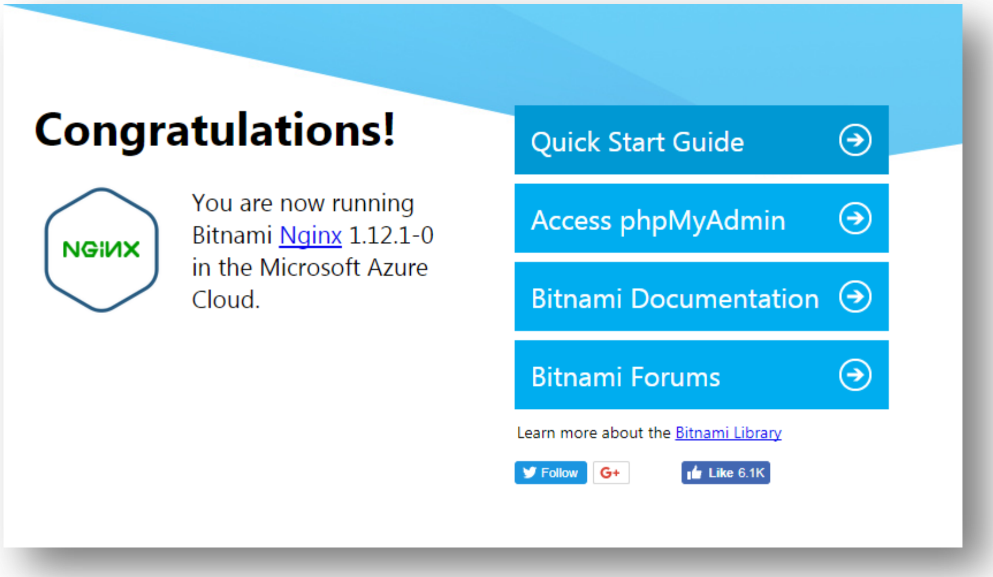
○ Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.

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



Policy installation - Standard

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.



Congratulations!

You are now running Bitnami Nginx 1.12.1-0 in the Microsoft Azure Cloud.

Learn more about the Bitnami Library

You have finished exercise 4

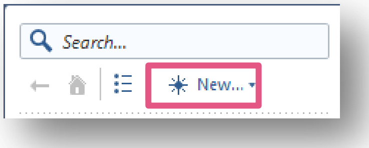
Exercise #5 – Connecting vSEC Controller

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

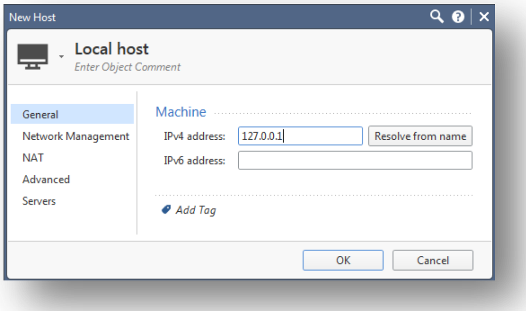
The suggested way of assigning those permissions is using Service Principal (SPN), you can find on appendix 1 the instructions on how to configure SPN.

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



Local host

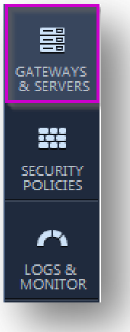
IPv4 address: 127.0.0.1

IPv6 address:

