AZURE CLOUDGUARD BOOTCAMP

Azure lab training guide

ABSTRACT

CloudGuard Network Security
Cloud Security Posture Management (CSPM)
Cloud Intelligence & Threat Hunting

Version

V5.0

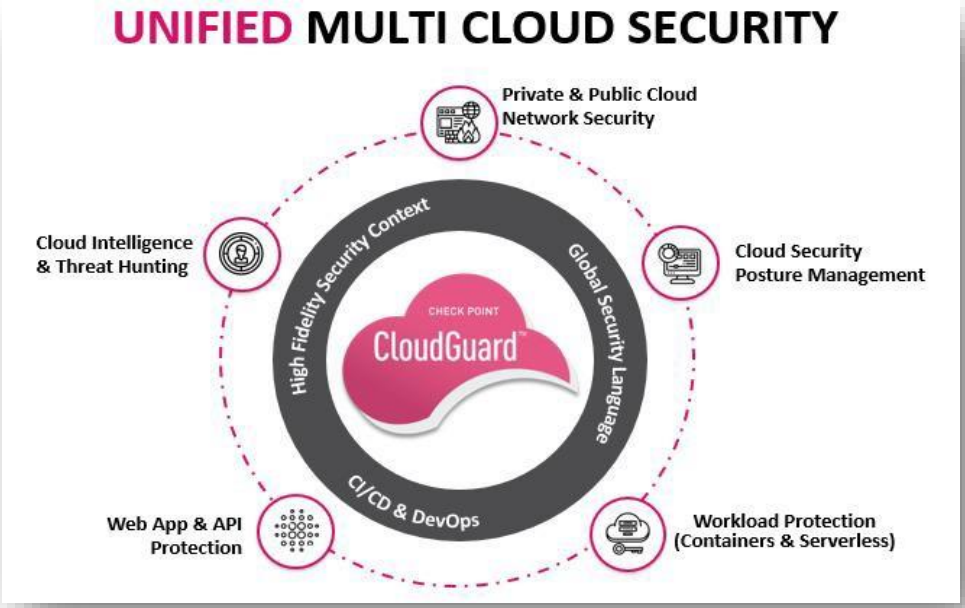
@Igor Freidin
Cyber Security Products Expert

Contents

Introduction

Cloud computing is widely adopted globally and expected to grow even faster in the coming years. The CloudGuard suite is a purpose-built solution designed to secure any public cloud (IaaS), private cloud (SDN/SDDC), branch connectivity (SD-WAN), applications (SaaS), visibility with compliance (CWPP), and serverless security, ensuring smooth and secure adoption of the cloud.

Check Point CloudGuard protects applications and data with advanced threat prevention security while enabling reliable connectivity in public and hybrid cloud environments.



The Check Point CloudGuard suite for Public cloud includes:

- **CloudGuard Network Security and Threat prevention**providing advanced threat prevention for enterprise networks in the public and private cloud.
- **CloudGuard Posture management** offering native security and compliance orchestration across the public cloud.
- **CloudGuard Threat intelligence service** consuming logs and user activities from cloud workloads while providing security insights from data.

This document will guide you through the steps required to get familiar with the AWS platform and how to deploy a basic day-to-day scenario with CloudGuard in place. You will understand and simulate a real-life use case to grasp the ease of deploying automated advanced security protection within the AWS cloud.

We prepared simples exercises to illustrate the benefits of having security integrated into a virtual networking platform. The exercises are incremental - they start from a basic setup and progress to more advanced scenarios.

Securing Azure IaaS infrastructure - hands-on lab objectives

The goal of these hands-on lab exercises is to give you practical real-life experience with Check Point CloudGuard products.

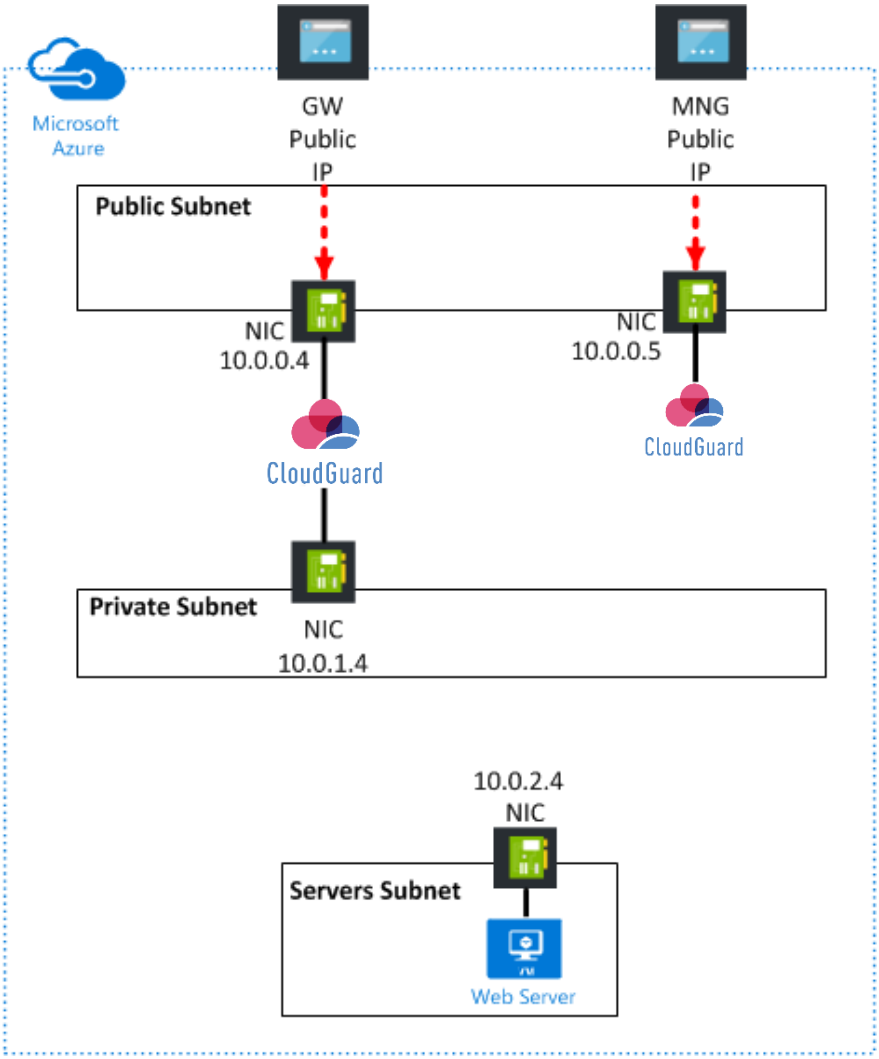
The objectives of the hands-on training are:

1. **Prepare your public cloud environment for deployment**
   This exercise will familiarize you with the Azure portal and concepts. It shows how to connect an Azure account to the CloudGuard service.
2. **Deploy Check Point R80.x management server on AWS**
   This exercise shows how to deploy an R81.x management server in your newly created environment on AWS. You will learn how to launch new web servers from the marketplace.
3. **Deploy a web server from Azure marketplace**
4. **Deploy the Check Point CloudGuard gateway on Azure**
   This exercise shows how to deploy a CloudGuard gateway into your Azure environment to improve transparency and enforcement of network traffic traversing through/from the environment.
5. **Configuring CloudGuard Controller**
   In this exercise, you will configure the CloudGuard controller to connect to your account in AWS.
6. **Advanced Troubleshooting (optional)**
   This optional exercise will teach you how to do basic debugging & validate that your gateway runs as designed.

Good Luck!

CloudGuard Azure training environment

Getting to know your training environment



	IP address
Management server	10.0.0.4 (can be different - autoassigned by Azure)
CloudGuard GW - frontend	10.0.0.5 (can be different - autoassigned by Azure)
CloudGuard GW - backend	10.0.1.4 (can be different - autoassigned by Azure)
Web server	10.0.2.x (can be different - autoassigned by Azure)

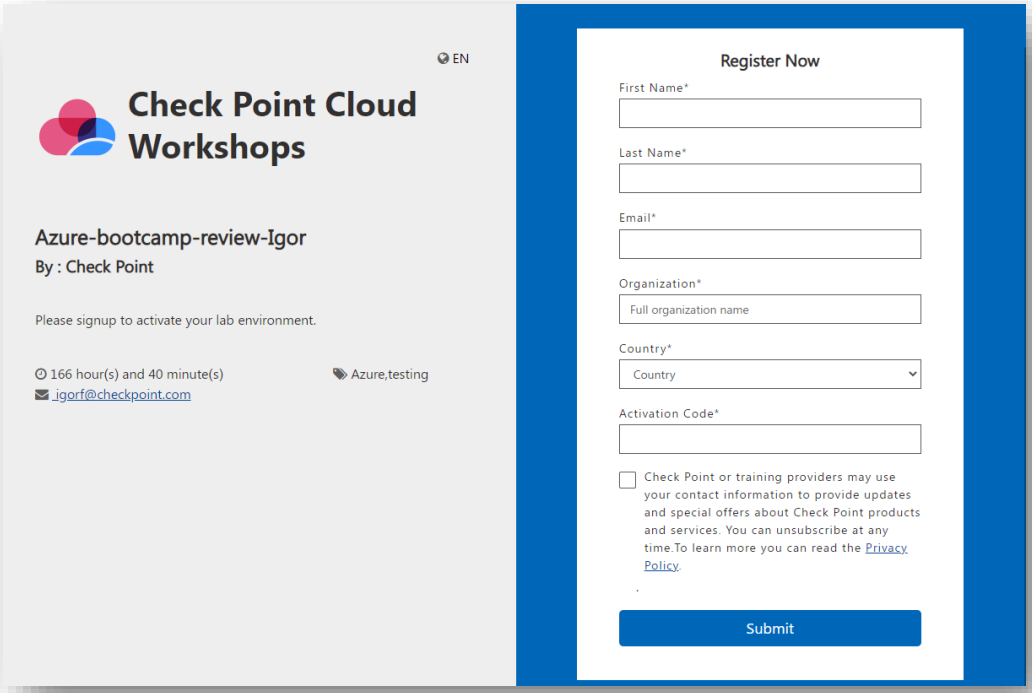
Connecting and setting up your work environment

Goal

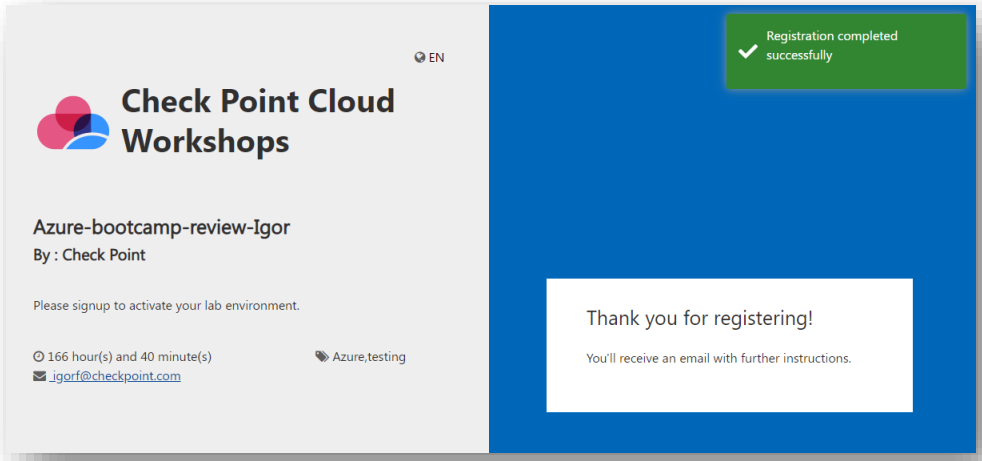
Getting familiar with the console and its options

Register and sign in to AWS

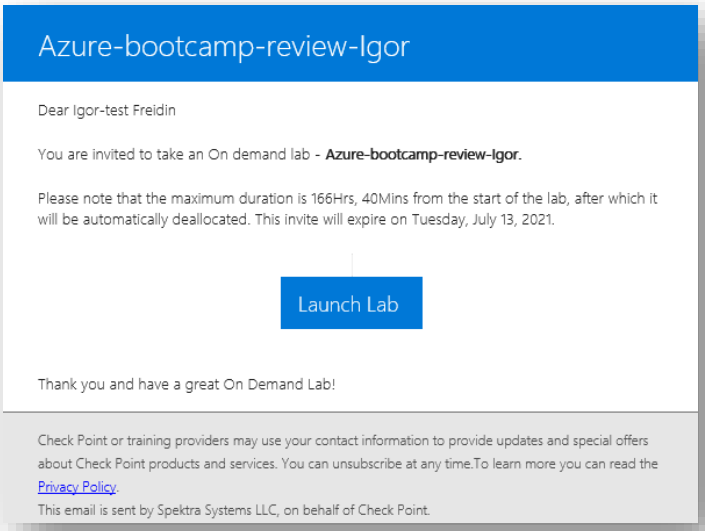
1. Browse to the link provided by your instructor.
2. Fill in your details for registration (an activation key can be found on the referral page) and click Submit.



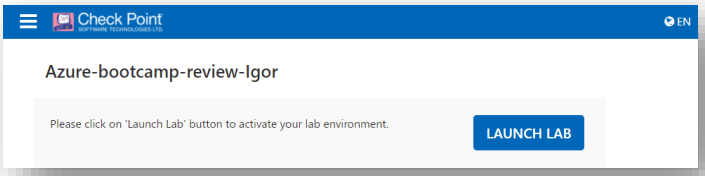
3. The next screen will show the message:

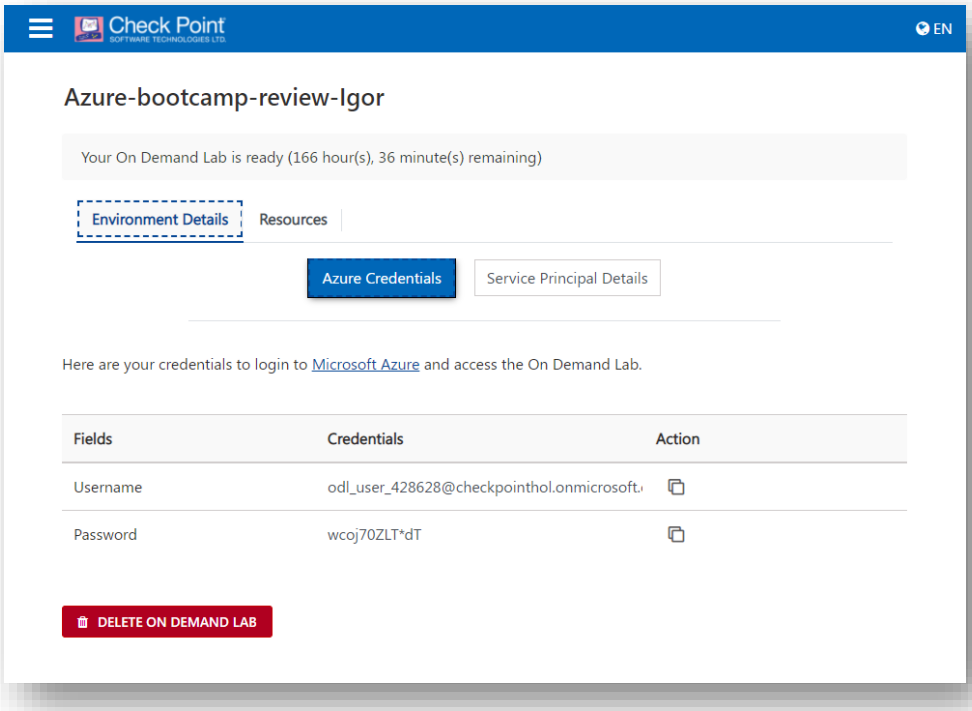


4. An email will be sent to you to start the lab. Open the email and click 'Launch Lab' to go to the starting page of the lab.



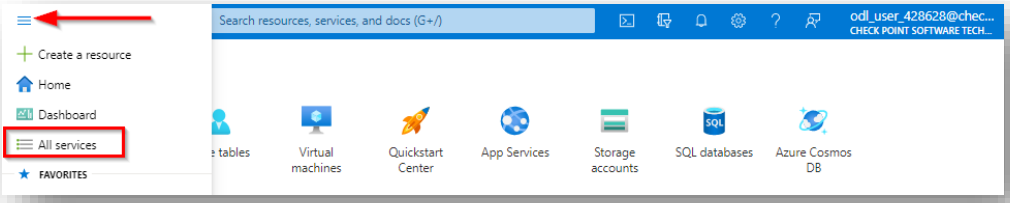
5. Click on the 'LAUNCH LAB' button to start the lab.



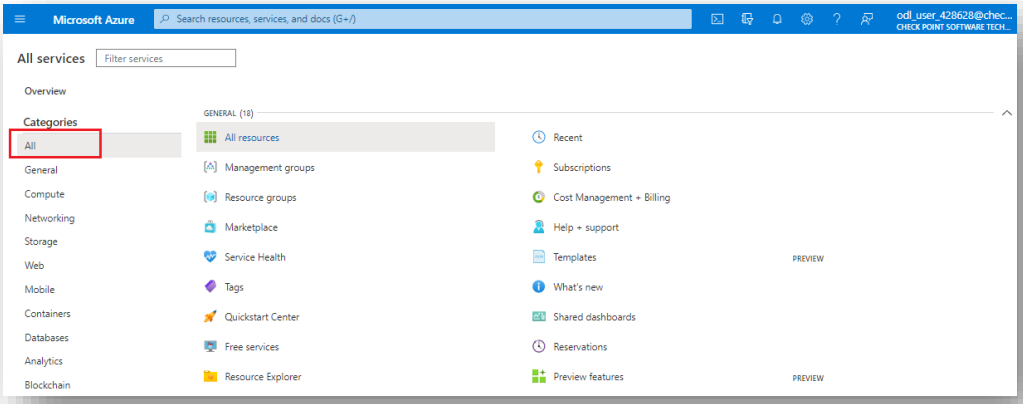


6. Your on-demand lab session has started and will be active for several hours.
   The web page shows your Azure credentials for this session and the sign-in link.
   You will be emailed the same information.

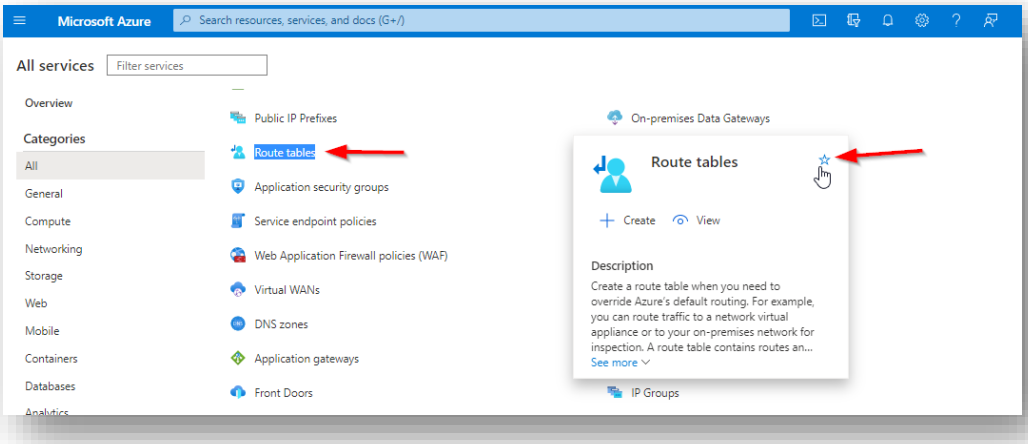
7. Click on the login to Microsoft Azure link for the on-demand lab, use the provided credentials.
8. Click on the portal menu icon and click on 'All services'.



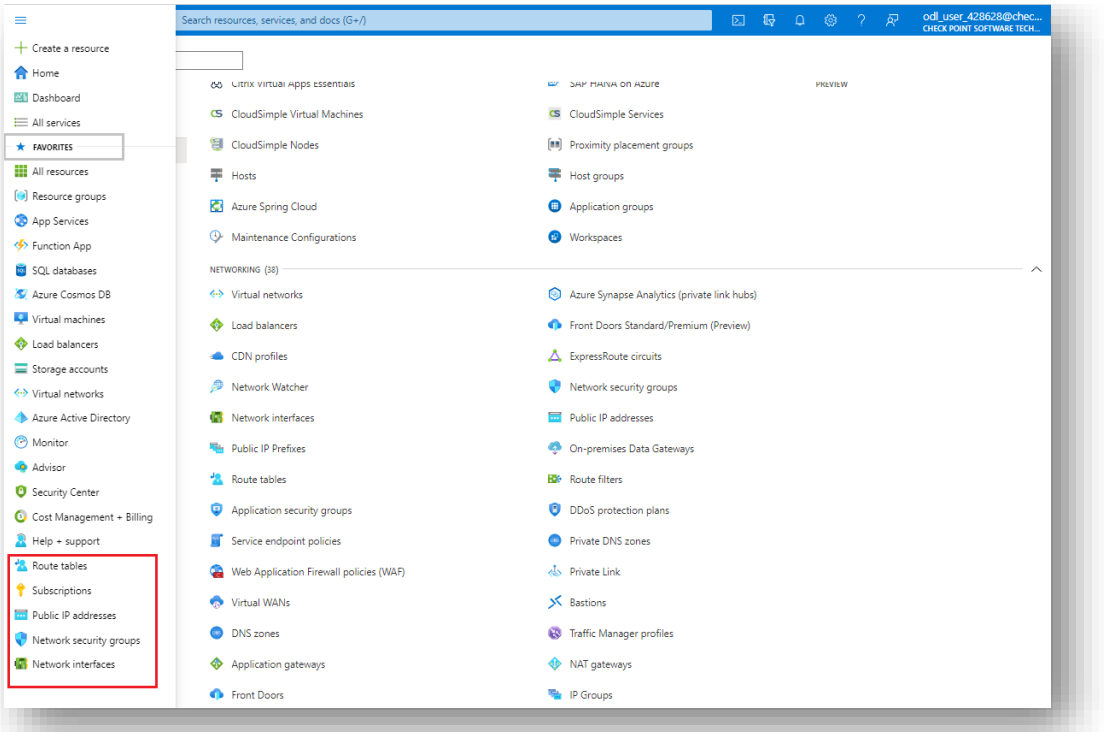
9. Click on All categories.



10. Search and hover over each of the services below. Click on start to add it to the favorites list.



a) Route tables
b) Subscriptions
c) Public IP addresses
d) Network security group
e) Network interfaces



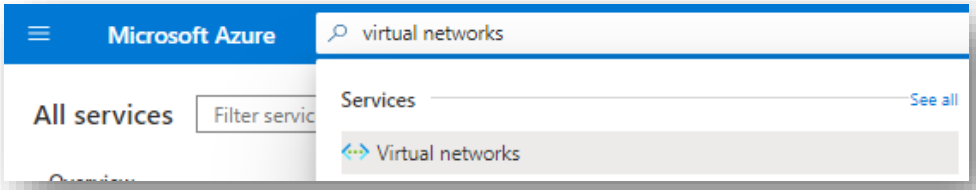
Exercise 1 - Build your Azure environment

Goal

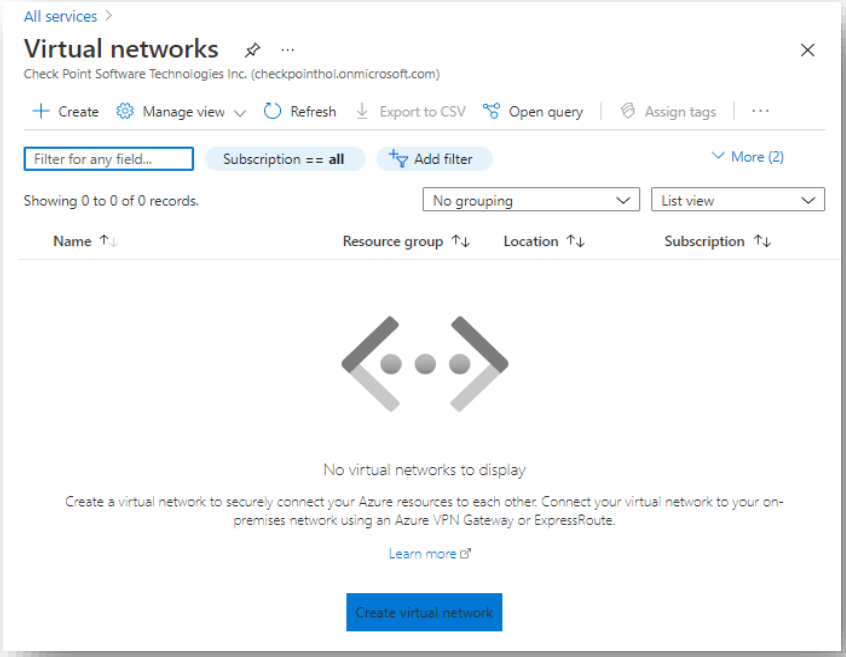
Creating basic Azure environment with vNET and subnets

Step 1. Create a vNET with two subnets

1. On the top search bar of the Azure portal search for and click on 'Virtual networks'.

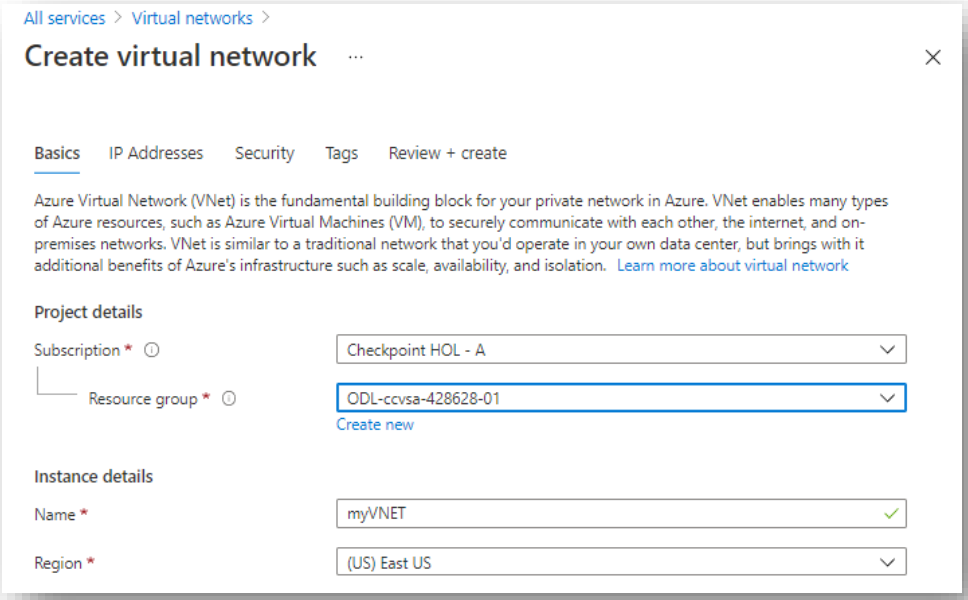


2. At the bottom of the window that appears click on 'Create virtual network'.



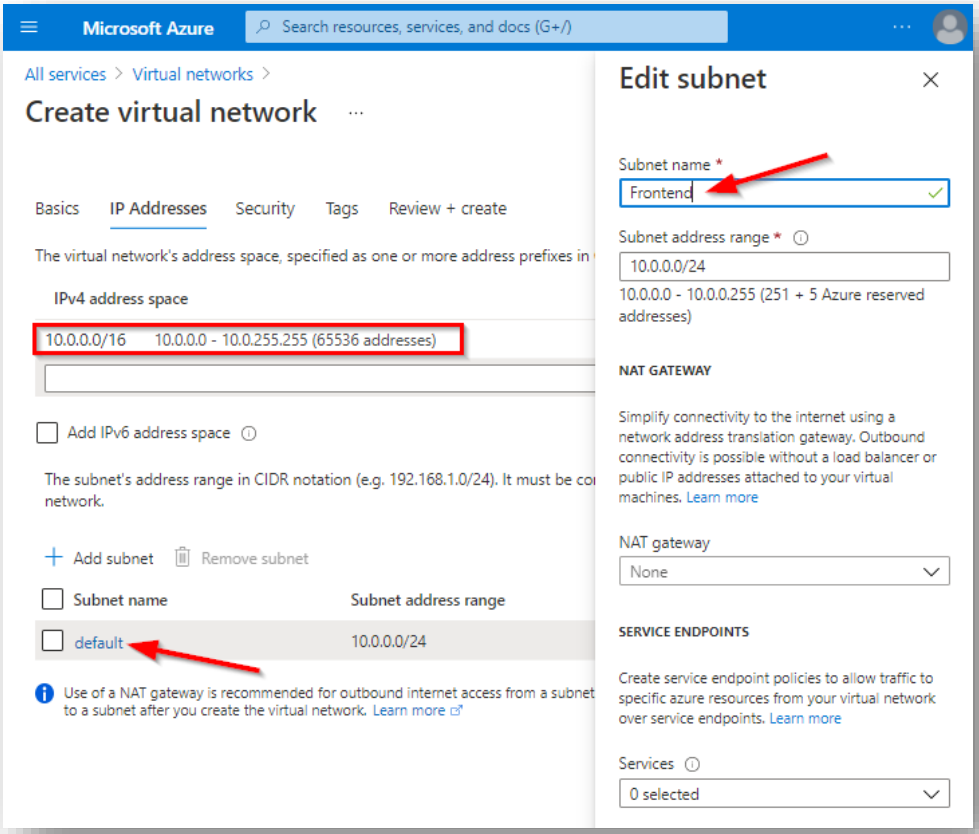
3. In the window that appears fill in the info per details below. Click on 'Next: IP Addresses'.

