Next Generation Data Center Security vSEC for AWS Training Lab guide

Ver. 4.0

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. This represents 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 AWS with its advanced threat prevention capabilities will allow you to deal with that security risk and minimize it.

This document will provide you with getting started steps required to get familiar with the AWS 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 AWS 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 AWS IaaS infrastructure Hands-on lab Objectives:

The target of this hands-on lab exercises is to provide you with practical real-life experience with the Check Point's vSEC For AWS 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 AWS console and concepts.

2. Deploy Check Point R80 management server on AWS
   The exercise will show you how to deploy R80 Management server in your newly created environment on AWS. You will also learn how to launch new web servers from the marketplace.

3. Deploy Check Point vSEC cluster on AWS
   This exercise will demo to you how to deploy a vSEC cluster into your AWS 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 vSEC controller to connect into your account in AWS.

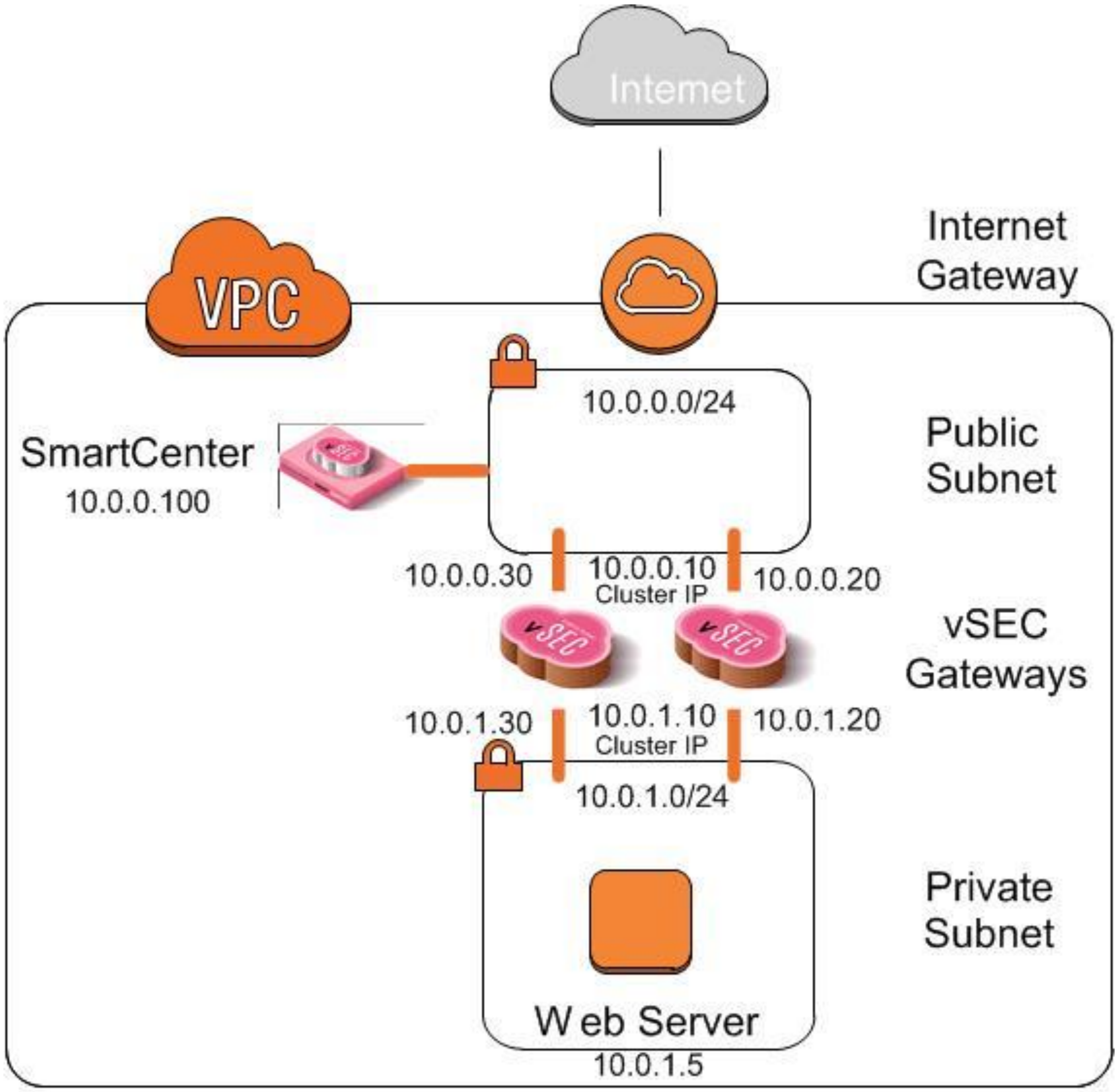
5. Optional Advanced troubleshooting
   This optional exercise will teach you how to do basic debugging and validate that your cluster is running as designed.

- **Note:** In this lab guide, there are two steps that are missing. This is to aid the training process.

Good Luck

vSEC for AWS training environment:

Getting to know your training environment



	IP address
vSEC MemberA – External	10.0.0.20/24
vSEC MemberA - Internal	10.0.1.20/24
vSEC MemberB – External	10.0.0.30/24
vSEC MemberB - Internal	10.0.1.30/24
Management Server	10.0.0.100/24
Web Server	10.0.1.5

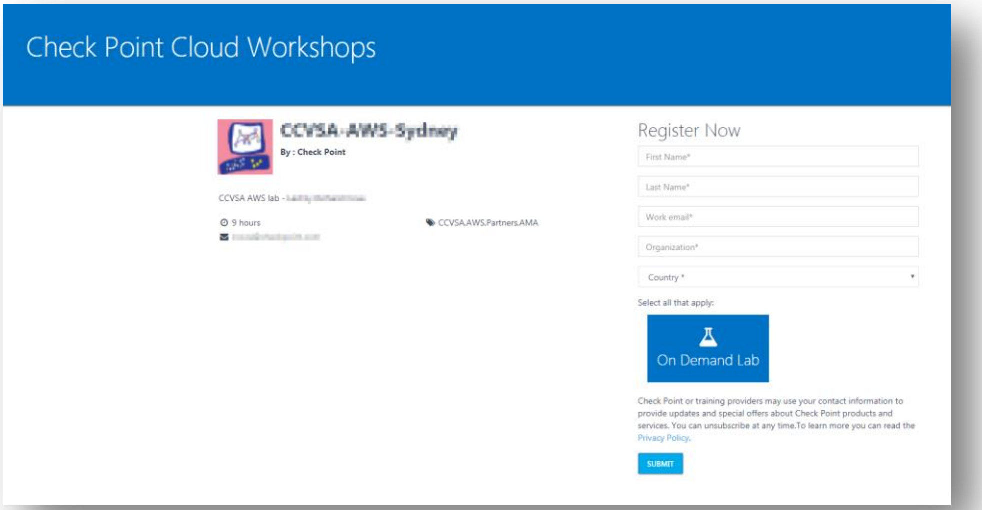
Connecting and setting up you work environment:

Purpose: To get familiar with the console and its options

Register and sign-in to AWS

1. Browse to the link that your trainer has provided for you

2. Fill in your details for registration and click “Submit”



Check Point Cloud Workshops

CCVSA-AWS-Sydney

By : Check Point

CCVSA AWS lab - [redacted]

9 hours

[redacted]

CCVSA.AWS.Partners.AMA

Register Now

First Name*

Last Name*

Work email*

Organization*

Country *

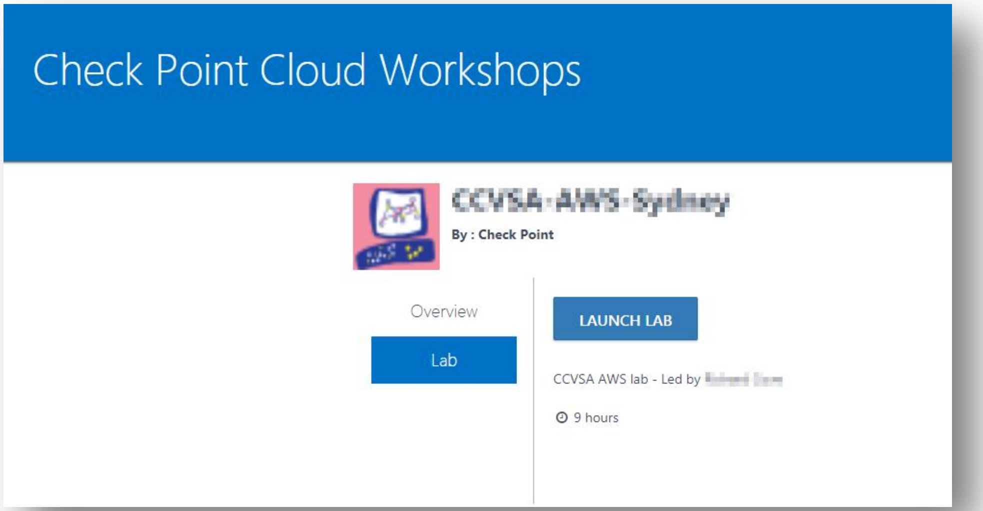
Select all that apply:

On Demand Lab

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

SUBMIT

3. On the next screen, Click on “Launch Lab”



Check Point Cloud Workshops

CCVSA-AWS-Sydney

By : Check Point

Overview

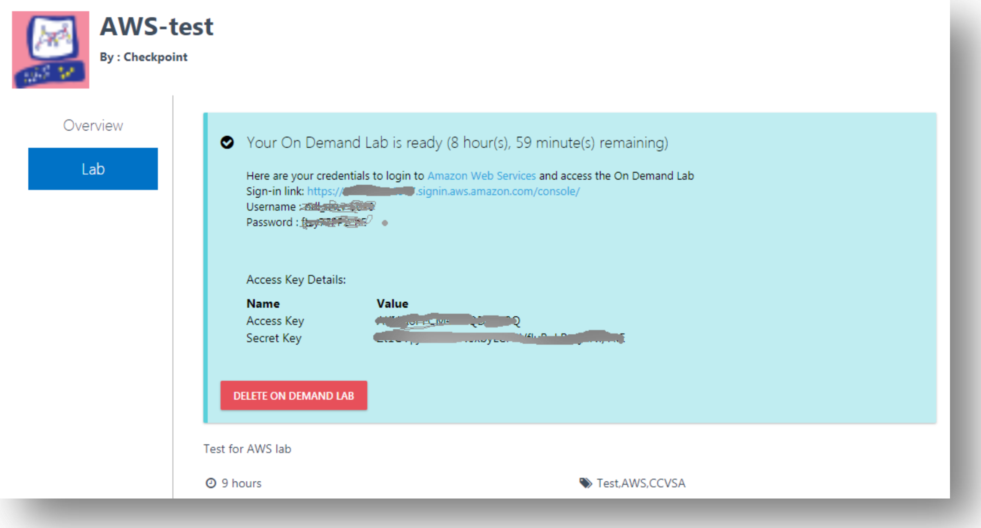
Lab

LAUNCH LAB

CCVSA AWS lab - Led by [redacted]

9 hours

4. You're On Demand Lab session has started and the session is active for several hours (as described on the page). The browser window will show your credentials for this session and the sign-in link (you will also get an email with this information).



Your On Demand Lab is ready (8 hour(s), 59 minute(s) remaining)

Here are your credentials to login to Amazon Web Services and access the On Demand Lab
Sign-in link: https://[redacted].signin.aws.amazon.com/console/
Username : [redacted]
Password : [redacted]

Access Key Details:

Name	Value
Access Key	[redacted]
Secret Key	[redacted]

Test for AWS lab

9 hours

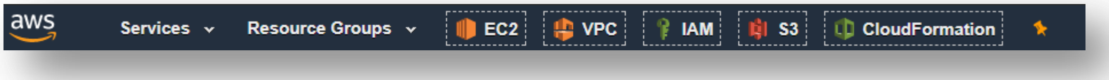
Test,AWS,CCVSA

5. Browse to the Amazon AWS portal using the provided sign-in link and use the credentials you were provided

Get familiar with AWS console

1. Add one click navigation shortcuts to the top bar by clicking on the Drawing Pin at the top of the page

2. From the dropdown window that shows up, drag the following services to the top bar (as shown in the screenshot below):
    - EC2
    - VPC
    - IAM
    - S3
    - CloudFormation



Naturally, you can add any desired service from the drop down window and also set its location on the bar at your convenience.
When you are done, just click the Drawing Pin to finish editing mode

3. Take a few minutes to review Amazon's different services (understanding the full breadth of the service offering)

4. Feel free to wander around those services (by clicking on them and reviewing their "landing page")

5. When you're done, go back to the portal home page by clicking on the home image on the left top corner of the screen

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

Exercise #1 – Build your own AWS environment

Purpose: To create the basic environment (VPC and subnets)

Description

This exercise will guide you through the steps required to setup your own private AWS environment in which we will be deploying our instances.

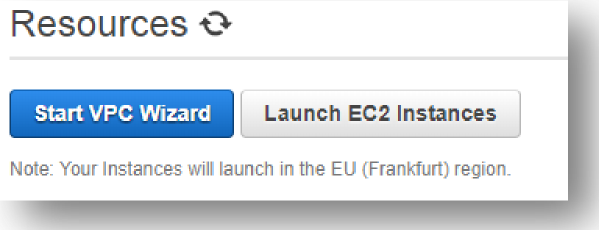
Method

Using AWS console you will create a new VPC (Virtual Private Cloud) in a designated region. You will then create subnets and locate them in a certain AZ (availability Zone). This newly created environment will be used in later exercise as new instances will be provisioned into this environment.

Create VPC

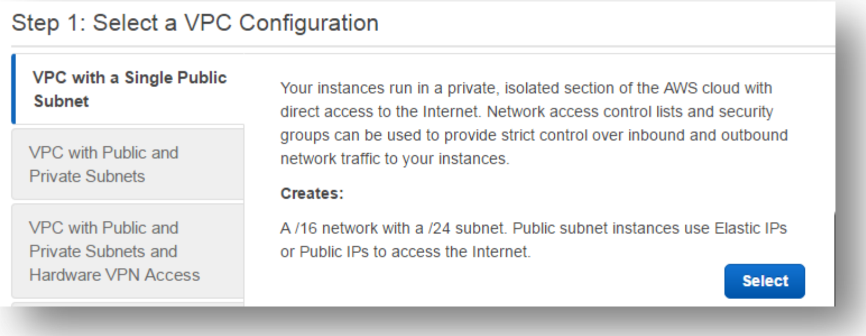
1. In the top navigation bar in the AWS console, on the top-right, take note of the region in which you'll be creating the VPC (choose a region like Frankfurt or Ohio). Ensure that you continue working in the same region for the rest of the exercises, as you cannot launch an instance into your VPC from a different region.

2. In the top navigation bar, click "VPC" dashboard, and then click "Start VPC Wizard".



Note: Your Instances will launch in the EU (Frankfurt) region.

3. Choose the first option, VPC with a Single Frontend Subnet, and then click Select.



Step 1: Select a VPC Configuration

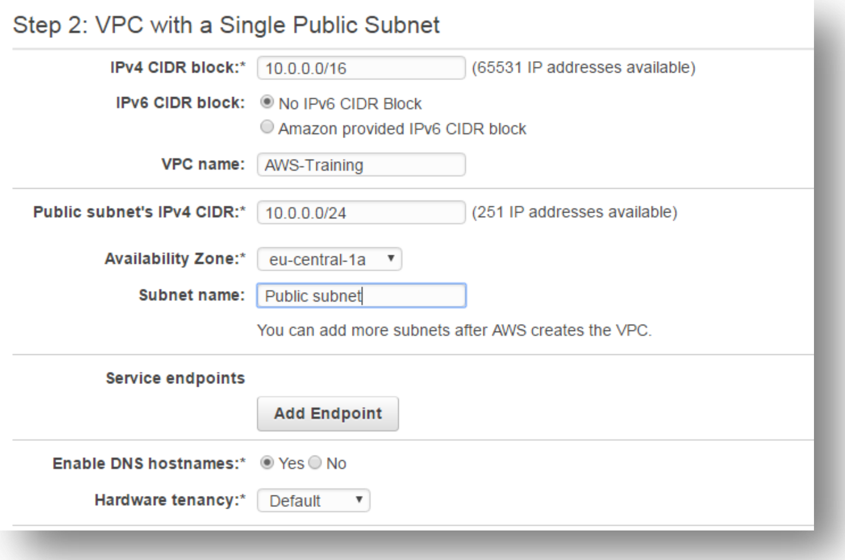
VPC with a Single Public Subnet
VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware VPN Access
Select

Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.

Creates:

A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.

4. On the configuration page, enter a name for your VPC in the VPC name field (ie. AWS-Training), and enter a name for your subnet in the Subnet name field (ie. Public subnet). This helps you to identify the VPC and subnet in the AWS VPC console after you've created them. Fill in the info as described:



Step 2: VPC with a Single Public Subnet

IPv4 CIDR block:* 10.0.0.0/16 (65531 IP addresses available)

IPv6 CIDR block: ● No IPv6 CIDR Block ○ Amazon provided IPv6 CIDR block

VPC name: AWS-Training

Public subnet's IPv4 CIDR:* 10.0.0.0/24 (251 IP addresses available)

Availability Zone:* eu-central-1a

Subnet name: Public subnet

You can add more subnets after AWS creates the VPC.

Service endpoints

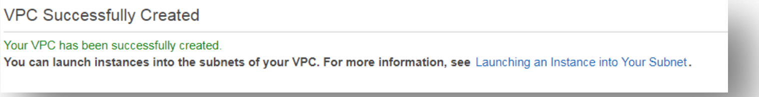
Enable DNS hostnames:* ● Yes ○ No

Hardware tenancy:* Default

- The IP CIDR block displays the IP address range that you'll use for your VPC (10.0.0.0/16), and the Public subnet’s IPv4 CIDR field displays the IP address range you'll use for the subnet (10.0.0.0/24). If you don't want to use the default CIDR ranges, you can specify your own.
- The Availability Zone list enables you to select the Availability Zone in which to create the subnet. Choose the one that ends with “1a” for you region.
- The “Enable DNS hostnames option”, when set to Yes, ensures that instances that are launched into your VPC automatically receive a DNS hostname.
- The Hardware tenancy option enables you to select whether instances launched into your VPC are run on shared or dedicated hardware. Selecting a dedicated tenancy incurs additional costs.

5. Click “Create VPC” to start creating the VPC with single subnet.

6. A status window shows the work in progress. When the work completes you will see the following message:



VPC Successfully Created

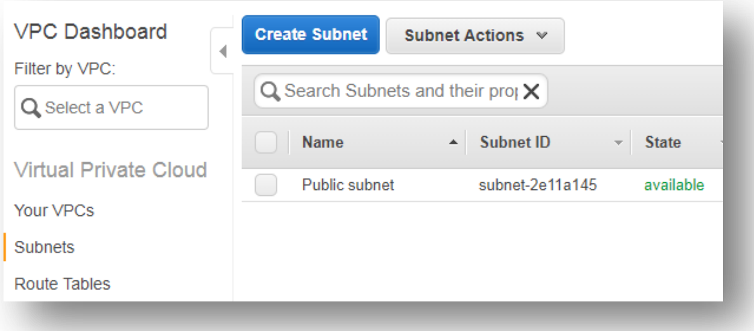
Your VPC has been successfully created.

You can launch instances into the subnets of your VPC. For more information, see Launching an Instance into Your Subnet.