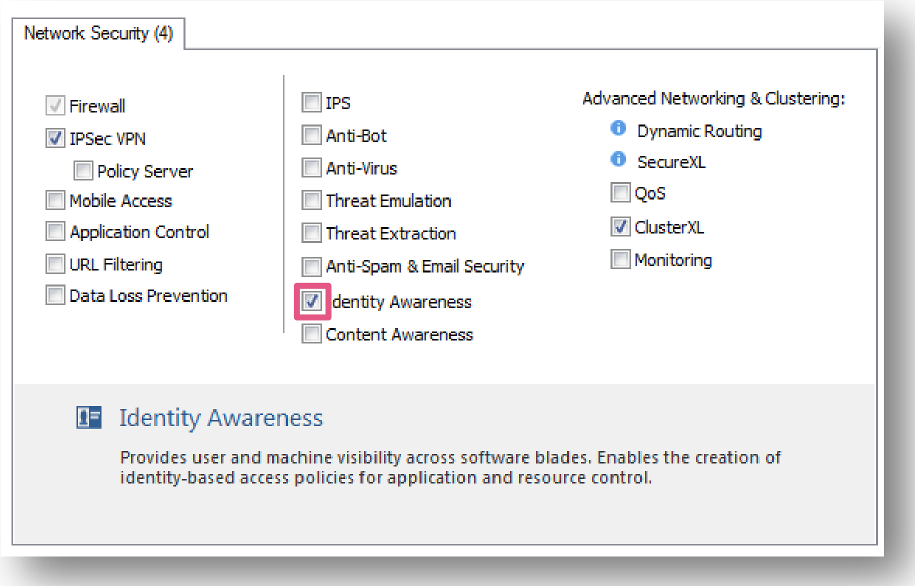
Name: Local Host
IPv4 address: 127.0.0.1

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.



Network Security (4)

☑ Firewall
☑ IPSec VPN
□ Policy Server
□ Mobile Access
□ Application Control
□ URL Filtering
□ Data Loss Prevention

□ IPS
□ Anti-Bot
□ Anti-Virus
□ Threat Emulation
□ Threat Extraction
□ Anti-Spam & Email Security
☑ dentity Awareness
□ Content Awareness

Advanced Networking & Clustering:
Dynamic Routing
SecureXL
□ QoS
☑ ClusterXL
□ Monitoring

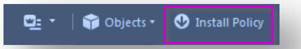
Identity Awareness

Provides user and machine visibility across software blades. Enables the creation of identity-based access policies for application and resource control.

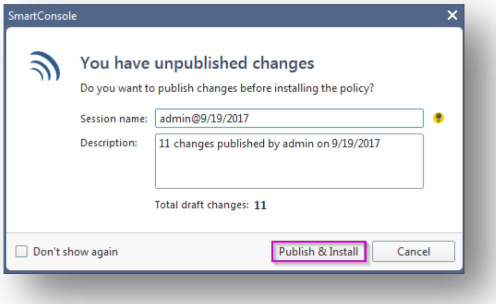
6. A window will be open, select the Terminal Servers & uncheck the AD query, Click next.

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



SmartConsole

You have unpublished changes

Do you want to publish changes before installing the policy?

Session name: admin@9/19/2017

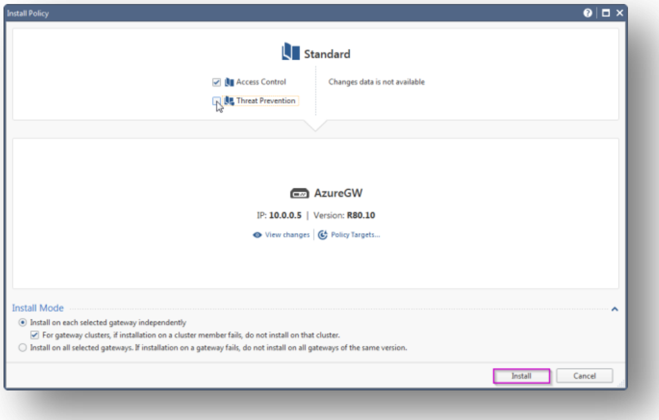
Description: 11 changes published by admin on 9/19/2017

Total draft changes: 11

□ Don't show again

Publish & Install | Cancel

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



Install Policy

Standard

☑ Access Control

□ Threat Prevention

Changes data is not available

AzureGW

IP: **10.0.0.5** | Version: **R80.10**

View changes | Policy Targets...

Install Mode

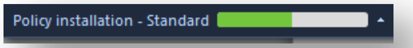
● Install on each selected gateway independently

☑ For gateway clusters, if installation on a cluster member fails, do not install on that cluster.

○ Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.