Setting	Value
Name	myVNET
Subscription	Leave subscription as is
Resource group	Resource Group that ends with -01 (the first one)
Location	Any Europe or US will do



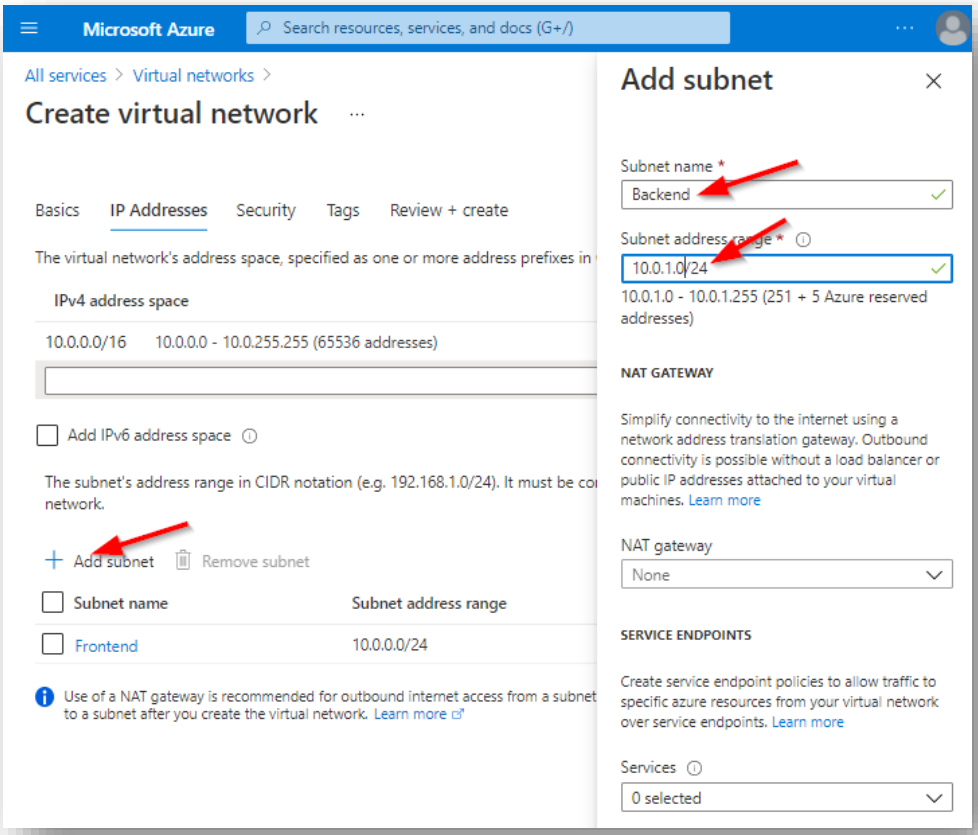
4. Make sure that your IPv4 address space listed is in the 10.0.0.0/16 range. Click on the 'default' subnet and change its 'Subnet name' to 'Frontend'. Check whether the subnet address range is 10.0.0.0/24.

Click 'Save'.

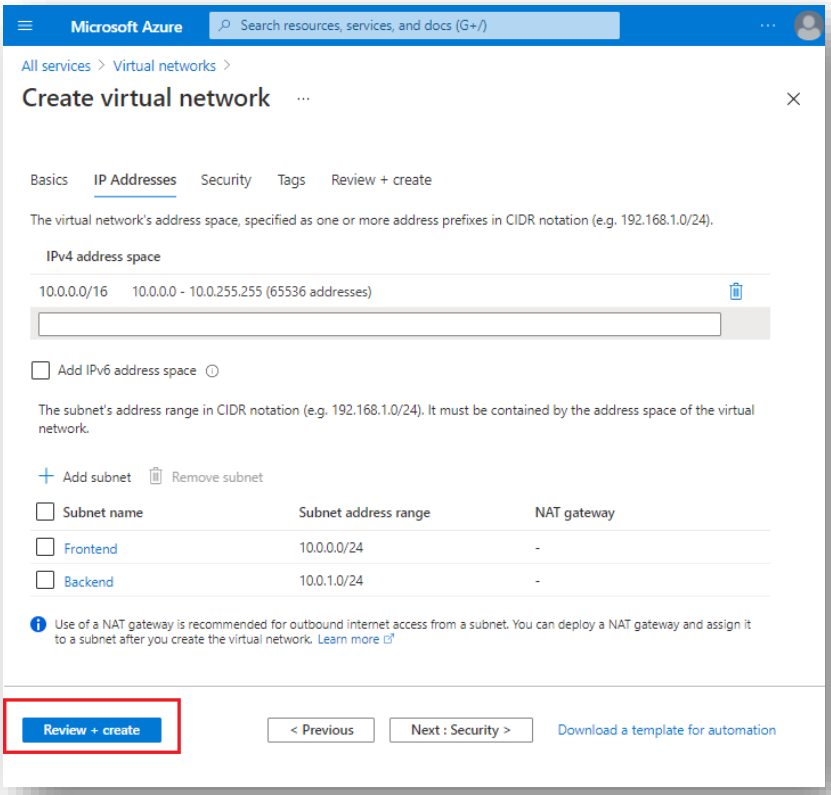


5. Click on "Add subnet". Name the new subnet as 'Backend' and give it the 10.0.1.0/24 address range.

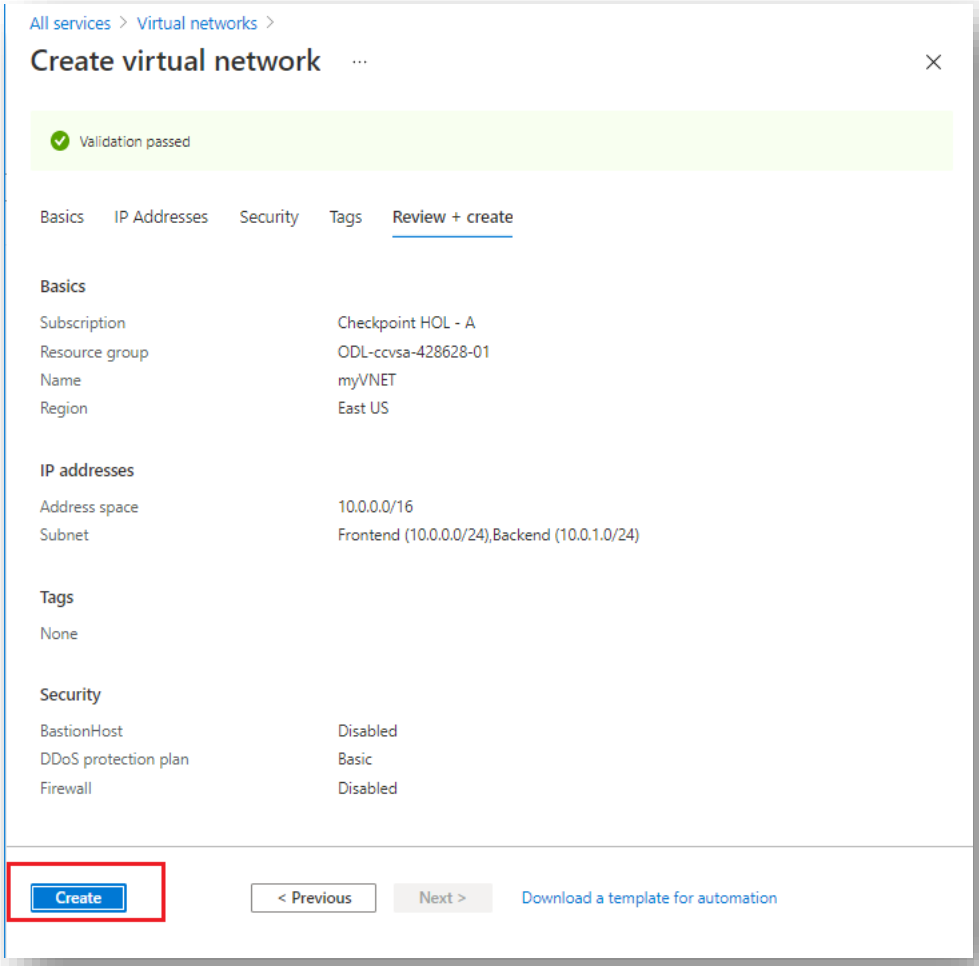
   Click on Add.

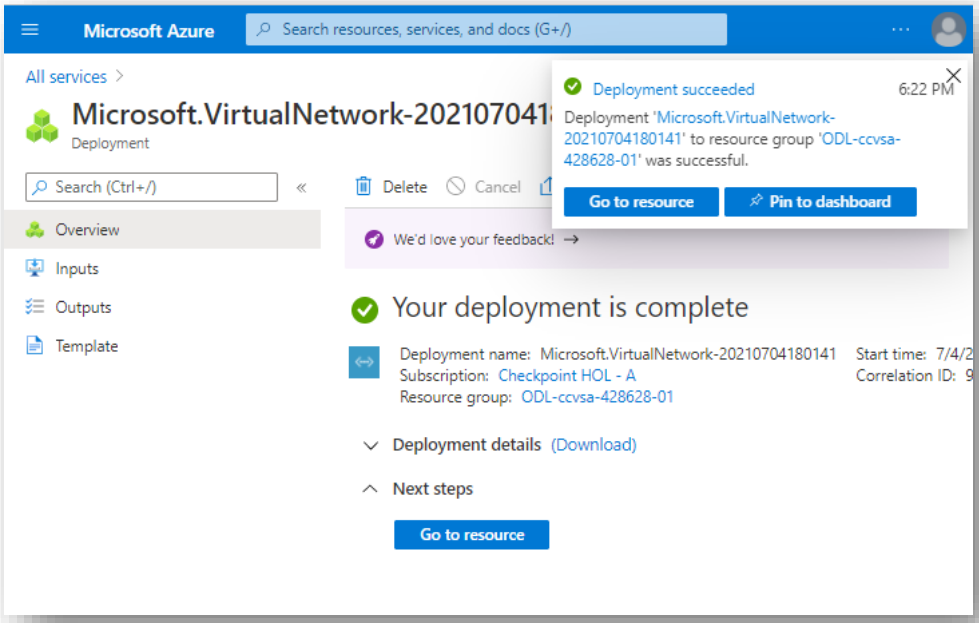


6. Verify the details and click on "Review and create".

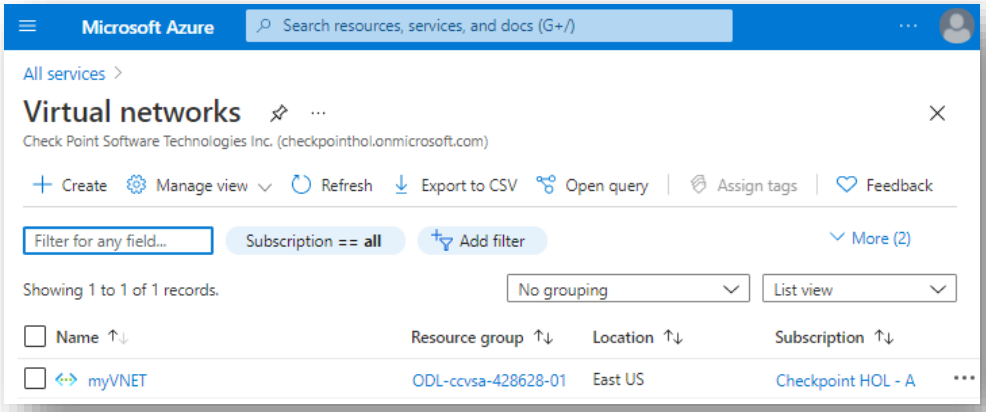


7. Verify validation is passed and click on Create





8. You should see the created vNET on the Virtual networks service.



You have finished exercise 1.

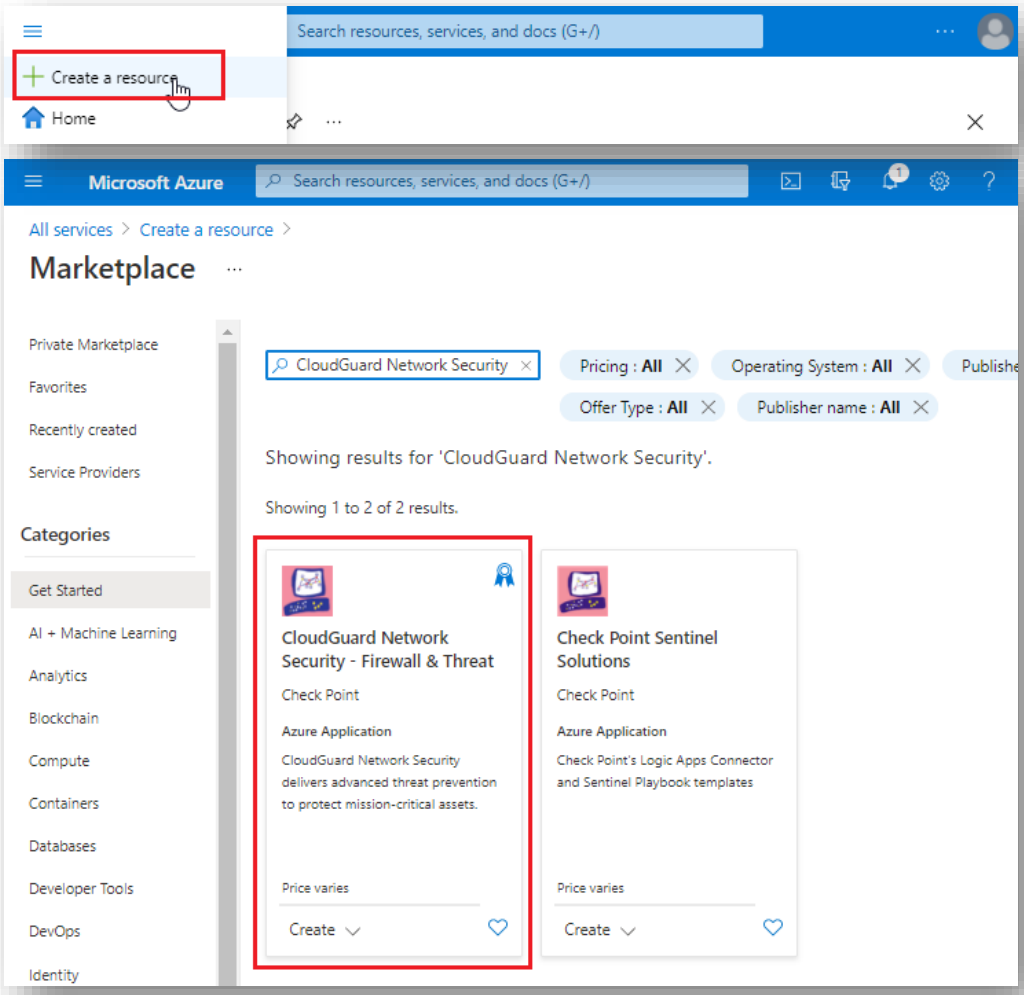
Exercise 2 - Deploy Check Point R80.x Management Server

Goal

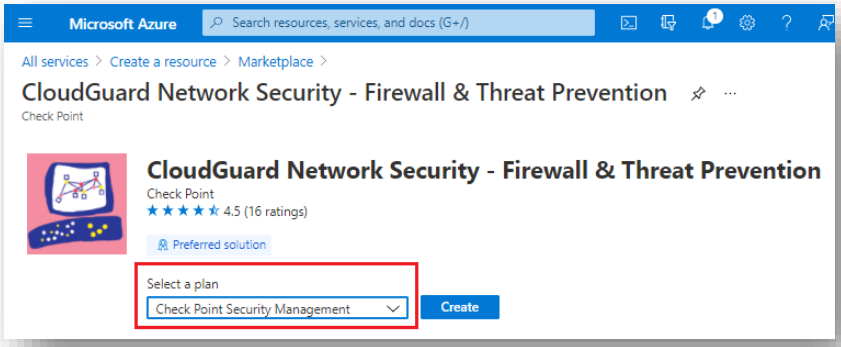
Deploying the Check Point management server using an Azure marketplace template

Step 1. locate the Azure marketplace template

1. Connect to the Azure portal, click on the portal menu icon -> 'Create a resource'. Search for 'CloudGuard Network Security' and select Firewall&Threat Azure application.

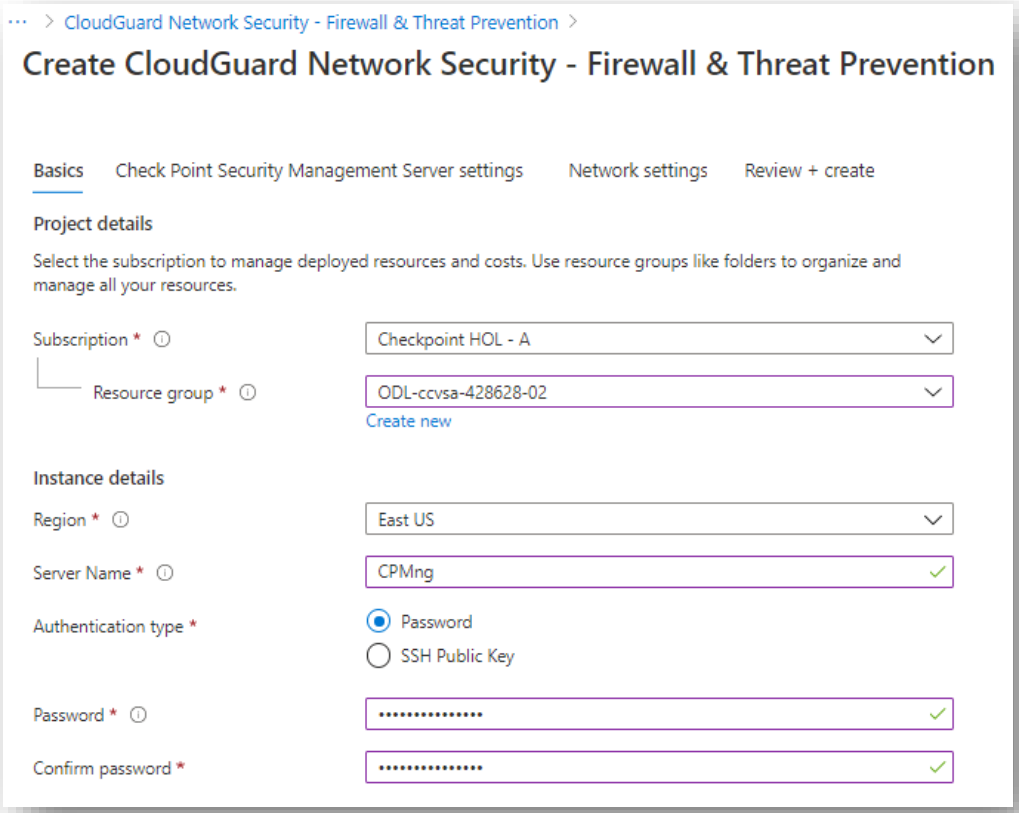


2. Change the plan to 'Check Point Security Management' and click Create.



Step 2. deploy Security Management

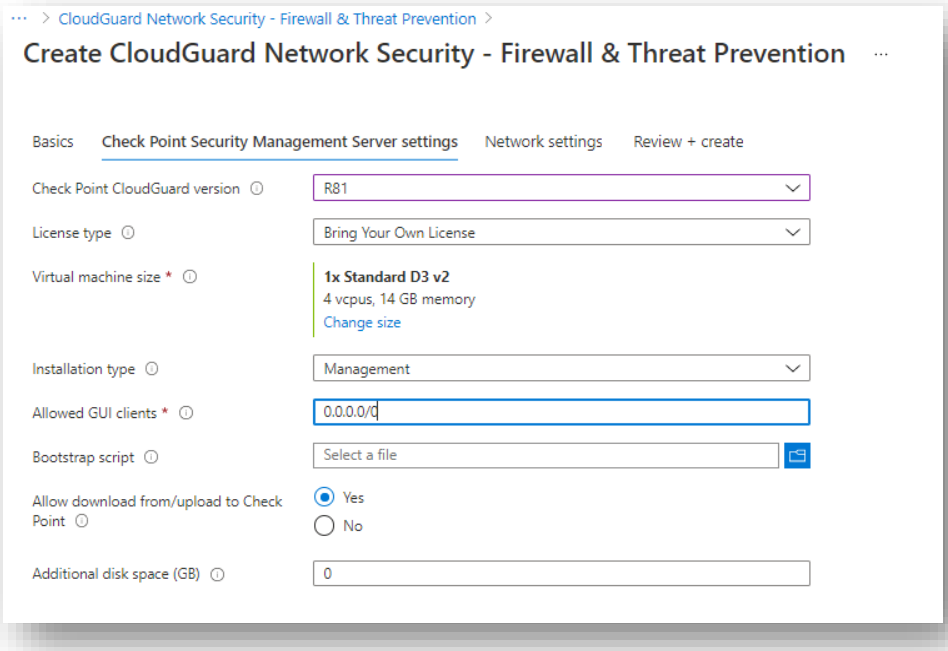
1. Fill in the info per the details below. Click on 'Next: Check Point Security Management Server settings'.