7. We’ve created a VPC with 1 public subnet; now let’s add another (Private) subnet to our environment.

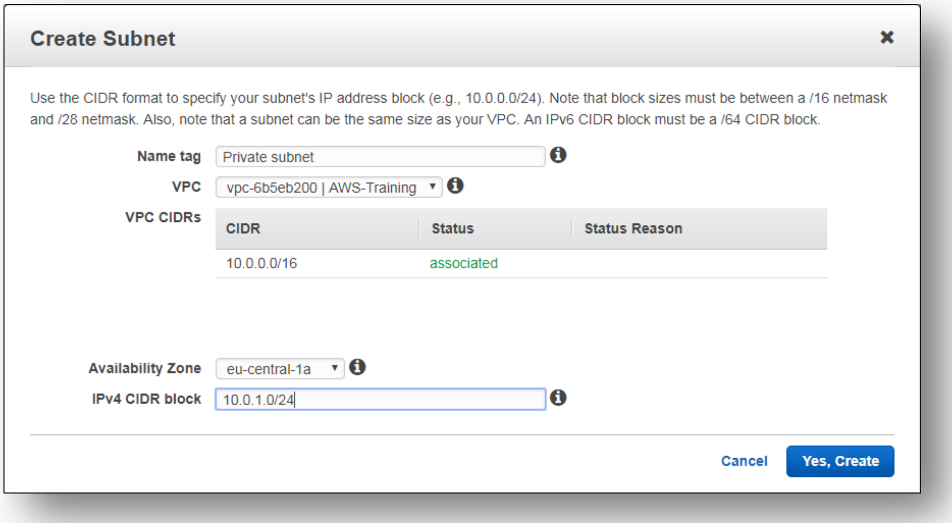
Create subnet

1. On the left side menu click “Subnets” and then click on “Create Subnet”.



Name	Subnet ID	State
Public subnet	subnet-2e11a145	available

2. In the window that appears;



Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag: Private subnet

VPC: vpc-6b5eb200 | AWS-Training

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

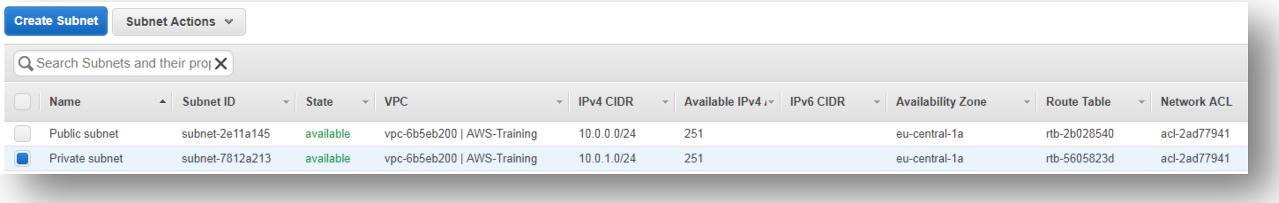
Availability Zone: eu-central-1a

IPv4 CIDR block: 10.0.1.0/24

Fill in the fields:

Name tag: Private subnet
VPC: AWS-Training
Availability Zone: the same as step 4 (the one that ends with “1a”)
IPv4 CIDR block: 10.0.1.0/24

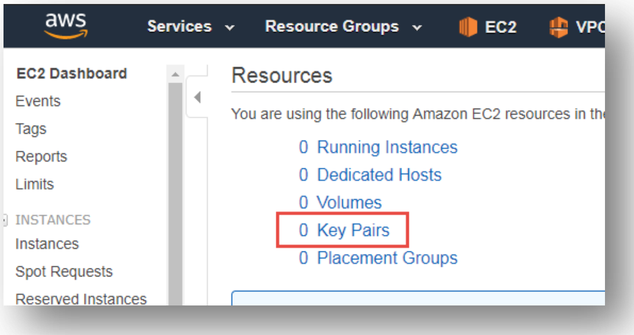
3. Click “Yes, Create”
The following screen should appear:



	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4 A	IPv6 CIDR	Availability Zone	Route Table	Network ACL
□	Public subnet	subnet-2e11a145	available	vpc-6b5eb200 | AWS-Training	10.0.0.0/24	251		eu-central-1a	rtb-2b028540	acl-2ad77941
☑	Private subnet	subnet-7812a213	available	vpc-6b5eb200 | AWS-Training	10.0.1.0/24	251		eu-central-1a	rtb-5605823d	acl-2ad77941

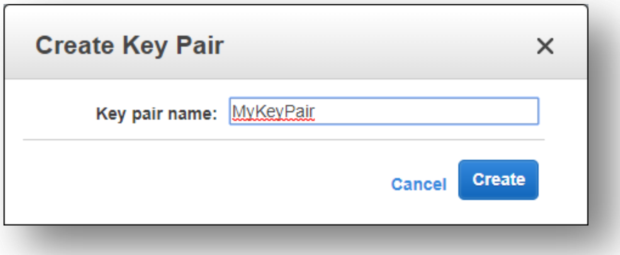
Create AWS Key Pair

1. When you will deploy the instances later you need a Key Pair that are used for authentication to the instances. In the top navigation bar, click “EC2” dashboard, and then click “Key Pairs”.



2. Click “Create Key Pair”

3. Choose a name (ie. MyKeyPair) and click “Create”



Key pair name: MyKeyPair

4. You are prompted to save the private key (pem file). Please save it somewhere convenient

   Top tip: To be able to use the private key with Putty, the pem file must be converted
   For help see here http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html

You successfully finished Exercise #1

Exercise #2 - Deploy Check Point R80.10 Management server

Purpose: To deploy the Check Point management server using a CloudFormation template

Description

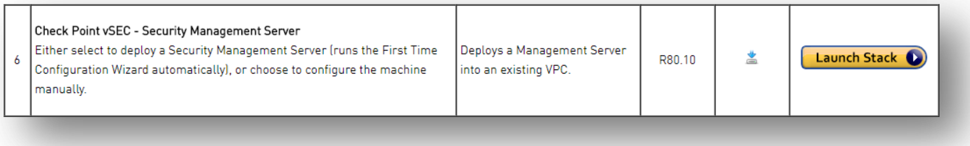
This exercise will guide you through the deployment of a Check Point R80.10 security management server in AWS.

Method

Using AWS portal you will provision a Check Point R80.10 virtual appliance on your AWS public cloud environment

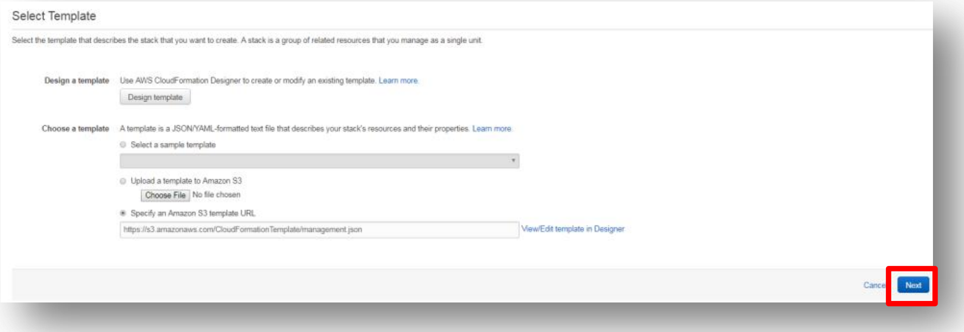
Provision the R80.10 Management server instance using CloudFormation template

1. Open SK111013 in your browser
2. Review the available CloudFormation templates
3. Click the “Launch Stack” button of the “Check Point vSEC - Security Management Server” on the right side of the page



6	Check Point vSEC - Security Management Server Either select to deploy a Security Management Server (runs the First Time Configuration Wizard automatically), or choose to configure the machine manually.	Deploys a Management Server into an existing VPC.	R80.10	⬇	Launch Stack

4. This will open the AWS console into the CloudFormation -> Stacks -> Create Stack window
5. The Check Point CloudFormation template for deploying a R80.10 Security Management Server is automatically chosen
   Click “Next”



Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template: Use AWS CloudFormation Designer to create or modify an existing template. Learn more.

Choose a template: A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.

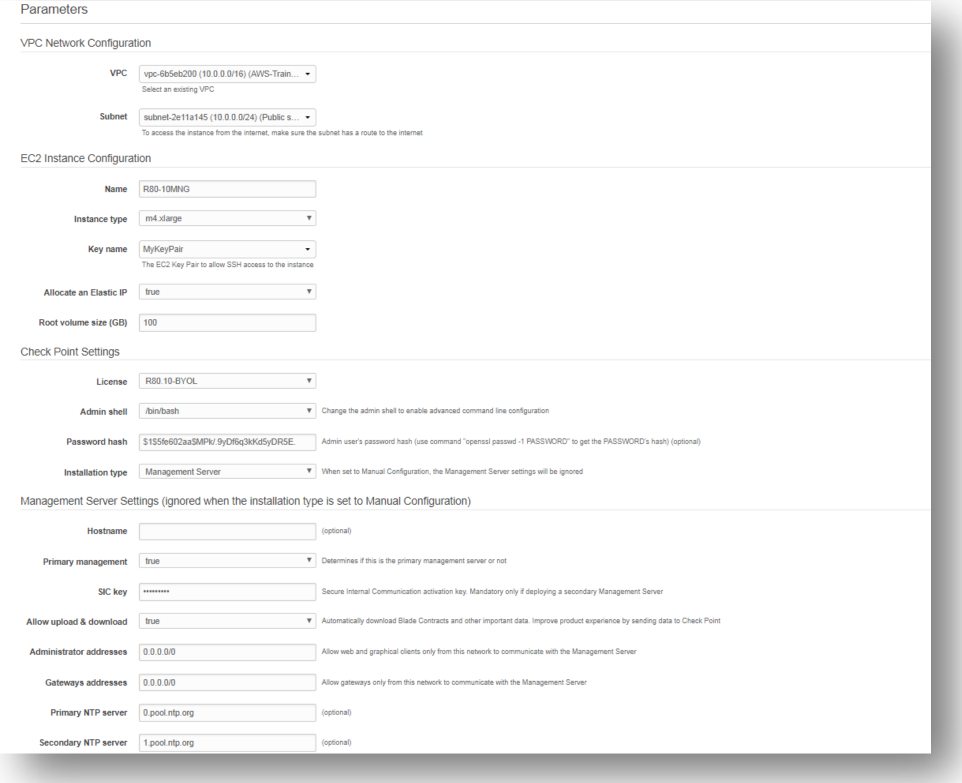
○ Select a sample template

○ Upload a template to Amazon S3

● Specify an Amazon S3 template URL

https://s3.amazonaws.com/CloudFormationTemplate/management.json

6. The next screen includes the information needed for deploying the R80.10 management server automatically
   Fill in the different fields as listed below:



Parameters

VPC Network Configuration

VPC: vpc-6b5eb200 (10.0.0.0/16) (AWS-Train…
Select an existing VPC

Subnet: subnet-2e11a145 (10.0.0.0/24) (Public s…
To access the instance from the internet, make sure the subnet has a route to the internet

EC2 Instance Configuration

Name: R80-10MNG

Instance type: m4.xlarge

Key name: MyKeyPair
The EC2 Key Pair to allow SSH access to the instance

Allocate an Elastic IP: true

Root volume size (GB): 100

Check Point Settings

License: R80.10-BYOL

Admin shell: /bin/bash — Change the admin shell to enable advanced command line configuration

Password hash: $1$5fe602aa$MPk/.9yDf6q3kKd5yDR5E. — Admin user's password hash (use command "openssl passwd -1 PASSWORD" to get the PASSWORD's hash) (optional)

Installation type: Management Server — When set to Manual Configuration, the Management Server settings will be ignored

Management Server Settings (ignored when the installation type is set to Manual Configuration)

Hostname: (optional)

Primary management: true — Determines if this is the primary management server or not

SIC key: ••••••••• — Secure Internal Communication activation key. Mandatory only if deploying a secondary Management Server

Allow upload & download: true — Automatically download Blade Contracts and other important data. Improve product experience by sending data to Check Point

Administrator addresses: 0.0.0.0/0 — Allow web and graphical clients only from this network to communicate with the Management Server

Gateways addresses: 0.0.0.0/0 — Allow gateways only from this network to communicate with the Management Server

Primary NTP server: 0.pool.ntp.org (optional)

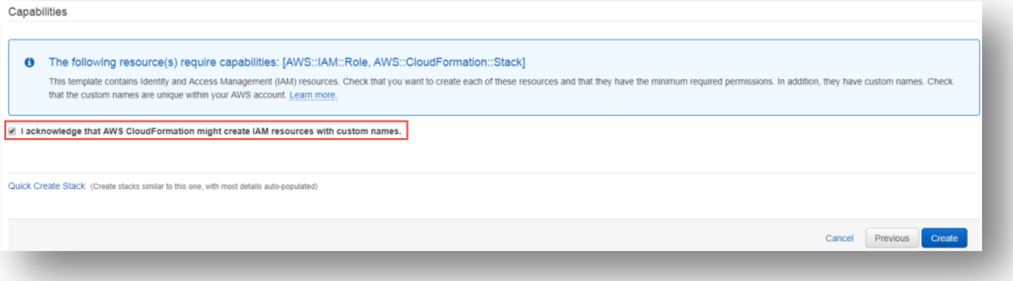
Secondary NTP server: 1.pool.ntp.org (optional)

Stack name: can be left as the default
VPC: AWS-Training
Subnet: Public subnet
Name: R80-10MNG
Instance Type: m4.xlarge
Key name: choose your own keys (which you can created in exercise #1)
License: R80.10-BYOL
Admin shell: /bin/bash/
Password hash: you can create the hash in this link: https://quickhash.com/ (must use MD5-Crypt3 algorithm)
Installation Type: Management Server
Primary management: true
Administrator addresses: 0.0.0.0/0
Gateway addresses: 0.0.0.0/0

Keep other settings as default and click "Next"

7. On the next screen, click "Next"

8. Review your defined configuration, acknowledge the remark and click "Create"



Capabilities

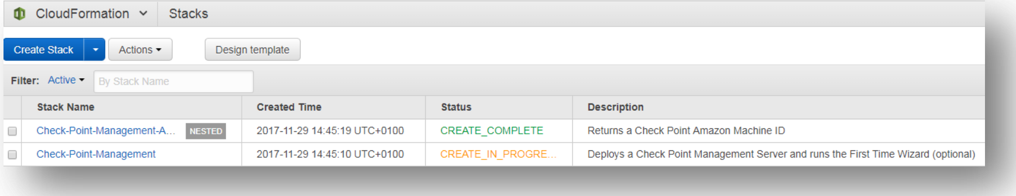
The following resource(s) require capabilities: [AWS::IAM::Role, AWS::CloudFormation::Stack]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more.

☑ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Quick Create Stack (Create stacks similar to this one, with most details auto-populated)

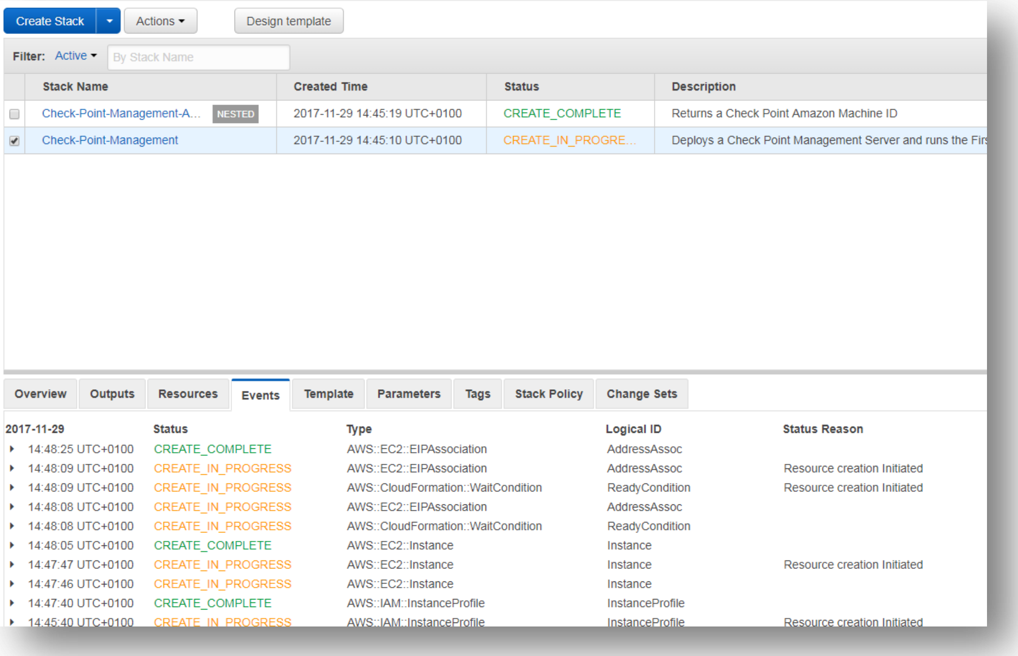
9. In the top navigation bar, click “CloudFormation” dashboard



Filter: Active By Stack Name

	Stack Name	Created Time	Status	Description
□	Check-Point-Management-A... NESTED	2017-11-29 14:45:19 UTC+0100	CREATE_COMPLETE	Returns a Check Point Amazon Machine ID
□	Check-Point-Management	2017-11-29 14:45:10 UTC+0100	CREATE_IN_PROGRE...	Deploys a Check Point Management Server and runs the First Time Wizard (optional)

10. If you mark the Check-Point-Management and click the Events tab you will be able to monitor the progress

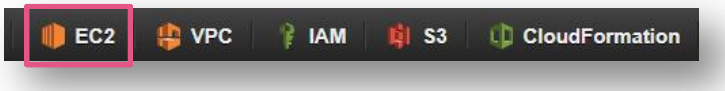


Filter: Active By Stack Name

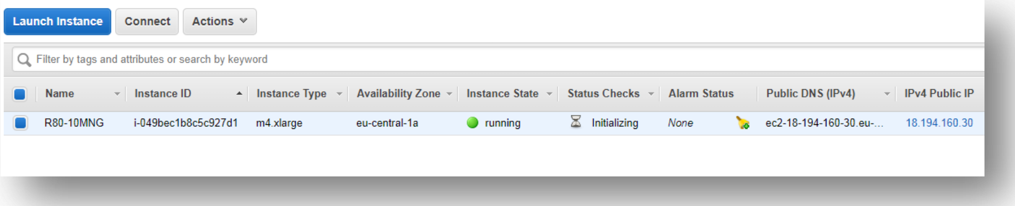
	Stack Name	Created Time	Status	Description
□	Check-Point-Management-A... NESTED	2017-11-29 14:45:19 UTC+0100	CREATE_COMPLETE	Returns a Check Point Amazon Machine ID
☑	Check-Point-Management	2017-11-29 14:45:10 UTC+0100	CREATE_IN_PROGRE...	Deploys a Check Point Management Server and runs the Firs

2017-11-29	Status	Type	Logical ID	Status Reason
14:48:25 UTC+0100	CREATE_COMPLETE	AWS::EC2::EIPAssociation	AddressAssoc	
14:48:09 UTC+0100	CREATE_IN_PROGRESS	AWS::EC2::EIPAssociation	AddressAssoc	Resource creation Initiated
14:48:09 UTC+0100	CREATE_IN_PROGRESS	AWS::CloudFormation::WaitCondition	ReadyCondition	Resource creation Initiated
14:48:08 UTC+0100	CREATE_IN_PROGRESS	AWS::EC2::EIPAssociation	AddressAssoc	
14:48:08 UTC+0100	CREATE_IN_PROGRESS	AWS::CloudFormation::WaitCondition	ReadyCondition	
14:48:05 UTC+0100	CREATE_COMPLETE	AWS::EC2::Instance	Instance	
14:47:47 UTC+0100	CREATE_IN_PROGRESS	AWS::EC2::Instance	Instance	Resource creation Initiated
14:47:46 UTC+0100	CREATE_IN_PROGRESS	AWS::EC2::Instance	Instance	
14:47:40 UTC+0100	CREATE_COMPLETE	AWS::IAM::InstanceProfile	InstanceProfile	
14:45:40 UTC+0100	CREATE_IN_PROGRESS	AWS::IAM::InstanceProfile	InstanceProfile	Resource creation Initiated

11. In the top navigation bar, click “EC2” dashboard



Click on “Instances” on the left pane and the below window will appear.

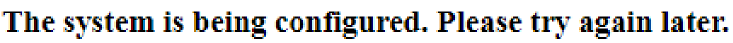


Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP
R80-10MNG	i-049bec1b8c5c927d1	m4.xlarge	eu-central-1a	running	Initializing	None	ec2-18-194-160-30.eu-...	18.194.160.30

Once the Instance State shows “Running” and Status Checks says “2/2 checks passed”, it’s up, but the Check Point First Time Wizard might still be running.
Please note –The total deployment might take ~30 min as it is installing and configuring our management server for the first time.