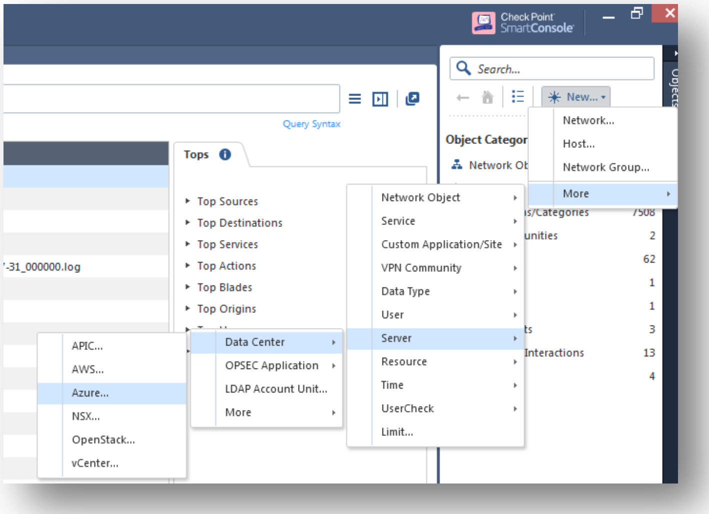
Install | Cancel

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

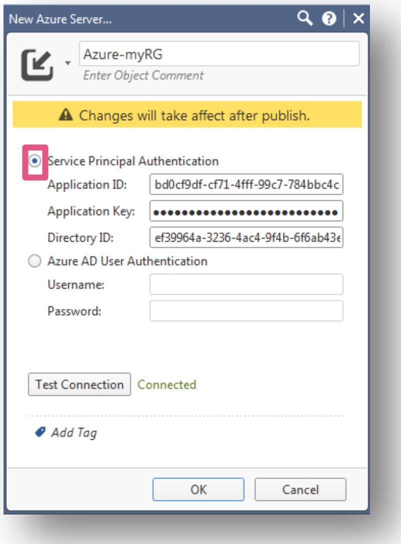


Policy installation - Standard

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):



New Azure Server...

Azure-myRG

Enter Object Comment

Changes will take affect after publish.

● Service Principal Authentication

Application ID: bd0cf9df-cf71-4fff-99c7-784bbc4c

Application Key: ••••••••••••••••••••••••••

Directory ID: ef39964a-3236-4ac4-9f4b-6f6ab43e

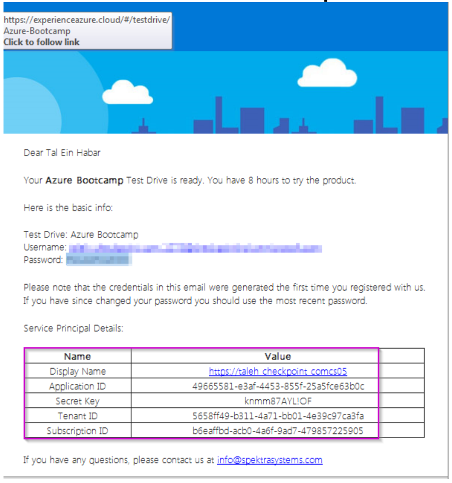
○ Azure AD User Authentication

Username:

Password:

Test Connection Connected

Move to Service Principal Authentication



https://experienceazure.cloud/#/testdrive/
Azure-Bootcamp
Click to follow link

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.

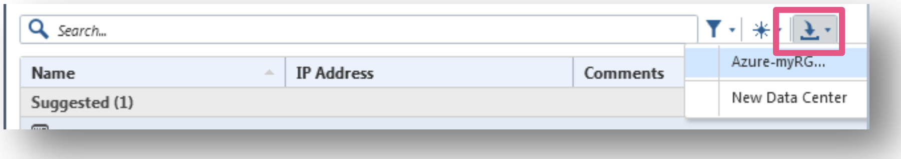
Service Principal Details:

