

# CheckPoint CloudGuard PaaS Solution for Application Services in Azure

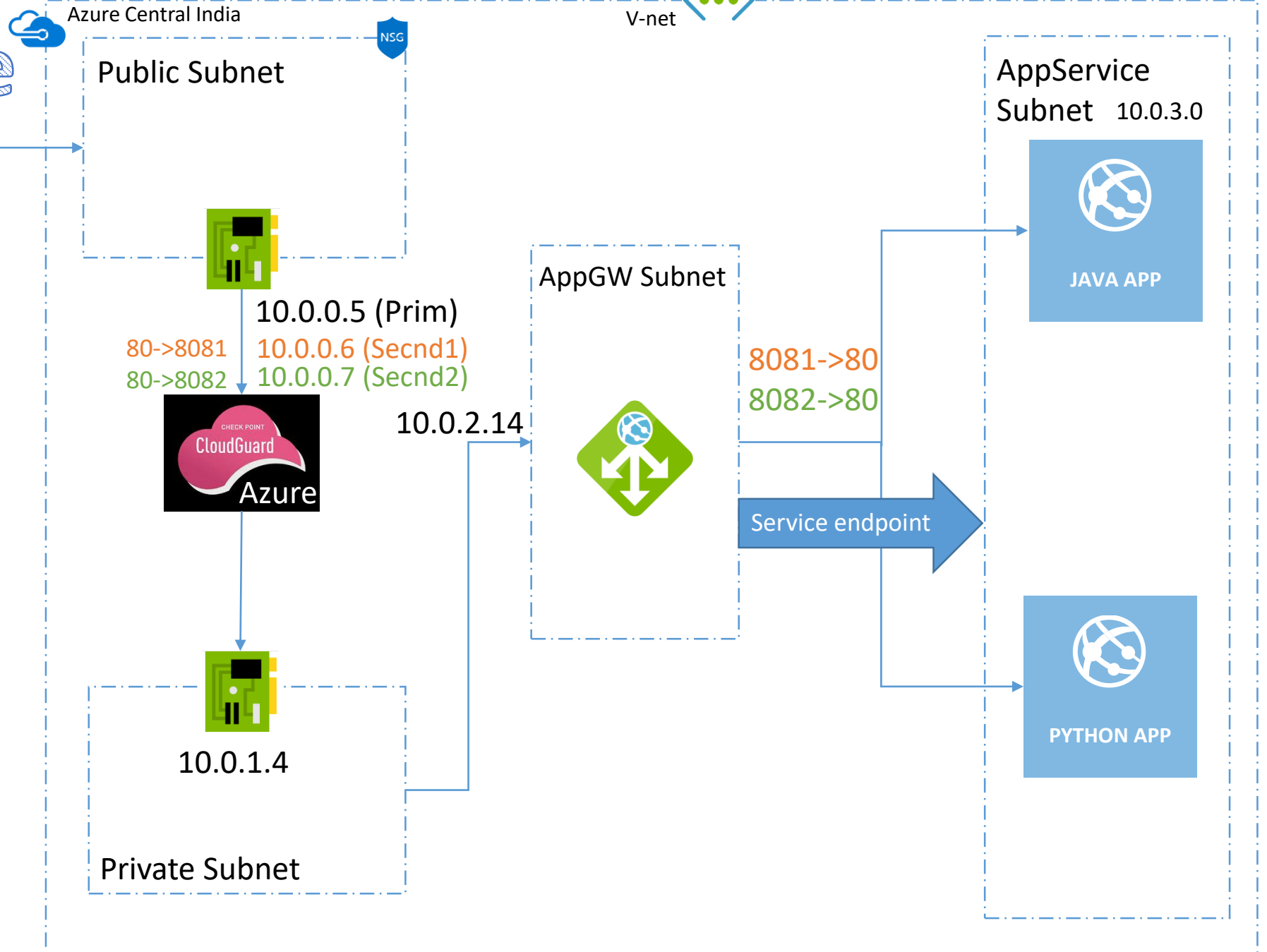


Solution found by:-  
Shalini Vishwakarma  
Amarpreet Singh

# Architecture

1.137.135.188.114  
2.137.135.253.55

Internet Users



# Log into Microsoft Azure cloud portal



- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

Home > Virtual networks

### Virtual networks

Check Point Software Technologies Inc.