Do Not Try to connect to the machine with SmartConsole before the it has finished the deployment

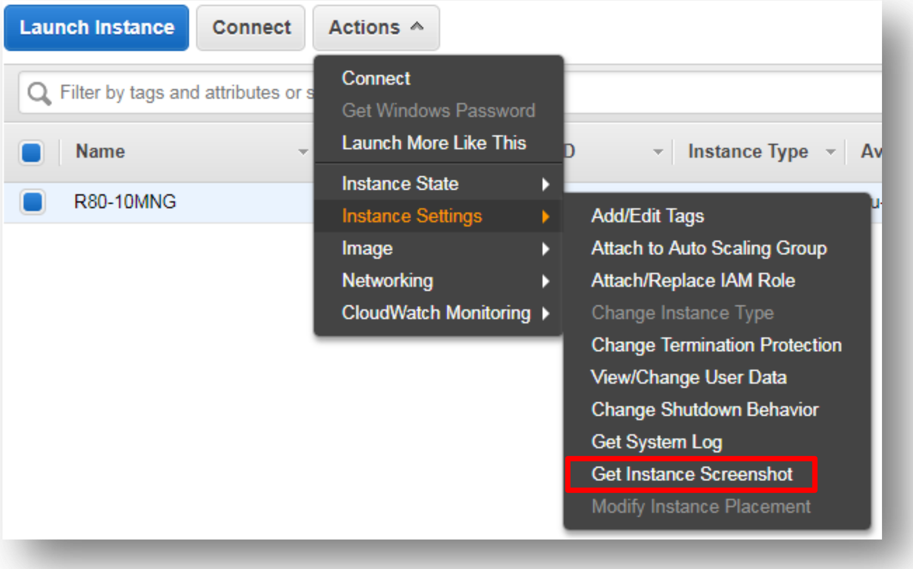
If you see the following message when connecting to the WebUI of the Management server, then the First Time Wizard is still running.



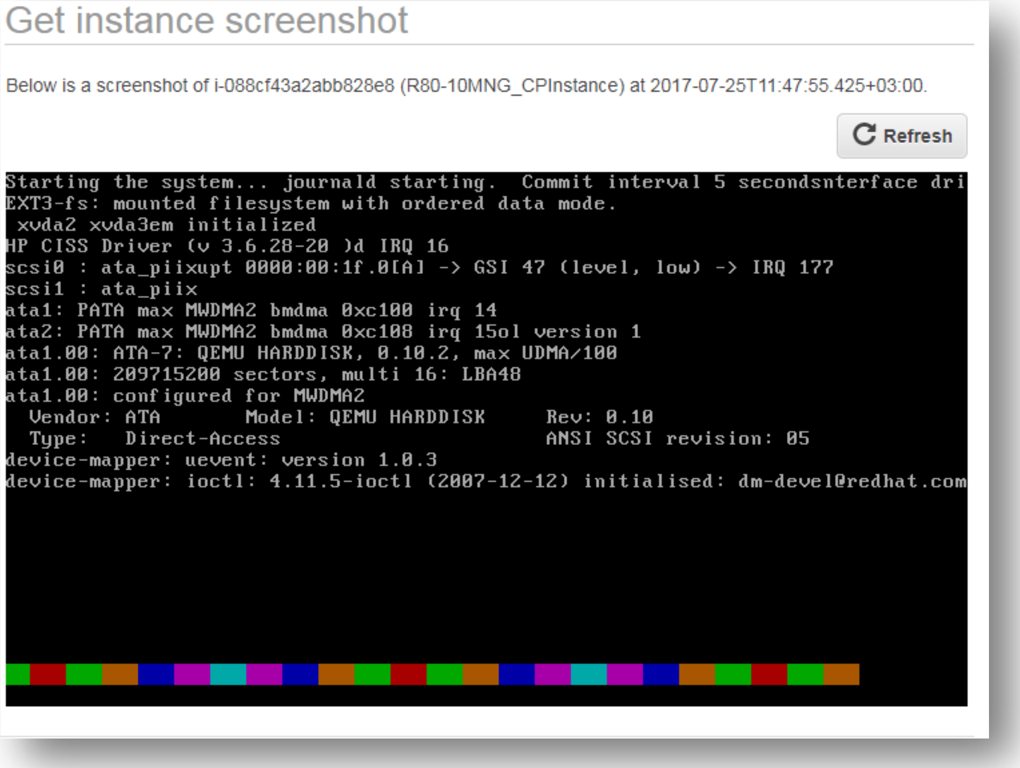
The system is being configured. Please try again later.

Notice that you can also see the public IP assigned to the Management server.

12. From the EC2 dashboard we can look at the instance screenshot.
    Click on “Action -> Instance Settings -> Get Instance Screenshot”



13. You can see the following screen that shows that the system is still not finished



Get instance screenshot

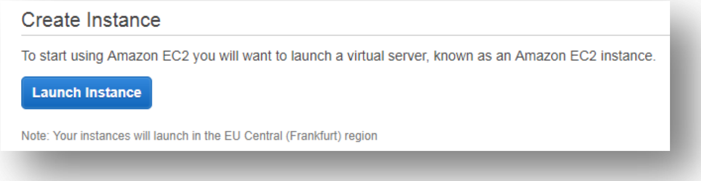
Below is a screenshot of i-088cf43a2abb828e8 (R80-10MNG_CPInstance) at 2017-07-25T11:47:55.425+03:00.

```
Starting the system... journald starting.  Commit interval 5 secondsnterface dri
EXT3-fs: mounted filesystem with ordered data mode.
 xvda2 xvda3em initialized
HP CISS Driver (v 3.6.28-20 )d IRQ 16
scsi0 : ata_piixupt 0000:00:1f.0[A] -> GSI 47 (level, low) -> IRQ 177
scsi1 : ata_piix
ata1: PATA max MWDMA2 bmdma 0xc100 irq 14
ata2: PATA max MWDMA2 bmdma 0xc108 irq 15ol version 1
ata1.00: ATA-7: QEMU HARDDISK, 0.10.2, max UDMA/100
ata1.00: 209715200 sectors, multi 16: LBA48
ata1.00: configured for MWDMA2
  Vendor: ATA       Model: QEMU HARDDISK     Rev: 0.10
  Type:   Direct-Access                      ANSI SCSI revision: 05
device-mapper: uevent: version 1.0.3
device-mapper: ioctl: 4.11.5-ioctl (2007-12-12) initialised: dm-devel@redhat.com
```

Provision the Web Server instance from Marketplace

14. While waiting for our R80.10 Management Server to finish the First Time Wizard, lets deploy our web server

15. In the top navigation bar, click "EC2" dashboard, and click "Launch Instance"

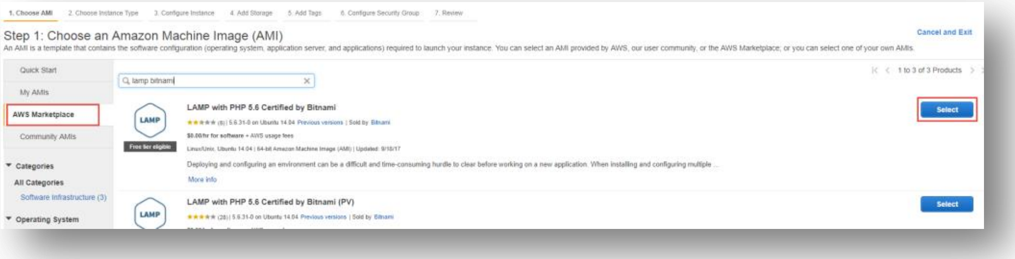


Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the EU Central (Frankfurt) region

16. In the following window, choose "AWS Marketplace" and search for "LAMP Bitnami" (as shown)



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

lamp bitnami

LAMP with PHP 5.6 Certified by Bitnami

★★★★★ (8) | 5.6.31-0 on Ubuntu 14.04 Previous versions | Sold by Bitnami

$0.00/hr for software + AWS usage fees

Linux/Unix, Ubuntu 14.04 | 64-bit Amazon Machine Image (AMI) | Updated: 9/18/17

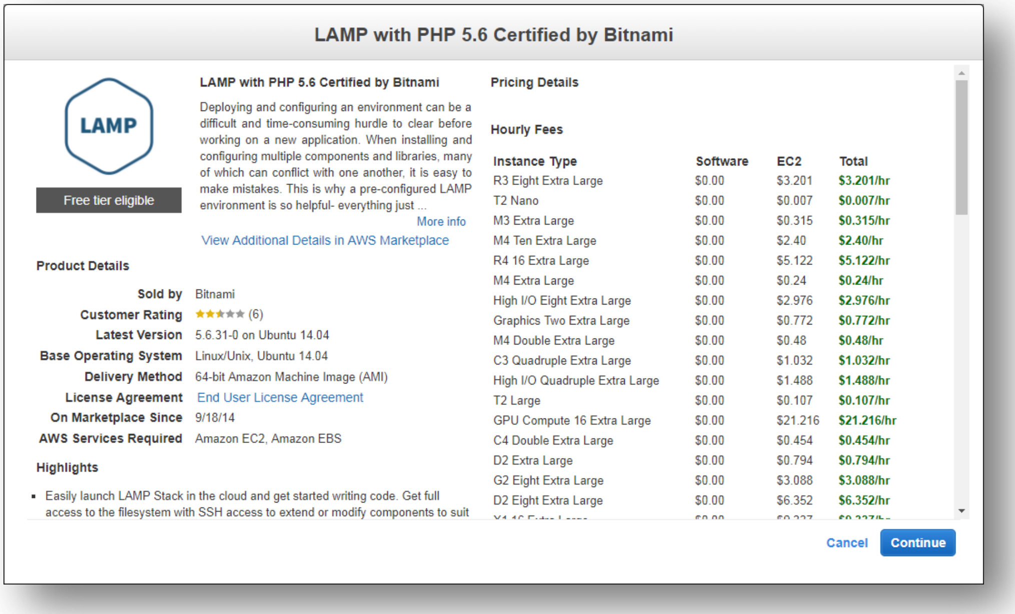
Deploying and configuring an environment can be a difficult and time-consuming hurdle to clear before working on a new application. When installing and configuring multiple ...

LAMP with PHP 5.6 Certified by Bitnami (PV)

★★★★★ (28) | 5.6.31-0 on Ubuntu 14.04 Previous versions | Sold by Bitnami

Click "Select"

17. Click “Continue”



LAMP with PHP 5.6 Certified by Bitnami

LAMP with PHP 5.6 Certified by Bitnami

Deploying and configuring an environment can be a difficult and time-consuming hurdle to clear before working on a new application. When installing and configuring multiple components and libraries, many of which can conflict with one another, it is easy to make mistakes. This is why a pre-configured LAMP environment is so helpful- everything just ...

View Additional Details in AWS Marketplace

Product Details

Sold by	Bitnami
Customer Rating	★★★★★ (6)
Latest Version	5.6.31-0 on Ubuntu 14.04
Base Operating System	Linux/Unix, Ubuntu 14.04
Delivery Method	64-bit Amazon Machine Image (AMI)
License Agreement	End User License Agreement
On Marketplace Since	9/18/14
AWS Services Required	Amazon EC2, Amazon EBS

Highlights

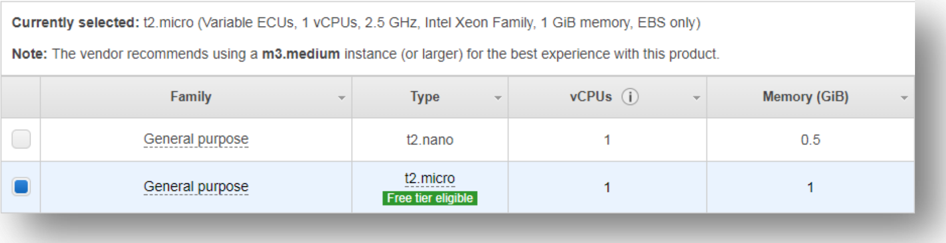
- Easily launch LAMP Stack in the cloud and get started writing code. Get full access to the filesystem with SSH access to extend or modify components to suit

Pricing Details

Hourly Fees

Instance Type	Software	EC2	Total
R3 Eight Extra Large	$0.00	$3.201	$3.201/hr
T2 Nano	$0.00	$0.007	$0.007/hr
M3 Extra Large	$0.00	$0.315	$0.315/hr
M4 Ten Extra Large	$0.00	$2.40	$2.40/hr
R4 16 Extra Large	$0.00	$5.122	$5.122/hr
M4 Extra Large	$0.00	$0.24	$0.24/hr
High I/O Eight Extra Large	$0.00	$2.976	$2.976/hr
Graphics Two Extra Large	$0.00	$0.772	$0.772/hr
M4 Double Extra Large	$0.00	$0.48	$0.48/hr
C3 Quadruple Extra Large	$0.00	$1.032	$1.032/hr
High I/O Quadruple Extra Large	$0.00	$1.488	$1.488/hr
T2 Large	$0.00	$0.107	$0.107/hr
GPU Compute 16 Extra Large	$0.00	$21.216	$21.216/hr
C4 Double Extra Large	$0.00	$0.454	$0.454/hr
D2 Extra Large	$0.00	$0.794	$0.794/hr
G2 Eight Extra Large	$0.00	$3.088	$3.088/hr
D2 Eight Extra Large	$0.00	$6.352	$6.352/hr

18. Choose the t2.micro server type

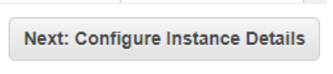


Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

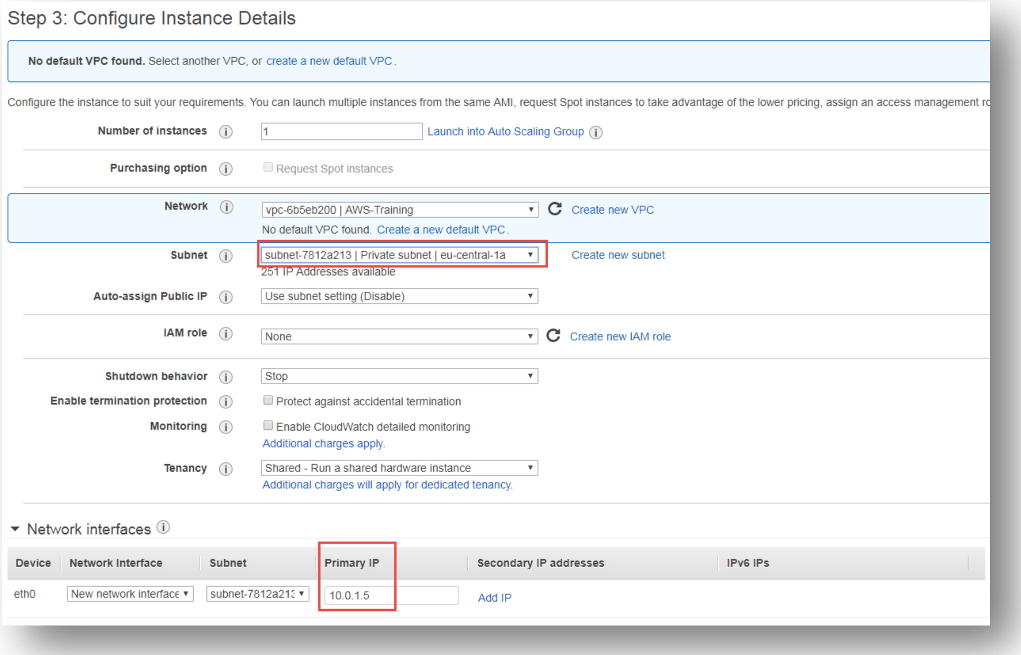
Note: The vendor recommends using a **m3.medium** instance (or larger) for the best experience with this product.

	Family	Type	vCPUs ⓘ	Memory (GiB)
□	General purpose	t2.nano	1	0.5
■	General purpose	t2.micro Free tier eligible	1	1

And then click on “Next: configure Instance Details” at the lower right corner of the screen.



19. On the next screen fill in the fields as described below:



Step 3: Configure Instance Details

No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management r

Number of instances	1
Purchasing option	□ Request Spot instances
Network	vpc-6b5eb200 | AWS-Training No default VPC found. Create a new default VPC.
Subnet	subnet-7812a213 | Private subnet | eu-central-1a 251 IP Addresses available
Auto-assign Public IP	Use subnet setting (Disable)
IAM role	None
Shutdown behavior	Stop
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

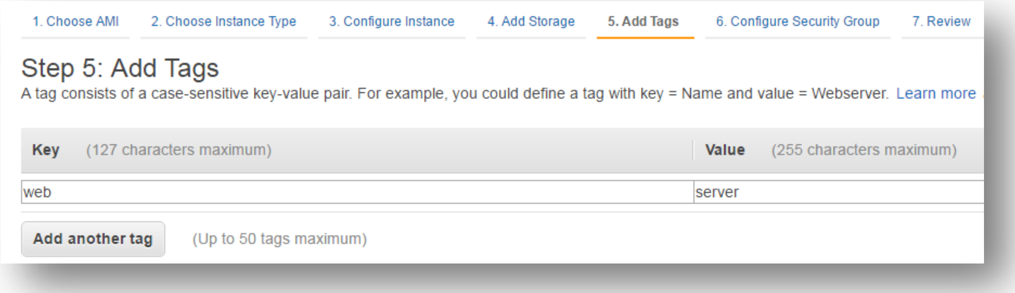
Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-7812a21	10.0.1.5	Add IP	

Network: AWS-Training
Subnet: Private subnet
Auto-assign public IP: Disable
Tenancy: Shared
Network Interface – Primary IP: 10.0.1.5

20. Click "Next", and again "Next" till you are at step 5

21. On the Add Tags page, click on "Add Tag"



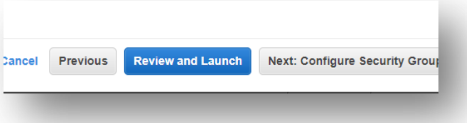
Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. Learn more

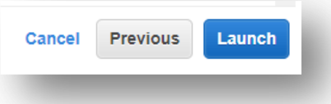
Key (127 characters maximum)	Value (255 characters maximum)
web	server

Fill in the fields: Key=web, Value=server

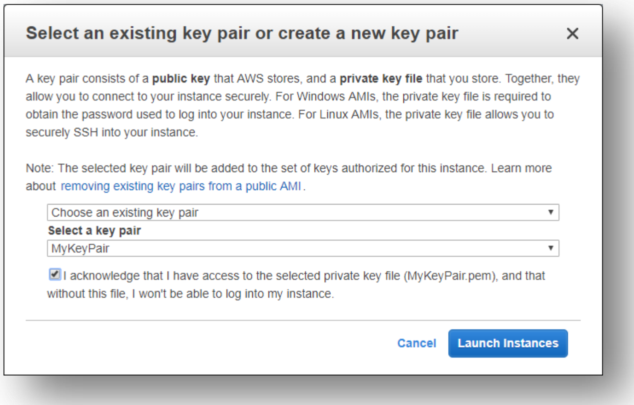
22. Finish the instance deployment process by clicking "Review and Launch"



23. Review the configuration and then click "Launch" in the lower right part of the screen



24. When asked, use the same key pair that you've already used before and check the box. Then click "Launch Instances"



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

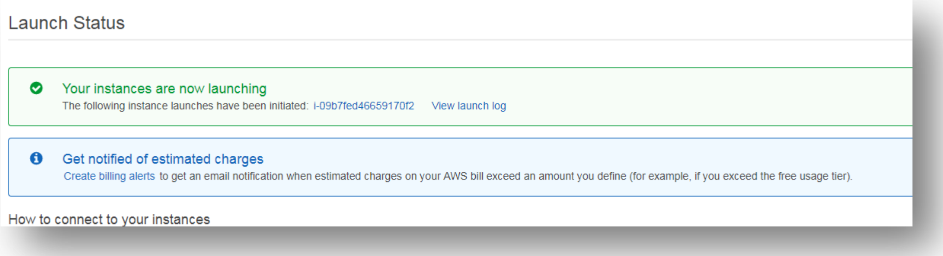
Choose an existing key pair

Select a key pair

MyKeyPair

☑ I acknowledge that I have access to the selected private key file (MyKeyPair.pem), and that without this file, I won't be able to log into my instance.