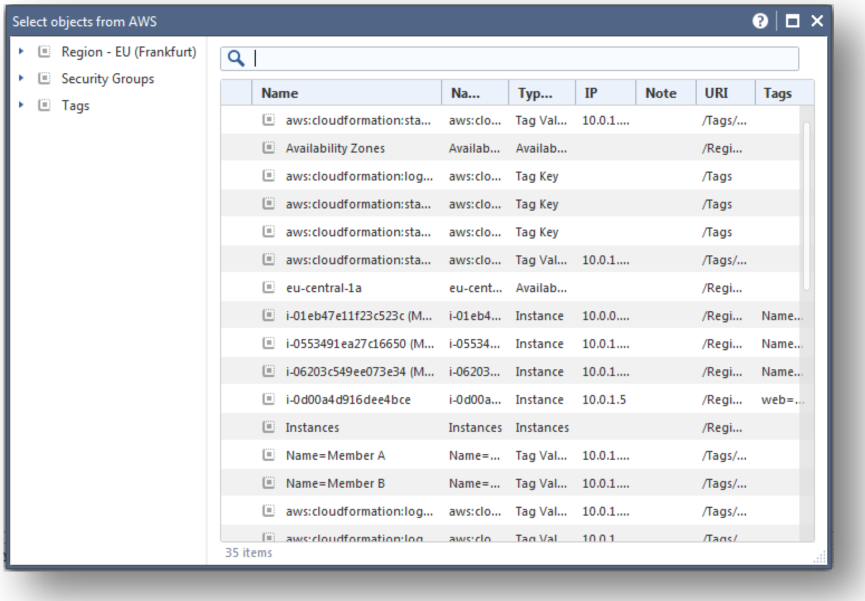
Name	Value	
Display Name	https://taleh checkpoint comcs05	
Application ID	49665581-e3af-4453-855f-25a5fce63b0c	
Secret Key	knmm87AYL!OF	
Tenant ID	5658ff49-b311-4a71-bb01-4e39c97ca3fa	
Subscription ID	b6eaffbd-acb0-4a6f-9ad7-479857225905	

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

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.





Name	Na...	Typ...	IP	Note	URI	Tags
aws:cloudformation:sta...	aws:clo...	Tag Val...	10.0.1....		/Tags/...	
Availability Zones	Availab...	Availab...			/Regi...	
aws:cloudformation:log...	aws:clo...	Tag Key			/Tags	
aws:cloudformation:sta...	aws:clo...	Tag Key			/Tags	
aws:cloudformation:sta...	aws:clo...	Tag Key			/Tags	
aws:cloudformation:sta...	aws:clo...	Tag Val...	10.0.1....		/Tags/...	
eu-central-1a	eu-cent...	Availab...			/Regi...	
i-01eb47e11f23c523c (M...	i-01eb4...	Instance	10.0.0....		/Regi...	Name...
i-0553491ea27c16650 (M...	i-05534...	Instance	10.0.1....		/Regi...	Name...
i-06203c549ee073e34 (M...	i-06203...	Instance	10.0.1....		/Regi...	Name...
i-0d00a4d916dee4bce	i-0d00a...	Instance	10.0.1.5		/Regi...	web=...
Instances	Instances	Instances			/Regi...	
Name=Member A	Name=...	Tag Val...	10.0.1....		/Tags/...	
Name=Member B	Name=...	Tag Val...	10.0.1....		/Tags/...	
aws:cloudformation:log...	aws:clo...	Tag Val...	10.0.1....		/Tags/...	
aws:cloudformation:log	aws:clo	Tag Val	10.0.1		/Tags/	

35 items

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

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)?

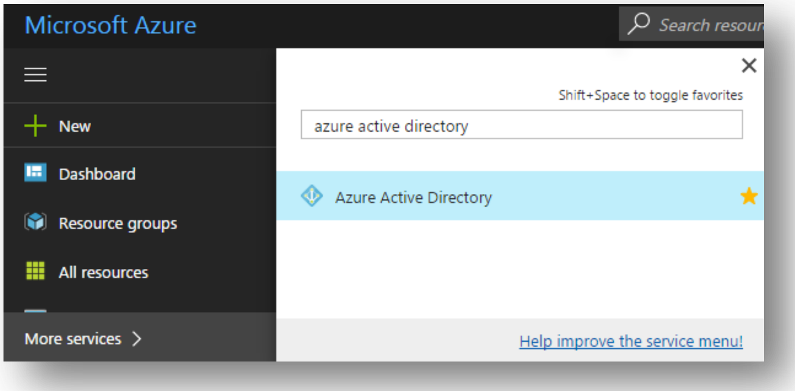
3. Add another server on the Web subnet and verify that traffic between two servers on the subnets are actually traversing through the firewall (micro-segmentation or AKA East - west protection)

You have finished exercise 6

Appendix #1 – SPN definitions

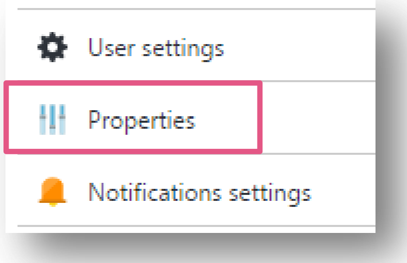
Please follow the below to create a service principal and assign it with the relevant permissions.