+ Add Edit columns Refresh Assign tags

**Subscriptions:** Checkpoint HOL - A

Filter by name... ODL-checkpointtemplate-93364-02 All locations All tags No grouping

1 items

| NAME ↑↓                          | RESOURCE GROUP ↑↓ | LOCATION ↑↓  | SUBSCRIPTION ↑↓ |
|----------------------------------|-------------------|--------------|-----------------|
| <input type="checkbox"/> IL-Vnet |                   | North Europe |                 |

IL-Vnet - Subnets - Microsoft Azure

Virtual networks - Microsoft Azure

Application Gateways - Microsoft

Microsoft Azure App Service - W

Microsoft Azure App Service - W

portal.azure.com/#@checkpointhol.onmicrosoft.com/resource/subscriptions/b6eaffbd-acb0-4a6f-9ad7-479857225905/resourceGroups/ODL-checkpointtemplate-93364-02/providers/Microsoft...

Microsoft Azure

Search resources, services, and docs (G+)

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Security Center

Cost Management + Billing

Help + support

Home > Virtual networks > IL-Vnet - Subnets

IL-Vnet - Subnets

Virtual network

Search (Ctrl+)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peerings

Service endpoints

Properties

Locks

Export template

Monitoring

Diagnostics settings

+ Subnet + Gateway subnet

Search subnets

| NAME       | ADDRESS RANGE | IPV4 AVAILABLE ADDRESSES | DELEGATED TO | SECURITY GROUP |
|------------|---------------|--------------------------|--------------|----------------|
| Frontend   | 10.0.0.0/24   | 247                      | -            | -              |
| Backend    | 10.0.1.0/24   | 250                      | -            | -              |
| AppGW      | 10.0.2.0/24   | 249                      | -            | -              |
| AppService | 10.0.3.0/24   | 251                      | -            | -              |

Type here to search

11:33 26-09-2019



IL-Vnet - Microsoft Azure

Virtual networks - Microsoft Azure

Application Gateways - Microsoft Azure

Microsoft Azure App Service - Windows

Microsoft Azure App Service - Windows

portal.azure.com/#@checkpointhol.onmicrosoft.com/resource/subscriptions/b6eaffbd-acb0-4a6f-9ad7-479857225905/resourceGroups/ODL-checkpointtemplate-93364-02/providers/Microsoft...

Microsoft Azure

Search resources, services, and docs (G+)

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Security Center

Cost Management + Billing

Help + support

IL-Vnet

Virtual network

Search (Ctrl+)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peerings

Service endpoints

Properties

Locks

Export template

Monitoring

Diagnostics settings

Refresh

Move

Delete

Resource group (change)

Address space : 10.0.0.0/16

Location : North Europe

DNS servers : Azure provided DNS service

Subscription (change)

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

Tags (change) : [Click here to add tags](#)

Connected devices

Search connected devices

| DEVICE               | TYPE                | IP ADDRESS | SUBNET   |
|----------------------|---------------------|------------|----------|
| CPMgmt-eth0          | Network interface   | 10.0.0.4   | Frontend |
| CPSingleGateway-eth0 | Network interface   | 10.0.0.5   | Frontend |
| CPSingleGateway-eth0 | Network interface   | 10.0.0.7   | Frontend |
| CPSingleGateway-eth0 | Network interface   | 10.0.0.6   | Frontend |
| CPSingleGateway-eth1 | Network interface   | 10.0.1.4   | Backend  |
| ILAppGW              | Application Gateway | 10.0.2.14  | AppGW    |

Type here to search

11:34 26-09-2019

# **Creating Application Services(Web App) and configuring it.**







- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

Home > App Services > ILAppJava - Networking

ILAppJava - Networking  
App Service

Search (Ctrl+/)

Settings

- Configuration
- Authentication / Authorizati...
- Application Insights
- Identity
- Backups
- Custom domains
- TLS/SSL settings
- Networking
- Scale up (App Service plan)
- Scale out (App Service plan)
- WebJobs
- Push
- MySQL In App
- Properties
- Locks
- Export template