25. The next screen will show you the deployment status



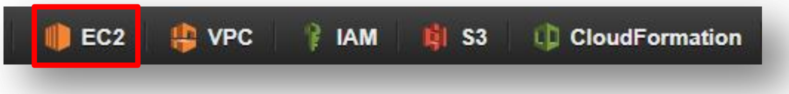
Launch Status

Your instances are now launching
The following instance launches have been initiated: i-09b7fed46659170f2 View launch log

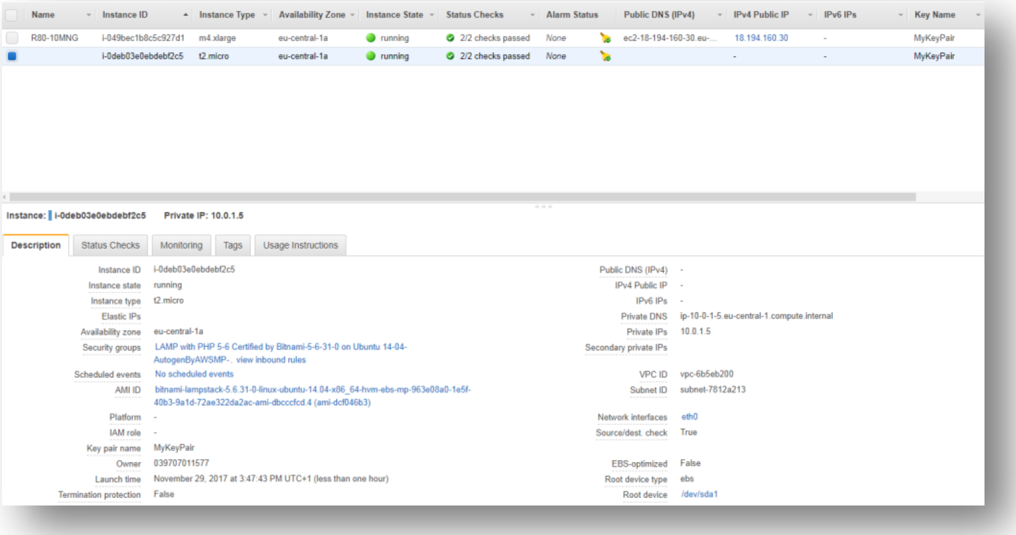
Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

26. In the top navigation bar, click "EC2" dashboard



27. Click on "Instances" on the left pane and the below window will appear.
Once you mark that newly created server you will see the following screen:



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name
R80-10MNG	i-049bec1b8c5c927d1	m4.xlarge	eu-central-1a	running	2/2 checks passed	None	ec2-18-194-160-30.eu-...	18.194.160.30	-	MyKeyPair
	i-0deb03e0ebdebf2c5	t2.micro	eu-central-1a	running	2/2 checks passed	None		-	-	MyKeyPair

Instance: i-0deb03e0ebdebf2c5   Private IP: 10.0.1.5

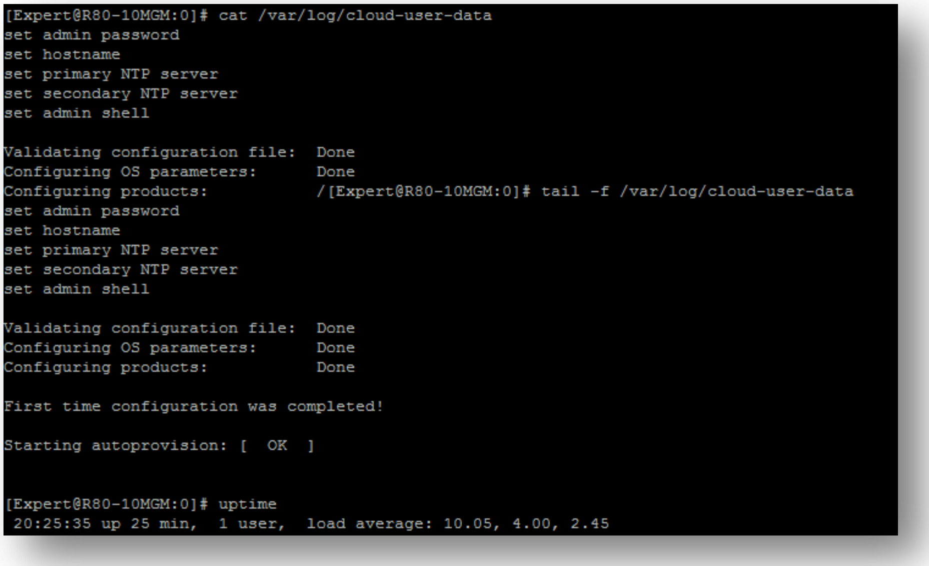
Instance ID	i-0deb03e0ebdebf2c5
Instance state	running
Instance type	t2.micro
Elastic IPs	
Availability zone	eu-central-1a
Security groups	LAMP with PHP 5-6 Certified by Bitnami-5-6-31-0 on Ubuntu 14-04-AutogenByAWSMP-. view inbound rules
Scheduled events	No scheduled events
AMI ID	bitnami-lampstack-5.6.31-0-linux-ubuntu-14.04-x86_64-hvm-ebs-mp-963e08a0-1e5f-40b3-9a1d-72ae322da2ac-ami-dbcccfcd.4 (ami-dcf046b3)
Platform	-
IAM role	-
Key pair name	MyKeyPair
Owner	039707011577
Launch time	November 29, 2017 at 3:47:43 PM UTC+1 (less than one hour)
Termination protection	False
Public DNS (IPv4)	-
IPv4 Public IP	-
IPv6 IPs	-
Private DNS	ip-10-0-1-5.eu-central-1.compute.internal
Private IPs	10.0.1.5
Secondary private IPs	
VPC ID	vpc-6b5eb200
Subnet ID	subnet-7812a213
Network interfaces	eth0
Source/dest. check	True
EBS-optimized	False
Root device type	ebs
Root device	/dev/sda1

Once the Instance State shows “Running” and Status Checks says “2/2 checks passed”, it’s up and ready.

Download SmartConsole and log in to Check Point Management

28. Next step is to download the SmartConsole GUI to allow us to define the rules on our Check Point Gateway to allow access to the Web (LAMP) server

29. We need to make sure the management server is running and has completed the First Time Wizard. There are several ways to check this:
    a. Open an SSH session to the Management server using your predefined Key (for example you may use Putty)
    Check for ‘First time configuration was completed!’ with:
    ‘tail –f /var/log/cloud-user-data’

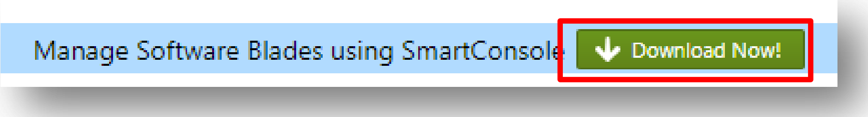


```
[Expert@R80-10MGM:0]# cat /var/log/cloud-user-data
set admin password
set hostname
set primary NTP server
set secondary NTP server
set admin shell

Validating configuration file:  Done
Configuring OS parameters:      Done
Configuring products:           /[Expert@R80-10MGM:0]# tail -f /var/log/cloud-user-data
set admin password
set hostname
set primary NTP server
set secondary NTP server
set admin shell

Validating configuration file:  Done
Configuring OS parameters:      Done
Configuring products:           Done

First time configuration was completed!

Starting autoprovision: [  OK  ]


[Expert@R80-10MGM:0]# uptime
 20:25:35 up 25 min,  1 user,  load average: 10.05, 4.00, 2.45
```

   b. Connect to the Gaia portal of the Management server via the public IP, using HTTPS. You can find the public IP of the Management server on the EC2 Instances screen. I you get in, the First Time Wizard was completed.

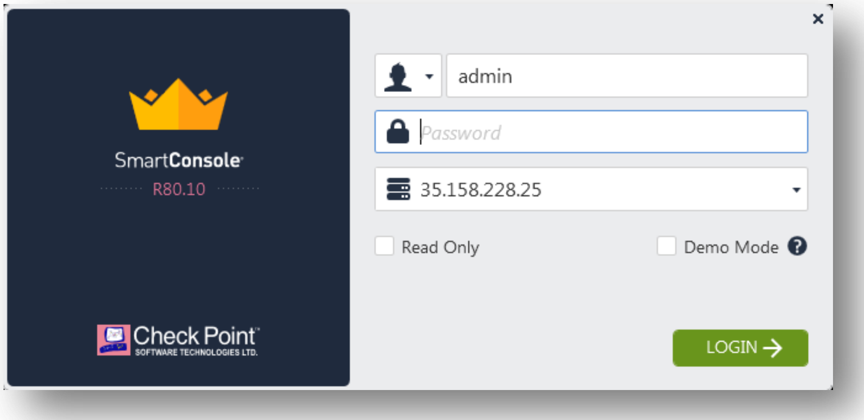
30. When the Management is up and running, connect to the Gaia portal of the Management server via the public IP, using HTTPS. You can find the public IP of the Management server on the EC2 Instances screen

31. If you already have Check Point R80.10 SmartConsole installed, skip this step.
    If not, download it from the link on the upper central screen:



32. Install it with the default configuration.

33. Open the SmartConsole and log in using your credentials:



User: admin
Password: the one that you defined in exercise 2 step 6 (the password that you created a hash of)
IP address: public ip of the management server

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

You successfully finished Exercise #2

Exercise #3 - Deploy Check Point vSEC cluster on AWS

Purpose: To deploy a Check Point vSEC Gateway cluster using a CloudFormation template

Description

This exercise will guide you through the deployment of a Check Point's vSEC cluster on the environment created in AWS.

Method

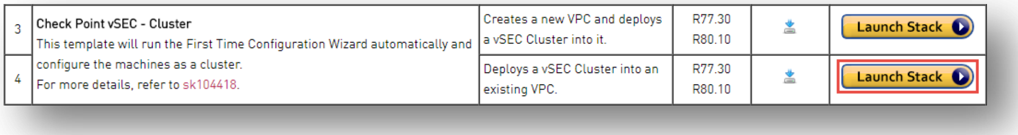
Using AWS portal you will provision the latest vSEC Gateway Cluster to protect workloads deployed on your AWS public cloud environment

Provision the R80.10 vSEC Cluster instances using CloudFormation template

1. Open SK111013 in your browser

2. Review the available CloudFormation templates

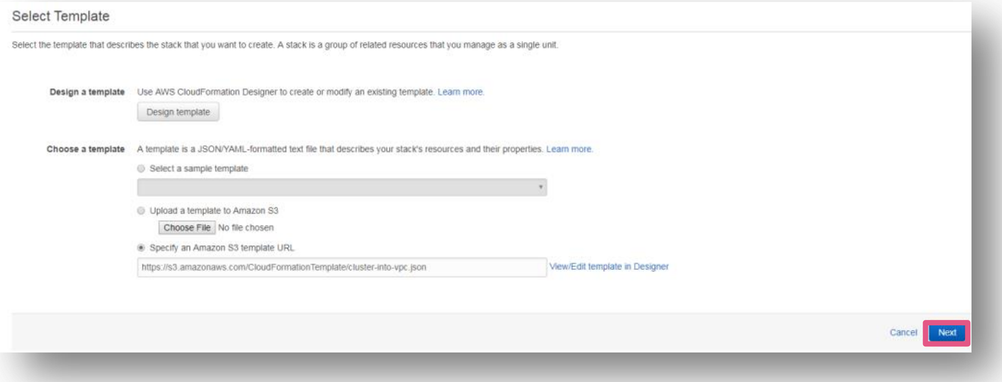
3. Click on the "Launch Stack" button of the "Check Point vSEC – Cluster / Deploys a vSEC Cluster into an existing VPC" on the right side of the page.



3	**Check Point vSEC - Cluster** This template will run the First Time Configuration Wizard automatically and configure the machines as a cluster. For more details, refer to sk104418.	Creates a new VPC and deploys a vSEC Cluster into it.	R77.30 R80.10	⤓	Launch Stack
4		Deploys a vSEC Cluster into an existing VPC.	R77.30 R80.10	⤓	Launch Stack

4. This will open the AWS console into the CloudFormation -> Stacks -> Create Stack window

5. The Check Point CloudFormation template for deploying vSEC Cluster is automatically chosen
Click "Next"



Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. Learn more.

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.

○ Select a sample template

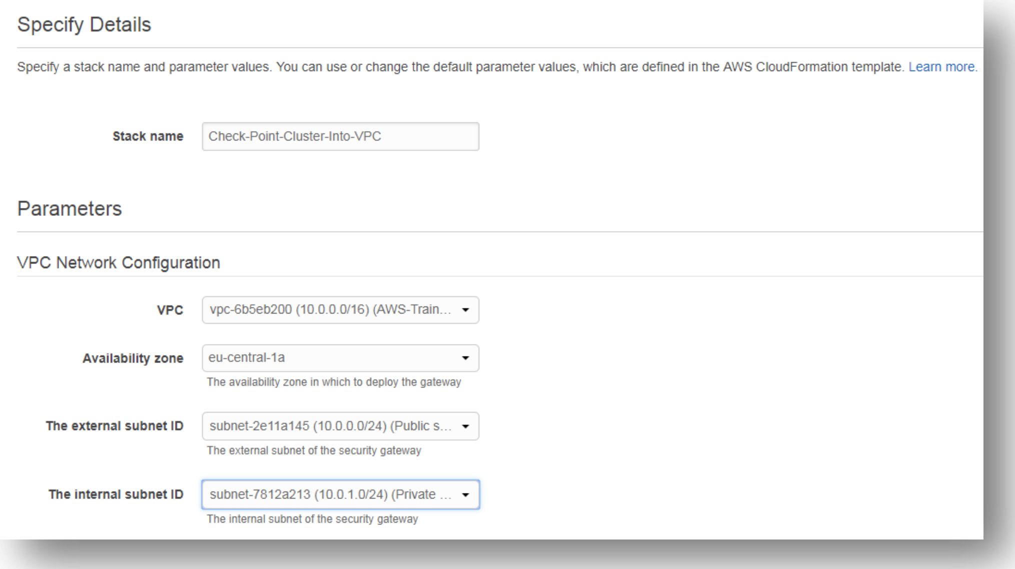
○ Upload a template to Amazon S3

Choose File No file chosen

● Specify an Amazon S3 template URL

https://s3.amazonaws.com/CloudFormationTemplate/cluster-into-vpc.json

6. The next screen includes the information needed for deploying the R80.10 vSEC Cluster automatically
Fill in the different fields as listed below:



Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.

Stack name	Check-Point-Cluster-Into-VPC

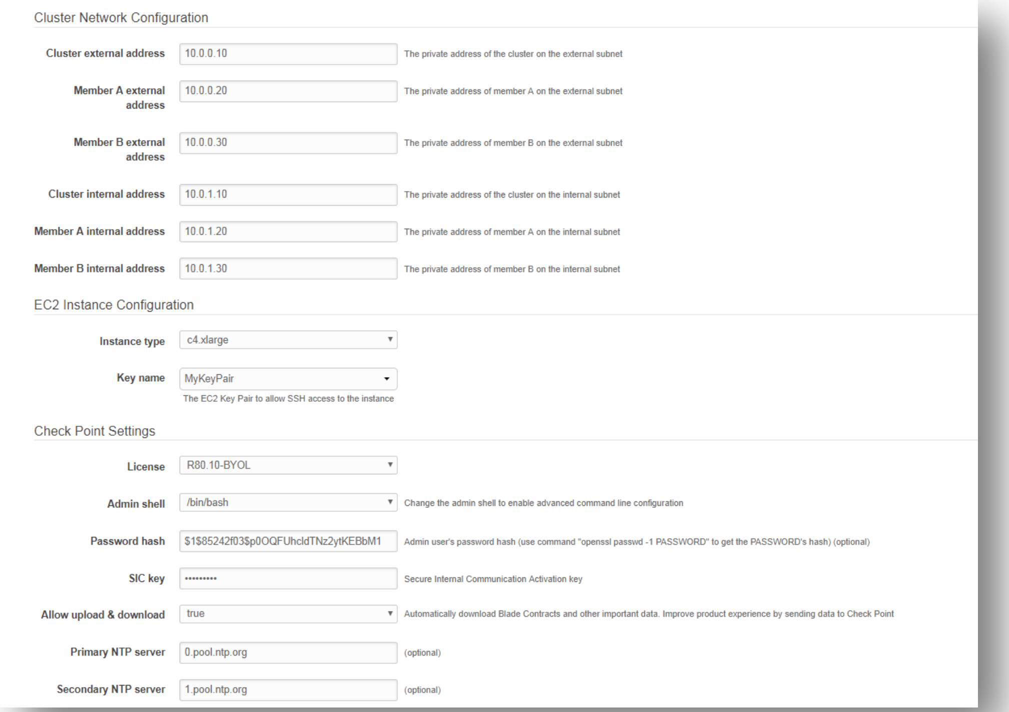
Parameters

VPC Network Configuration

VPC	vpc-6b5eb200 (10.0.0.0/16) (AWS-Train...
Availability zone	eu-central-1a The availability zone in which to deploy the gateway
The external subnet ID	subnet-2e11a145 (10.0.0.0/24) (Public s... The external subnet of the security gateway
The internal subnet ID	subnet-7812a213 (10.0.1.0/24) (Private ... The internal subnet of the security gateway

Stack name: can be left as the default
VPC: AWS-Training
Availability zone: the same as in previous exercises (the one that ends with “1a”)
External subnet: Public subnet
Internal subnet: Private subnet

7. Continue filling the fields as per the data below:



Cluster Network Configuration

Cluster external address	10.0.0.10	The private address of the cluster on the external subnet
Member A external address	10.0.0.20	The private address of member A on the external subnet
Member B external address	10.0.0.30	The private address of member B on the external subnet
Cluster internal address	10.0.1.10	The private address of the cluster on the internal subnet
Member A internal address	10.0.1.20	The private address of member A on the internal subnet
Member B internal address	10.0.1.30	The private address of member B on the internal subnet

EC2 Instance Configuration

Instance type	c4.xlarge	
Key name	MyKeyPair The EC2 Key Pair to allow SSH access to the instance	

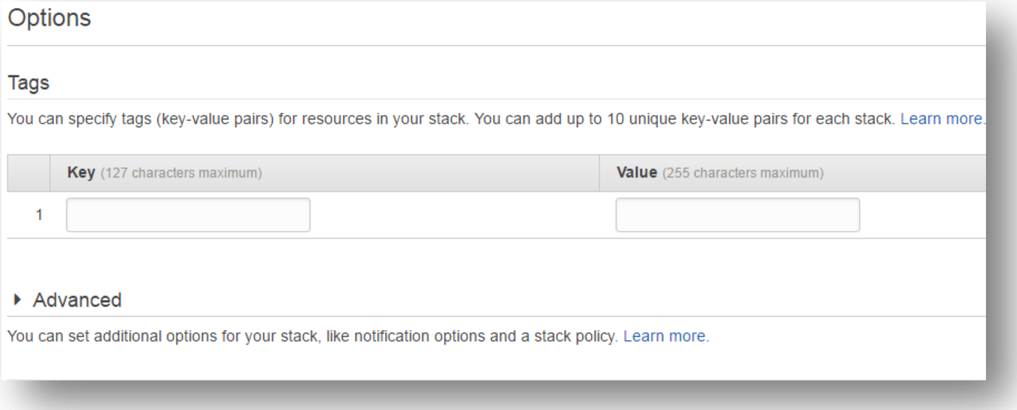
Check Point Settings

License	R80.10-BYOL	
Admin shell	/bin/bash	Change the admin shell to enable advanced command line configuration
Password hash	$1$85242f03$p0OQFUhcldTNz2ytKEBbM1	Admin user's password hash (use command "openssl passwd -1 PASSWORD" to get the PASSWORD's hash) (optional)
SIC key	••••••••••	Secure Internal Communication Activation key
Allow upload & download	true	Automatically download Blade Contracts and other important data. Improve product experience by sending data to Check Point
Primary NTP server	0.pool.ntp.org	(optional)
Secondary NTP server	1.pool.ntp.org	(optional)

Cluster Network Configuration section: leave at the default
Instance type: You can leave at the default or change per the instructor guideline
Key name: use the same key pair that you've already used in previous exercises
License: R80.10-BYOL
Admin shell: /bin/bash
Password hash: use the same as defined on the management on exercise 2 step 6
SIC key: choose your own (ie. secret123) (Note: SIC must be minimum 8 alpha numeric characters)

When you are done, please click "Next"

8. The following window appears, this is where you can tag your instances (optional)



Options

Tags

You can specify tags (key-value pairs) for resources in your stack. You can add up to 10 unique key-value pairs for each stack. Learn more.