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

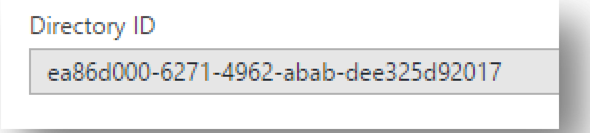


azure active directory

18. Click on properties



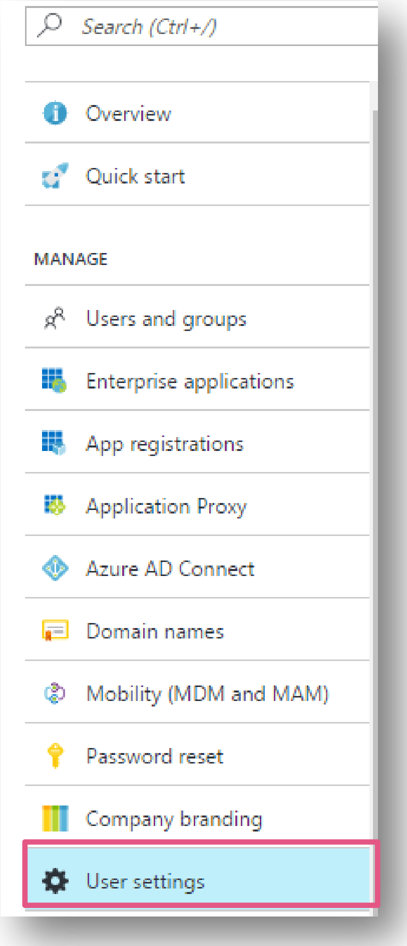
19. Copy aside the directory ID for later use