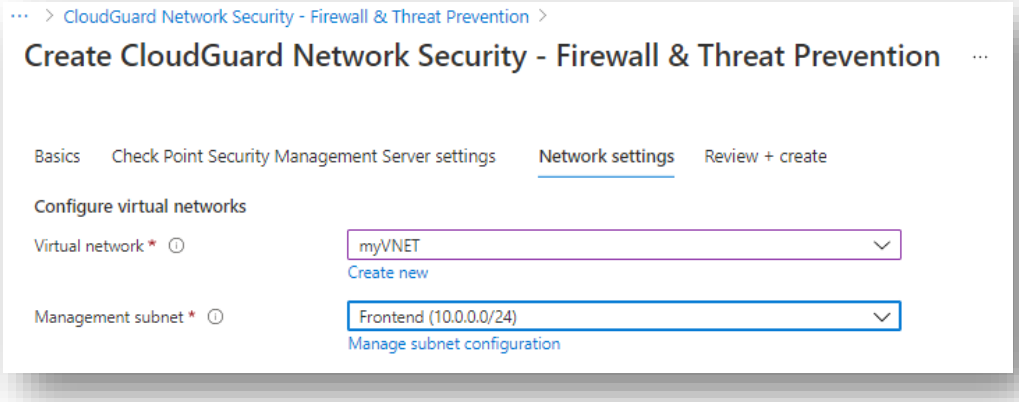
Setting	Value
Subscription	Leave the default one
Resource group	Resource Group that ends with -02 (the 2nd on the list)
Region	Same as in exercise one
Name	CPMng
Password	Choose your own (12-digits min, inc. uppercase+lowercase+number)

2. Fill in the info per the details below. Click on 'Next : Network Settings'.

Setting	Value
Check Point CloudGuard version	R81
License type	Bring Your Own License
Virtual machine size	Leave as is (or choose a smaller one if instructed to do so)
Installation type	Management
Allowed GUI clients	0.0.0.0/0

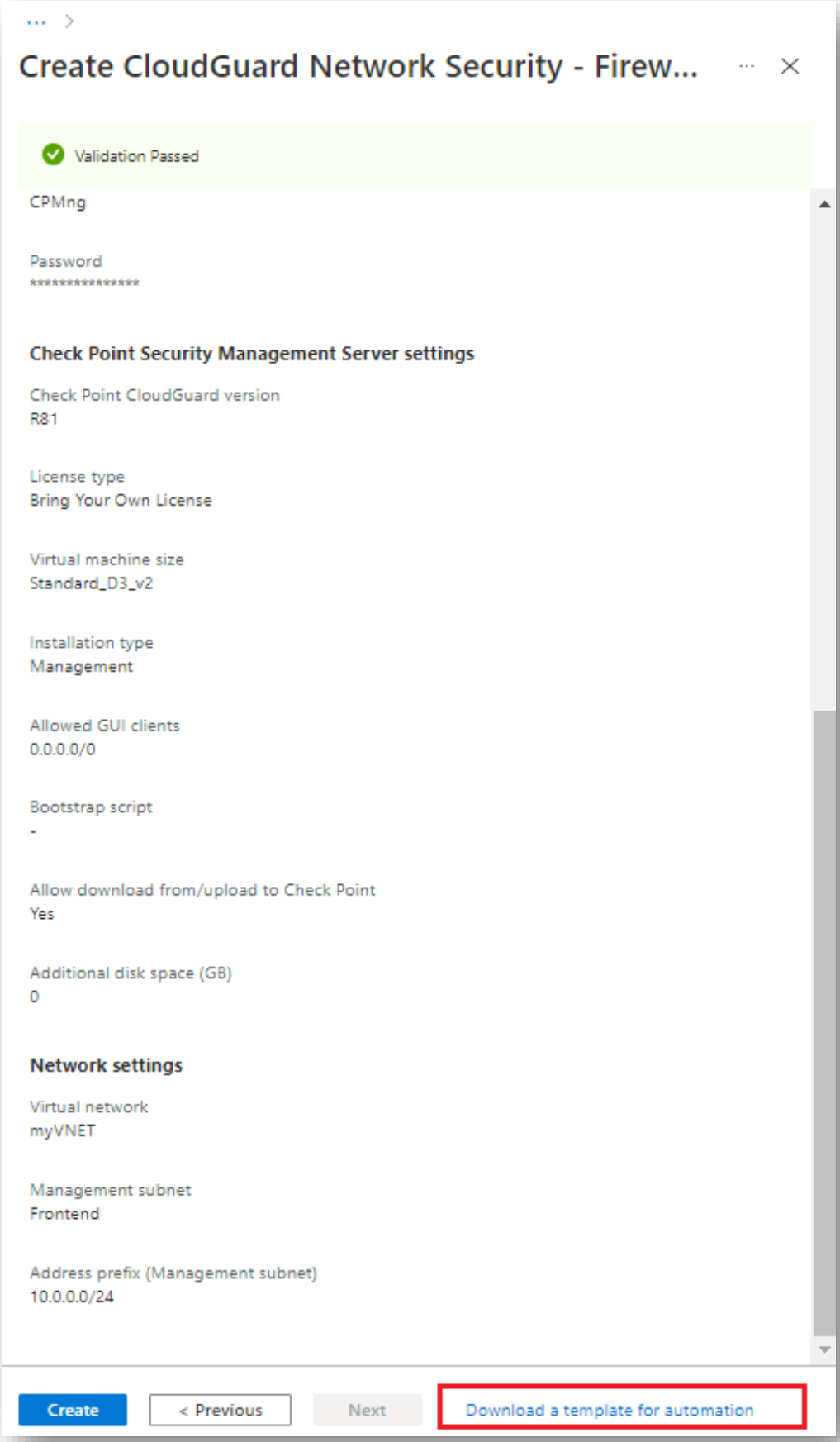


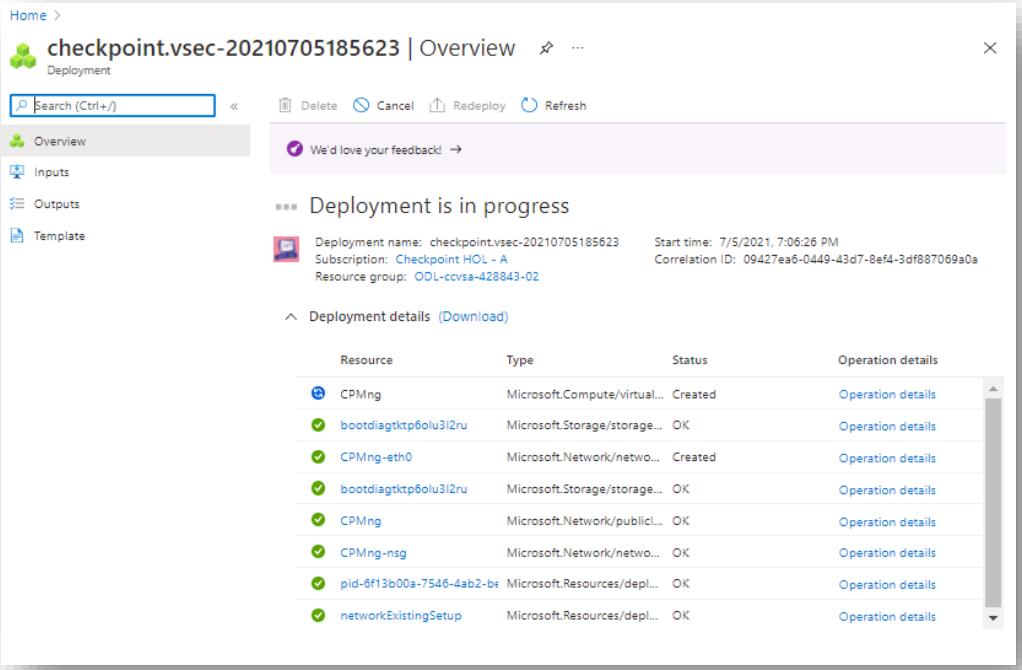
3. Under the Virtual network choose the 'myVNET' that we created in exercise 1, and for Management subnet choose the network named 'Frontend'.
Click on 'Next : Review + Create >'.

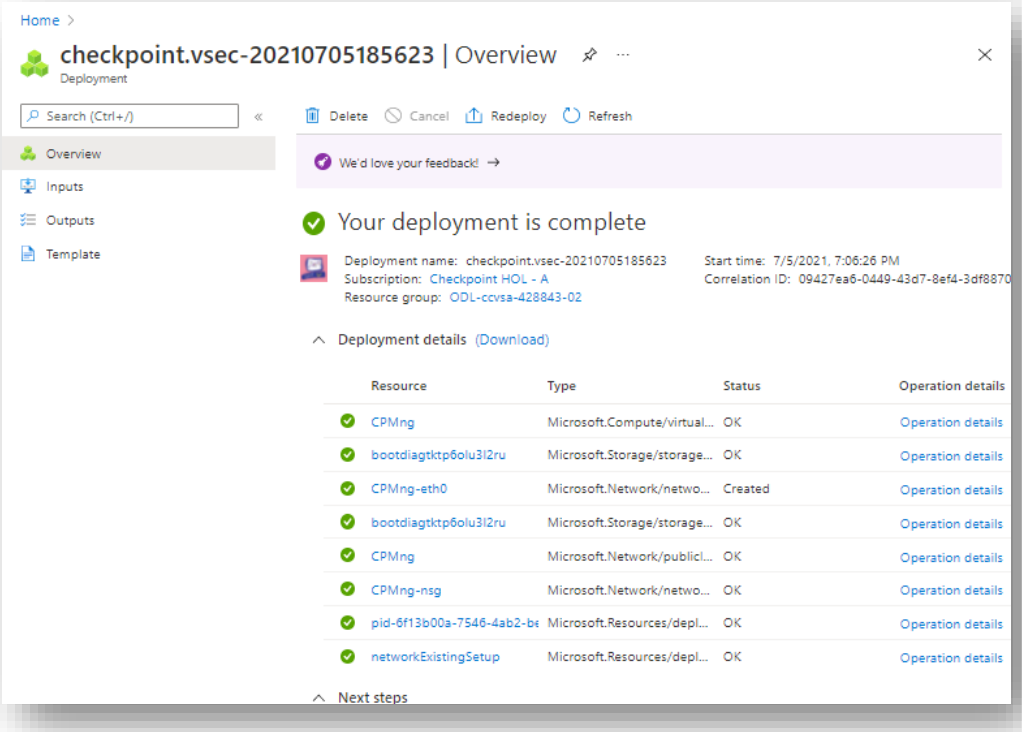


4. Verify whether you passed the validation. You can click on 'Download a template for automation' for feature deployments.
Click on 'Create'.

Deployment of R81 Security Management takes about 10 minutes.

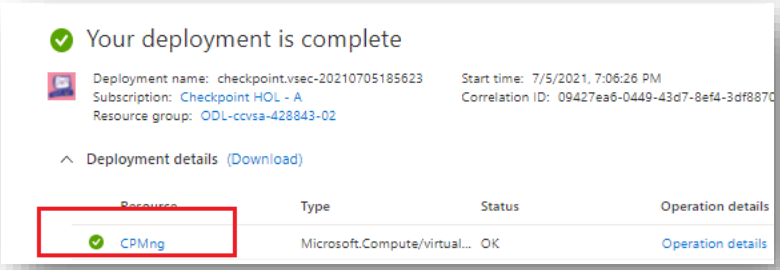

Create CloudGuard Network Security - Firew...
Validation Passed
CPMng
Password
****
Check Point Security Management Server settings
Check Point CloudGuard version
R81
License type
Bring Your Own License
Virtual machine size
Standard_D3_v2
Installation type
Management
Allowed GUI clients
0.0.0.0/0
Bootstrap script
-
Allow download from/upload to Check Point
Yes
Additional disk space (GB)
0
Network settings
Virtual network
myVNET
Management subnet
Frontend
Address prefix (Management subnet)
10.0.0.0/24
Create
< Previous
Next
Download a template for automation

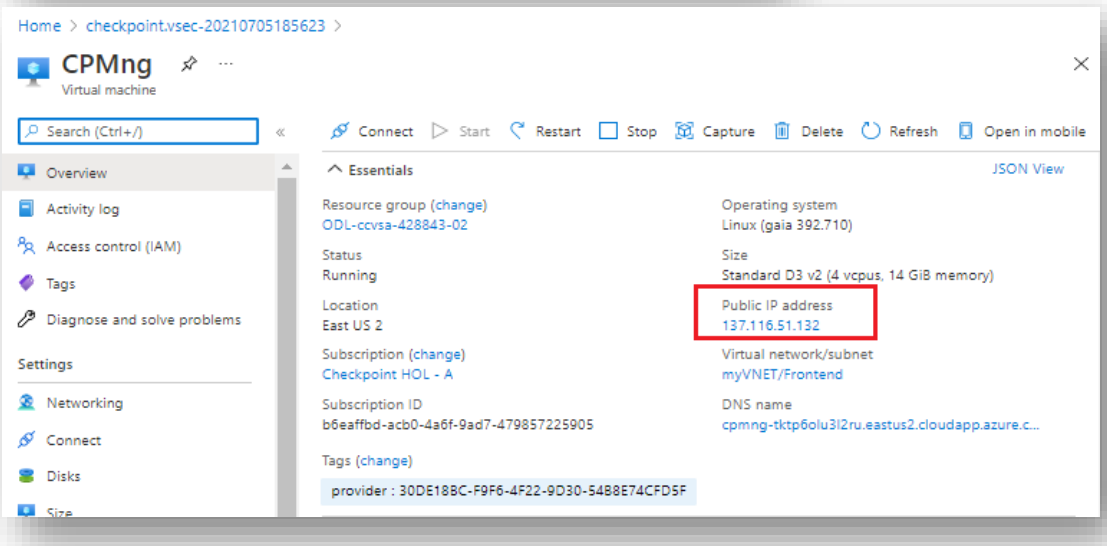

Home >
checkpoint.vsec-20210705185623 | Overview
Deployment
Search (Ctrl+/)
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Refresh
We'd love your feedback! →
Deployment is in progress
Deployment name: checkpoint.vsec-20210705185623
Subscription: Checkpoint HOL - A
Resource group: ODL-ccvsa-428843-02
Start time: 7/5/2021, 7:06:26 PM
Correlation ID: 09427ea6-0449-43d7-8ef4-3df887069a0a
Deployment details (Download)
Resource Type Status Operation details
CPMng Microsoft.Compute/virtual... Created Operation details
bootdiagtktp6olu3l2ru Microsoft.Storage/storage... OK Operation details
CPMng-eth0 Microsoft.Network/netwo... Created Operation details
bootdiagtktp6olu3l2ru Microsoft.Storage/storage... OK Operation details
CPMng Microsoft.Network/publicI... OK Operation details
CPMng-nsg Microsoft.Network/netwo... OK Operation details
pid-6f13b00a-7546-4ab2-be Microsoft.Resources/depl... OK Operation details
networkExistingSetup Microsoft.Resources/depl... OK Operation details

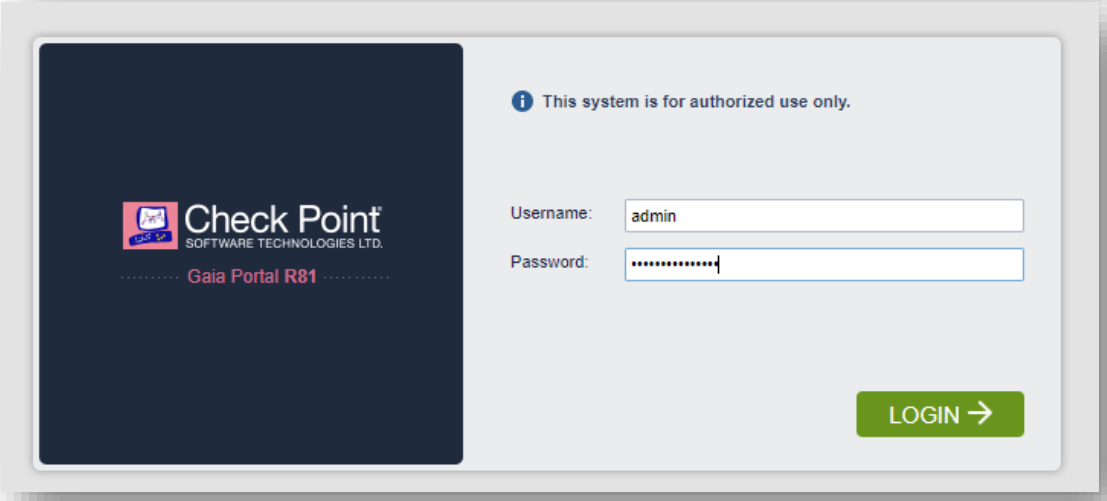

Home >
checkpoint.vsec-20210705185623 | Overview
Deployment
Search (Ctrl+/)
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Refresh
We'd love your feedback! →
Your deployment is complete
Deployment name: checkpoint.vsec-20210705185623
Subscription: Checkpoint HOL - A
Resource group: ODL-ccvsa-428843-02
Start time: 7/5/2021, 7:06:26 PM
Correlation ID: 09427ea6-0449-43d7-8ef4-3df8870
Deployment details (Download)
Resource Type Status Operation details
CPMng Microsoft.Compute/virtual... OK Operation details
bootdiagtktp6olu3l2ru Microsoft.Storage/storage... OK Operation details
CPMng-eth0 Microsoft.Network/netwo... Created Operation details
bootdiagtktp6olu3l2ru Microsoft.Storage/storage... OK Operation details
CPMng Microsoft.Network/publicI... OK Operation details
CPMng-nsg Microsoft.Network/netwo... OK Operation details
pid-6f13b00a-7546-4ab2-be Microsoft.Resources/depl... OK Operation details
networkExistingSetup Microsoft.Resources/depl... OK Operation details
Next steps

Step 3. connect to Security Management and start the CloudGuard service

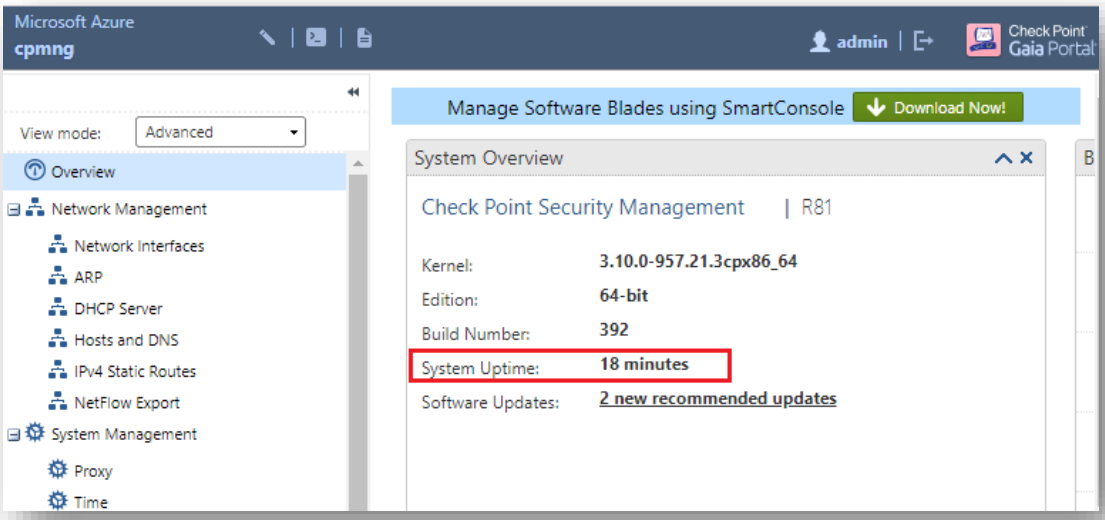
1. Click on the 'CPmng' virtual machine and connect to the GAIA portal by browsing the listed public IP address https://<public IP address>.
   Wait at least 10 minutes after Azure deployment for Security Management is finished before connecting GAIA portal
   The username is 'admin' and the password the one you configured before.



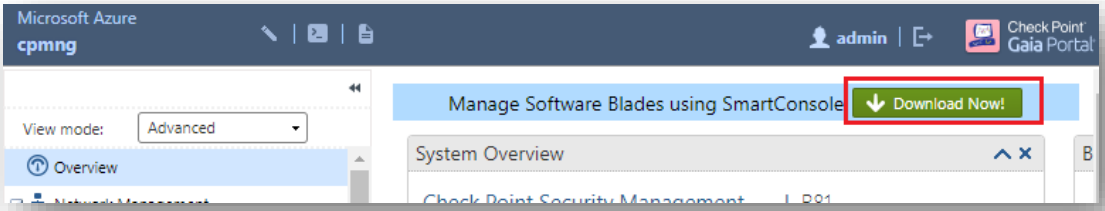




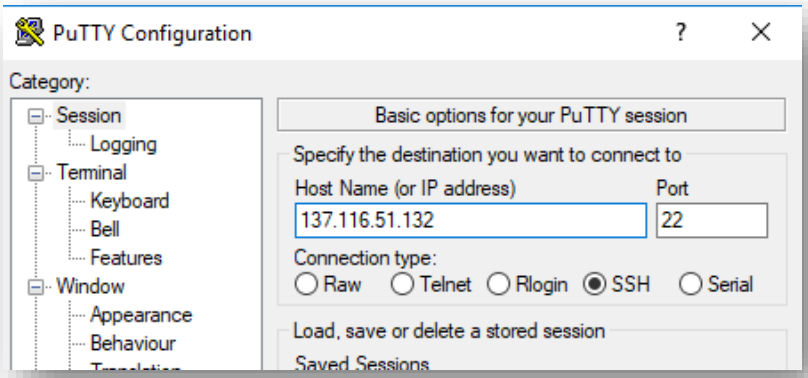
2. Verify whether the System Uptime is over 5 minutes to have all backend resources created and ready.



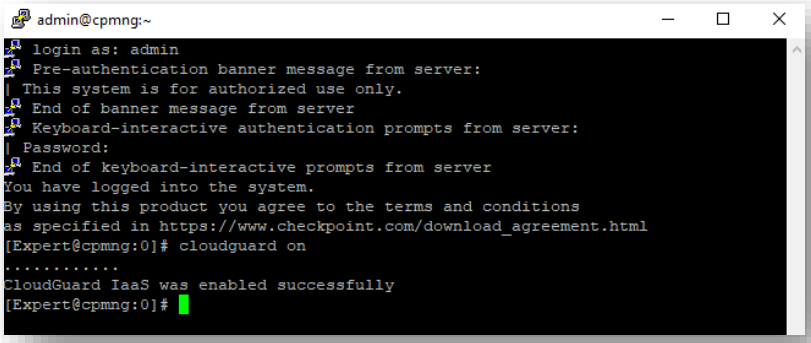
3. Download and install Check Point R81 SmartConsole.



4. Connect to the Security Management server public IP address with an SSH session. Use the same credentials as you did for the GAIA web portal.

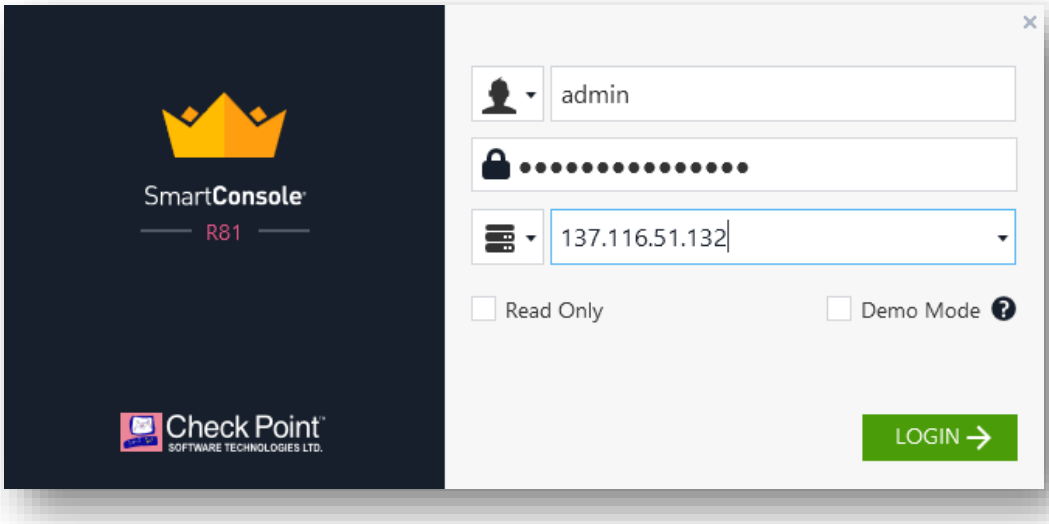


5. Execute the 'cloudguard on' command to enable the CloudGuard controller.



Step 4. connect to the Security Management

1. Open the R81 SmartConsole GUI and connect to the Security Management server public IP address. Use the same credentials as you did for the GAIA web portal.



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

You have finished exercise 2.

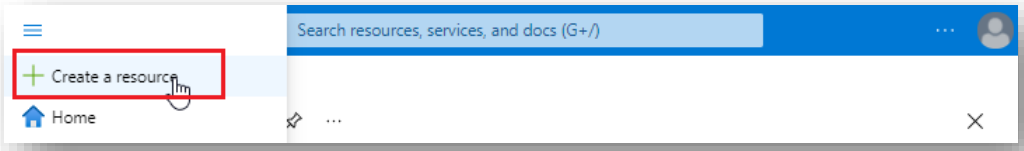
Exercise 3 - Deploy CloudGuard Gateway

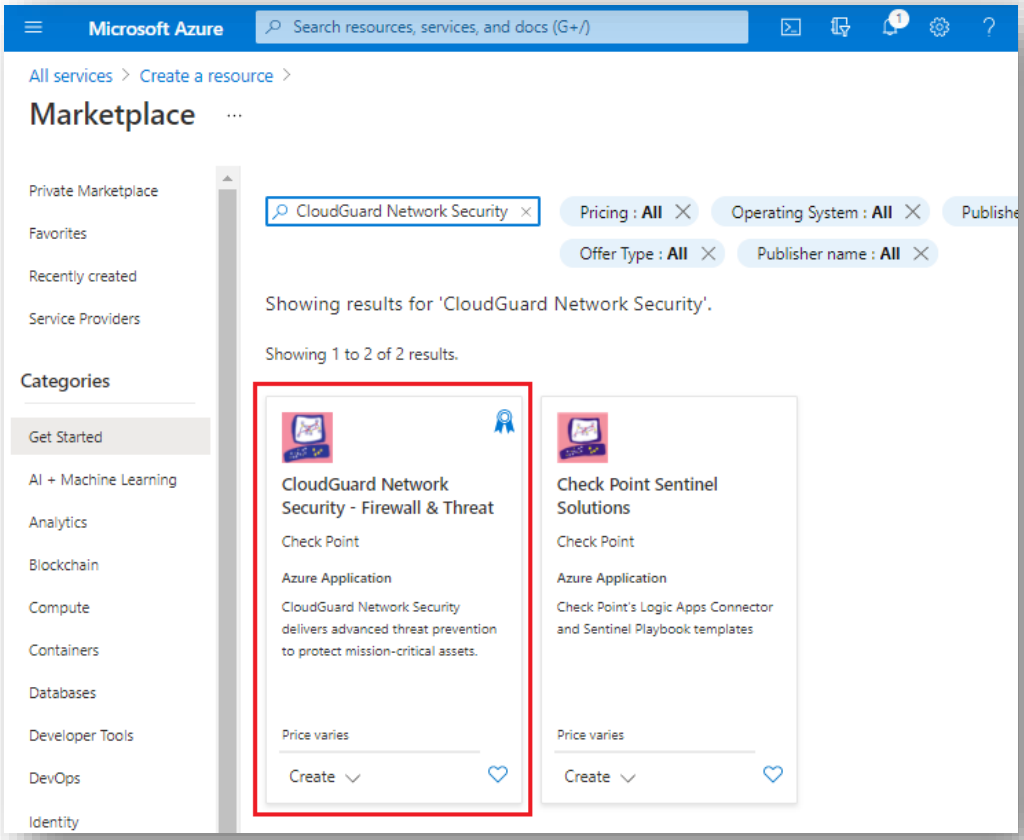
Goal

Deploying the Check Point CloudGuard gateway using an Azure Resource Manager template

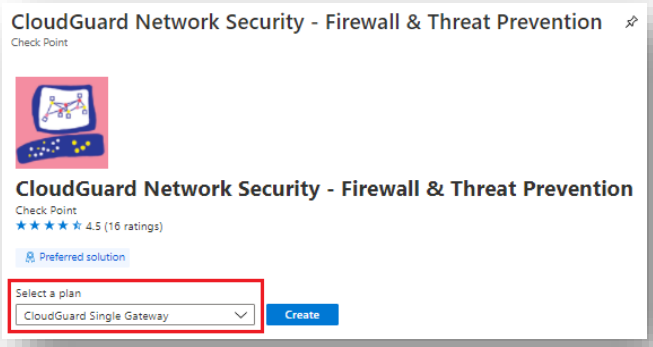
Step 1. locate the Azure marketplace template

1. Connect to Azure portal, click on the portal menu icon -> 'Create a resource'. Search for 'CloudGuard Network Security' and select the Firewall&Threat Azure application.