App Service plan

- App Service plan
- Quotas
- Change App Service plan

VNet Integration

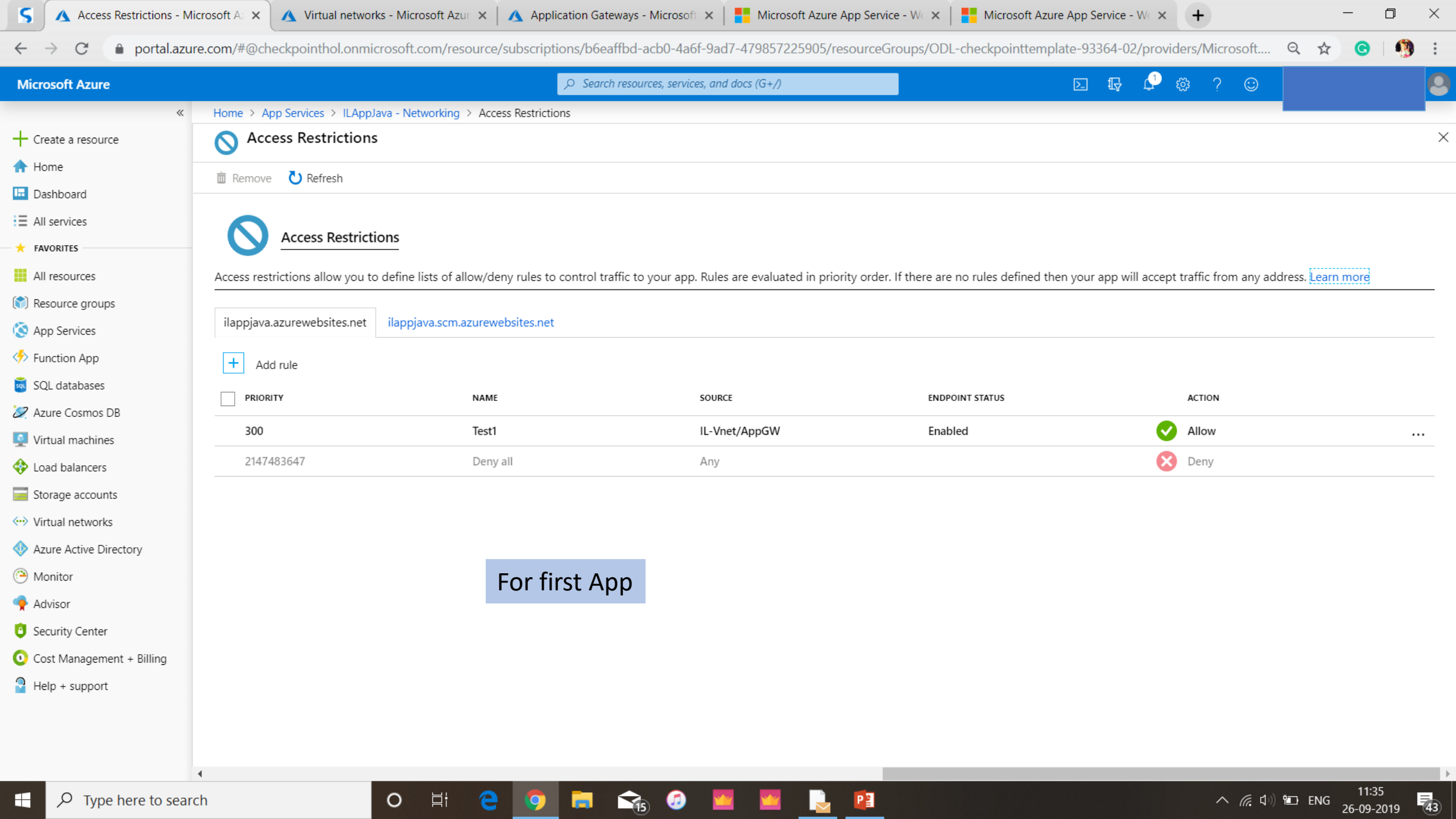
- Securely access resources available in or through your Azure VNet.  
[Learn More](#)  
[Click here to configure](#)