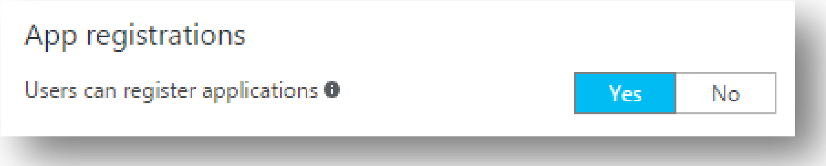
Directory ID

ea86d000-6271-4962-abab-dee325d92017

20. Now, enter the “user settings” section

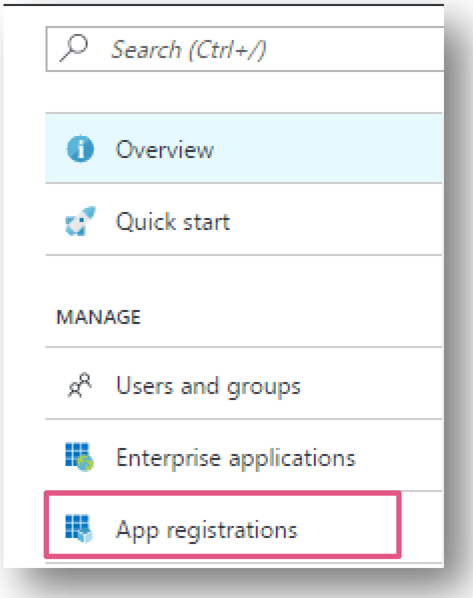


21. Check the App registrations setting. It should set to Yes.

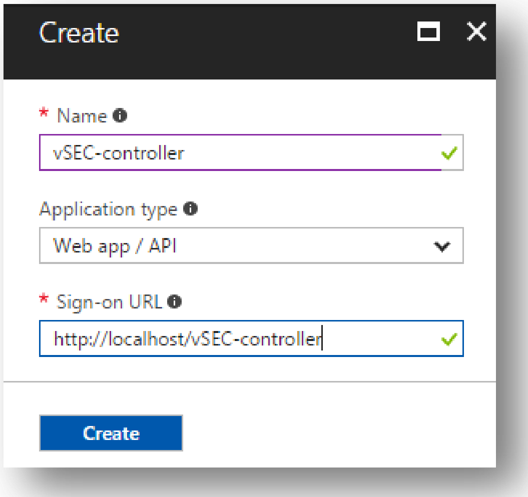

App registrations

Users can register applications [✓ Yes] No

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



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



Create

* Name

vSEC-controller

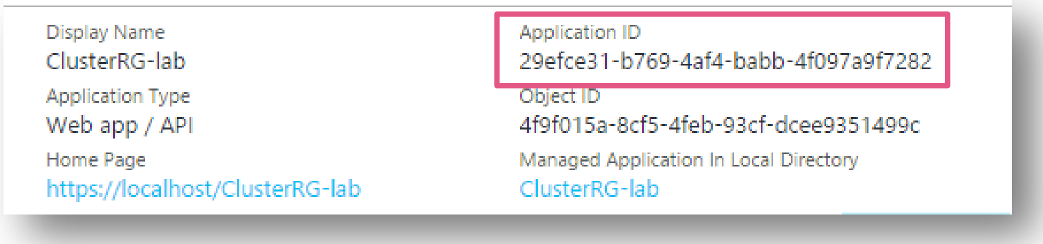
Application type

Web app / API

* Sign-on URL

http://localhost/vSEC-controller

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



Display Name
ClusterRG-lab

Application Type
Web app / API

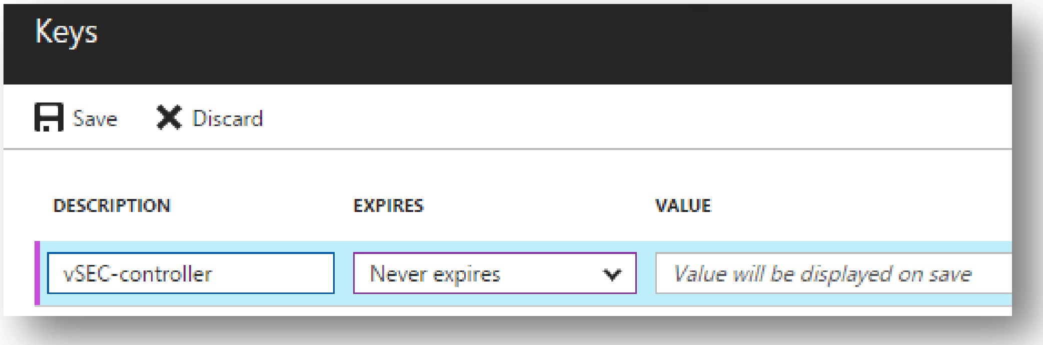
Home Page
https://localhost/ClusterRG-lab

Application ID
29efce31-b769-4af4-babb-4f097a9f7282

Object ID
4f9f015a-8cf5-4feb-93cf-dcee9351499c

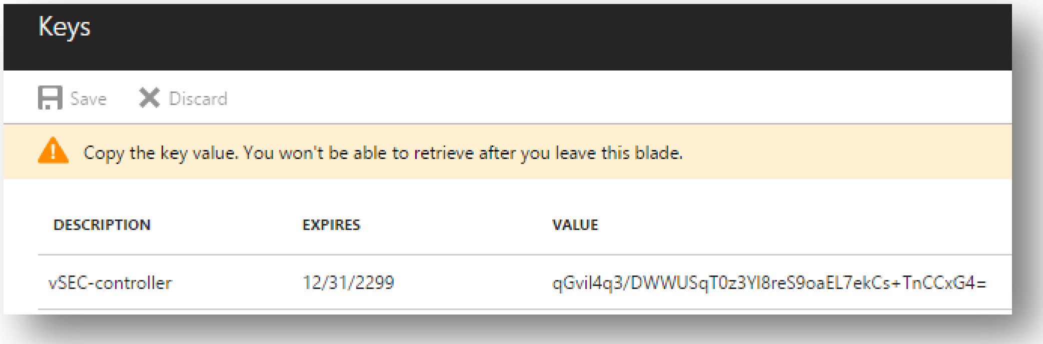
Managed Application In Local Directory
ClusterRG-lab