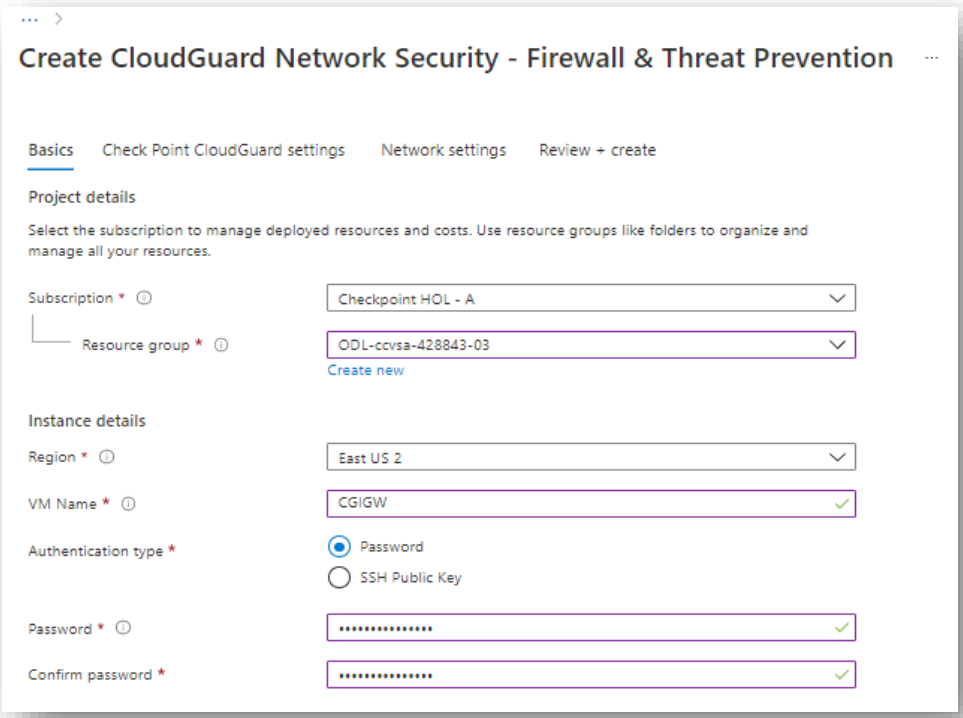


2. Change the plan to 'CloudGuard Single Gateway' and click Create.



Step two: deploy Security Management

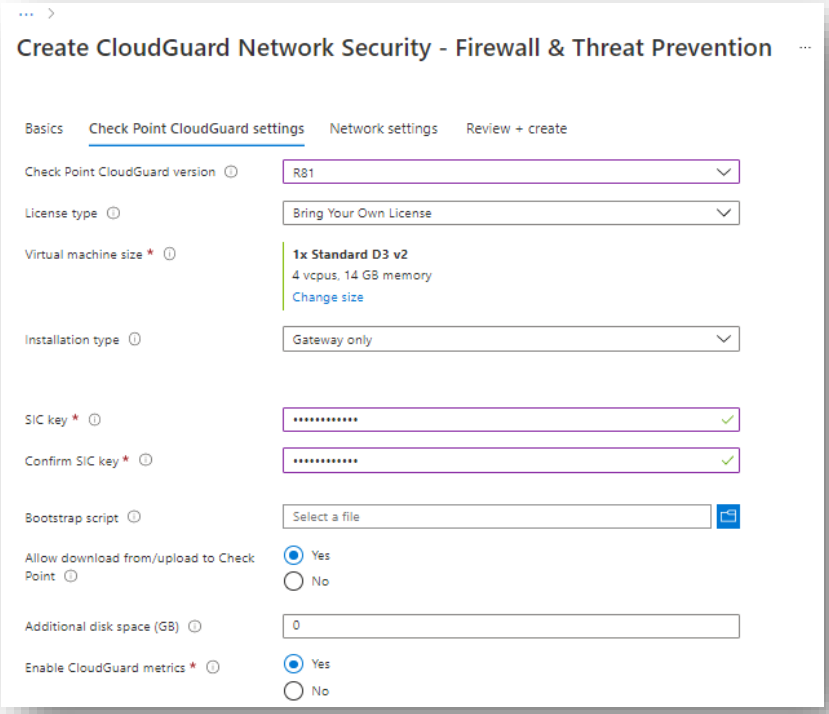
1. Fill in the info per the details below. Click on 'Next: Check Point CloudGuard settings'.



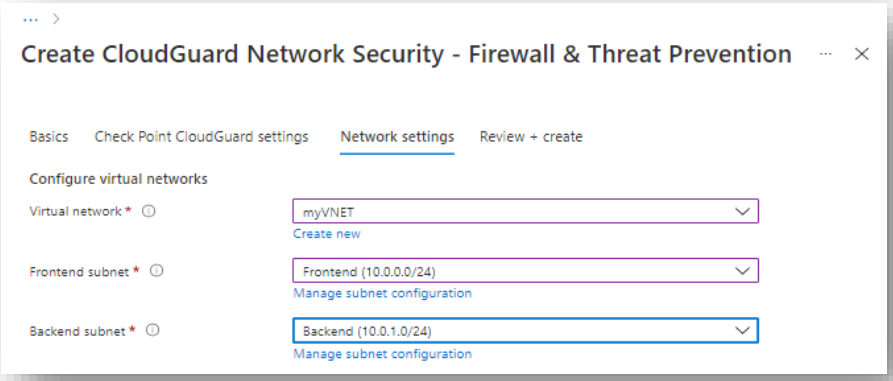
Setting	Value
Subscription	Leave the default one
Resource group	Resource Group that ends with -03 (the 3rd on the list)
Region	Same as in exercise one
Name	CGIGW
Password	Choose your own (12-digits min, inc. uppercase+lowercase+number)

2. Fill in the info per the details below. Click on 'Next : Network Settings'.

Setting	Value
Check Point CloudGuard version	R81
License type	Bring Your Own License
Virtual machine size	Leave as is (or choose a smaller one if instructed to do so)
Installation type	Gateway only

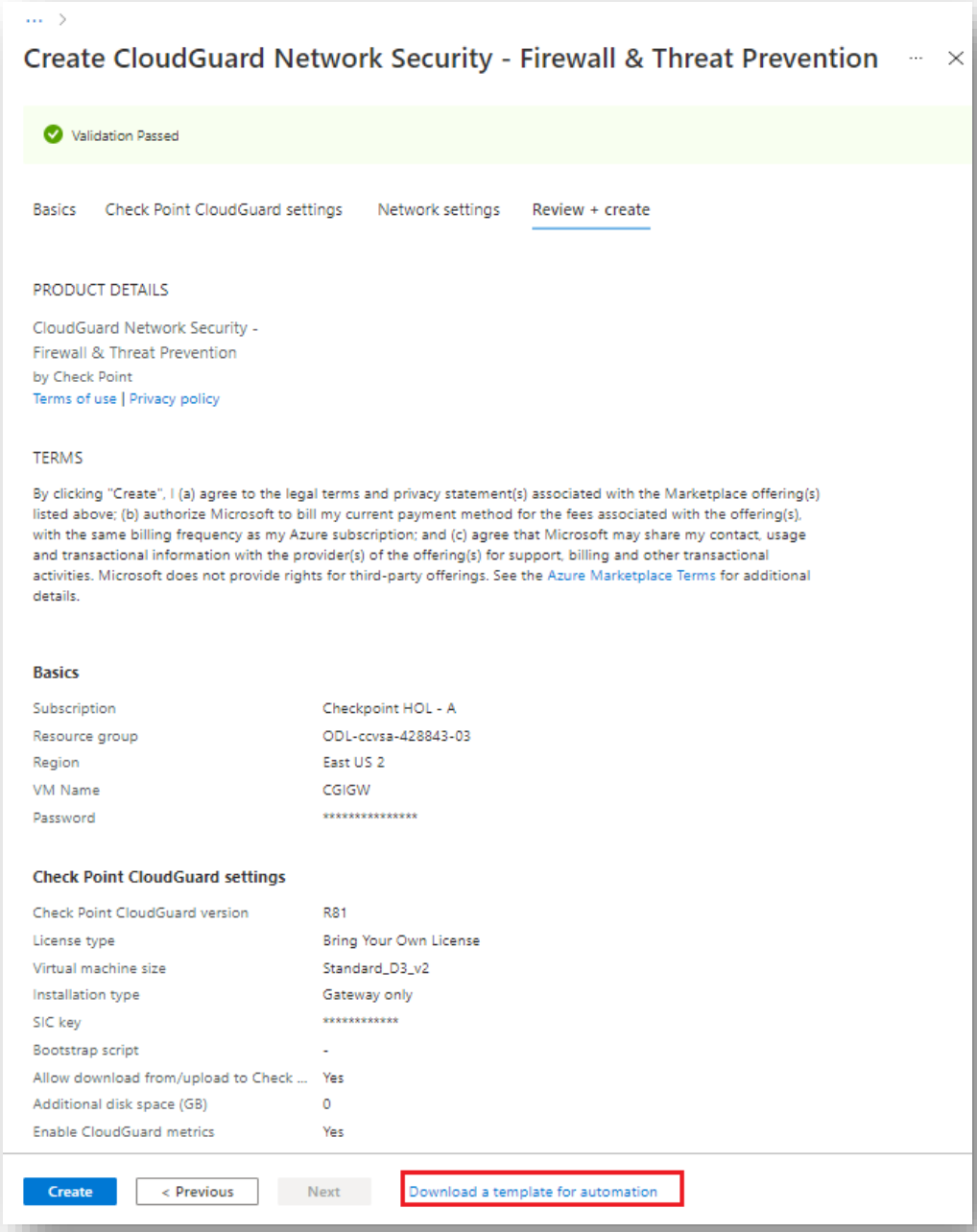


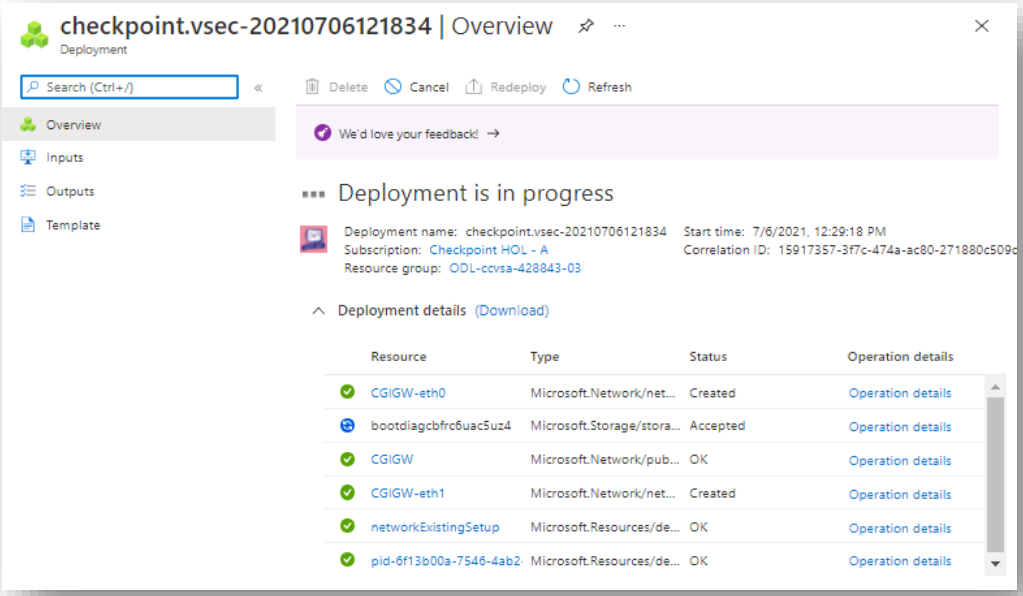
3. Under the Virtual network choose the 'myVNET' that we created in exercise 1. For Frontend subnet choose the network named ‘Frontend'. For Backend subnet choose the network named 'Backend'.
   Click on ‘Next : Review + Create >’.

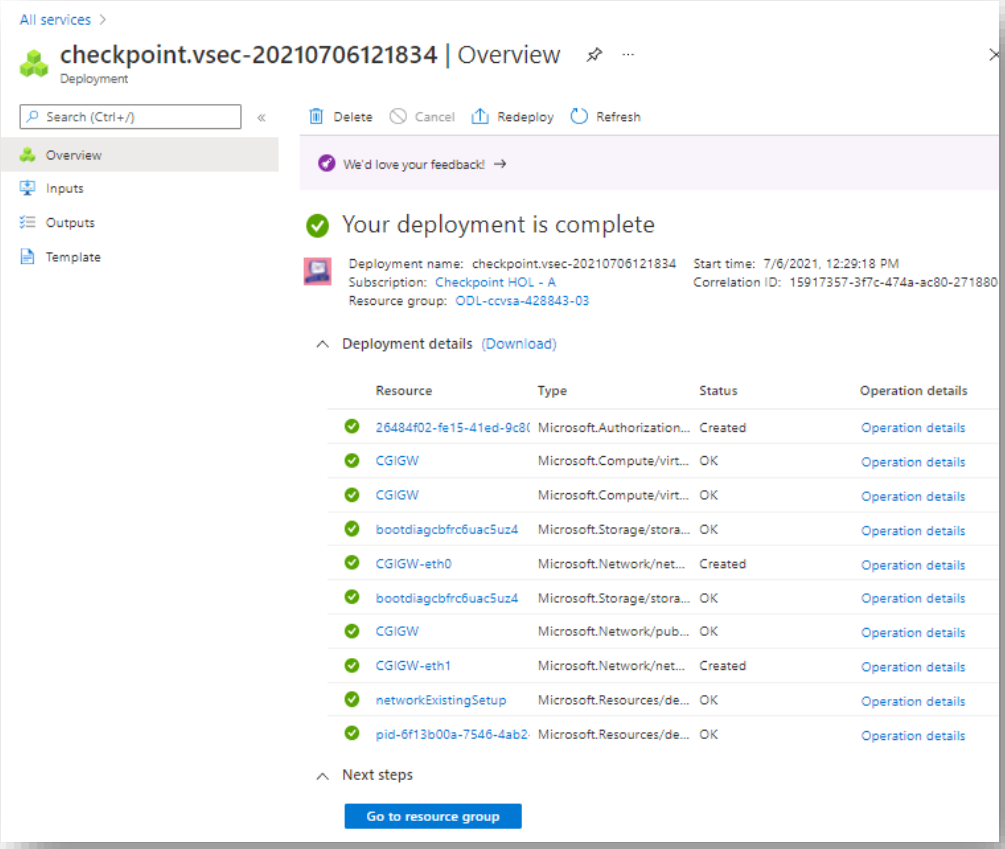


4. Verify whether you passed the validation. You can click on 'Download a template for automation' for feature deployments.
   Click on 'Create'.

   Deployment of the R81 CloudGuard gateway takes less than five minutes.


Create CloudGuard Network Security - Firewall & Threat Prevention
Validation Passed
Basics
Check Point CloudGuard settings
Network settings
Review + create
PRODUCT DETAILS
CloudGuard Network Security - Firewall & Threat Prevention
by Check Point
Terms of use | Privacy policy
TERMS
By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.
Basics
Subscription Checkpoint HOL - A
Resource group ODL-ccvsa-428843-03
Region East US 2
VM Name CGIGW
Password **********
Check Point CloudGuard settings
Check Point CloudGuard version R81
License type Bring Your Own License
Virtual machine size Standard_D3_v2
Installation type Gateway only
SIC key **********
Bootstrap script -
Allow download from/upload to Check ... Yes
Additional disk space (GB) 0
Enable CloudGuard metrics Yes
Create
< Previous
Next
Download a template for automation

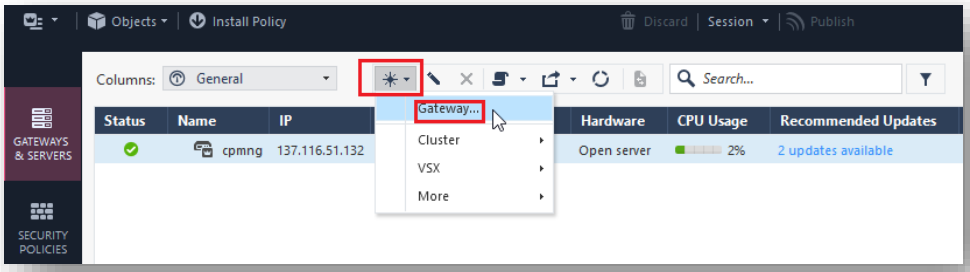

checkpoint.vsec-20210706121834 | Overview
Deployment
Search (Ctrl+/)
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Refresh
We'd love your feedback! →
Deployment is in progress
Deployment name: checkpoint.vsec-20210706121834
Subscription: Checkpoint HOL - A
Resource group: ODL-ccvsa-428843-03
Start time: 7/6/2021, 12:29:18 PM
Correlation ID: 15917357-3f7c-474a-ac80-271880c509c
Deployment details (Download)
Resource
Type
Status
Operation details
CGIGW-eth0 Microsoft.Network/net... Created Operation details
bootdiagcbfrc6uac5uz4 Microsoft.Storage/stora... Accepted Operation details
CGIGW Microsoft.Network/pub... OK Operation details
CGIGW-eth1 Microsoft.Network/net... Created Operation details
networkExistingSetup Microsoft.Resources/de... OK Operation details
pid-6f13b00a-7546-4ab2 Microsoft.Resources/de... OK Operation details


All services
checkpoint.vsec-20210706121834 | Overview
Deployment
Search (Ctrl+/)
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Refresh
We'd love your feedback! →
Your deployment is complete
Deployment name: checkpoint.vsec-20210706121834
Subscription: Checkpoint HOL - A
Resource group: ODL-ccvsa-428843-03
Start time: 7/6/2021, 12:29:18 PM
Correlation ID: 15917357-3f7c-474a-ac80-271880
Deployment details (Download)
Resource
Type
Status
Operation details
26484f02-fe15-41ed-9c8(Microsoft.Authorization... Created Operation details
CGIGW Microsoft.Compute/virt... OK Operation details
CGIGW Microsoft.Compute/virt... OK Operation details
bootdiagcbfrc6uac5uz4 Microsoft.Storage/stora... OK Operation details
CGIGW-eth0 Microsoft.Network/net... Created Operation details
bootdiagcbfrc6uac5uz4 Microsoft.Storage/stora... OK Operation details
CGIGW Microsoft.Network/pub... OK Operation details
CGIGW-eth1 Microsoft.Network/net... Created Operation details
networkExistingSetup Microsoft.Resources/de... OK Operation details
pid-6f13b00a-7546-4ab2 Microsoft.Resources/de... OK Operation details
Next steps
Go to resource group

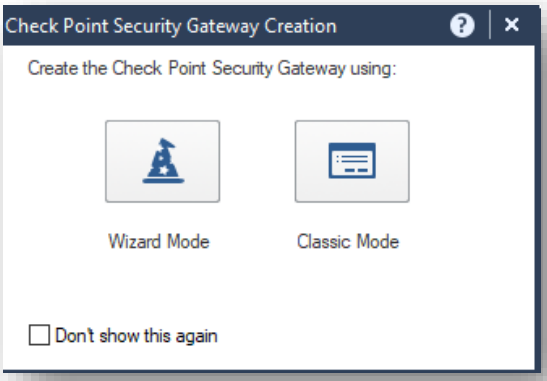
Step 3. create a CloudGuard gateway object in Security Management

1. Log in to the R81 management server and configure the cluster object
   Detailed instructions are in **sk109360** .

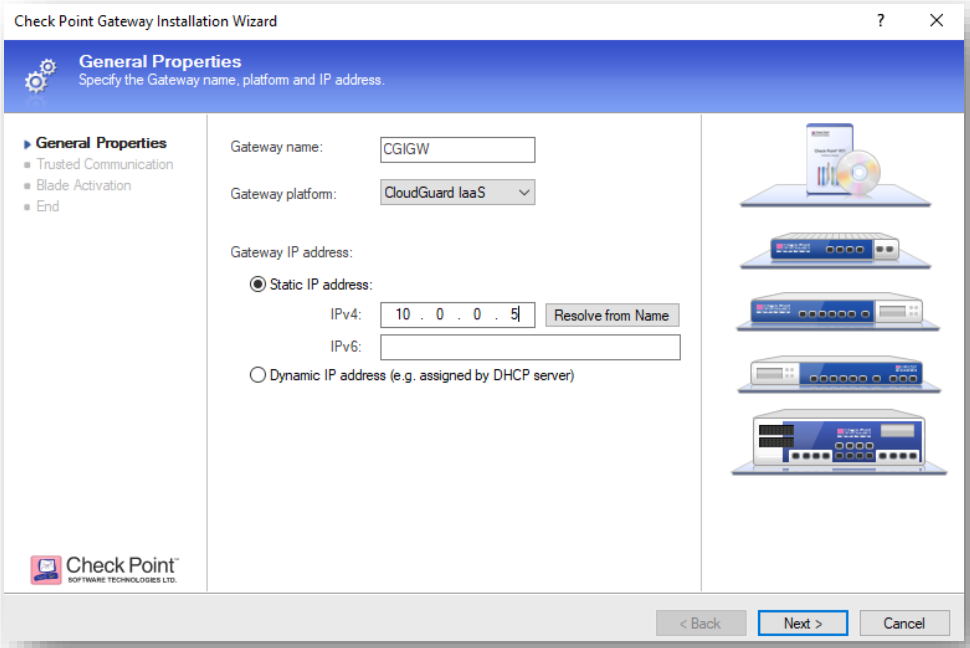
2. Click GATEWAYS & SERVERS on the left menu.
   Click on New wizard -> Gateway.



3. Choose Wizard Mode.

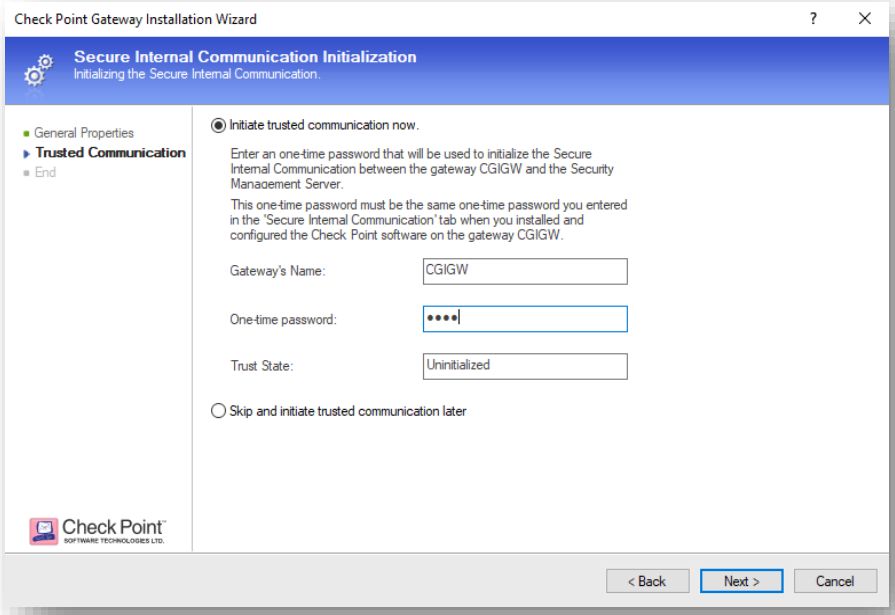


   a. Fill in the details as described below and click Next.