Azure CDN

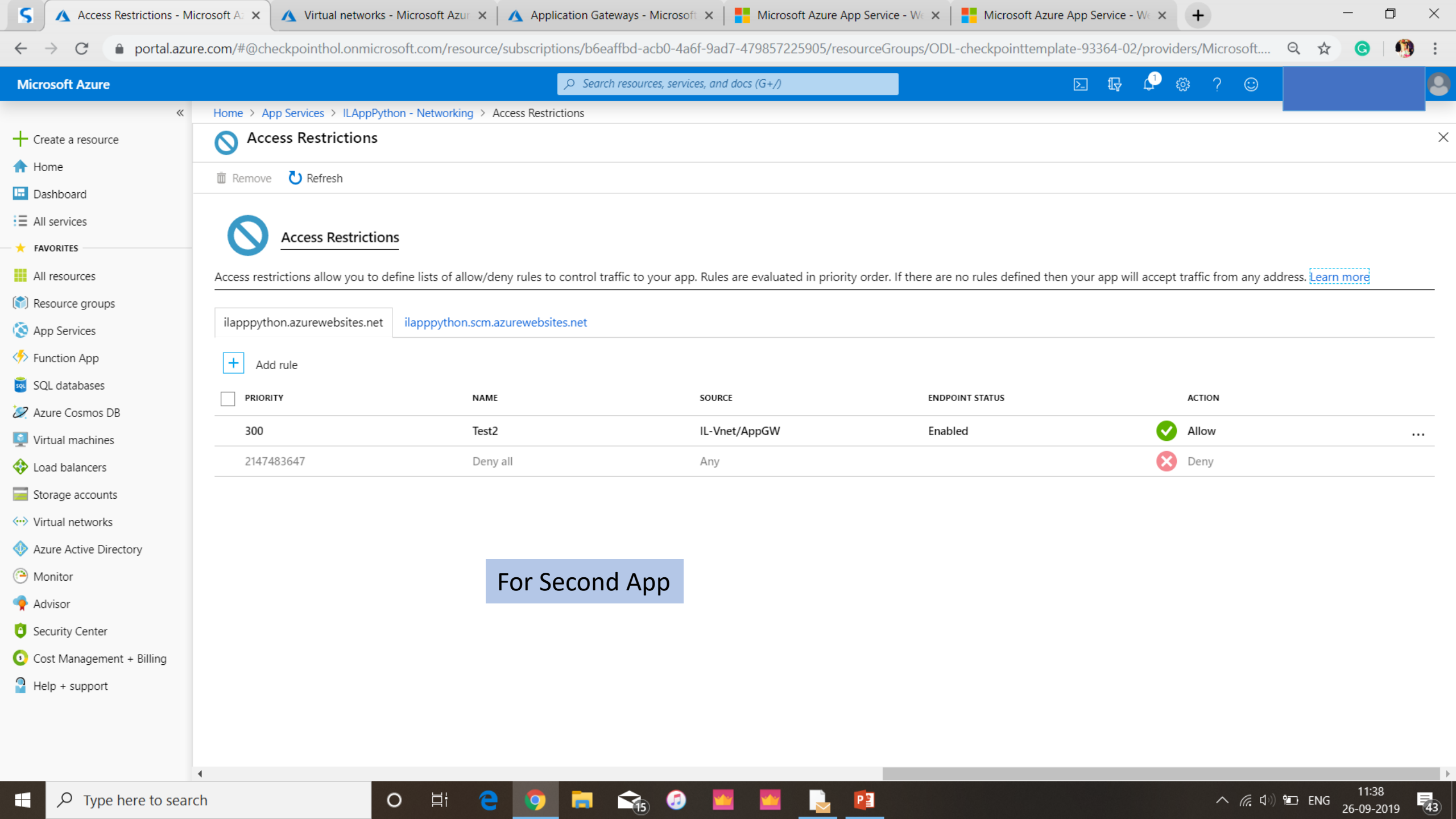
- Secure, reliable content delivery with broad global reach and rich feature set  
[Learn More](#)  
[Configure Azure CDN for your app](#)

Access Restrictions

- Define and manage rules that control access to your application.  
[Learn More](#)  
[Configure Access Restrictions](#)



For first App



For Second App

For the third app (testing-app-IL)  
Do not perform access restriction configuration  
as this app is just to show that this app is directly accessible to internet via app's URL

Home > App Services

### App Services

Check Point Software Technologies Inc.