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



DESCRIPTION	EXPIRES	VALUE
vSEC-controller	Never expires	*Value will be displayed on save*

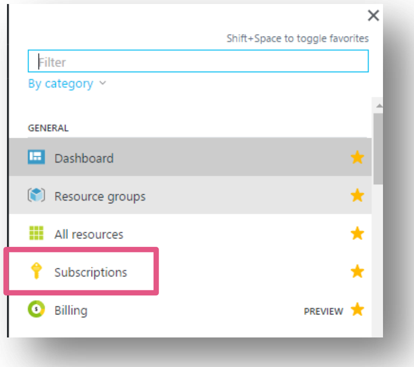
After you click, save the key value appears, copy it to a safe place as you cannot retrieve it later (In this lab and after).



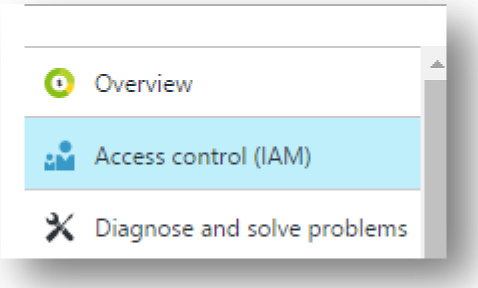
Copy the key value. You won't be able to retrieve after you leave this blade.

DESCRIPTION	EXPIRES	VALUE
vSEC-controller	12/31/2299	qGvil4q3/DWWUSqT0z3Yl8reS9oaEL7ekCs+TnCCxG4=

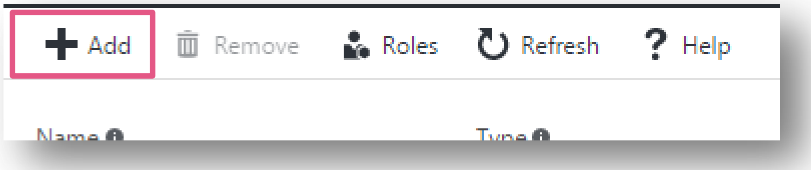
26. In the left Azure menu bar on the left choose “Subscriptions”



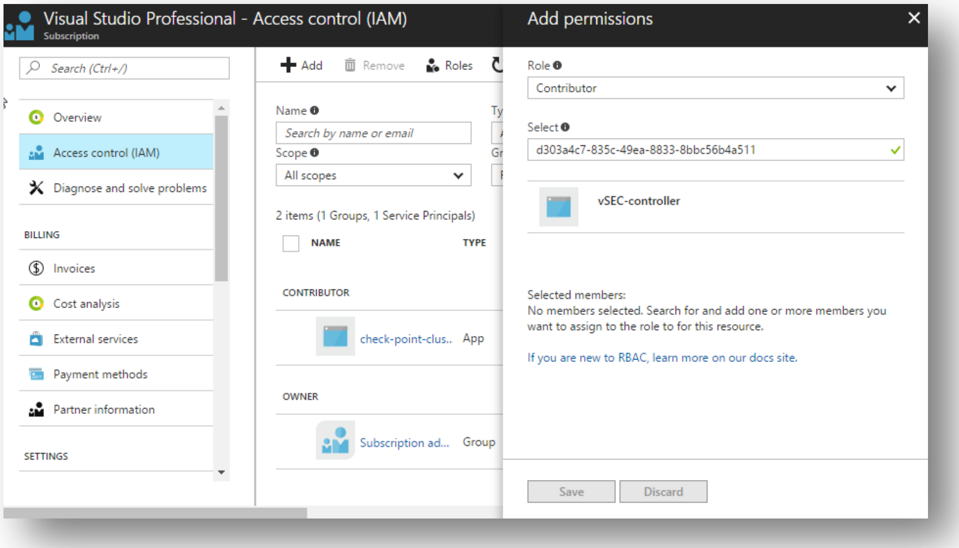
27. Choose your subscriptions and click on Access Control (IAM)



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



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



2 items (1 Groups, 1 Service Principals)

Role: Contributor

Select: d303a4c7-835c-49ea-8833-8bbc56b4a511

vSEC-controller

Selected members:
No members selected. Search for and add one or more members you want to assign to the role to for this resource.

If you are new to RBAC, learn more on our docs site.

30. Click “Save