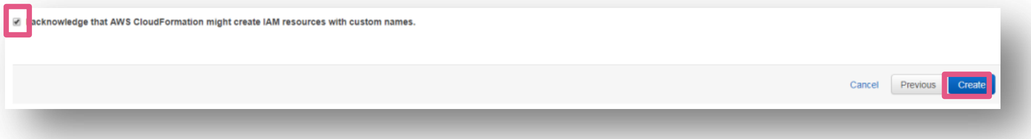
	Key (127 characters maximum)	Value (255 characters maximum)
1		

▸ Advanced

You can set additional options for your stack, like notification options and a stack policy. Learn more.

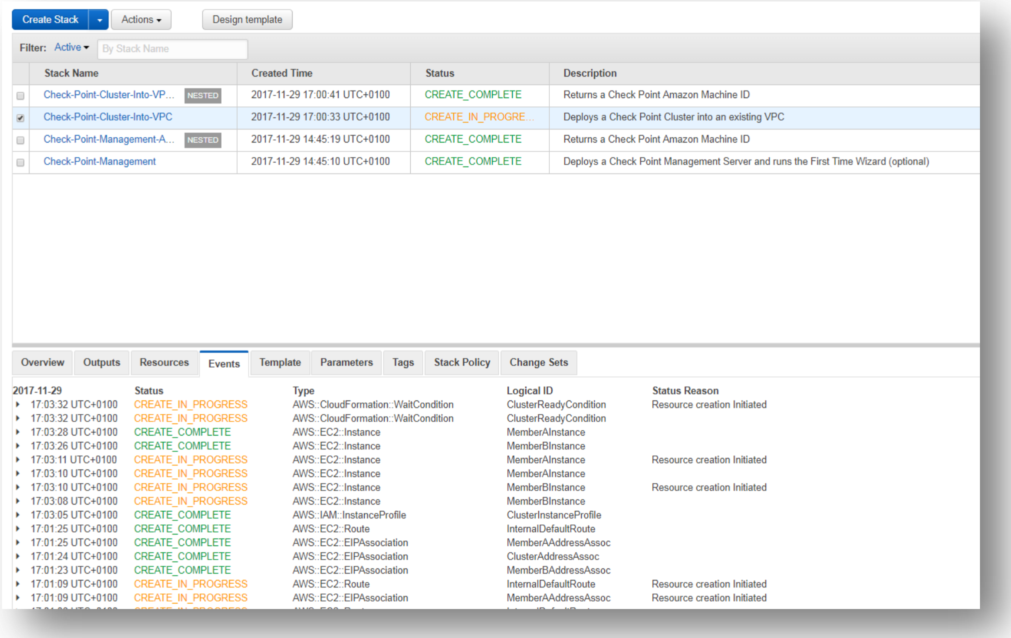
Click "Next" when done

9. In the next window, you can review the new Cluster about to be provisioned and when you're done, check the box at the bottom and click on "Create"



☑ acknowledge that AWS CloudFormation might create IAM resources with custom names.

10. The Cluster will now be created. You will be transferred into the "CloudFormation" page.
Refresh to see the progress.
You can see more details of the creation process when you mark a line and choose "Events" at the bottom part (as shown)



Filter: Active By Stack Name

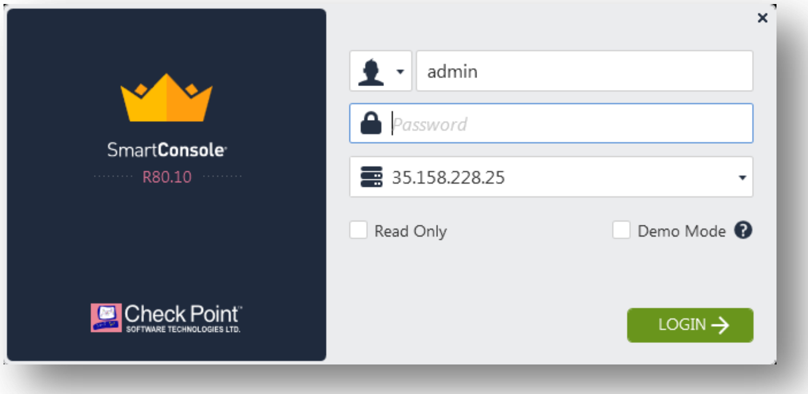
	Stack Name	Created Time	Status	Description
□	Check-Point-Cluster-Into-VP... NESTED	2017-11-29 17:00:41 UTC+0100	CREATE_COMPLETE	Returns a Check Point Amazon Machine ID
☑	Check-Point-Cluster-Into-VPC	2017-11-29 17:00:33 UTC+0100	CREATE_IN_PROGRE...	Deploys a Check Point Cluster into an existing VPC
□	Check-Point-Management-A... NESTED	2017-11-29 14:45:19 UTC+0100	CREATE_COMPLETE	Returns a Check Point Amazon Machine ID
□	Check-Point-Management	2017-11-29 14:45:10 UTC+0100	CREATE_COMPLETE	Deploys a Check Point Management Server and runs the First Time Wizard (optional)

2017-11-29	Status	Type	Logical ID	Status Reason
17:03:32 UTC+0100	CREATE_IN_PROGRESS	AWS::CloudFormation::WaitCondition	ClusterReadyCondition	Resource creation Initiated
17:03:32 UTC+0100	CREATE_IN_PROGRESS	AWS::CloudFormation::WaitCondition	ClusterReadyCondition	
17:03:28 UTC+0100	CREATE_COMPLETE	AWS::EC2::Instance	MemberAInstance	
17:03:26 UTC+0100	CREATE_COMPLETE	AWS::EC2::Instance	MemberBInstance	
17:03:11 UTC+0100	CREATE_IN_PROGRESS	AWS::EC2::Instance	MemberAInstance	Resource creation Initiated
17:03:10 UTC+0100	CREATE_IN_PROGRESS	AWS::EC2::Instance	MemberAInstance	
17:03:10 UTC+0100	CREATE_IN_PROGRESS	AWS::EC2::Instance	MemberBInstance	Resource creation Initiated
17:03:08 UTC+0100	CREATE_IN_PROGRESS	AWS::EC2::Instance	MemberBInstance	
17:03:05 UTC+0100	CREATE_COMPLETE	AWS::IAM::InstanceProfile	ClusterInstanceProfile	
17:01:25 UTC+0100	CREATE_COMPLETE	AWS::EC2::Route	InternalDefaultRoute	
17:01:25 UTC+0100	CREATE_COMPLETE	AWS::EC2::EIPAssociation	MemberAAddressAssoc	
17:01:24 UTC+0100	CREATE_COMPLETE	AWS::EC2::EIPAssociation	ClusterAddressAssoc	
17:01:23 UTC+0100	CREATE_COMPLETE	AWS::EC2::EIPAssociation	MemberBAddressAssoc	
17:01:09 UTC+0100	CREATE_IN_PROGRESS	AWS::EC2::Route	InternalDefaultRoute	Resource creation Initiated
17:01:09 UTC+0100	CREATE_IN_PROGRESS	AWS::EC2::EIPAssociation	MemberAAddressAssoc	Resource creation Initiated

Log in to SmartConsole and configure the cluster object

11. Once deployment process is done, log in to our R80.10 SmartCenter Server and configure the cluster object (detailed instructions can be found in SK104418, note to use the private IP addresses):

    a. Open the SmartConsole and log in using your credentials:



admin

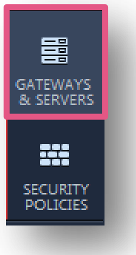
35.158.228.25

□ Read Only

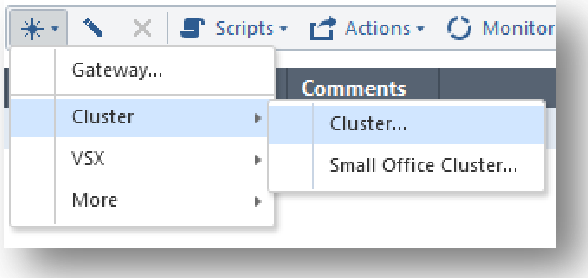
□ Demo Mode

User: admin
Password: the one that you defined in exercise 2 step 6 (the password that you created a hash of)
IP address: public IP of the management server

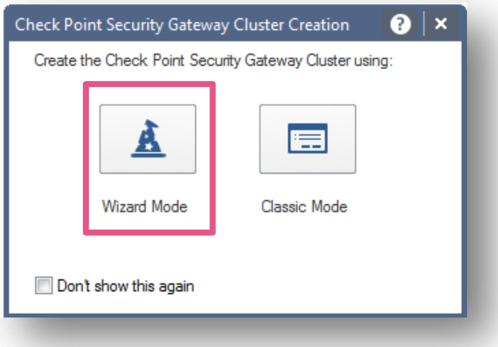
    b. Click the GATEWAYS & SERVERS on the left side of the screen



c. In the upper middle of the screen choose to add new Cluster object



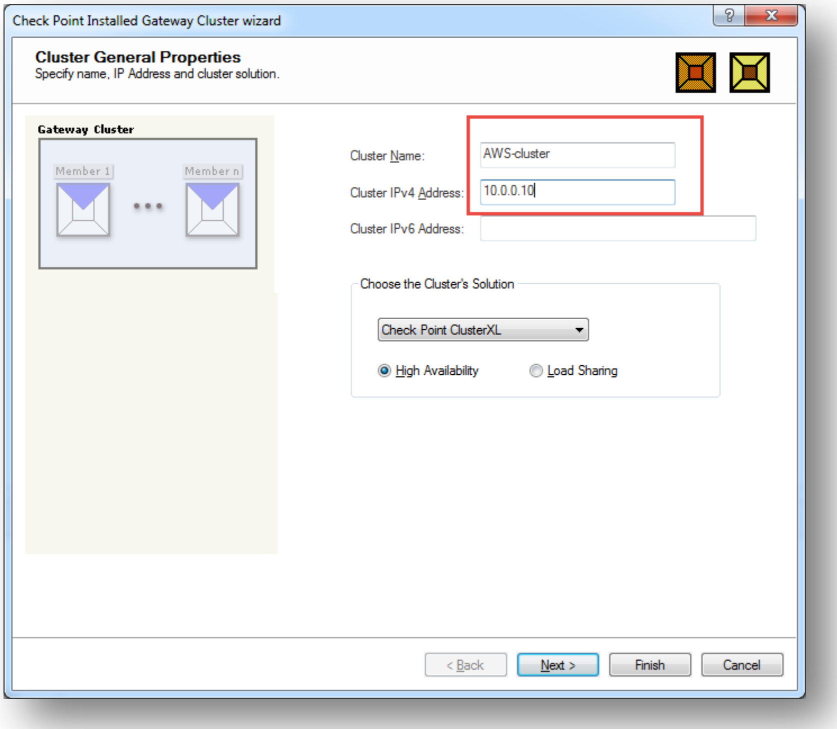
d. In the window that opens choose Wizard Mode


Check Point Security Gateway Cluster Creation

Create the Check Point Security Gateway Cluster using:

□ Don't show this again

e. Fill in the details on the opened window as described below:



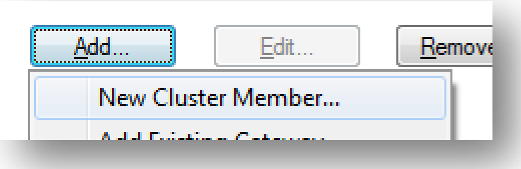
Cluster General Properties
Specify name, IP Address and cluster solution.

Cluster Name: AWS-cluster
Cluster IPv4 Address: 10.0.0.10
Cluster IPv6 Address:

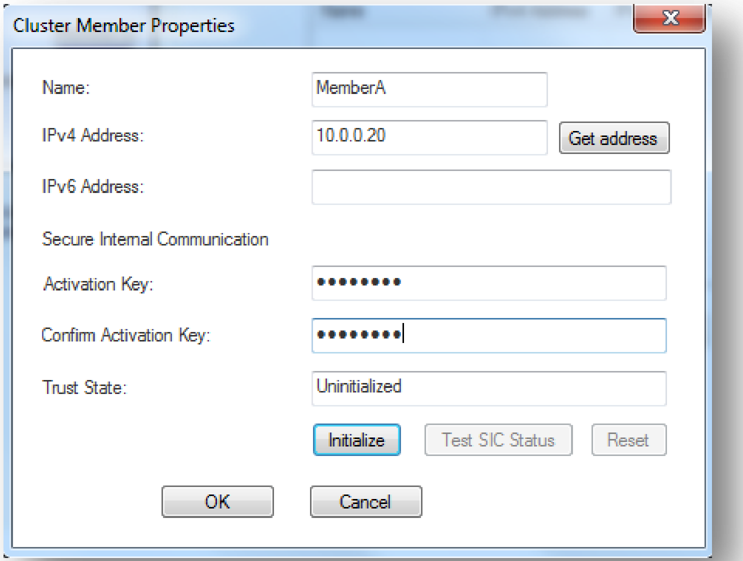
Choose the Cluster's Solution
Check Point ClusterXL
● High Availability ○ Load Sharing

Cluster name: AWS-cluster
Cluster IPv4 Address: 10.0.0.10
Leave the rest untouched and click "Next"

f. Click "Add / New Cluster Member"



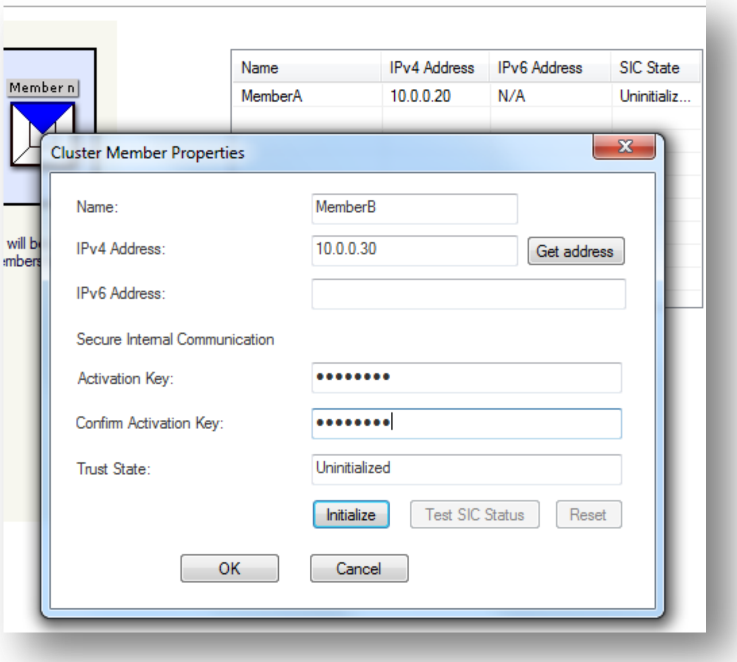
g. On the next window you will enter the members details, Enter the details for member A (we can use the private IP since the member and management are located on the same subnet)



Name: MemberA
IPv4 Address: 10.0.0.20
IPv6 Address:
Secure Internal Communication
Activation Key: ••••••••
Confirm Activation Key: ••••••••
Trust State: Uninitialized

Name: MemberA
IPv4 address: 10.0.0.20
Activation Key: The SIC key you defined on step 7 of this exercise.
Click on Initialize and make sure it changed into “Trust established”.
Click OK to close this screen.

h. Now do the same for the second member



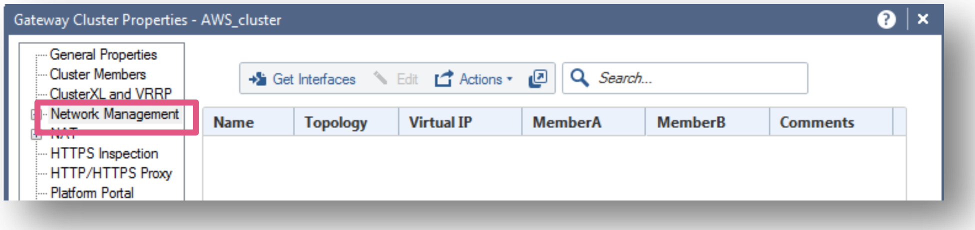
Name	IPv4 Address	IPv6 Address	SIC State
MemberA	10.0.0.20	N/A	Uninitializ...

Name: MemberB
IPv4 Address: 10.0.0.30
IPv6 Address:
Secure Internal Communication
Activation Key: ••••••••
Confirm Activation Key: ••••••••
Trust State: Uninitialized

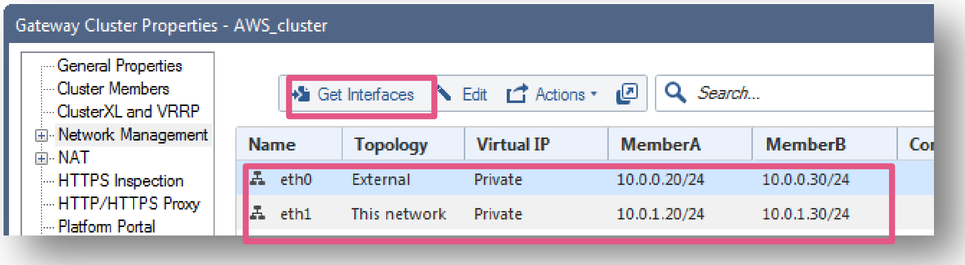
Name: MemberB
IPv4 address: 10.0.0.30
Activation Key: as you defined on step 7 of this exercise.
Click on Initialize and make sure it changed into “Trust established”.
Click OK to close this screen.

i. Click “Next” and then “Finish” (disregard the notice).

j. Open the Cluster object & move into Network Management

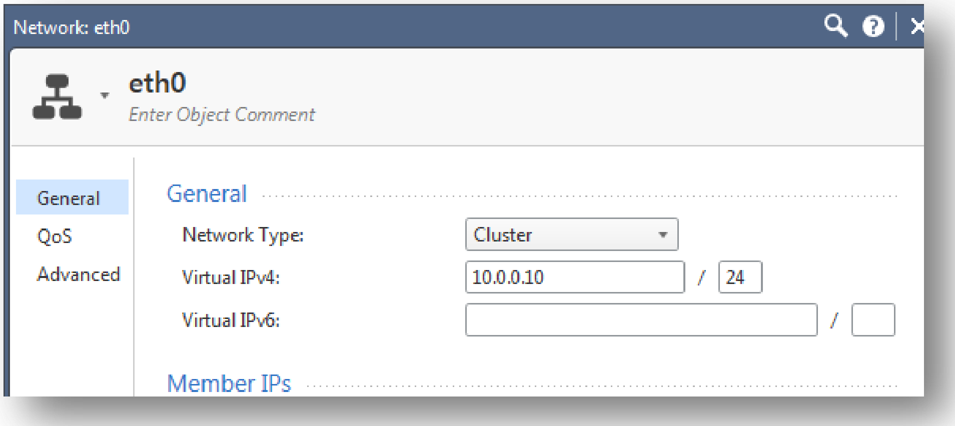


k. Click on the “Get Interfaces” and verify that they are imported correctly



Name	Topology	Virtual IP	MemberA	MemberB	Cor
eth0	External	Private	10.0.0.20/24	10.0.0.30/24	
eth1	This network	Private	10.0.1.20/24	10.0.1.30/24	

l. Double-click on eth0 and change the Network Type to Cluster, add the IP (10.0.0.10) and mask (24), then click “OK”

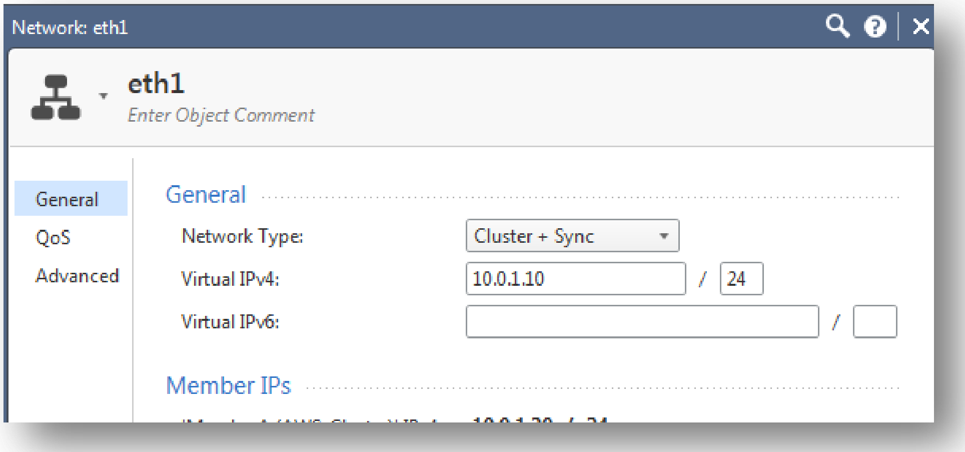


Network Type: Cluster

Virtual IPv4: 10.0.0.10 / 24

Virtual IPv6: /

m. Double-click on eth1 and change the Network Type into Cluster + Sync, add the IP (10.0.1.10) and mask (24), then click “OK”



Network: eth1

eth1

Enter Object Comment

General
QoS
Advanced

General

Network Type: Cluster + Sync

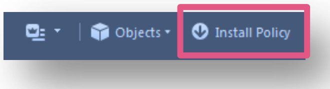
Virtual IPv4: 10.0.1.10 / 24

Virtual IPv6: /

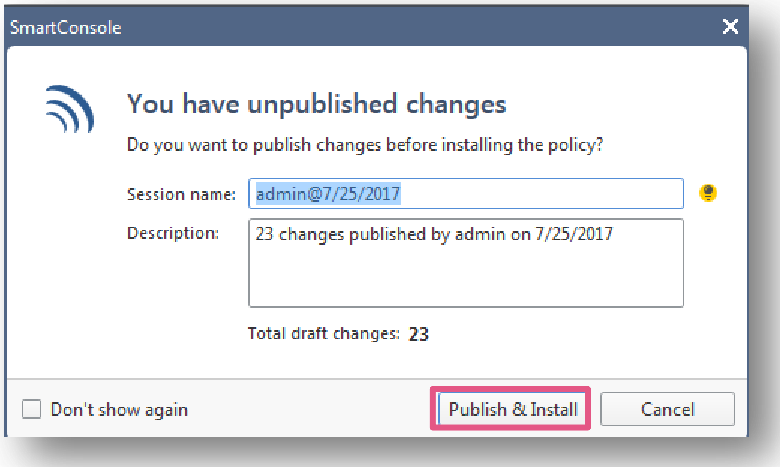
Member IPs

n. Click “OK” to close the Cluster object window

o. On the upper left side click “Install Policy”



p. Click “Publish & Install”



SmartConsole

You have unpublished changes

Do you want to publish changes before installing the policy?