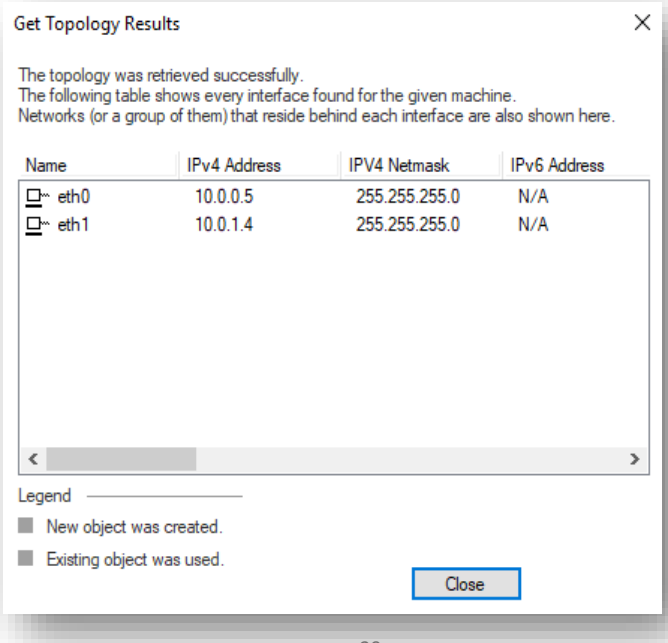


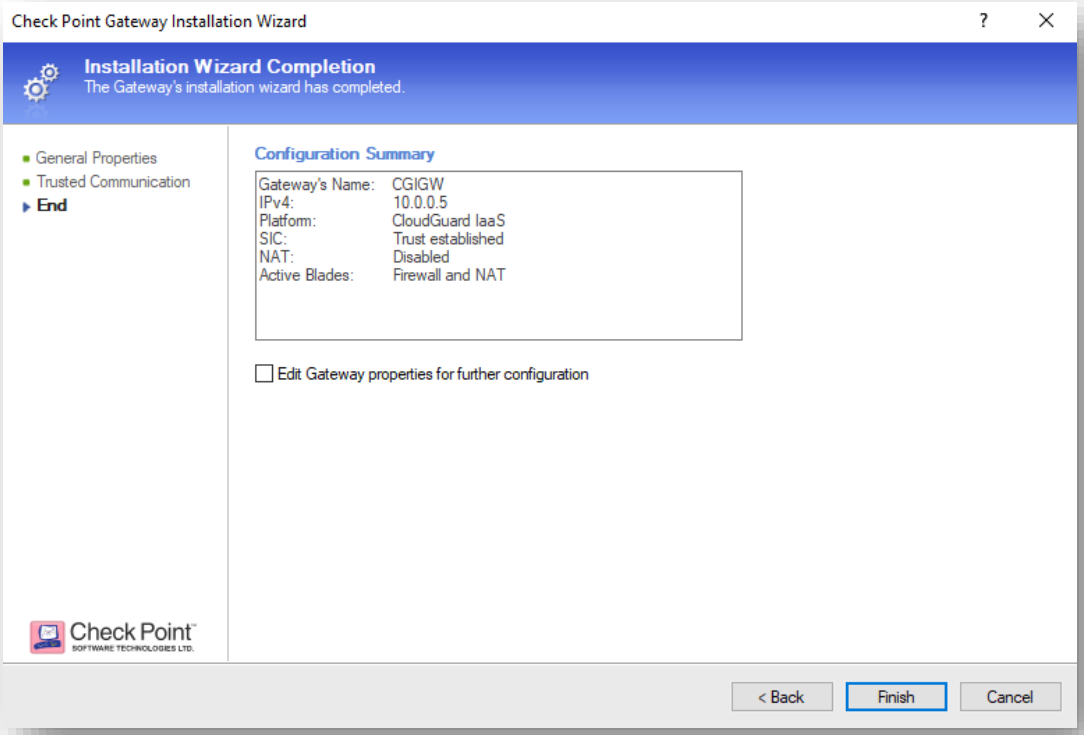
Setting	Value
Gateway name	CGIGW
Gateway platform	CloudGuard IaaS
Static IP address	10.0.0.5 , use the private IP in the 'Frontend' subnet. You can see it at Azure portal -> Virtual machines -> CGIGW -> Networking -> Private IP address

4. Fill in the one-time password that you configured in step 1 and click Next.



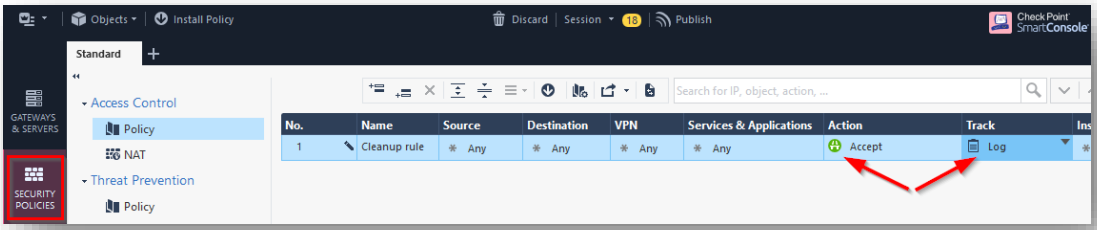
2. Verify whether you see two network interfaces in the Topology Results window. Click Close. Uncheck the 'Edit Gateway properties ….' and click Finish.



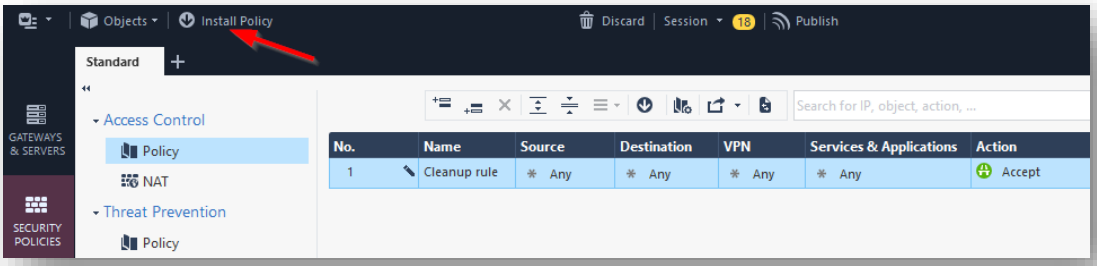


Step 4. create a security policy

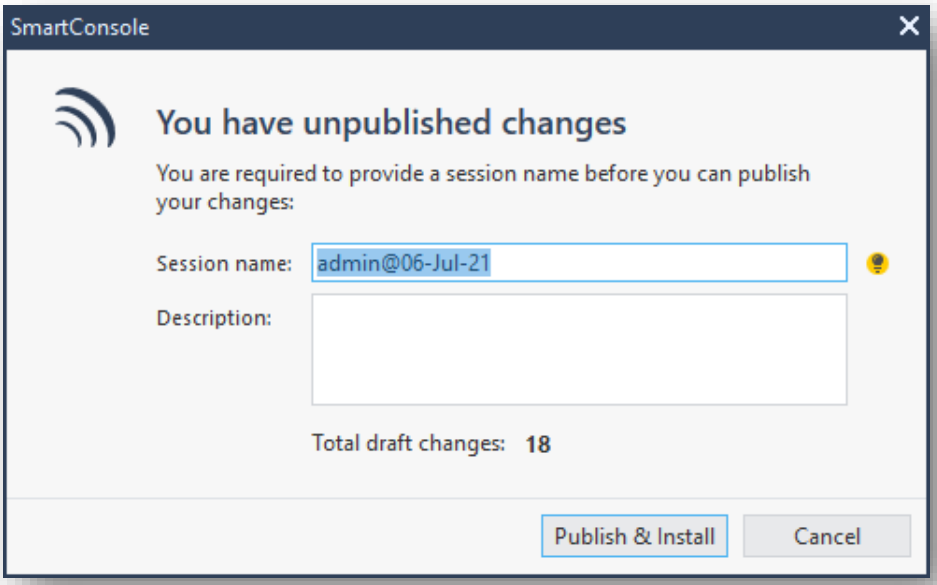
1. Navigate to the 'Security Policies' section, change the Access Control cleanup rule action from 'Drop' to 'Accept', and set Track to 'Log'.



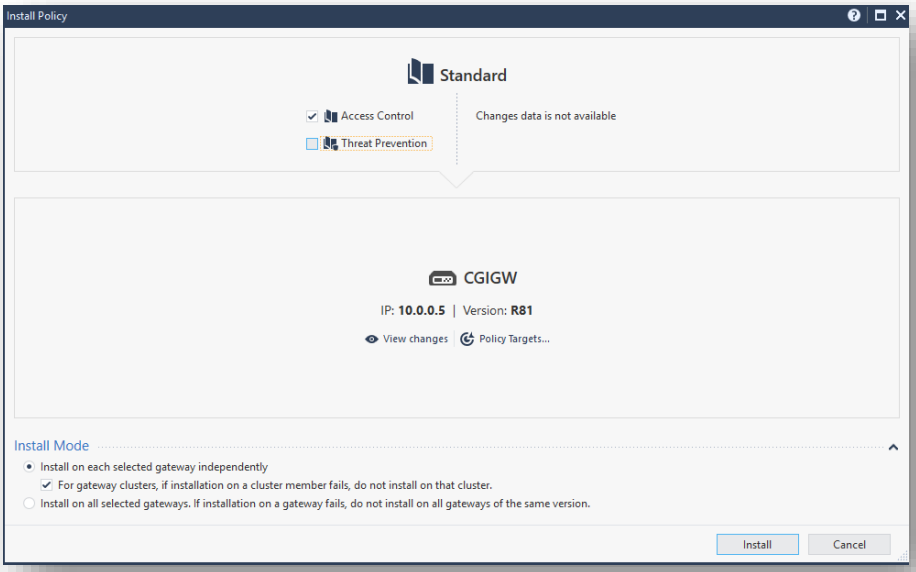
2. On the upper left click '**Install Policy**'.

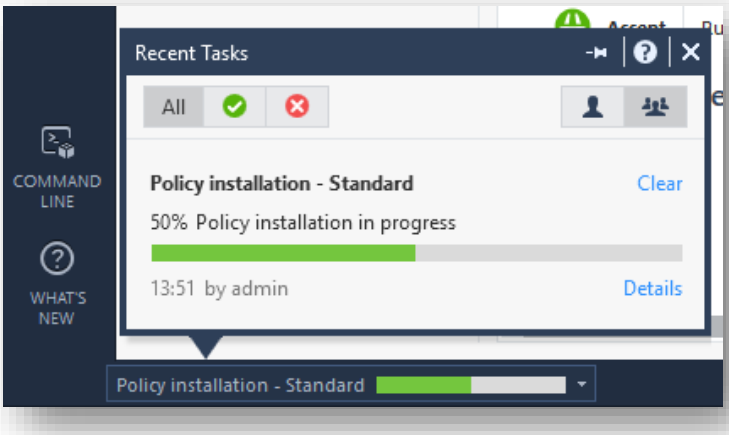


3. Click '**Publish & Install**'.

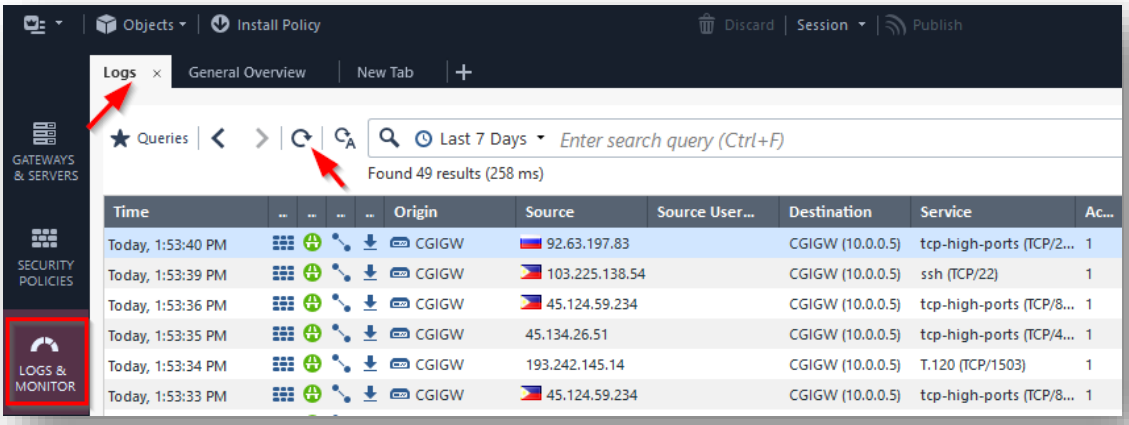


a. In the opened window uncheck Threat Prevention and click Install.
b. Check the bottom of the SmartConsole for the status of the policy installation.





4. Navigate to the 'Logs & Monitor' section - the Logs tab. Refresh the view and see logs originating from the CGIGW gateway.



You have finished exercise 3.

Exercise 4 - Deploying a web server

Goal

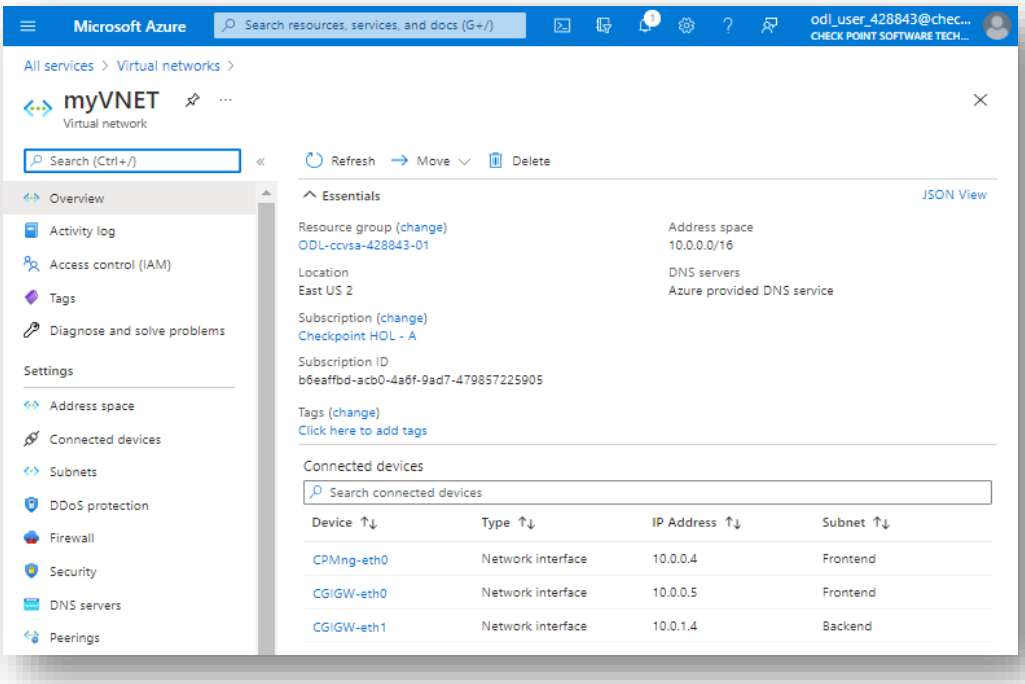
Provision the Web Server instance from Azure Marketplace and protect it by CloudGuard gateway

Step 1. create a subnet for a web server

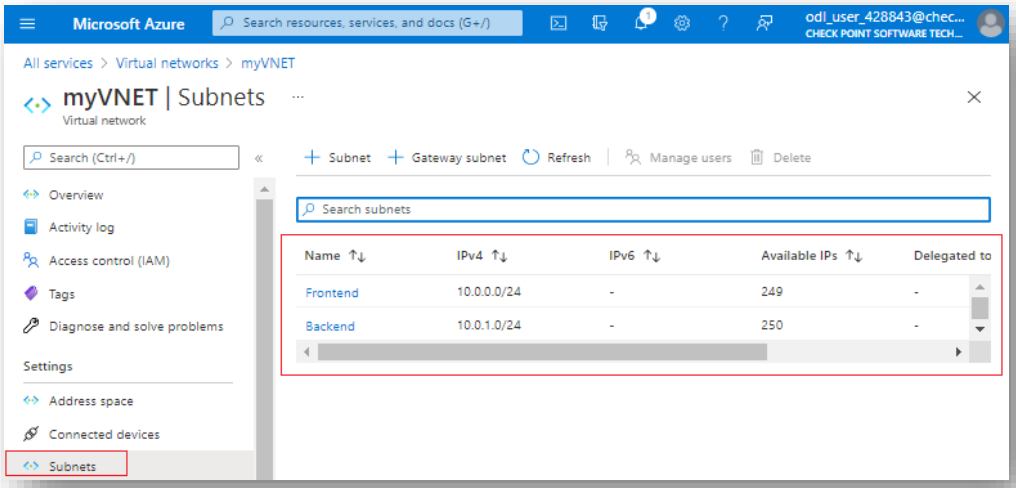
In this step we'll create a subnet called 'Web' to be used by a web server.

We will create Azure User Defined Routing (UDR) to inspect the web server's traffic by the CloudGuard gateway.

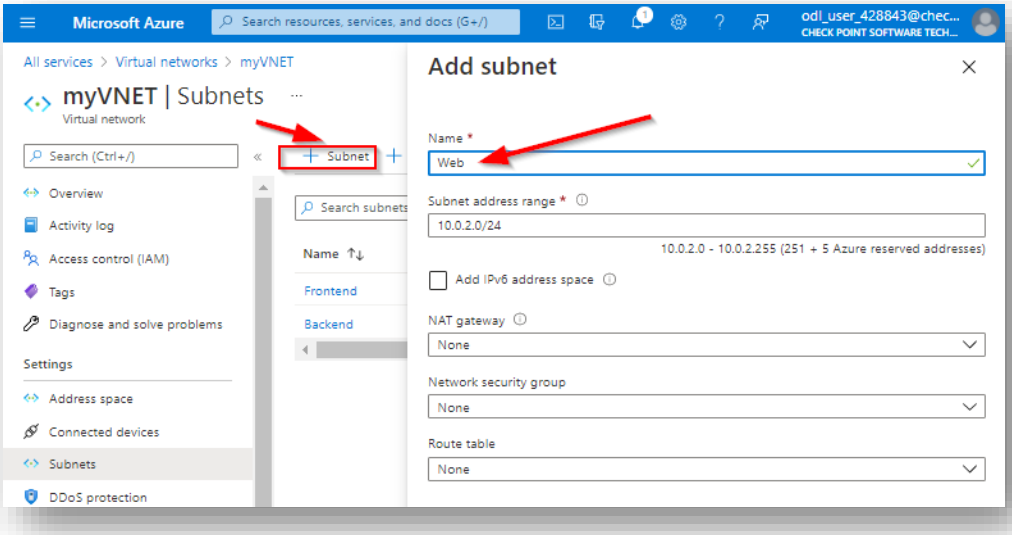
1. Navigate to the Azure portal '**Virtual networks**' service and click on the 'myVNET' network.



2. Click on '**Subnets**' to see the list of available subnets.

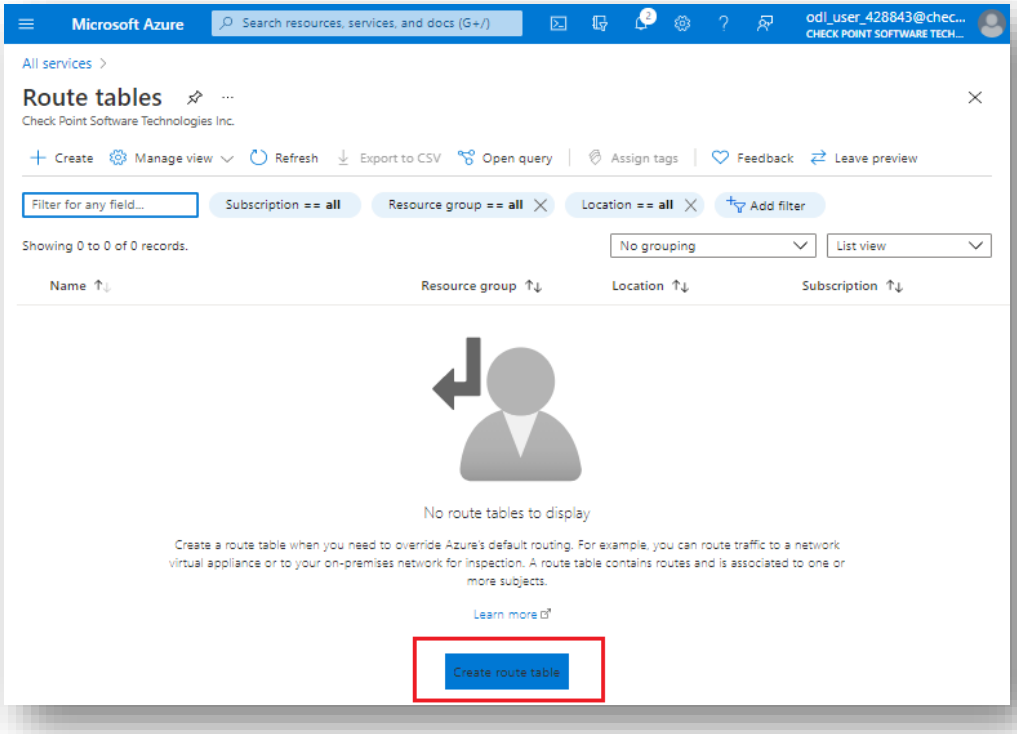


3. Click on the '**+ Subnet**'. Add the subnet named 'Web' with the subnet address range of 10.0.2.0/24.

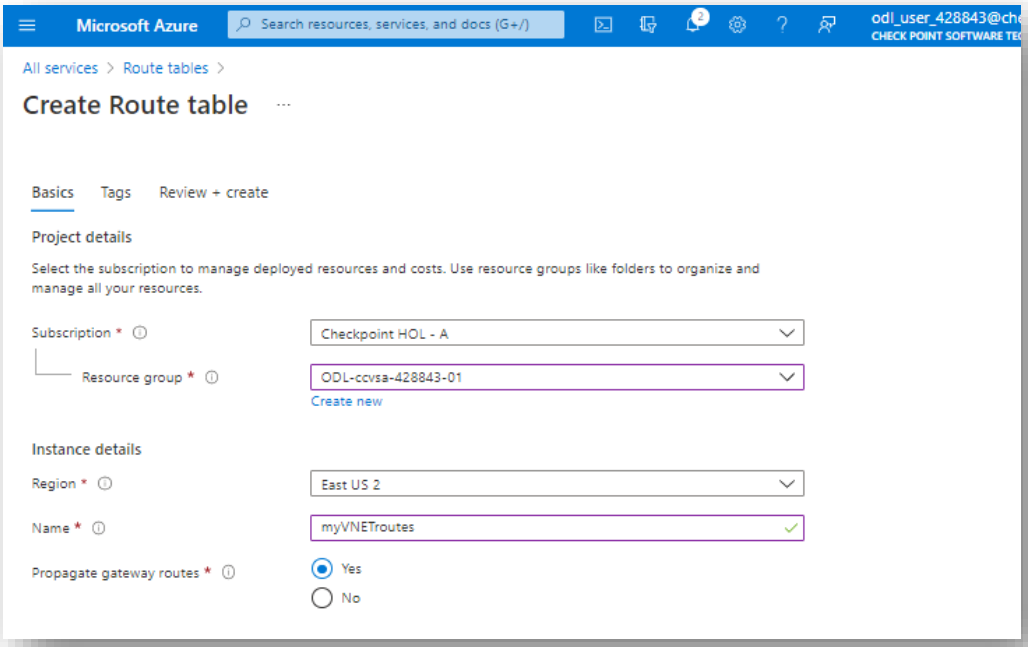


Step 2. create UDRs and associate them with the newly created subnet

1. Search the Azure portal for the 'Route tables' service and click on 'Create route table'.

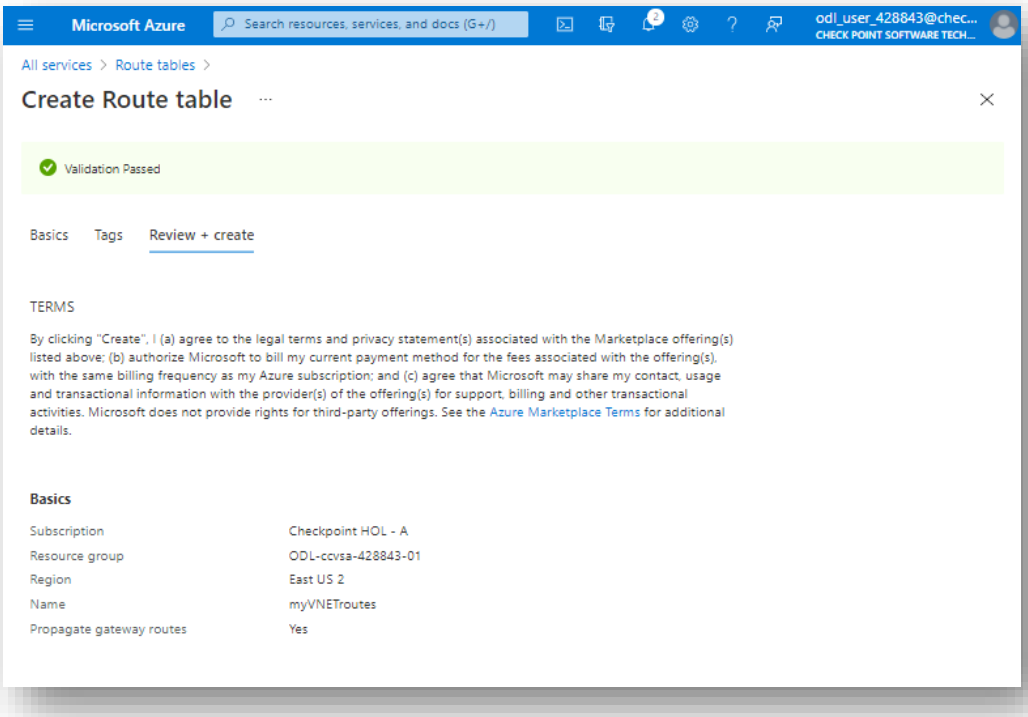


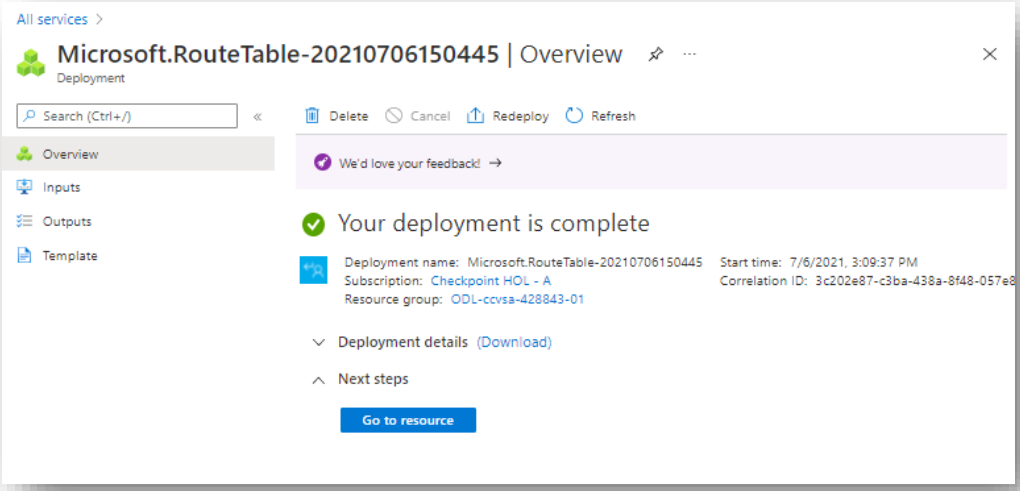
2. Fill in the details as described below and click 'Next : Tags'.