+ Add Edit columns Refresh Assign tags Start Restart Stop Delete

Subscriptions: Checkpoint HOL - A

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

3 items

| NAME           | STATUS  | APP TYPE | APP SERVICE PLAN | LOCATION     | SUBSCRIPTION       |
|----------------|---------|----------|------------------|--------------|--------------------|
| ILAppJava      | Running | Web App  | A [redacted]     | North Europe | Checkpoint HOL - A |
| ILAppPython    | Running | Web App  | A [redacted]     | North Europe | Checkpoint HOL - A |
| testing-app-IL | Running | Web App  | A [redacted]     | North Europe | Checkpoint HOL - A |

testing-app-IL  
App Service

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Security

Browse Stop Swap Restart Delete Get publish profile Reset publish profile

Click here to access our Quickstart guide for deploying code to your app →

Resource group (change) : [redacted]

Status : Running

Location : North Europe

Subscription (change) : [redacted]

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

Tags (change) : Click here to add tags

URL : <https://testing-app-il.azurewebsites.net>

App Service Plan : ASP-ODLcheckpointtemplate9336401-8712 (S1: 1)

FTP/deployment userna... : No FTP/deployment user set

FTP hostname : ftp://waws-prod-db3-137.ftp.azurewebsites.windows.net

FTPS hostname : ftps://waws-prod-db3-137.ftp.azurewebsites.windows.net



# Deploying CheckPoint CloudGuard Security Management & Single Gateway



- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

Home > New > CloudGuard IaaS - Firewall & Threat Prevention

## CloudGuard IaaS - Firewall & Threat Prevention

Check Point



### CloudGuard IaaS - Firewall & Threat Prevention

Check Point

Preferred solution

Select a software plan

Check Point Security Management

Create

Overview Plans

Check Point CloudGuard IaaS (formerly vSEC) delivers advanced, multi-layered threat prevention to protect customer assets in Azure from malware and sophisticated threats. As a Microsoft Azure certified solution, CloudGuard IaaS enables you to easily and seamlessly secure your workloads while providing secure connectivity across your cloud and on-premises environments.

Designed for the dynamic security requirements of cloud deployments, CloudGuard IaaS provides advanced threat protections to inspect traffic entering and leaving private subnets of customer VNets. Fully integrated security features include: Firewall, IPS, Application Control, IPsec VPN, Antivirus, Anti-Bot, and SandBlast sandboxing technology.

CloudGuard IaaS integrates with the Azure Security Center, providing the ability to rapidly provision CloudGuard IaaS security gateways in just a few clicks and allowing security alerts from CloudGuard IaaS to be viewed from the Security Center console.

CloudGuard IaaS provides consistent security policy management, enforcement, and reporting.

This solution lets you choose between Bring-Your-Own-License (BYOL) and Pay-As-You-Go (PAYG).

- BYOL comes with a 15 day free trial.
- PAYG comes with a 30 day evaluation license.

Premium Support is included in PAYG. More details can be found at <https://www.checkpoint.com/support-services/support-plans/>. To open a support ticket, you need to have a Check Point User Center account. You can sign up for one at <https://accounts.checkpoint.com>

Note: Check Point's Marketplace App includes 5 different plans. Choose the one that suits you best. If you are unsure, we recommend you start with "Check Point CloudGuard IaaS Single Gateway" or contact Check Point Support (link on the left).

Useful Links

- [Check Point CloudGuard Product Information](#)
- [Check Point Reference Architecture for Azure](#)
- [Check Point Next Generation Threat Prevention - NGTP & NGTX](#)

Go to create a resource on the left hand pane side type

- Checkpoint IaaS
- Press Enter
- Choose sec mgmt

Microsoft Azure

Search resources, services, and docs (G+)

Home > New > CloudGuard IaaS - Firewall & Threat Prevention > Create CloudGuard IaaS - Firewall & Threat Prevention > Basics