Session name: admin@7/25/2017

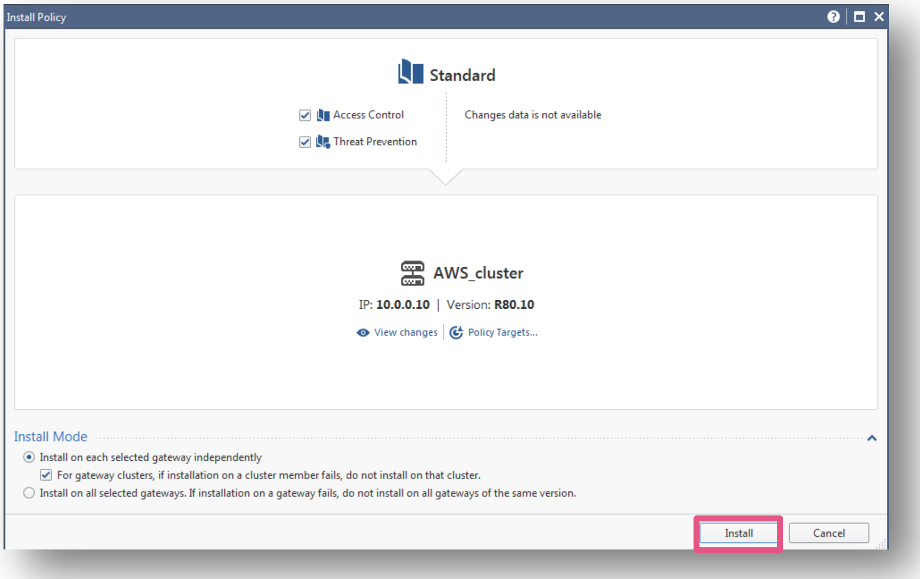
Description: 23 changes published by admin on 7/25/2017

Total draft changes: 23

□ Don't show again

Publish & Install | Cancel

q. In next window, uncheck Threat Prevention and click “Install”



Install Policy

Standard

☑ Access Control
☑ Threat Prevention

Changes data is not available

AWS_cluster

IP: **10.0.0.10** | Version: **R80.10**

View changes | Policy Targets...

Install Mode

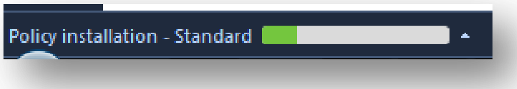
● Install on each selected gateway independently

☑ 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

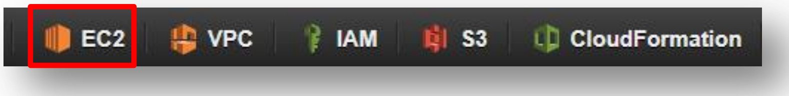
r. You can see the progress on the bottom left side



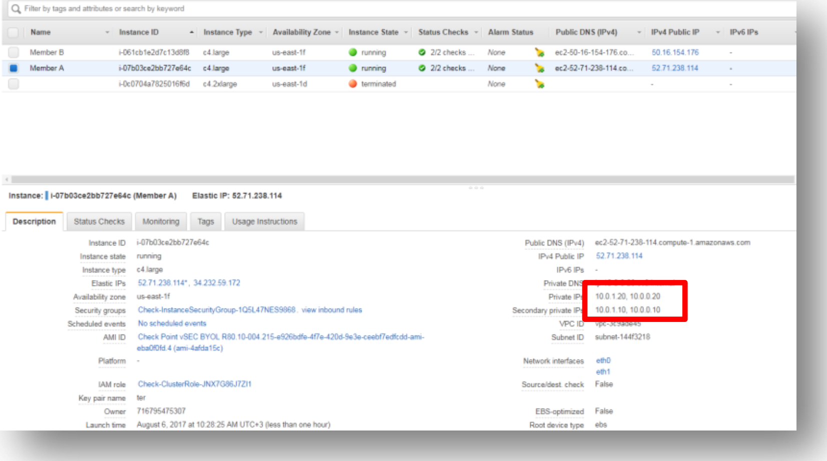
Policy installation - Standard

Adapt the route table to the cluster

1. In the AWS console in the top navigation bar, click "EC2" dashboard



2. On the Instances screen, mark one of the members of the cluster and check if it is holding the VIP address by looking at the IP addresses of the machine (10.0.0.10 and 10.0.1.10 means that it is), if it is not, change to the other one



Filter by tags and attributes or search by keyword

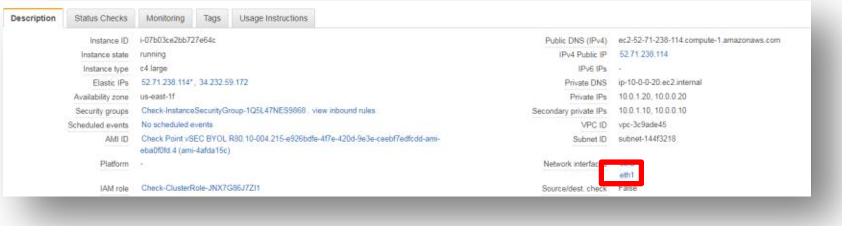
	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status		Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
□	Member B	i-061cb1e2d7c13d8f8	c4.large	us-east-1f	running	2/2 checks ...	None		ec2-50-16-154-176.co...	50.16.154.176	-
■	Member A	i-07b03ce2bb727e64c	c4.large	us-east-1f	running	2/2 checks ...	None		ec2-52-71-238-114.co...	52.71.238.114	-
□		i-0c0704a7825016f6d	c4.2xlarge	us-east-1d	terminated		None			-	-

Instance: i-07b03ce2bb727e64c (Member A) **Elastic IP: 52.71.238.114**

Description | Status Checks | Monitoring | Tags | Usage Instructions

Instance ID	i-07b03ce2bb727e64c	Public DNS (IPv4)	ec2-52-71-238-114.compute-1.amazonaws.com
Instance state	running	IPv4 Public IP	52.71.238.114
Instance type	c4.large	IPv6 IPs	-
Elastic IPs	52.71.238.114*, 34.232.59.172	Private DNS	
Availability zone	us-east-1f	Private IPs	10.0.1.20, 10.0.0.20
Security groups	Check-InstanceSecurityGroup-1Q5L47NES9868 . view inbound rules	Secondary private IPs	10.0.1.10, 10.0.0.10
Scheduled events	No scheduled events	VPC ID	vpc-3c9ade45
AMI ID	Check Point vSEC BYOL R80.10-004.215-e926bdfe-4f7e-420d-9e3e-ceebf7edfcdd-ami-eba0f0fd.4 (ami-4afda15c)	Subnet ID	subnet-144f3218
Platform	-	Network interfaces	eth0 eth1
IAM role	Check-ClusterRole-JNX7G86J7ZI1	Source/dest. check	False
Key pair name	ter		
Owner	716795475307	EBS-optimized	False
Launch time	August 6, 2017 at 10:28:25 AM UTC+3 (less than one hour)	Root device type	ebs

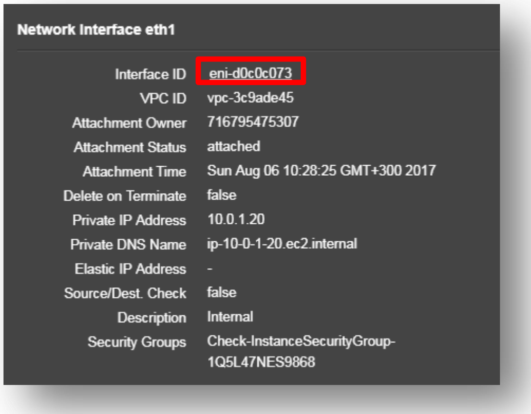
3. Click on the eth1



Instance ID i-07b03ce2bb727e64c
Instance state running
Instance type c4.large
Elastic IPs 52.71.238.114*, 34.232.59.172
Availability zone us-east-1f
Security groups Check-InstanceSecurityGroup-1Q5L47NES9868 . view inbound rules
Scheduled events No scheduled events
AMI ID Check Point vSEC BYOL R80.10-004.215-e926bdfe-4f7e-420d-9e3e-ceebf7edfcdd-ami-eba0f0fd.4 (ami-4afda15c)
Platform -
IAM role Check-ClusterRole-JNX7G86J7ZI1

Public DNS (IPv4) ec2-52-71-238-114.compute-1.amazonaws.com
IPv4 Public IP 52.71.238.114
IPv6 IPs -
Private DNS ip-10-0-0-20.ec2.internal
Private IPs 10.0.1.20, 10.0.0.20
Secondary private IPs 10.0.1.10, 10.0.0.10
VPC ID vpc-3c9ade45
Subnet ID subnet-144f3218
Network interfaces eth1
Source/dest. check False

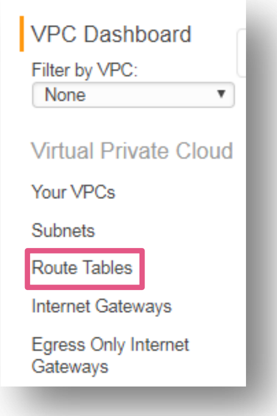
4. Write down the Interface ID (starts with eni). You will need it later



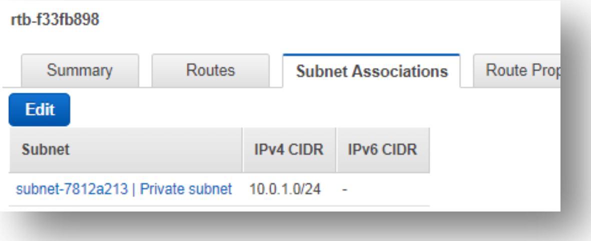
Network Interface eth1

Interface ID eni-d0c0c073
VPC ID vpc-3c9ade45
Attachment Owner 716795475307
Attachment Status attached
Attachment Time Sun Aug 06 10:28:25 GMT+300 2017
Delete on Terminate false
Private IP Address 10.0.1.20
Private DNS Name ip-10-0-1-20.ec2.internal
Elastic IP Address -
Source/Dest. Check false
Description Internal
Security Groups Check-InstanceSecurityGroup-1Q5L47NES9868

5. Our next step is to define a route to forward the traffic from the Private subnet via the Check Point Gateway cluster. Click “VPC” (on the top level bar) and choose Route Tables on the left side menu



6. Mark one of the routing tables and check under Subnet Association to find the one for network 10.0.1.0 (at the bottom of the screen)

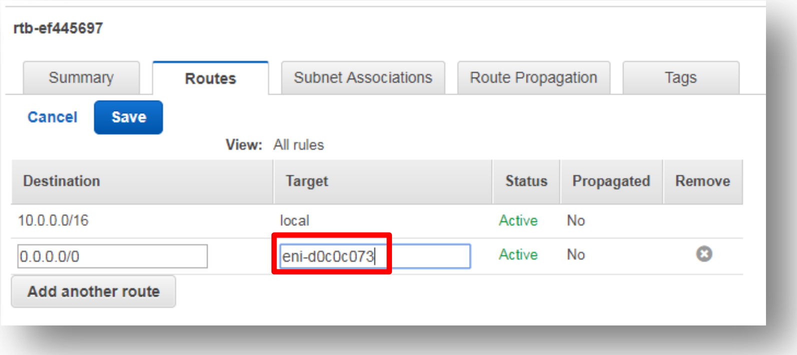


rtb-f33fb898

Subnet	IPv4 CIDR	IPv6 CIDR
subnet-7812a213 | Private subnet	10.0.1.0/24	-

7. Move into the Routes tab and click "Edit"

8. Change the Target field of the 0.0.0.0/0 route to the Interface ID that we've found on step 15



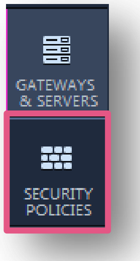
rtb-ef445697

Destination	Target	Status	Propagated	Remove
10.0.0.0/16	local	Active	No	
0.0.0.0/0	eni-d0c0c073	Active	No	⊗

9. Click "Save"

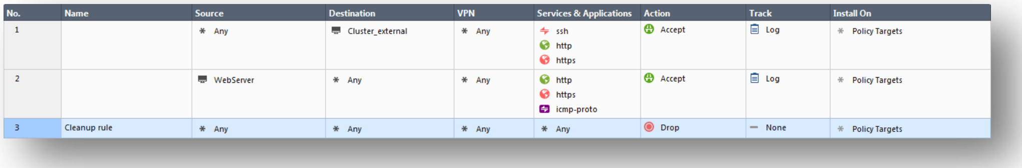
Create objects, access rules and NAT rules in SmartConsole

1. In the Check Point SmartConsole GUI, on the left bar choose SECURITY POLICIES

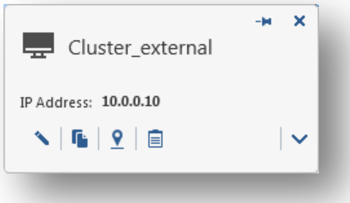


2. Create objects, access rules and NAT rules like these. For details, review Appendix #1 below

Allow and log ssh, http and https from Internet to cluster external IP

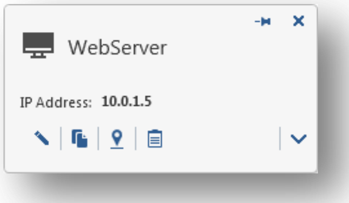


No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1		Any	Cluster_external	Any	ssh http https	Accept	Log	Policy Targets
2		WebServer	Any	Any	http https icmp-proto	Accept	Log	Policy Targets
3	Cleanup rule	Any	Any	Any	Any	Drop	None	Policy Targets



Cluster_external

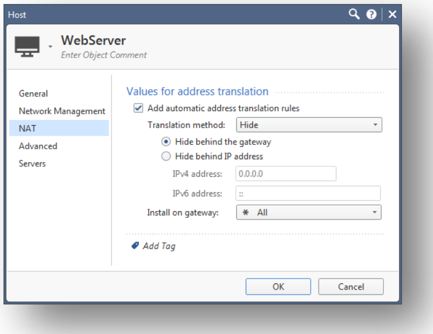
IP Address: 10.0.0.10



WebServer

IP Address: 10.0.1.5

NAT Hide WebServer behind cluster



Host

WebServer

Enter Object Comment

Values for address translation

☑ Add automatic address translation rules

Translation method: Hide

● Hide behind the gateway

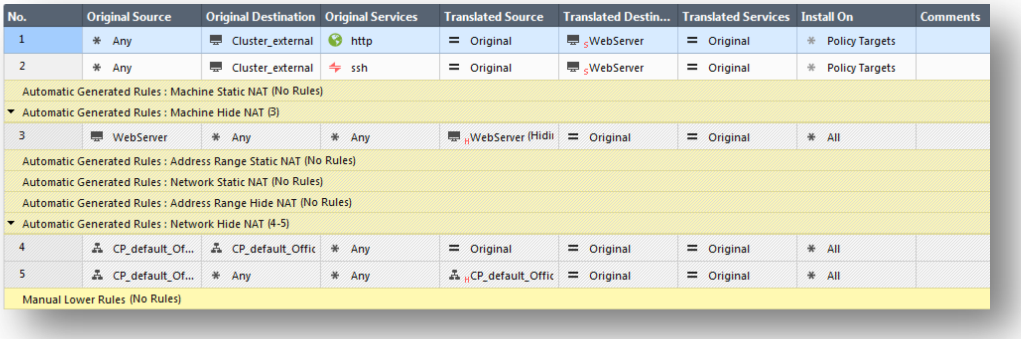
○ Hide behind IP address

IPv4 address: 0.0.0.0

IPv6 address: ::

Install on gateway: * All

NAT anyone accessing cluster external IP on ssh or http to WebServer

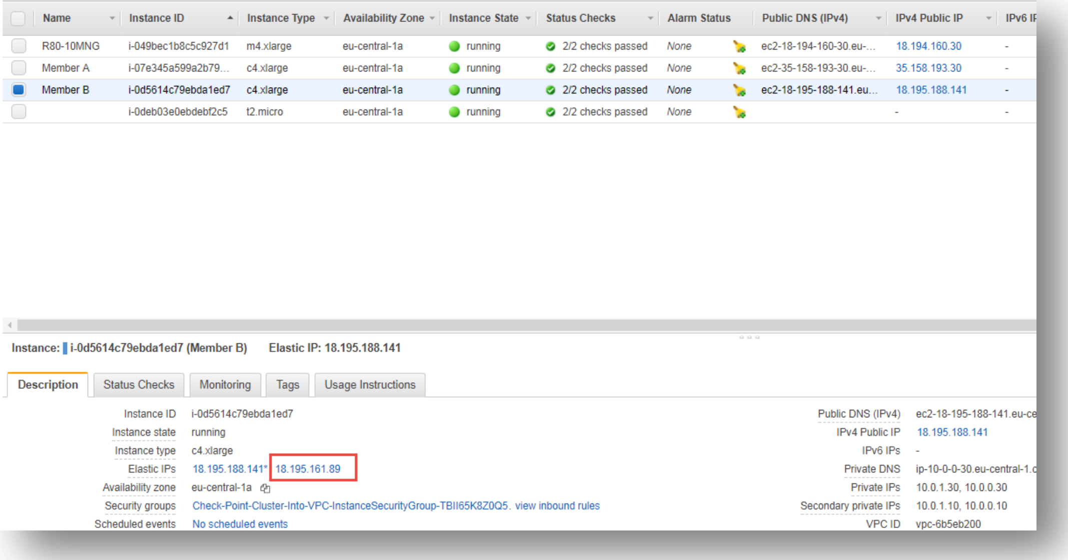


No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On	Comments
1	* Any	Cluster_external	http	= Original	S WebServer	= Original	* Policy Targets	
2	* Any	Cluster_external	ssh	= Original	S WebServer	= Original	* Policy Targets	
Automatic Generated Rules : Machine Static NAT (No Rules)								
Automatic Generated Rules : Machine Hide NAT (3)								
3	WebServer	* Any	* Any	H WebServer (Hidi	= Original	= Original	* All	
Automatic Generated Rules : Address Range Static NAT (No Rules)								
Automatic Generated Rules : Network Static NAT (No Rules)								
Automatic Generated Rules : Address Range Hide NAT (No Rules)								
Automatic Generated Rules : Network Hide NAT (4-5)								
4	CP_default_Of...	CP_default_Offic	* Any	= Original	= Original	= Original	* All	
5	CP_default_Of...	* Any	* Any	H CP_default_Offic	= Original	= Original	* All	
Manual Lower Rules (No Rules)								