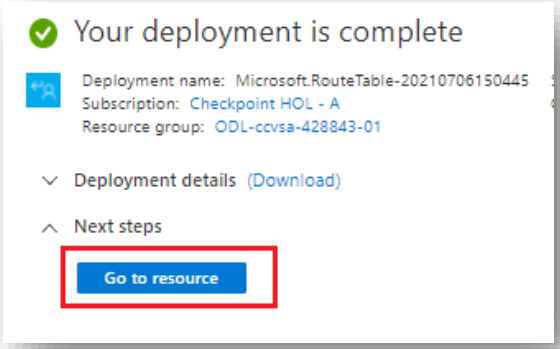
Setting	Value
Name	myVNETroutes
Resource Group	Choose the resource group that ends with -01 (the 1st on the list)
Location	Use the same location as in the first exercise

3. Skip the tags creation, click on 'Next : Review + Create'. See the validation passed and click on Create.

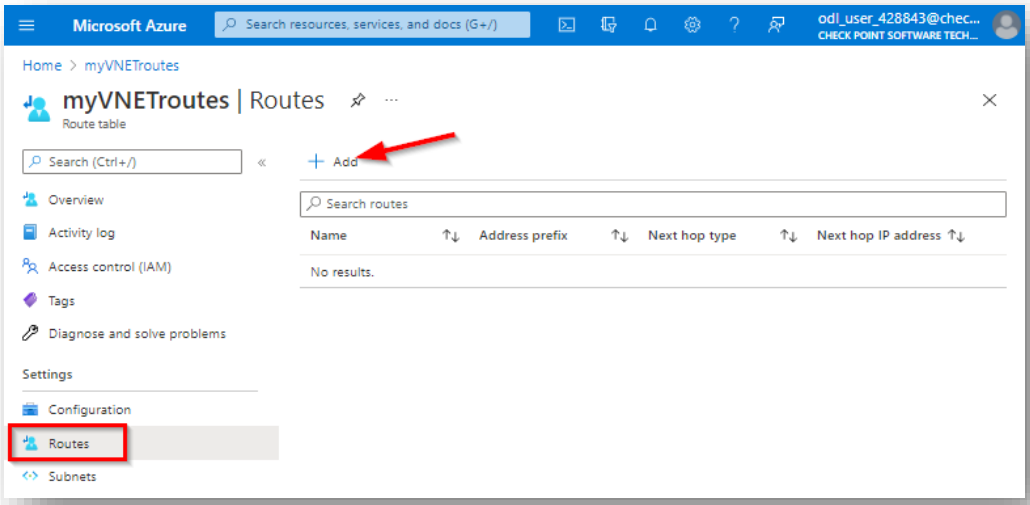




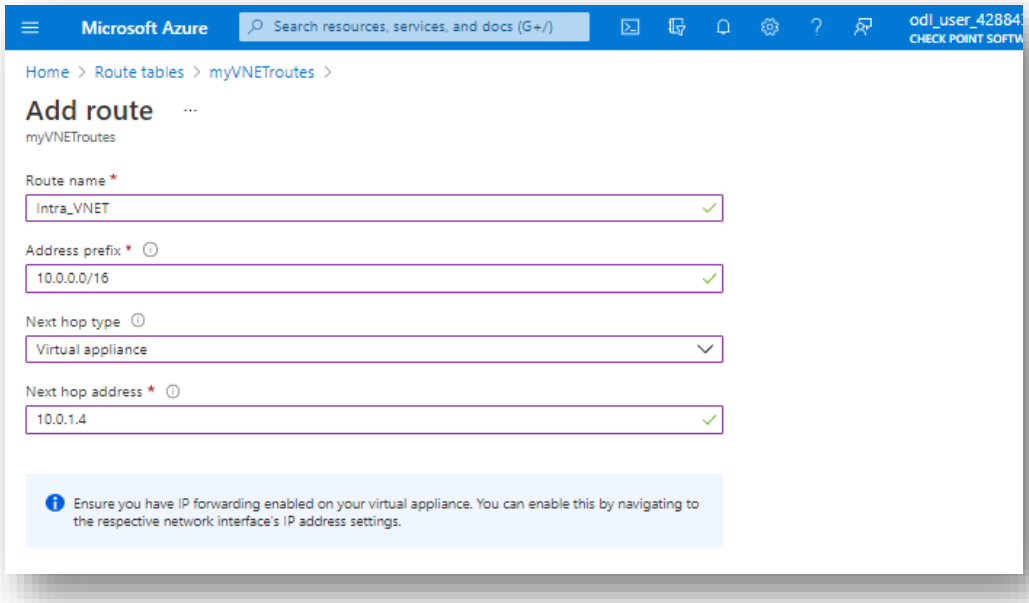
4. Click on the 'Go to resource' link.



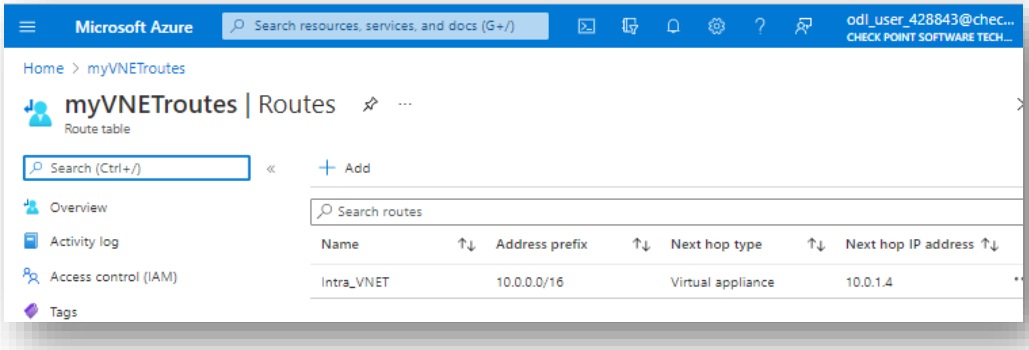
5. Click on the Routes and then click on '+ Add'.



6. Fill in the details as described below and click 'OK'.



Setting	Value
Route name	Intra_VNET
Address prefix	10.0.0.0/16
Next hop type	Virtual appliance
Next hop address	10.0.1.4 , use the private IP of CGIGW GW eth1. You can see it at Azure portal -> Virtual machines -> CGIGW -> Networking -> CGIGW-eth1 -> NIC Private IP



This will create a route entry, which will direct all VNET related traffic to CloudGuard gateway. This includes traffic between subnets as well as traffic between instances in the same subnet, effectively inserting macro as well as micro segmentation.

7. Repeat step 6 and add a new route with the details below:

Setting	Value
Route name	DefaultGW
Address prefix	0.0.0.0/0
Next hop type	Virtual appliance
Next hop address	10.0.1.4 , use the private IP of CGIGW GW eth1. You can see it at Azure portal -> Virtual machines -> CGIGW -> Networking -> CGIGW-eth1 -> NIC Private IP

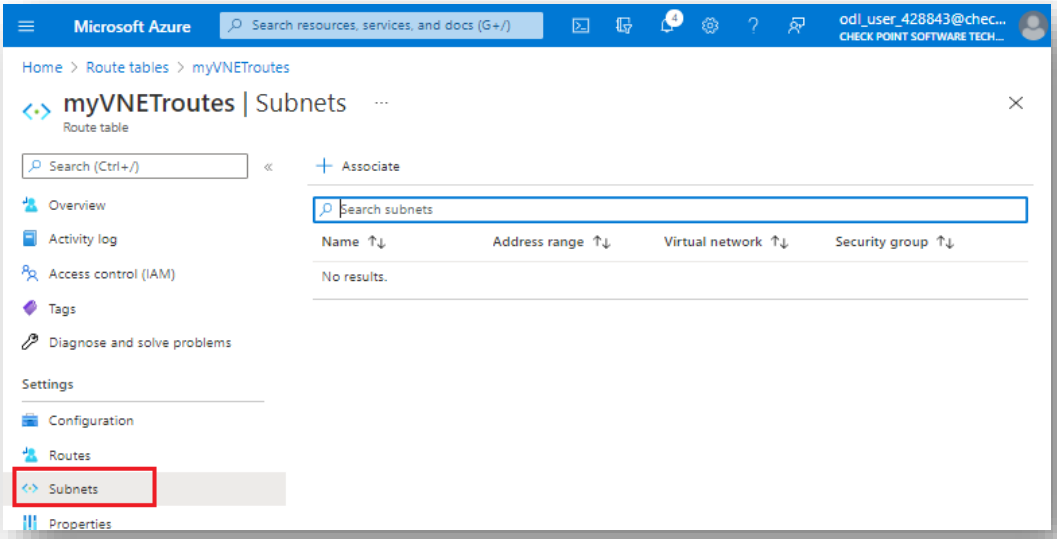
This will create a route entry, which will direct all Internet related traffic to CloudGuard.

8. Repeat step 6 and add a new route with the details below:
Traffic between subnets as well as traffic between instances in the same subnet, effectively inserting macro as well as microsegmentation.

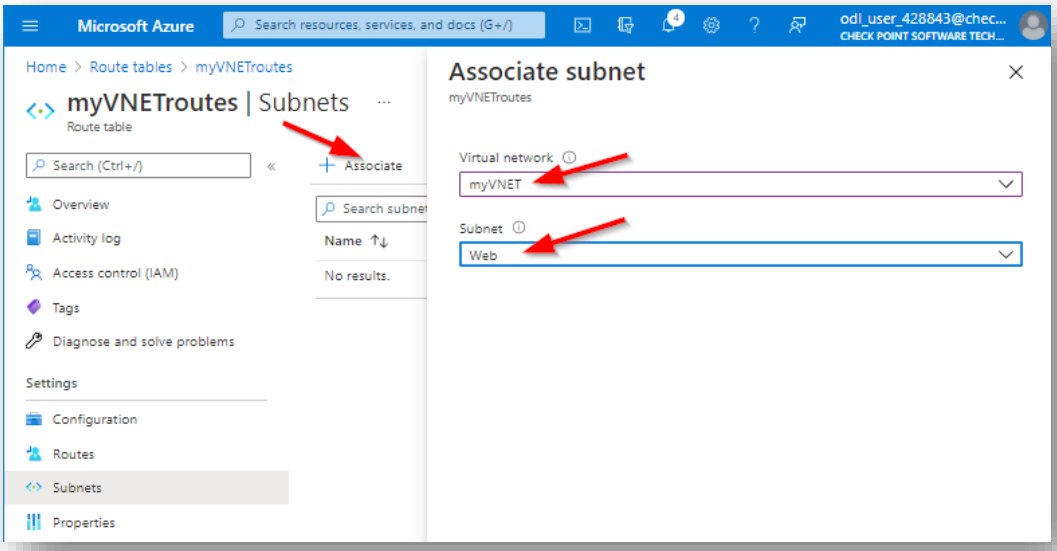
Setting	Value
Route name	Micorsegmentation-subnet-10.0.2.0
Address prefix	10.0.2.0/24
Next hop type	Virtual appliance
Next hop address	10.0.1.4 , use the private IP of CGIGW GW eth1. You can see it at Azure portal -> Virtual machines -> CGIGW -> Networking -> CGIGW-eth1 -> NIC Private IP

This will create a route entry, which will direct all Internet related traffic to CloudGuard.

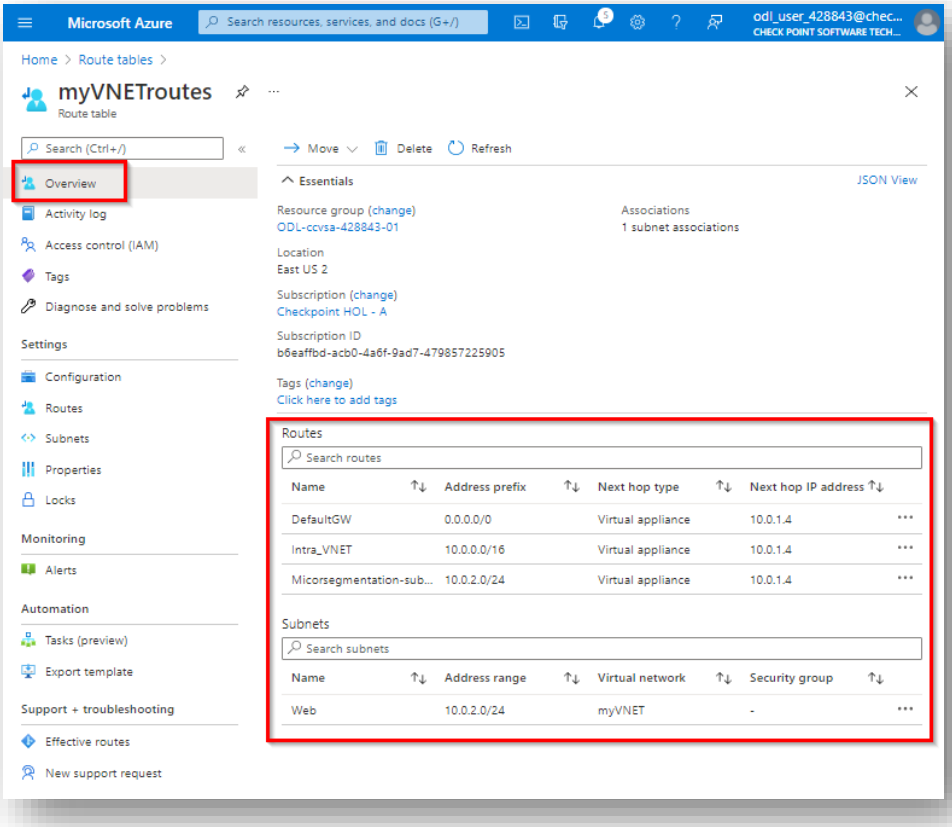
9. The created routes stay ineffective until associated with some subnet so that the subnet will enforce the configured routes. Navigate to the 'Route tables' service -> myVNETroutes and click on Subnets.



10. Click on 'Associate'. Select 'myVNET' for virtual network and 'Web' for subnet. Click OK.

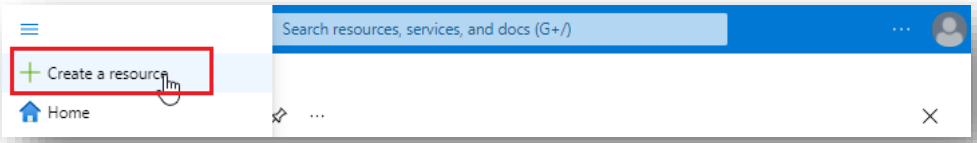


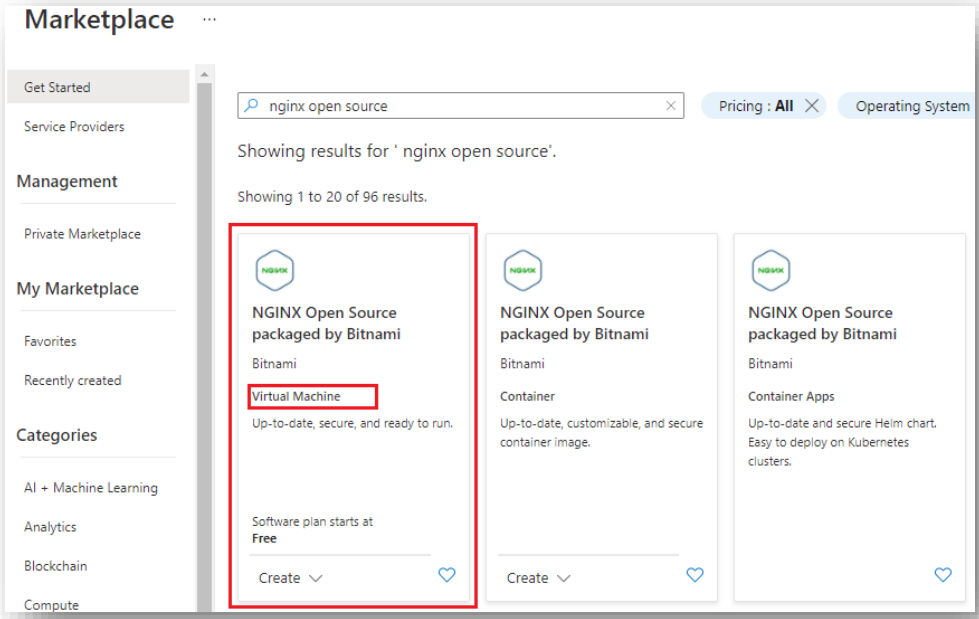
11. Navigate to Overview and verify the configuration.



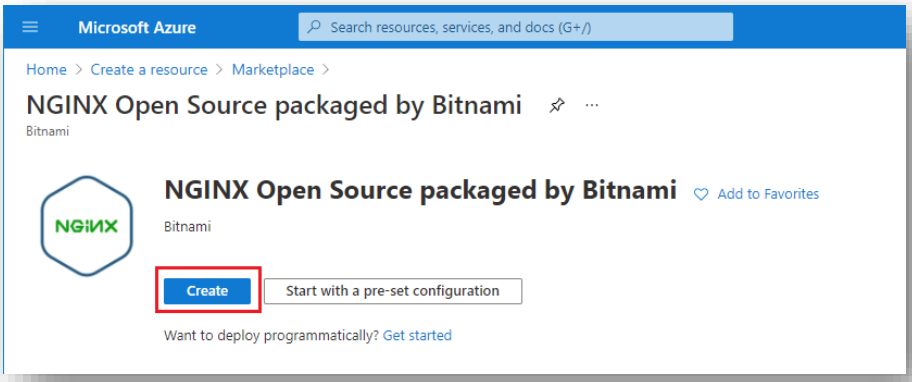
Step 3. Provision the Web Server instance from the Azure Marketplace

1. Connect to the Azure portal, click on the portal menu icon -> 'Create a resource'. Search for 'nginx open source' and select NGINX Open Source packaged by Bitnami virtual machine

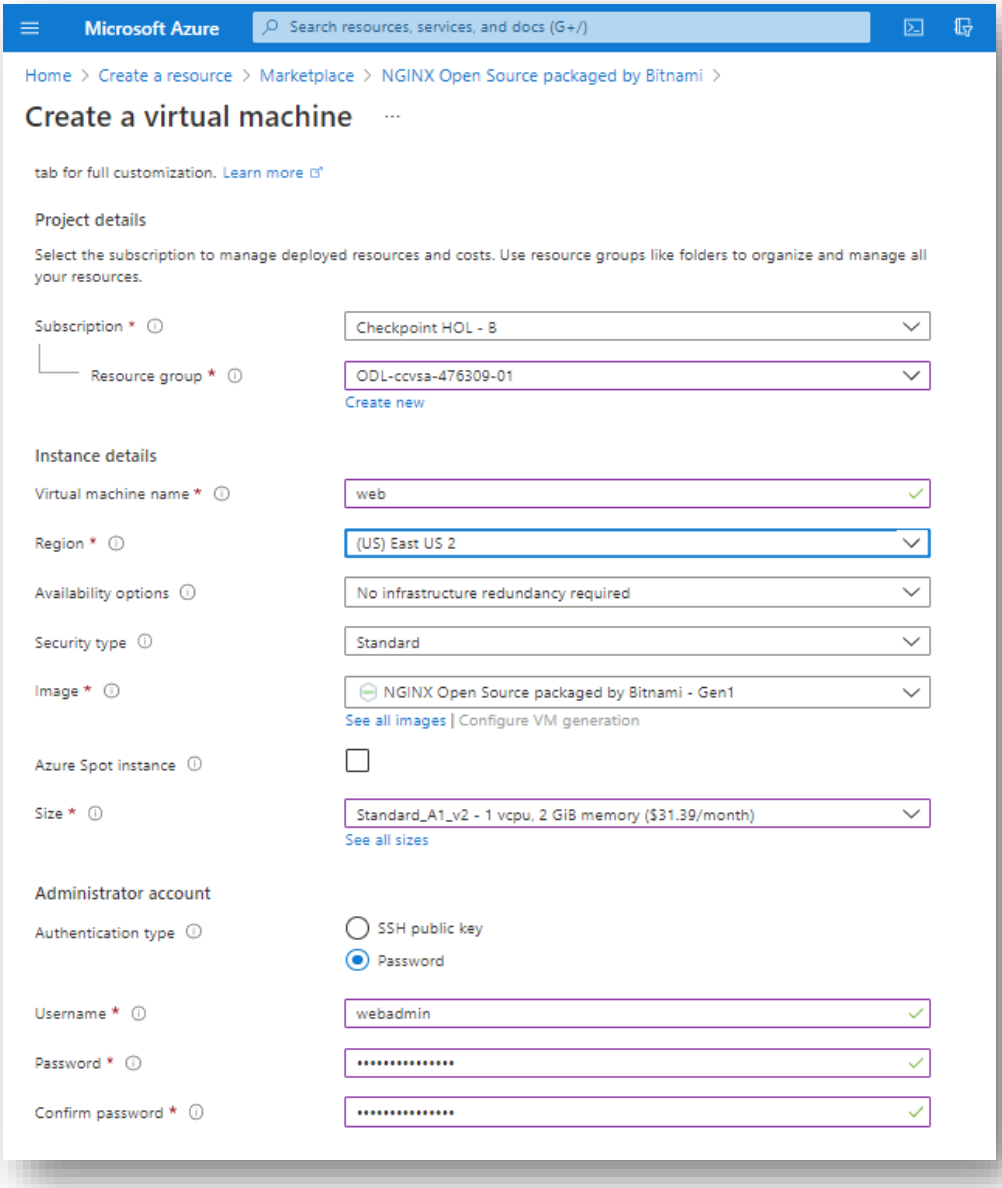




2. Click on '**Create**'.



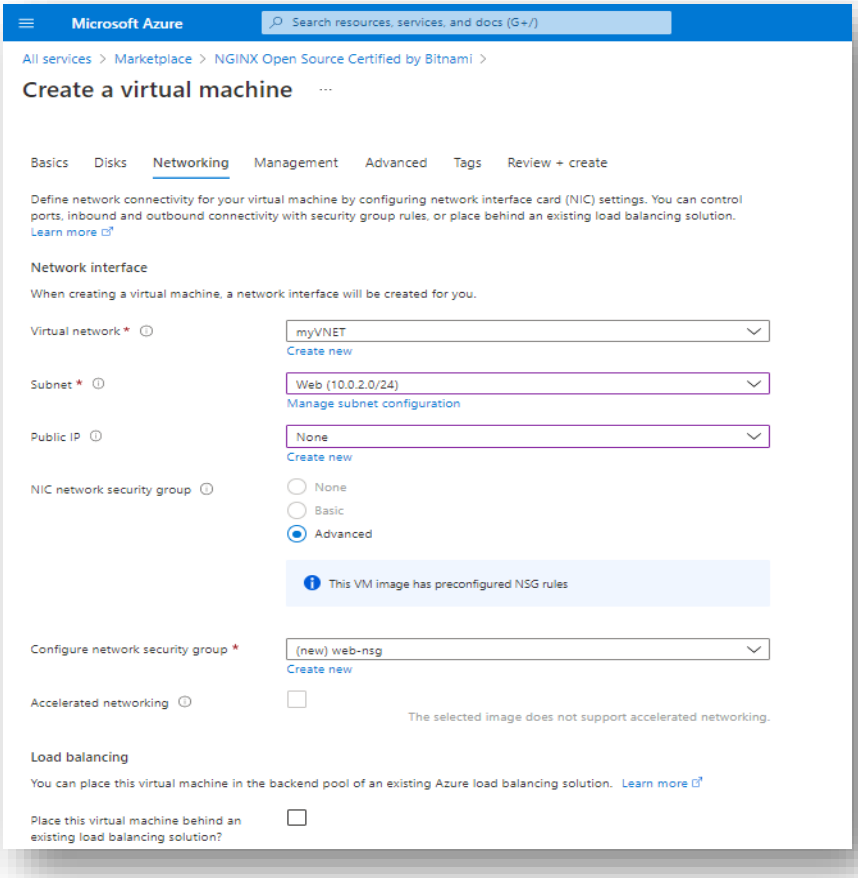
3. Fill in the info per the details below. Click on 'Next : Disks'.



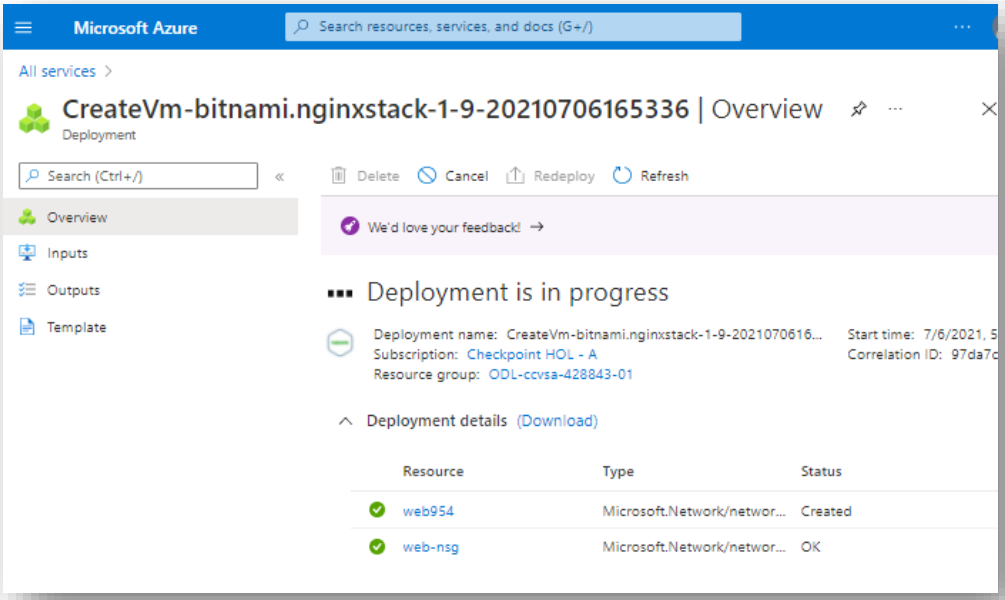
Setting	Value
Resource Group	The one ending with '01'
Virtual machine name	web
Subscription	leave as is
Region	use the same location as in exercise 1
Size	Click 'See all sizes' and manually choose 'Standard_A1_v2'
Authentication type	Password
User name	webadmin
Password	Choose your own

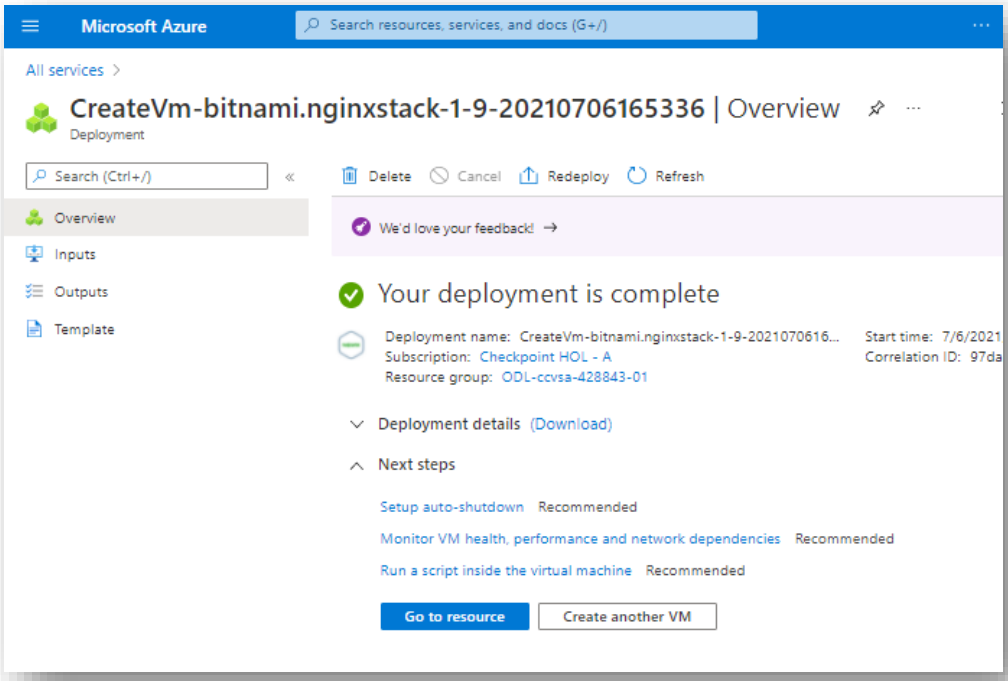
4. Click on '**Next: Networking**>'.
5. Fill in the info per the details below. Click on 'Next : Disks'.
   Click on 'Review + Create'.