3. Install the policy

Test your environment

4. To test that your Web server is accessible from Internet, browse to the cluster public VIP address
TIP: In EC2 / Instances. The active member holds the cluster public VIP address. The cluster public VIP address is the one without a star

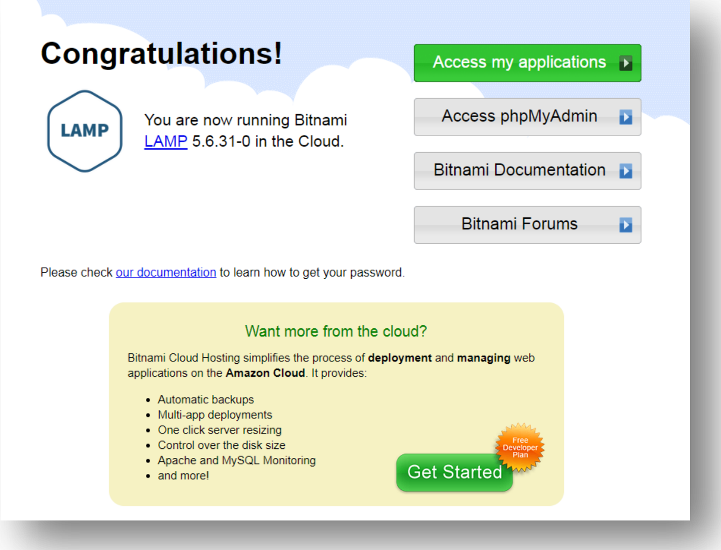


☐	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IP
☐	R80-10MNG	i-049bec1b8c5c927d1	m4.xlarge	eu-central-1a	● running	✓ 2/2 checks passed	*None*	ec2-18-194-160-30.eu-...	18.194.160.30	-
☐	Member A	i-07e345a599a2b79...	c4.xlarge	eu-central-1a	● running	✓ 2/2 checks passed	*None*	ec2-35-158-193-30.eu-...	35.158.193.30	-
■	Member B	i-0d5614c79ebda1ed7	c4.xlarge	eu-central-1a	● running	✓ 2/2 checks passed	*None*	ec2-18-195-188-141.eu...	18.195.188.141	-
☐		i-0deb03e0ebdebf2c5	t2.micro	eu-central-1a	● running	✓ 2/2 checks passed	*None*		-	-

Instance: i-0d5614c79ebda1ed7 (Member B) **Elastic IP: 18.195.188.141**

Instance ID	i-0d5614c79ebda1ed7	Public DNS (IPv4)	ec2-18-195-188-141.eu-ce
Instance state	running	IPv4 Public IP	18.195.188.141
Instance type	c4.xlarge	IPv6 IPs	-
Elastic IPs	18.195.188.141* 18.195.161.89	Private DNS	ip-10-0-0-30.eu-central-1.c
Availability zone	eu-central-1a	Private IPs	10.0.1.30, 10.0.0.30
Security groups	Check-Point-Cluster-Into-VPC-InstanceSecurityGroup-TBII65K8Z0Q5. view inbound rules	Secondary private IPs	10.0.1.10, 10.0.0.10
Scheduled events	No scheduled events	VPC ID	vpc-6b5eb200

5. Success!!



Congratulations!

You are now running Bitnami LAMP 5.6.31-0 in the Cloud.

Please check our documentation to learn how to get your password.

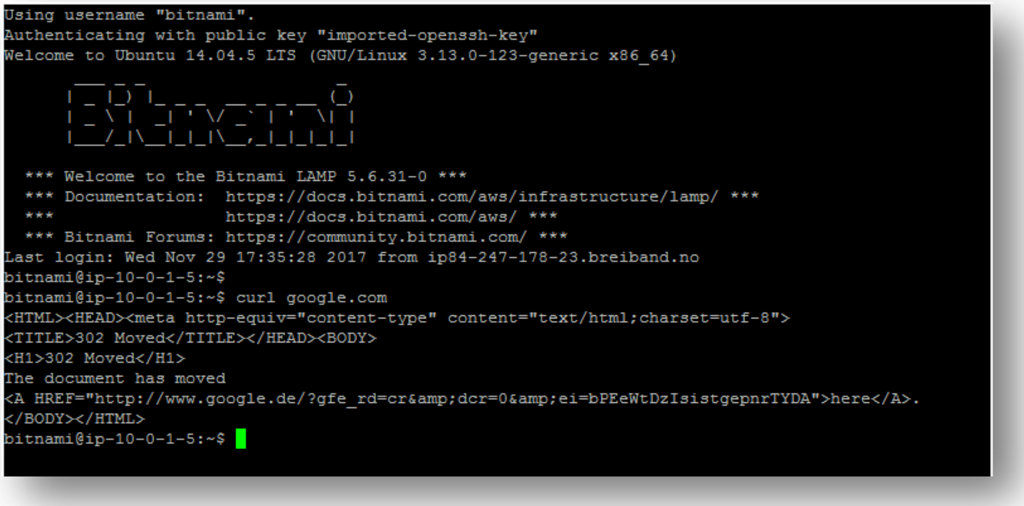
Want more from the cloud?

Bitnami Cloud Hosting simplifies the process of **deployment** and **managing** web applications on the **Amazon Cloud**. It provides:

- Automatic backups
- Multi-app deployments
- One click server resizing
- Control over the disk size
- Apache and MySQL Monitoring
- and more!

6. Review logs

7. To test outgoing communication, SSH to cluster public VIP address with the key we created before (username: bitnami).
And generate some traffic. Ie. “curl google.com”



```
Using username "bitnami".
Authenticating with public key "imported-openssh-key"
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 3.13.0-123-generic x86_64)
       ___ _ _                   _
      | _ |_) |_ _ _  __ _ _ __ (_)
      | _ \ |  _| ' \/ _` | '  \| |
      |___/_|\__|_|_|\__,_|_|_|_|_|

  *** Welcome to the Bitnami LAMP 5.6.31-0 ***
  *** Documentation:  https://docs.bitnami.com/aws/infrastructure/lamp/ ***
  ***                 https://docs.bitnami.com/aws/ ***
  *** Bitnami Forums: https://community.bitnami.com/ ***
Last login: Wed Nov 29 17:35:28 2017 from ip84-247-178-23.breiband.no
bitnami@ip-10-0-1-5:~$
bitnami@ip-10-0-1-5:~$ curl google.com
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="http://www.google.de/?gfe_rd=cr&amp;dcr=0&amp;ei=bPEeWtDzIsistgepnrTYDA">here</A>.
</BODY></HTML>
bitnami@ip-10-0-1-5:~$
```

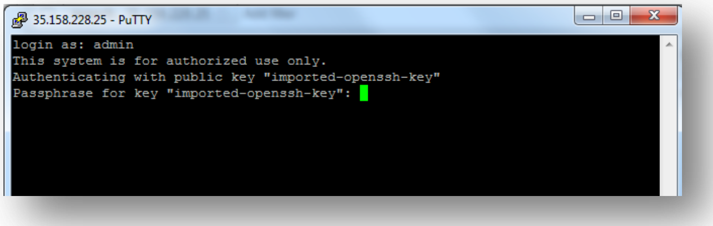
You successfully finished Exercise #3

Exercise #4 – Configuring the vSEC Controller

Purpose: To configure vSEC Controller trust to AWS account

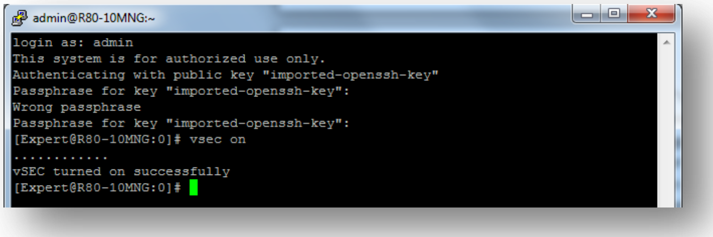
Enable vSEC Controller

1. Open an SSH session to the Management server using your predefined Key (for example you may use Putty):



```
login as: admin
This system is for authorized use only.
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
```

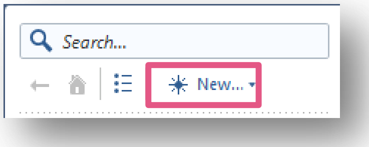
2. Run command vsec on



```
login as: admin
This system is for authorized use only.
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
Wrong passphrase
Passphrase for key "imported-openssh-key":
[Expert@R80-10MNG:0]# vsec on
...........
vSEC turned on successfully
[Expert@R80-10MNG:0]#
```

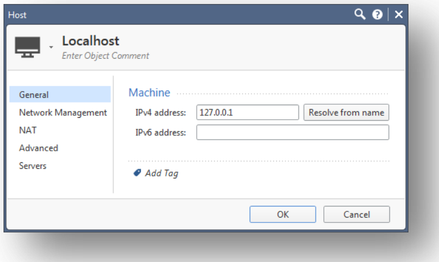
Enable Identity Awareness Web API

3. In Check Point SmartConsole, on the upper right section choose New object



4. Choose "Host…"

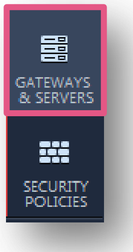
5. Create a new host object with the following parameters:



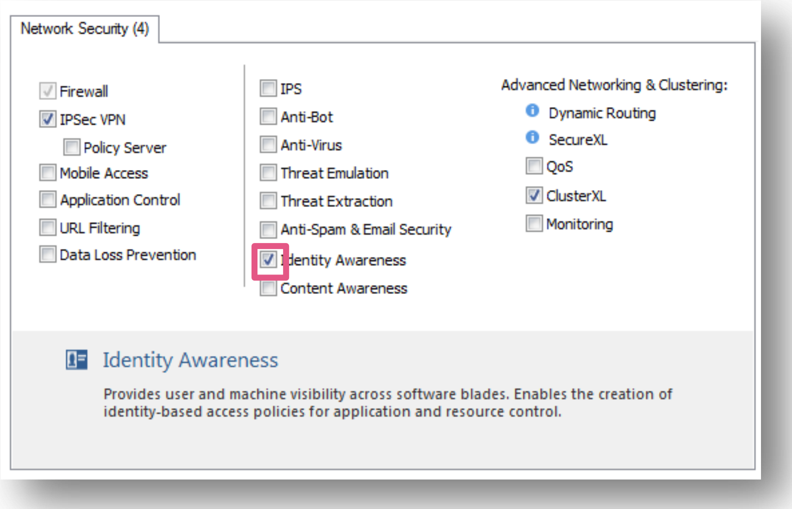
Localhost
Enter Object Comment
IPv4 address: 127.0.0.1
IPv6 address:

Name: Localhost
IPv4 address: 127.0.0.1
Click "OK"

6. At the left bar choose GATEWAYS & SERVERS



7. Double-click the cluster object and 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

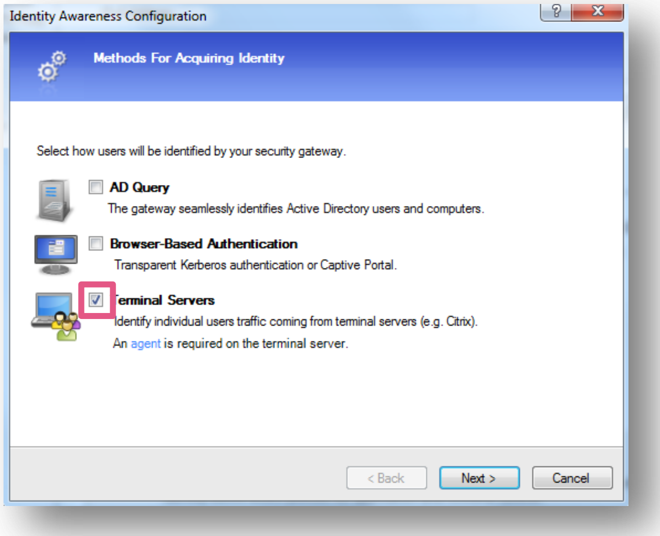
□ IPS
□ Anti-Bot
□ Anti-Virus
□ Threat Emulation
□ Threat Extraction
□ Anti-Spam & Email Security
☑ Identity Awareness
□ Content Awareness

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.

8. A window will be open, select the Terminal Servers and uncheck the AD Query, Click "Next"


Identity Awareness Configuration

Methods For Acquiring Identity

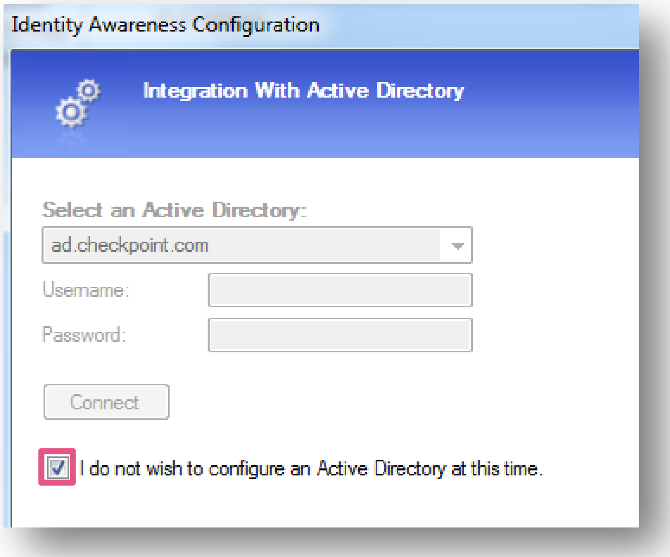
Select how users will be identified by your security gateway.

□ **AD Query**
The gateway seamlessly identifies Active Directory users and computers.

□ **Browser-Based Authentication**
Transparent Kerberos authentication or Captive Portal.

☑ **Terminal Servers**
Identify individual users traffic coming from terminal servers (e.g. Citrix).
An agent is required on the terminal server.

9. Select the option: “I do not wish to configure an Active Directory at this time” and then click “Next” -> “Finish”



Identity Awareness Configuration

Integration With Active Directory

Select an Active Directory: ad.checkpoint.com

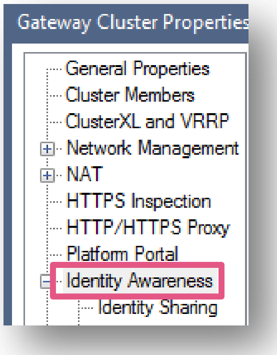
Username:

Password:

Connect

☑ I do not wish to configure an Active Directory at this time.

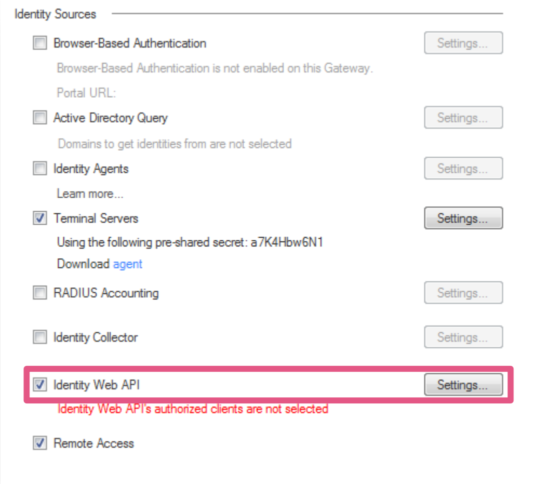
10. Move into the Identity Awareness section



Gateway Cluster Properties

- General Properties
- Cluster Members
- ClusterXL and VRRP
- Network Management
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- Platform Portal
- Identity Awareness
  - Identity Sharing

11. Uncheck Terminal Servers, check Identity Web API and click “Settings”



Identity Sources

☐ Browser-Based Authentication — Settings...

Browser-Based Authentication is not enabled on this Gateway.

Portal URL:

☐ Active Directory Query — Settings...

Domains to get identities from are not selected

☐ Identity Agents — Settings...

Learn more...

☑ Terminal Servers — Settings...

Using the following pre-shared secret: a7K4Hbw6N1

Download agent

☐ RADIUS Accounting — Settings...

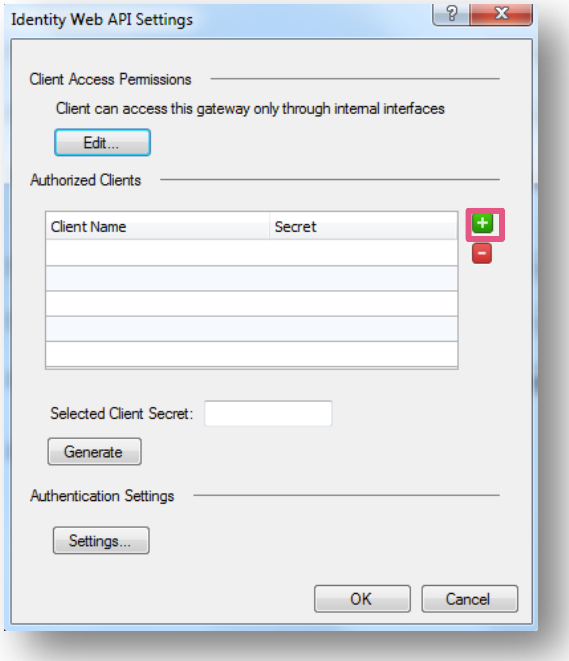
☐ Identity Collector — Settings...

☑ Identity Web API — Settings...

Identity Web API's authorized clients are not selected

☑ Remote Access

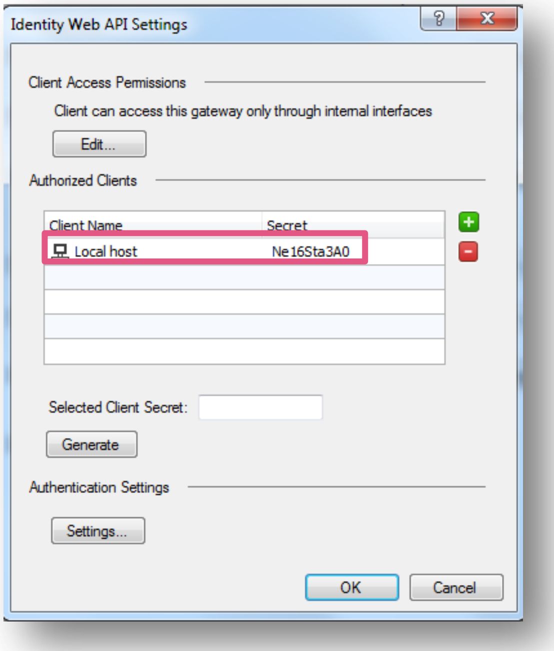
12. On the new window, click the green + sign on the right



Client can access this gateway only through internal interfaces

Client Name	Secret

13. Choose the Localhost object



Client can access this gateway only through internal interfaces

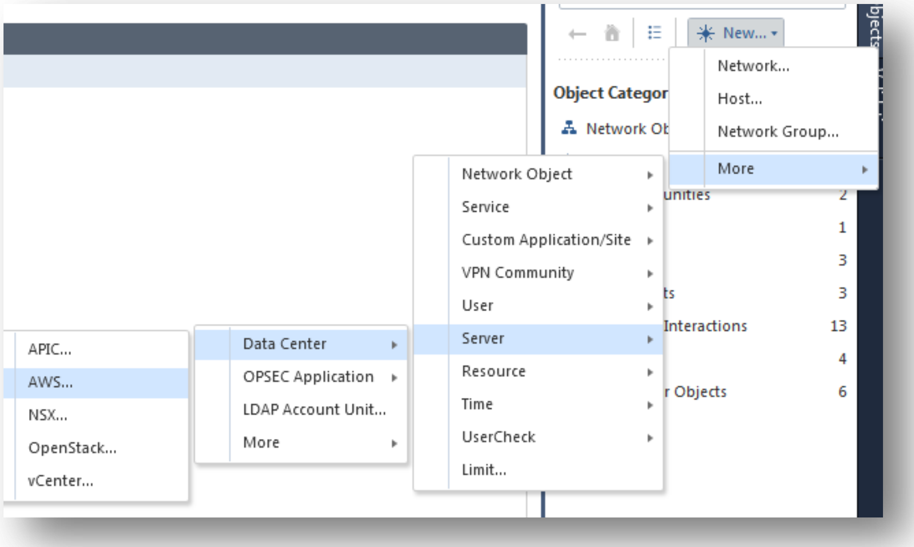
Client Name	Secret
Local host	Ne16Sta3A0

14. Click "OK" twice

15. A message will popup, click "Yes"

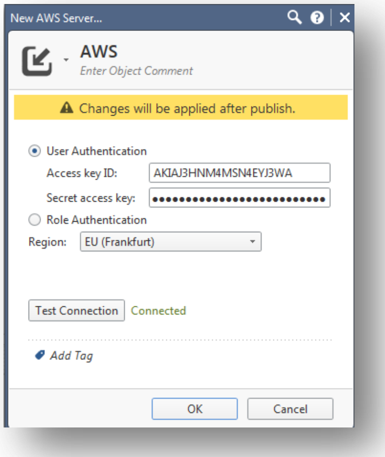
Connect vSEC Controller to AWS

16. Now we will create the trusted connection between the vSEC Controller and the AWS account In SmartConsole, create a new server object. "More -> Server -> Data Center - > AWS…"



17. Choose a name for the new object
    Configure credentials for the AWS server using Access Key and Secret Key (you got these in the email when the On Demand Lab session was started was started). If you don't use the On Demand Lab training accounts, see Appendix #2 below, to create your own keys.
    Choose the AWS region where your environment operates

    Click "Test Connection", and it should say "Connected"


New AWS Server...