Setting	Value
Virtual Network	myVNET
Subnet	web (10.0.2.0/24)
Public IP address	None
Network security group	Advanced



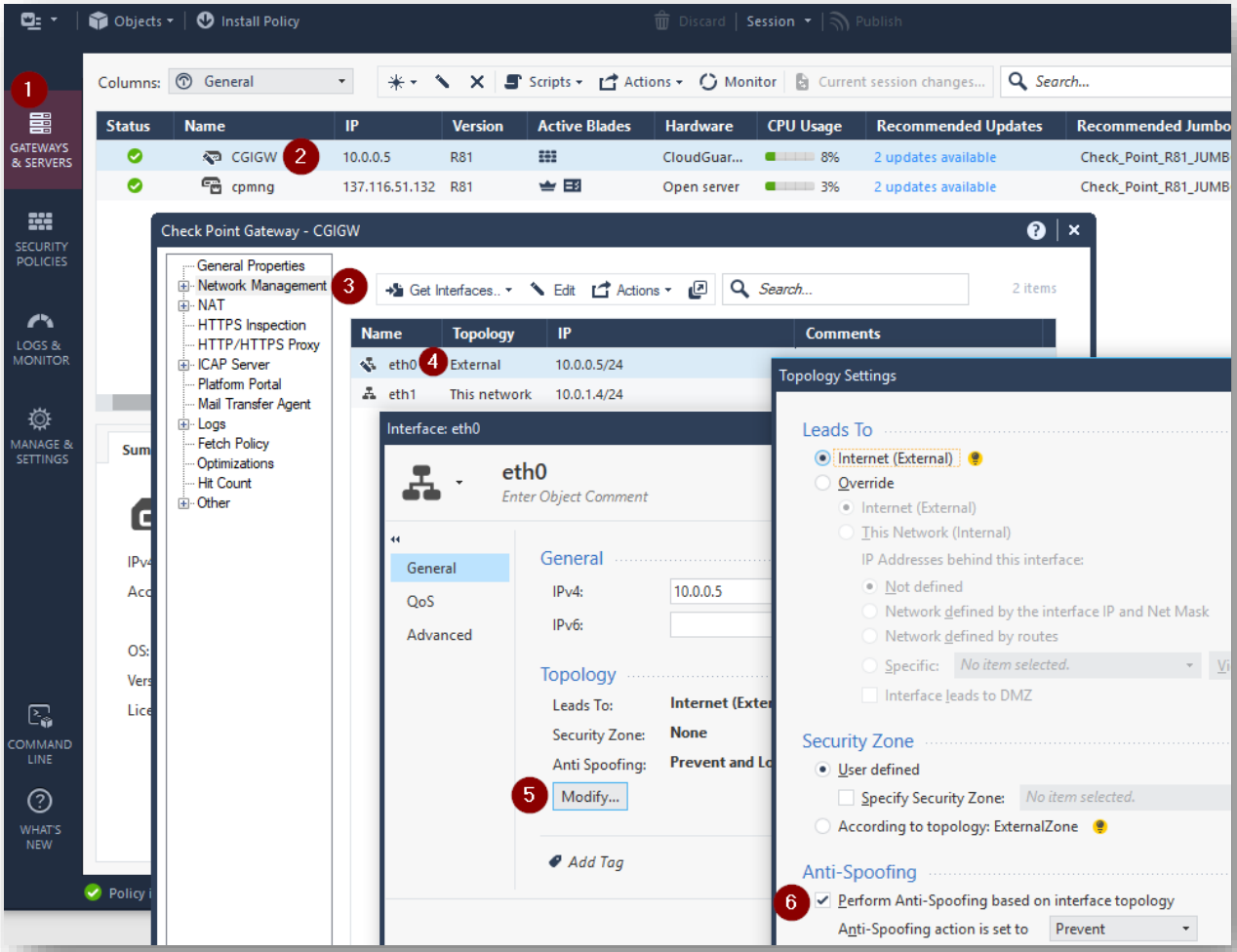
6. Validate the virtual machine details and click '**Create**' to start deployment.
   Note: there is no way to set the virtual machine private IP address at that stage, Azure will provide auto-assigned with an IP (DHCP), and you are able to change it later on (after deployment).





Step 4. creation of security policy

1. Login to the R81 management server.
2. Navigate to the 'Gateway & Servers' tab and doubleclick on CGIGW object.
3. Select Network Management -> eth0 -> Modify and uncheck the 'Perform Anti-Spoofing' selection.



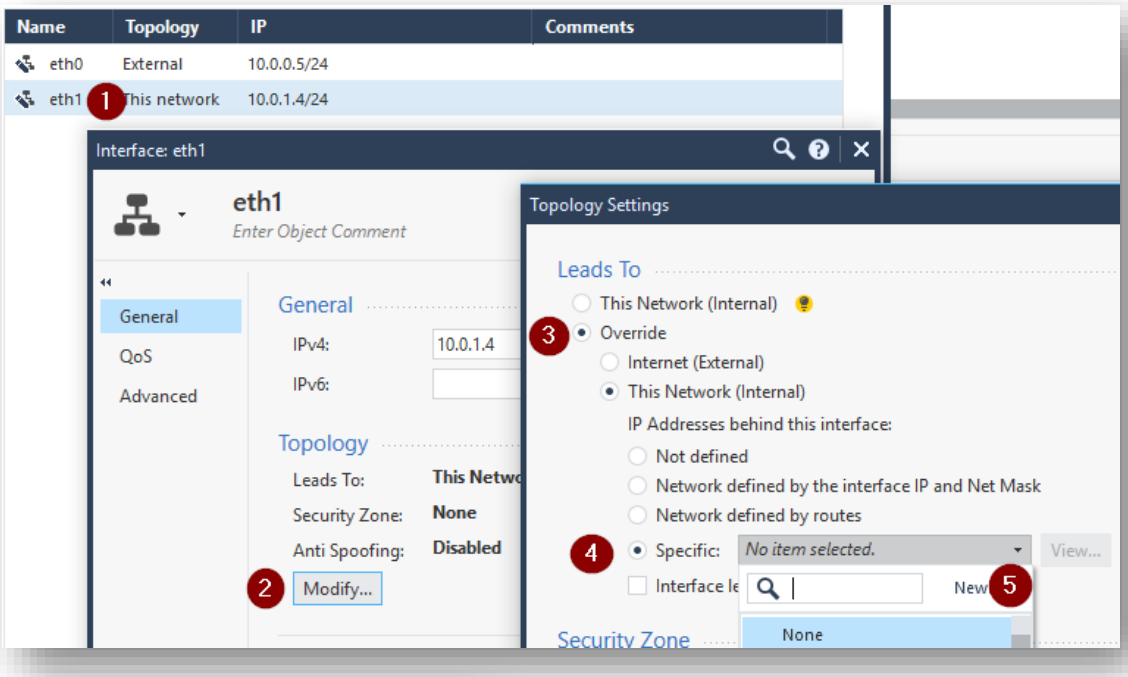
4. Click '**OK**' twice and repeat the previous step for eth1.

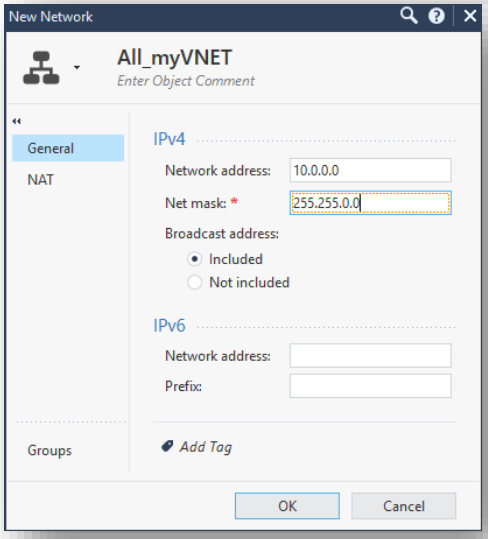
5. Doubleclick eth1. Click on General -> Modify -> Override -> Specific -> New -> Network. Create a new network object.

   Name: All_myVNET

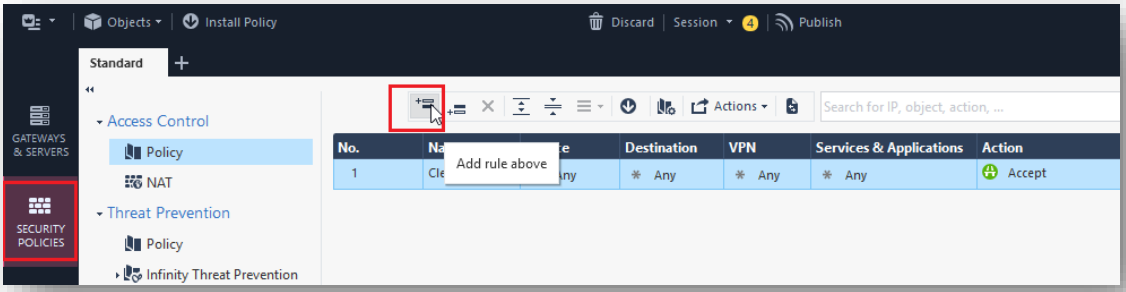
   Network address: 10.0.0.0

   Net mask: 255.255.0.0



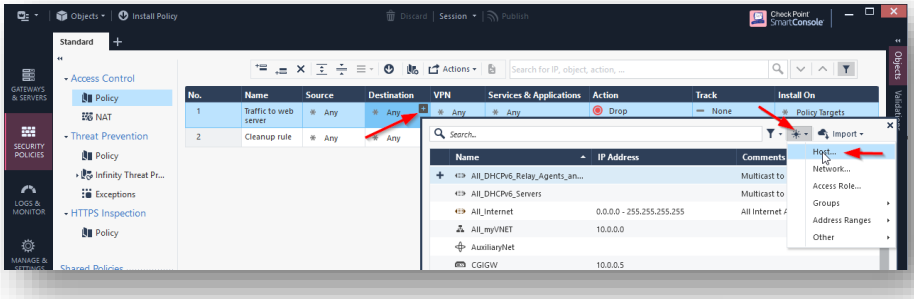


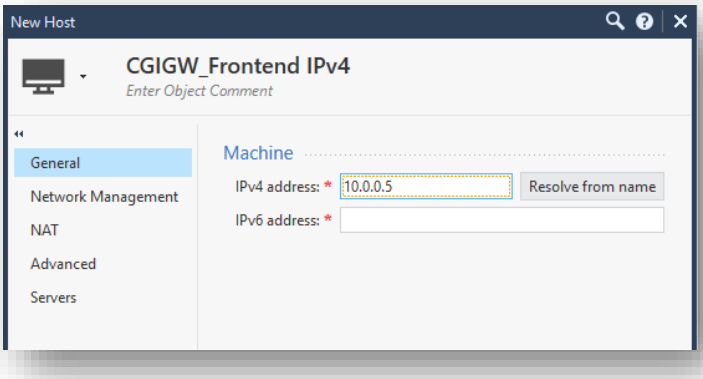
6. Click OK four times until all windows are closed, and you are back to the main view.
7. Navigate to the 'Security Policies' tab and click on 'Add rule above' icon.



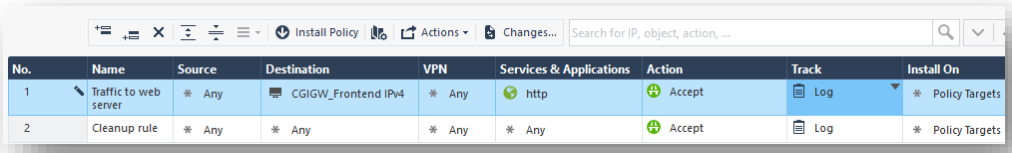
8. Add rule allowing HTTP traffic to the Web server from the internet:
   a. Name: Traffic to Web server
   b. Source: Any
   c. Destination: click on the + sign -> New -> Host.
      Name the object 'CGIGW_Frontend IPv4' and assign it IP 10.0.05, the private IP address of CGIGW in the Frontend network.

      Click OK to acknowledge the 'Multiple Object…' warning.

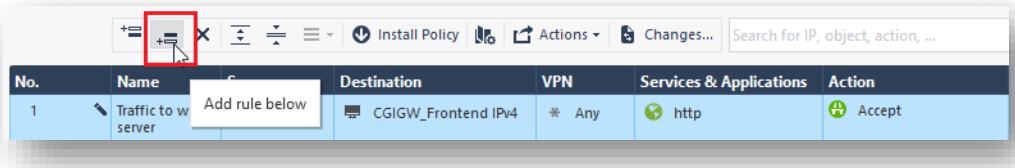




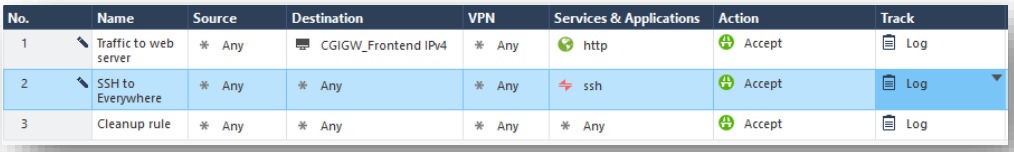
   d. Services & Applications: click on the + sign, search for HTTP, and click the + sign again.
   e. Action: change to Accept
   f. Track: change to Log



9. Mark the rule you have just created and click on the 'Add rule below' icon.



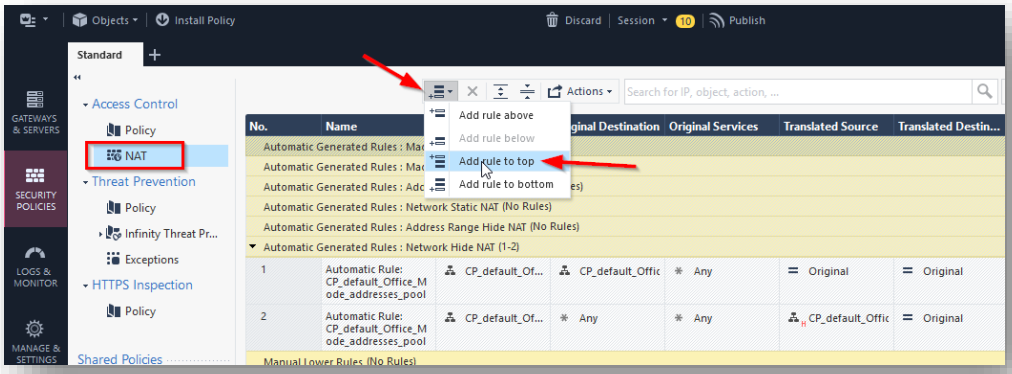
10. Create another rule for administration and troubleshooting of the lab.
    a. Name: SSH to Everywhere
    b. Source: Any
    c. Destination: Any
    d. Services & Applications: click on the + sign, search for ssh, and click the + sign again.
    e. Action: Accept
    f. Track: Log
11. Verify whether your ruleset looks like this:



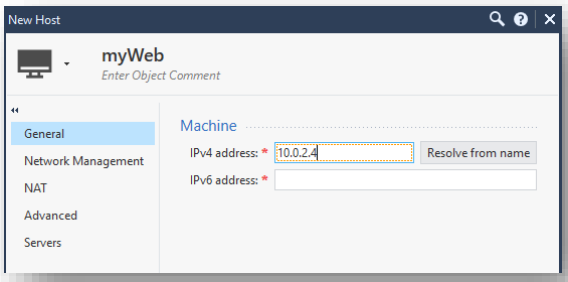
No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Traffic to web server	Any	CGIGW_Frontend IPv4	Any	http	Accept	Log
2	SSH to Everywhere	Any	Any	Any	ssh	Accept	Log
3	Cleanup rule	Any	Any	Any	Any	Accept	Log

Step 5. create a NAT policy to access the web server

1. Navigate to the NAT policy section, click on Add Rue -> Add rule to top.

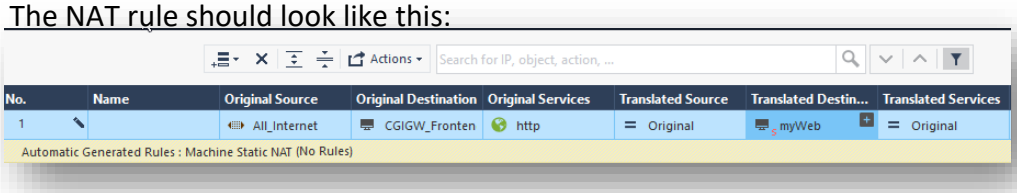


2. Create the following NAT rule to protect the connections to the web server.
    a. Original Source: All_Internet
    b. Original Destination: CGIGW_Frontend IPv4
    c. Original Service: HTTP
    d. Translated Source: Original
    e. Translated Destination: click on the + sign -> New -> Host.
    Create a host named 'myWeb' and IP 10.0.2.4, the private IP address of the 'web' virtual machine in the Azure portal.

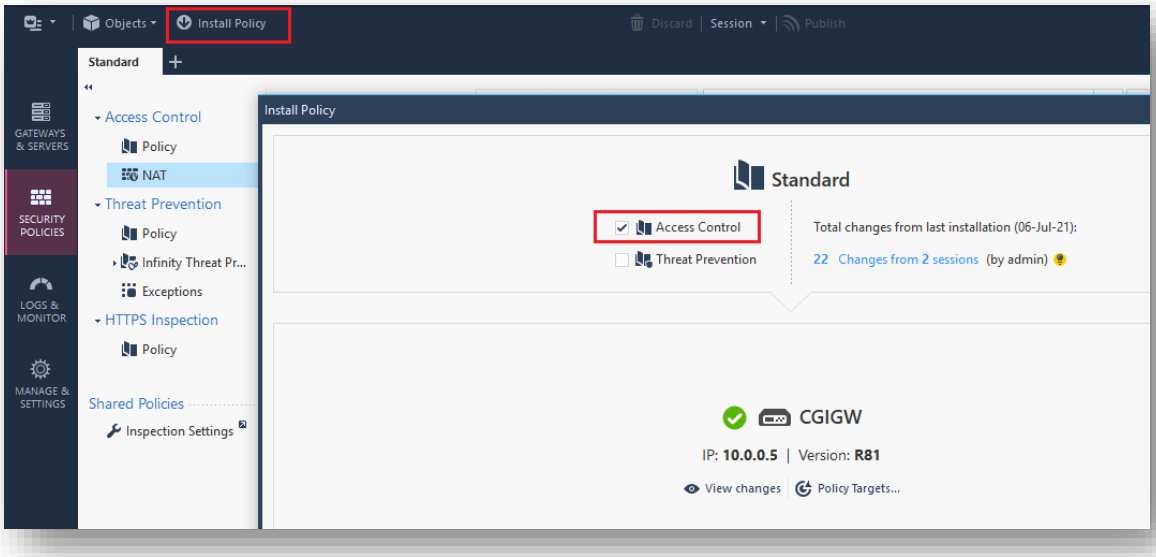


    f. Service: Original

The NAT rule should look like this:

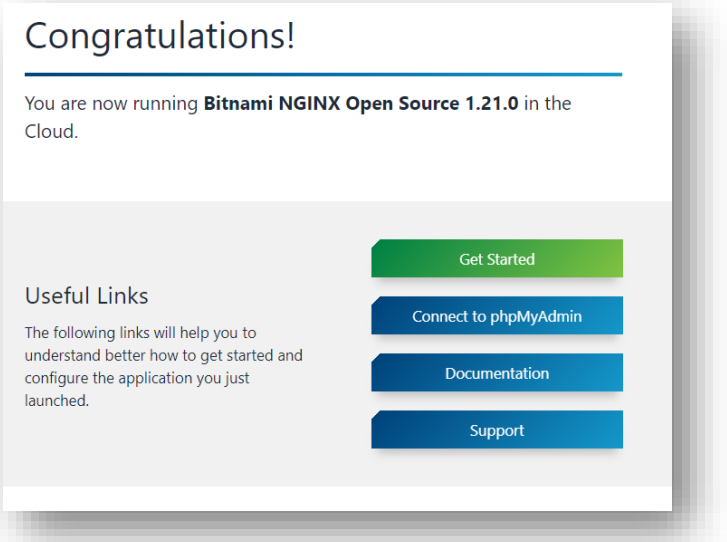


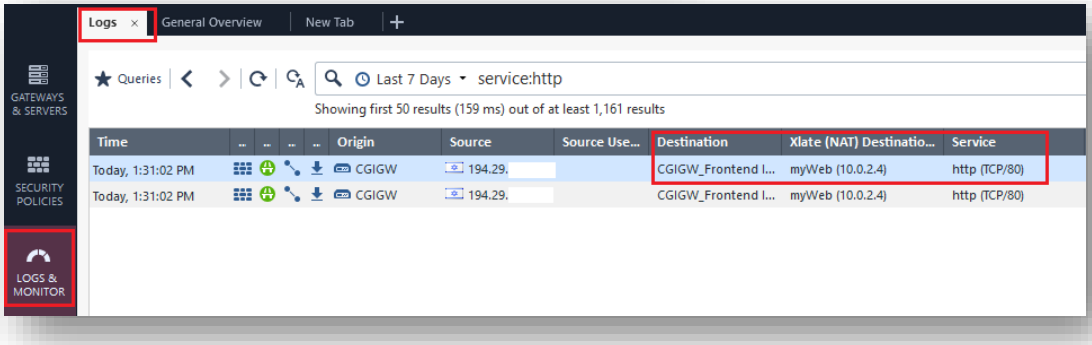
3. On the Install the access control policy on CloudGuard gateway



Step 6. test connectivity with the web server

1. Verify connectivity to the web server by browsing to the CloudGuard gateway public IP address web site below.





You have finished exercise 4.

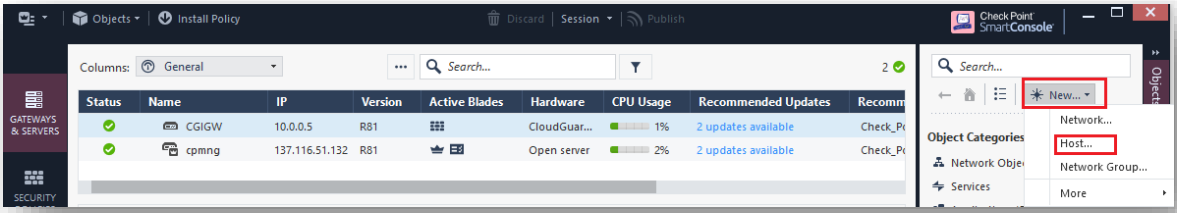
Exercise 5 - Configuring the CloudGuard Controller

Goal

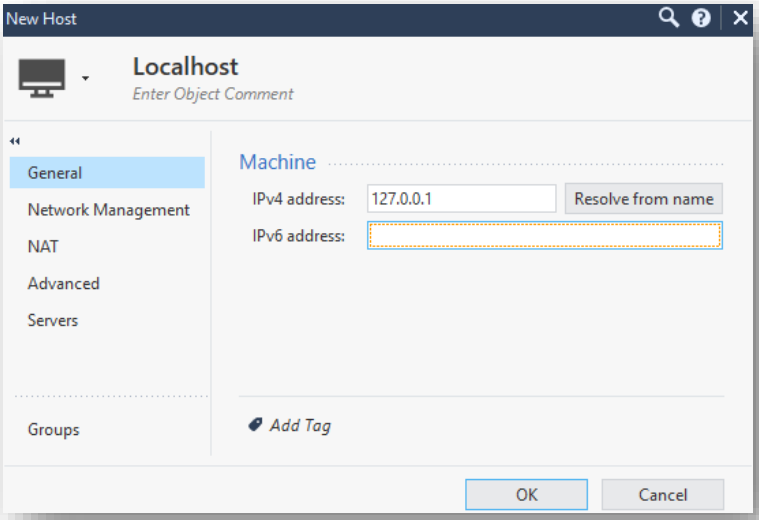
Configure Azure's service principal name (SPN) to allow Check Point security management to access Azure API

Step 1. Enable CloudGuard Controller on the management server

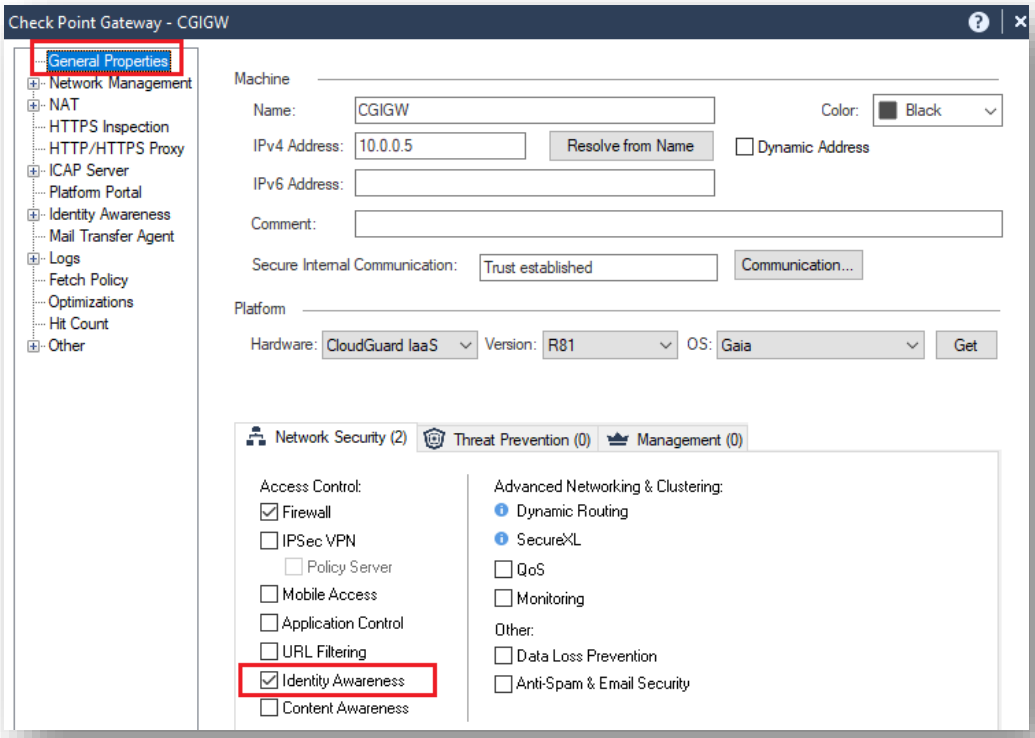
1. Open the installed SmartConsole and connect to the management server. Click the Objects pane on the right, click 'New' -> Host.



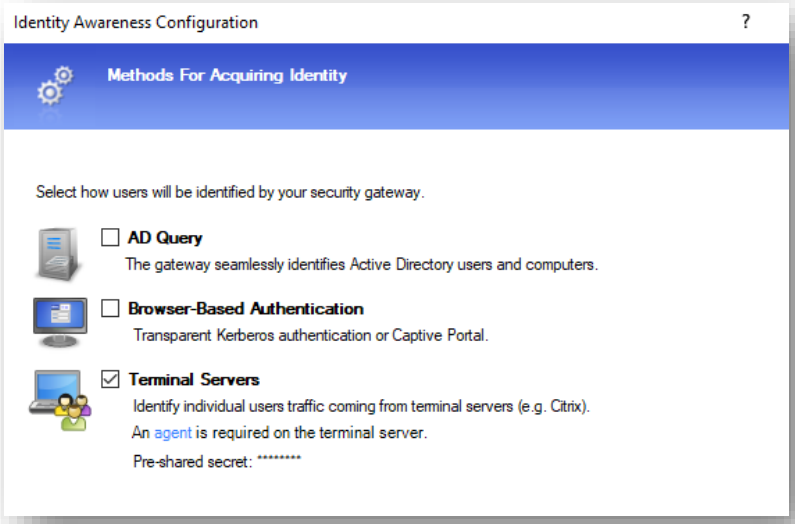
2. Create a host object with Name=Localhost and IPv4 address=127.0.0.1



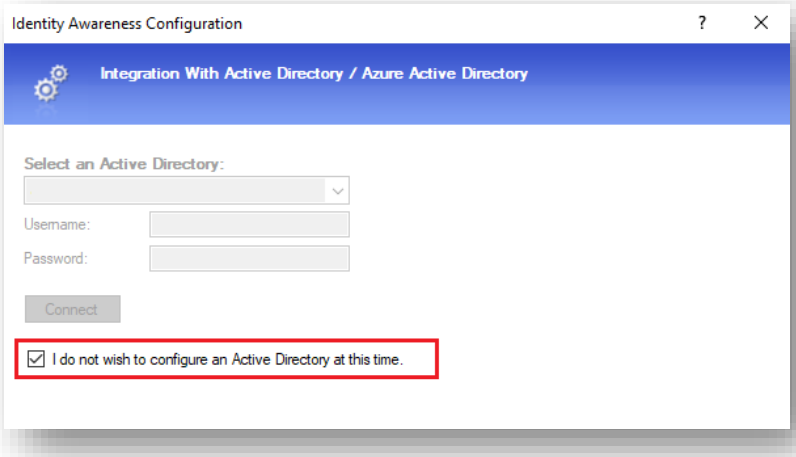
3. Doubleclick the CGIGW object -> General Properties -> Identity Awareness.

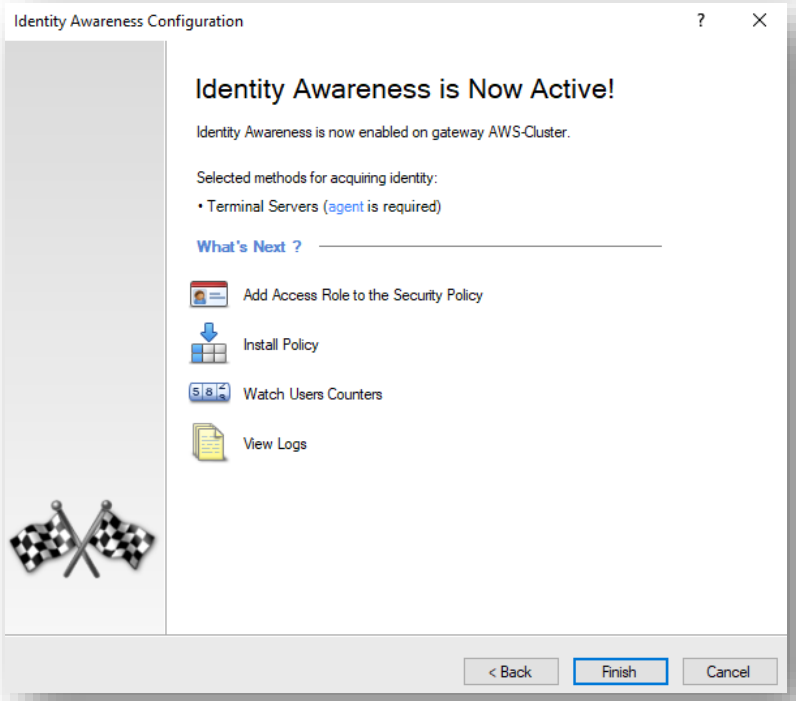


4. A window will open. Select the Terminal Servers and uncheck the AD Query. Click '**Next**'.

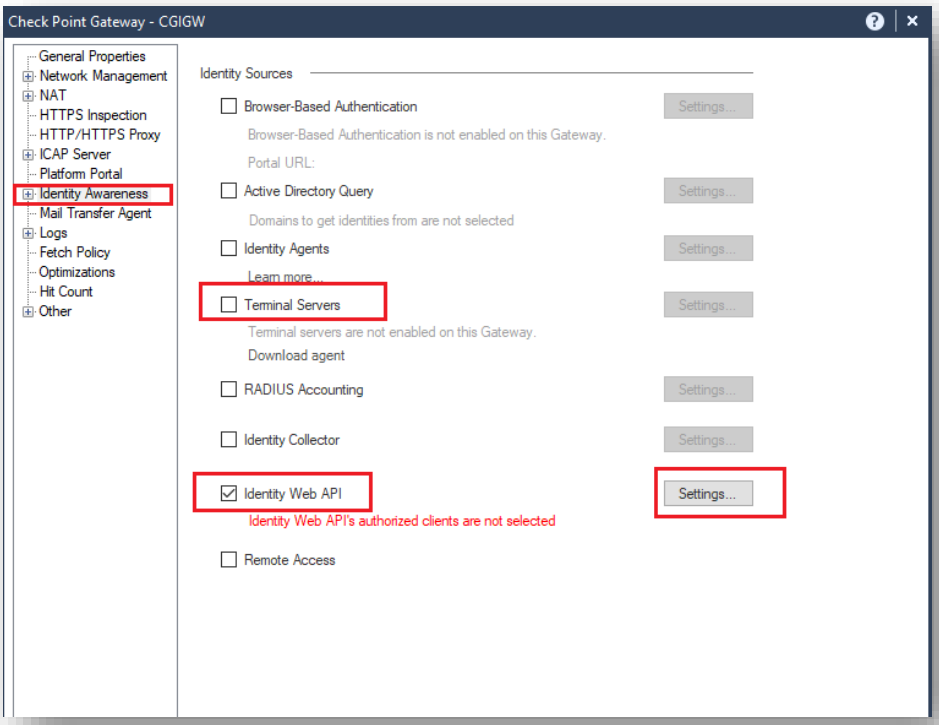


5. Select the option: "I don't want to configure Active Directory at this time" and click Next -> Finish -> OK.

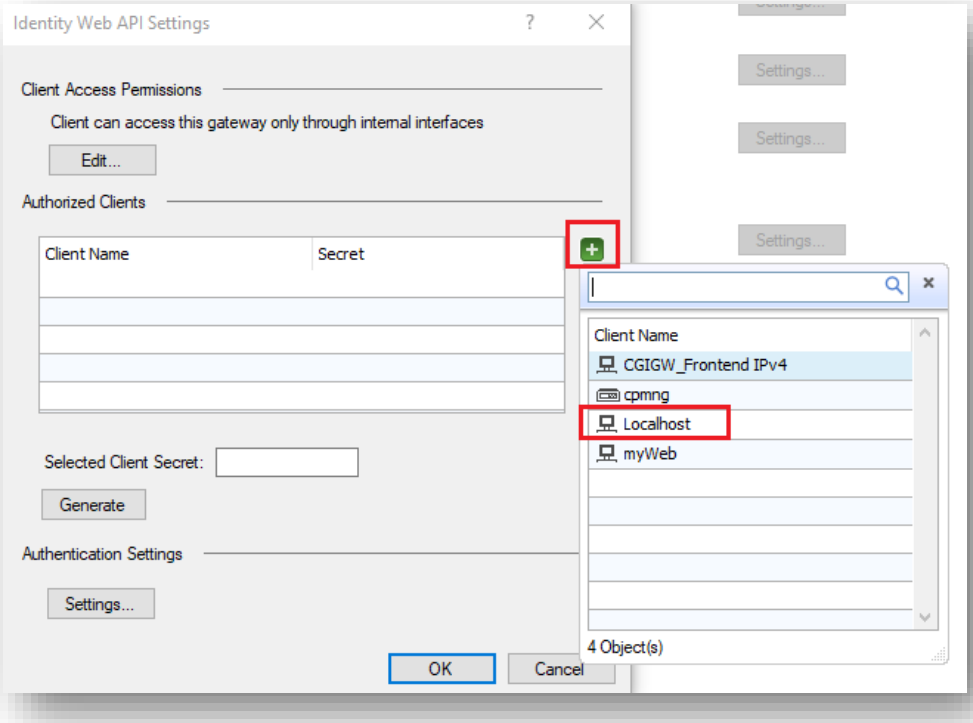


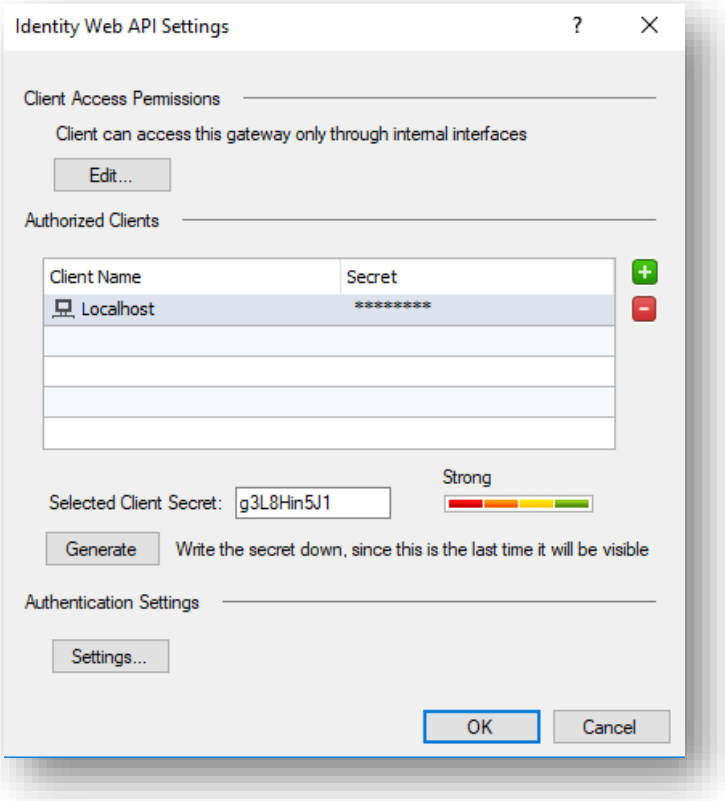


6. Change to the Identity Awareness section, uncheck the Terminal Servers, and check the 'Identity Web API'. Click Settings.

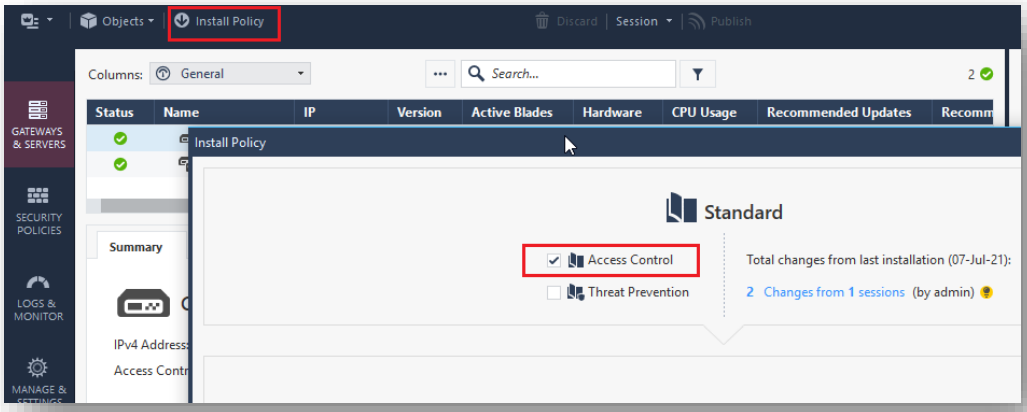


7. In the new window click the green + sign on the right. Click the green + sign on the right. Locate and choose a host called 'Localhost'.



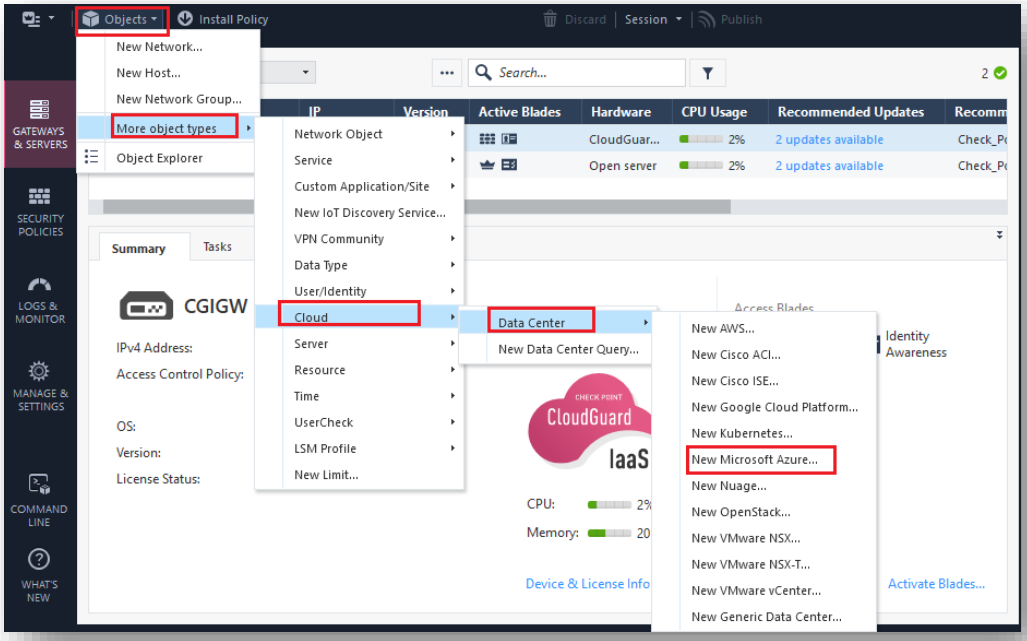


8. Click '**OK**' twice to close the CGICW object editing.
9. Click 'Yes' for the platform administration web portal warning.
10. Install access policy on the CGICW gateway.

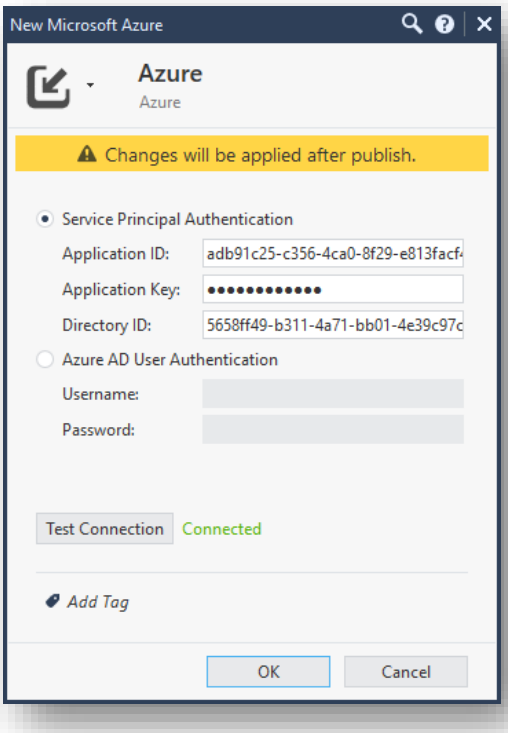


Step 2: Connect CloudGuard Controller to the Azure account

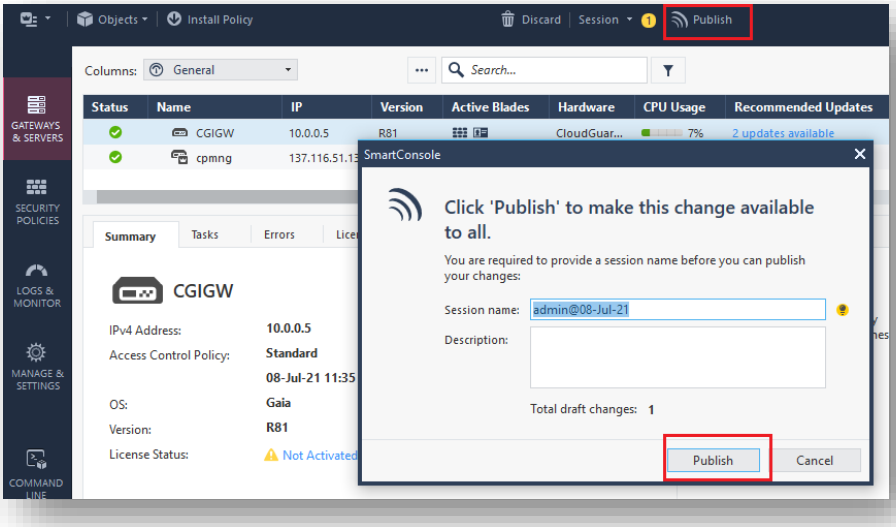
1. We will create a trusted connection between the CloudGuard Controller and the Azure account. Open SmartConsole, click on Objects -> More object types -> Cloud -> Data Center -> New AWS.



2. Name the Azure object and use the Application ID, Secret key (as for Application Key field) and Tenant ID (as for Directory ID field) you got in the registration email. Click on 'Test Connection' to see a Connected status.



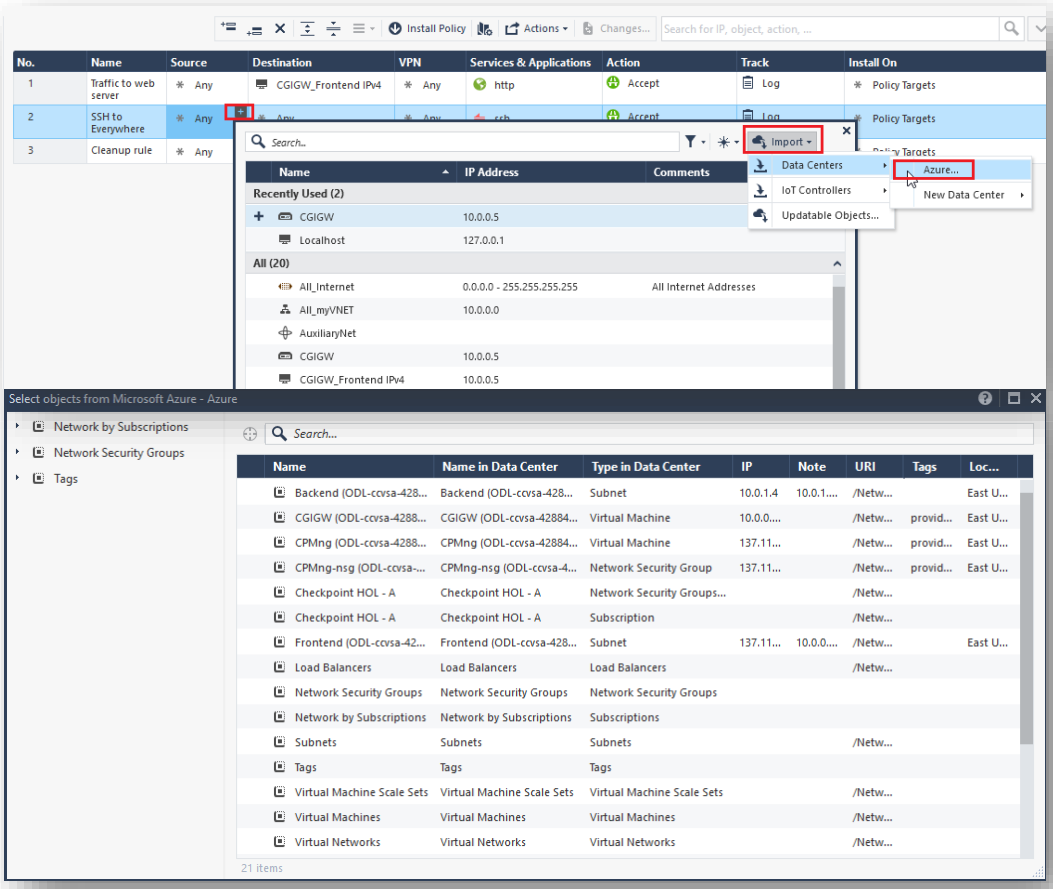
3. Publish the policy.



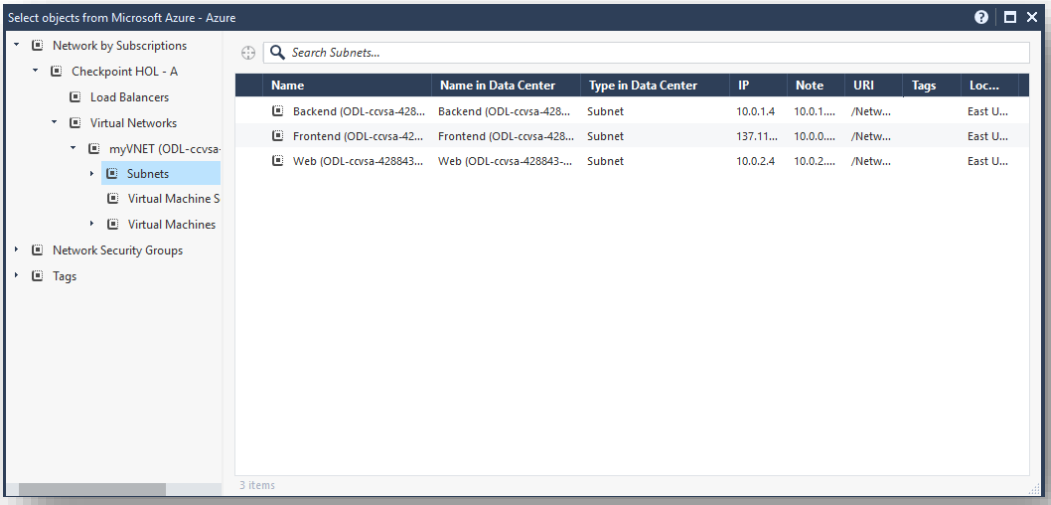
Step 3. Verify CloudGuard Controller integration with Security management

We will verify whether the security policy can include Azure objects following the integration of CloudGuard Controller and Azure.

a. Navigate to the SECURITY POLICIES tab and click the + sign in the security rule.
b. Click on Import -> Data Centers -> Azure. You'll get a list of Azure objects sorted by Subscriptions, Security Group, or Tags.



3. You can import objects from the Azure cloud in 3 ways:
   1. **Subscriptions view** to import Azure vNETs, Subnets, or virtual machines to your Security Policy
   2. **Security Groups view** to import all virtual machines from the same security group
   3. **Tags view Security** to import all virtual machines that have a specific Tag Key



You have finished exercise 5.

Exercise 6 - Advanced scenarios

Goal

Explore additional features in the Azure environment.

Test scenarios:

1. Initiate 'fw monitor' on the gateway and inspect traffic traversing the gateway. See sk30583 for more details.

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

3. Add another server on the Web subnet.

4. Verify whether traffic between two servers on the same subnet does not traverse through the firewall (there is no microsegmentation or East - West protection). It can be verified in logs or using the fw monitor on the gateway.

   a. Delete / add the route (No-microsegmentation-subnet-10.0.2.0) that prevents micro segmentation. The routing change in Azure can take ~2 minutes.

   b. Verify whether traffic between two servers on the subnets traverses through the firewall (there is microsegmentation or aka East - West protection). It can be verified in logs or using the fw monitor on the gateway.

You have finished exercise 6.