AWS
Enter Object Comment

Changes will be applied after publish.

● User Authentication
Access key ID: AKIAJ3HNM4MSN4EYJ3WA
Secret access key: ••••••••••••••••••••••••••
○ Role Authentication
Region: EU (Frankfurt)

Test Connection Connected

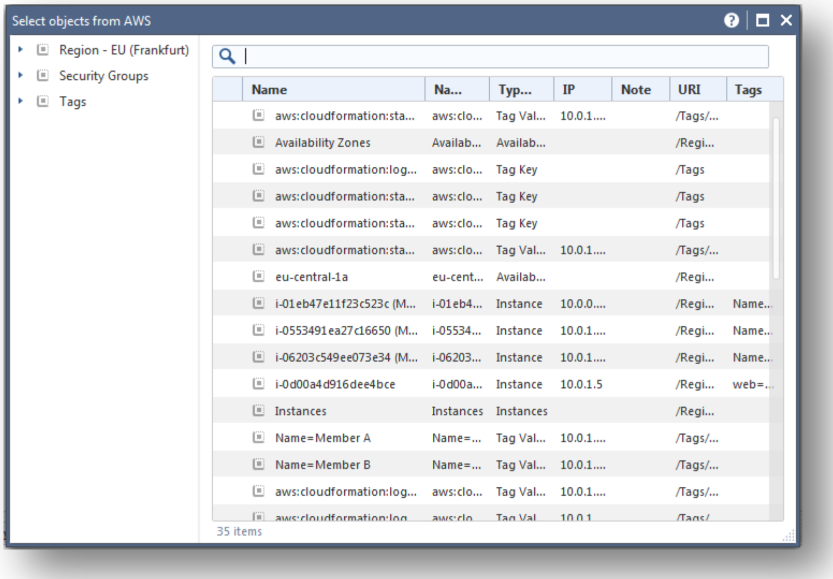
Add Tag

OK Cancel

18. Install the policy

Verify vSEC Controller

1. Import the WebServer object from the created AWS Server to your policy using the Import option (look for 3 ways for doing that)



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 AWS VPCs, Subnets or Instances to your Security Policy.

b) **Tags view** to import all instances that have specific Tag Key or to import all instances that have specific Tag Key with a specific value.

c) Search view to import the object directly

<u>You successfully finished Exercise #4</u>

Exercise #5 – 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. Verify that the script in charge of communicating with AWS is running on each cluster member.

   [Expert@HostName]# cpwd_admin list | grep -E "PID|AWS_HAD"

   The output should have a line similar to:

   ```
   APP         PID    STAT  #START  START_TIME             MON  COMMAND
   AWS_HAD     3663   E     1       [12:58:48] 15/1/2015   N    python
   /opt/CPsuite-R77/fw1/scripts/aws_had.py
   ```

2. Connect to the one of the Gateways via SSH & run a script to check that the definitions of the cluster are properly configured:
   [Expert@HostName]# cd $FWDIR/scripts/
   [Expert@HostName]# $FWDIR/Python/bin/python -m aws_ha_test

   If all tests were successful, the script should output:
   All tests were successful!
   Otherwise, an error message is displayed that should help you troubleshoot the problem.

3. Verify that the cluster members are communicating properly: ***cphaprob state***
   Example:

   ```
   [Expert@HostName:0]# cphaprob state

   Cluster Mode:   High Availability (Active Up) with IGMP Membership
   Number      Unique Address  Assigned Load   State
   1 (local)   10.0.1.20       0%              Active
   2           10.0.1.30       100%            Standby
   ```

4. Initiate "fw monitor" on the active cluster node and inspect traffic traversing the cluster. Look at sk30583 for "fw monitor" usage

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

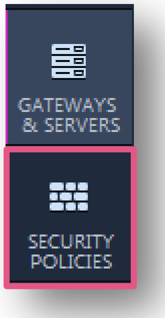
6. Initiate a cluster Failover in one of the following ways
   a. Initiate "**clusterXL_admin down**" command (don't forget to set it up again when done, by replacing "down" with up")
   b. "ifdown" one of the interfaces on the active member (don't forget to up it by replacing "ifdown" with "ifup" when done"
   c. Reboot active member

   Review the route table for the Private subnet and which member holds the VIP's before and after a failover. Noticed the change?

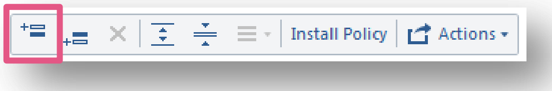
   Make sure test web site is still accessible after failover

Appendix #1: Check Point policy

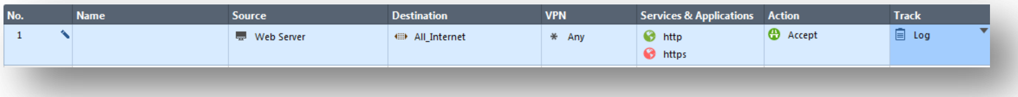
1. In the Check Point SmartConsole GUI, on the left bar choose SECURITY POLICIES



2. Create a new rule by clicking the “Add rule above” icon from the upper middle bar

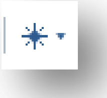


3. This rule will allow http traffic from the Web server to the internet .
   Fill in the relevant fields:

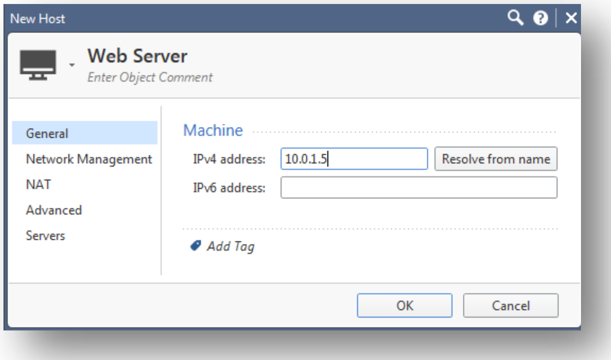


No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1		Web Server	All_Internet	Any	http https	Accept	Log

s. Source: (click on the + sign, choose new -> Host)



Name: Web Server
IPv4 Address: 10.0.1.5



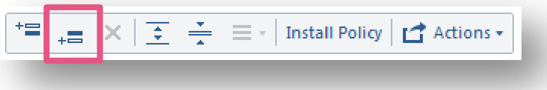
Web Server
Enter Object Comment

IPv4 address: 10.0.1.5
IPv6 address:

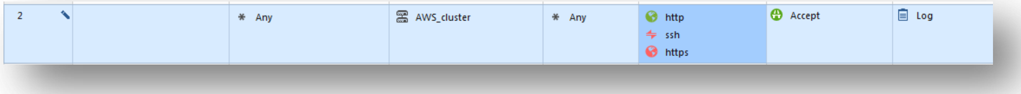
Click OK.

t. Destination: (click on the + sign) choose “All_Internet”
u. Services & Applications: (click on the + sign) search for HTTP and HTTPS
v. Action: Allow
w. Track: Log

4. Mark the newly created rule and create a new rule by choosing the Add rule below from the upper middle bar



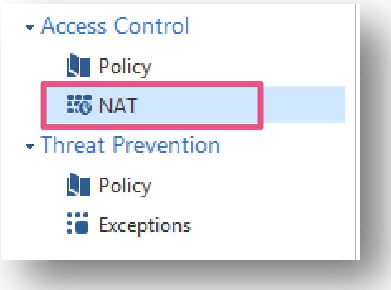
5. This rule will allow traffic from the internet into the Web server (in order to allow access into the web server, Fill in the relevant fields:



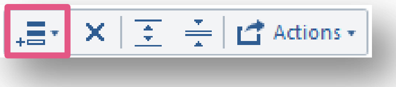
2		Any	AWS_cluster	Any	http ssh https	Accept	Log

x. Source: Leave “Any”
y. Destination: (click on the + sign) choose “AWS_cluster”
z. Services & Applications: (click on the + sign) search for HTTP, HTTPS and SSH
aa. Action: Allow
bb. Track: Log

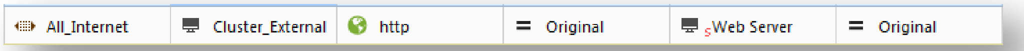
6. Change into the NAT section,



7. The next step will add a NAT rule (the first rule) that translate the IP of the cluster into the Web server. Choose “Add rule to top” from the upper middle bar

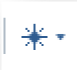


8. Fill in the relevant fields:

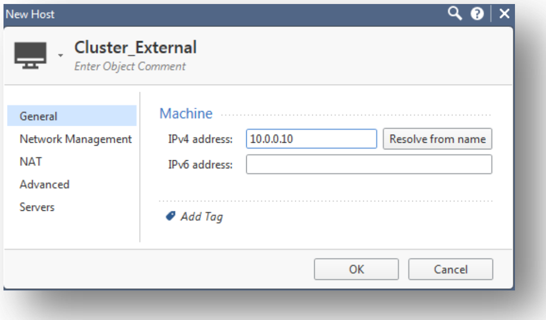


All_Internet	Cluster_External	http	= Original	Web Server	= Original

cc. Original Source: Leave “All_Internet”
dd. Original Destination: (click on the + sign)



Name: Cluster_External
IPv4 Address: 10.0.0.10



New Host

Cluster_External
Enter Object Comment

General
Network Management
NAT
Advanced
Servers

Machine

IPv4 address: 10.0.0.10 | Resolve from name
IPv6 address:

Add Tag

OK | Cancel

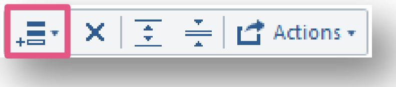
Click OK.

ee. Services & Applications: (click on the + sign) search for HTTP

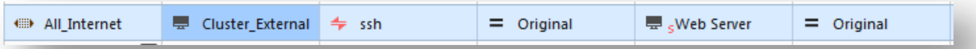
ff. Translated Source: Original

gg. Translated Destination: (click on the + sign) choose “Web server”

9. Mark the newly created rule, Choose the Add rule below from the upper middle bar



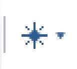
10. Fill in the relevant fields:



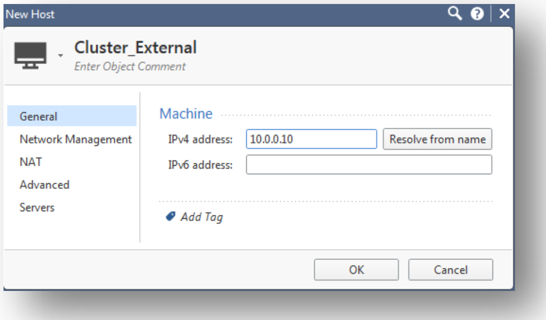
All_Internet	Cluster_External	ssh	= Original	Web Server	= Original

hh. Original Source: Leave “All_Internet”

ii. Original Destination: (click on the + sign)



Name: Cluster_External
IPv4 Address: 10.0.0.10



New Host

Cluster_External

Enter Object Comment

Machine

IPv4 address: 10.0.0.10

IPv6 address:

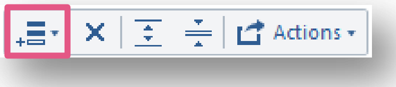
Click OK.

jj. Services & Applications: (click on the + sign) search for SSH

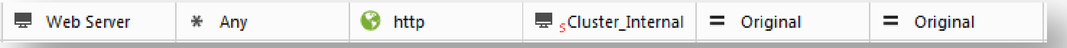
kk. Translated Source: Original

ll. Translated Destination: (click on the + sign) choose “Web server”

11. Mark the newly created rule, Choose the Add rule Above from the upper middle bar



12. Fill in the relevant fields:



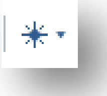
Web Server	Any	http	Cluster_Internal	Original	Original

mm. Original Source: Leave “Web Server”

nn. Original Destination: Any

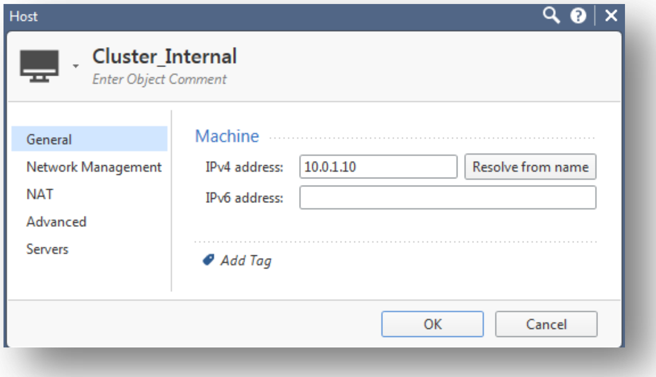
oo. Services & Applications: (click on the + sign) search for HTTP

pp. Translated Source: (click on the + sign)



Name: Cluster_Internal

IPv4 Address: 10.0.1.10



Host

Cluster_Internal

Enter Object Comment

Machine

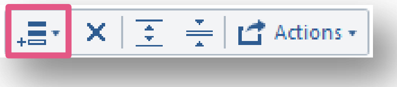
IPv4 address: 10.0.1.10

IPv6 address:

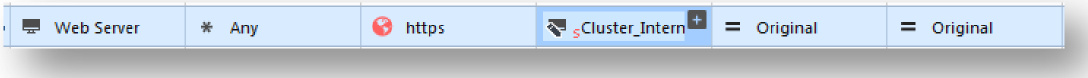
Click OK.

qq. Translated Destination: Original

13. Mark the newly created rule, Choose the Add rule below from the upper middle bar



14. Fill in the relevant fields:



rr. Original Source: Leave "Web Server"

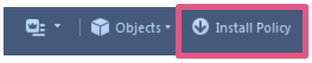
ss. Original Destination: Any

tt. Services & Applications: (click on the + sign) search for HTTPS

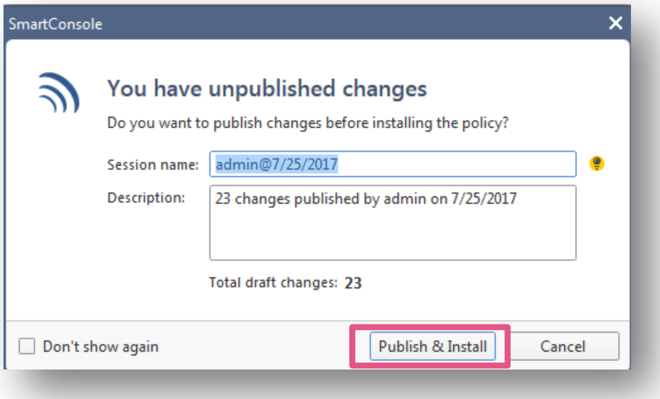
uu. Translated Source: Cluster_Inetrnal

vv. Translated Destination: Original

15. On the upper left side click "Install Policy"



16. Click the "Publish & Install"



SmartConsole

You have unpublished changes

Do you want to publish changes before installing the policy?

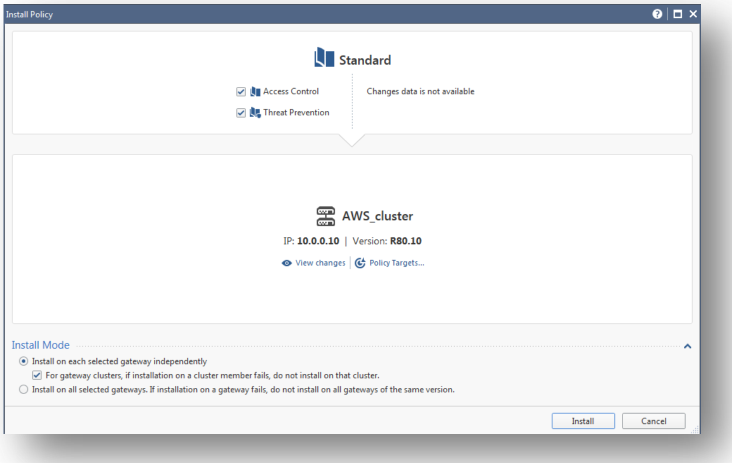
Session name: admin@7/25/2017

Description: 23 changes published by admin on 7/25/2017

Total draft changes: 23

□ Don't show again

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



Install Policy

Standard

☑ Access Control

☑ Threat Prevention

Changes data is not available

AWS_cluster

IP: **10.0.0.10** | Version: **R80.10**

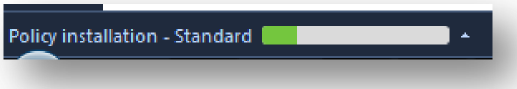
Install Mode

● Install on each selected gateway independently

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

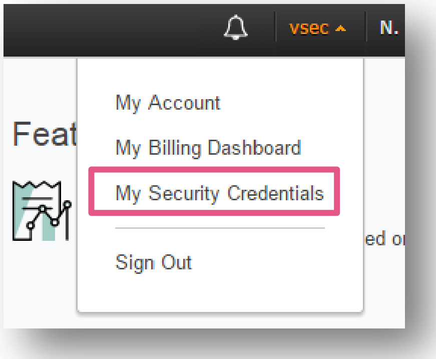
○ Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.

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

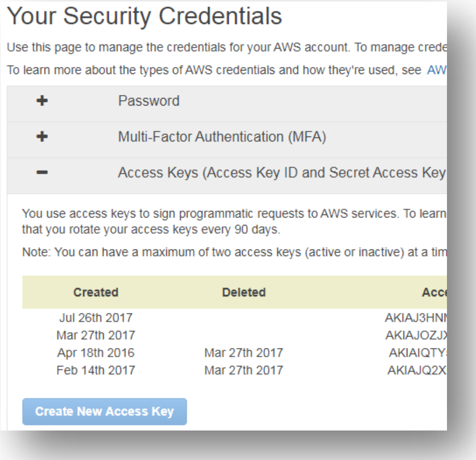


Appendix #2: vSEC Controller Access key generation

1. Go to the AWS console. On the upper right side under the user name choose My Security credentials.



2. Expend the Access Keys section by pressing the + sign



Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage crede

To learn more about the types of AWS credentials and how they're used, see AW

+ Password
+ Multi-Factor Authentication (MFA)
− Access Keys (Access Key ID and Secret Access Key

You use access keys to sign programmatic requests to AWS services. To learn that you rotate your access keys every 90 days.

Note: You can have a maximum of two access keys (active or inactive) at a tim

Created	Deleted	Acce
Jul 26th 2017		AKIAJ3HNI
Mar 27th 2017		AKIAJOZJX
Apr 18th 2016	Mar 27th 2017	AKIAIQTY
Feb 14th 2017	Mar 27th 2017	AKIAJQ2X

3. Choose Create New access Key. Copy the newly created keys into a safe place since you can't review the Secret Access Key once you leave this screen.

4. Click "Close"

Answers to the tricks:

1. If the deployment of the cluster fails, you need to go and approve the EULA for the gateway in the marketplace first. Search in the marketplace for Check Point vSEC & run through the installation process until you start to deploy. Then you can kill the installation. Then rerun the cloud formation template again.

   Easy way!
   Browse to https://aws.amazon.com/marketplace/pp/B071GRKY38?ref=cns_srchrow
   Click “Continue”, “Manual Launch” and then “Accept Software Terms”

2. If your password does not work at the Gaia portal, connect to the management server via SSH & run command: set user admin password, this will reset the password for the Gaia portal.