1 Basics  
Configure basic settings

2 Check Point Security Manag...  
Configure additional settings

3 Network settings  
Configure network settings

4 Summary  
CloudGuard IaaS - Firewall & Thr...

5 Buy

Basics

\* Server Name ⓘ

\* Authentication type  

Password SSH public key

\* Password ⓘ

\* Confirm password

Subscription

\* Resource group ⓘ  

Create new

\* Location  

(Europe) North Europe

OK

Configure according to :-

➤ Your given name and password

➤ Resource group

➤ Location

IMP

Note:-Choose R80.20 for this lab in 2. point

portal.azure.com/#create/hub

Microsoft Azure

Home > New > CloudGuard IaaS - Firewall & Threat Prevention > Create CloudGuard IaaS - Firewall & Threat Prevention > Basics

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Security Center

Cost Management + Billing

Help + support

Basics

\* Server Name ⓘ

\* Authentication type  

Password SSH public key

\* Password ⓘ

\* Confirm password

Subscription

\* Resource group ⓘ  

Create new

\* Location  

(Europe) North Europe

OK

Configure according to :-

➤ Your given name and password

➤ Resource group

➤ Location

IMP

Note:-Choose R80.20 for this lab in 2. point

Type here to search

11:41  
26-09-2019



- Create a resource
- Home
- Dashboard
- All services
- FAVORITES
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Billing
- Help + support

Home > New > CloudGuard IaaS - Firewall & Threat Prevention

## CloudGuard IaaS - Firewall & Threat Prevention

Check Point



### CloudGuard IaaS - Firewall & Threat Prevention

Check Point

Preferred solution

Select a software plan

- Check Point CloudGuard IaaS Single Gat...
- Check Point CloudGuard IaaS R80.10 Cluster
- Check Point CloudGuard IaaS Scale Set
- Check Point CloudGuard IaaS Single Gateway
- Check Point Security Management
- CloudGuard IaaS High Availability

Create

Overview Plans

Check Point CloudGuard IaaS is a multi-layered threat prevention to protect customer assets in Azure from malware and sophisticated threats. As a Microsoft Azure Marketplace solution, it allows you to easily and seamlessly secure your workloads while providing secure connectivity across your cloud and on-premises environments.

Designed for the dynamic security requirements of cloud deployments, CloudGuard IaaS provides advanced threat protections to inspect traffic entering and leaving private subnets of customer VNets. Fully integrated security features include: Firewall, IPS, Application Control, IPsec VPN, Antivirus, Anti-Bot, and SandBlast sandboxing technology.

CloudGuard IaaS integrates with the Azure Security Center, providing the ability to rapidly provision CloudGuard IaaS security gateways in just a few clicks and allowing security alerts from CloudGuard IaaS to be viewed from the Security Center console.

CloudGuard IaaS provides consistent security policy management, enforcement, and reporting.

This solution lets you choose between Bring-Your-Own-License (BYOL) and Pay-As-You-Go (PAYG).

- BYOL comes with a 15 day free trial.
- PAYG comes with a 30 day evaluation license.

Premium Support is included in PAYG. More details can be found at <https://www.checkpoint.com/support-services/support-plans/>. To open a support ticket, you need to have a Check Point User Center account. You can sign up for one at <https://accounts.checkpoint.com>

Note: Check Point's Marketplace App includes 5 different plans. Choose the one that suits you best. If you are unsure, we recommend you start with "Check Point CloudGuard IaaS Single Gateway" or contact Check Point Support (link on the left).

Useful Links

- [Check Point CloudGuard Product Information](#)
- [Check Point Reference Architecture for Azure](#)
- [Check Point Next Generation Threat Prevention - NGTP & NGTX](#)

Go to create a resource on the left hand pane side type

- Checkpoint IaaS
- Press Enter
- Choose single GW

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Security Center

Cost Management + Billing

Help + support

### Create CloudGuard IaaS - Fire...

1 Basics  
Configure basic settings

2 Check Point CloudGuard set...  
Configure CloudGuard settings

3 Network settings  
Configure network settings

4 Summary  
CloudGuard IaaS - Firewall & Thr...

5 Buy

Basics

\* VM Name

\* Authentication type

Password SSH public key

\* Password

\* Confirm password

Subscription

\* Resource group

Create new

\* Location

(Europe) North Europe

OK

Configure according to :-

- Your given name and password
- Resource group
- Location

IMP

Note:-Choose R80.20 for this lab in 2. point

# After the creation of security management & Single GW

## 1. Go to NIC under Settings

CPSingleGateway - Networking

Virtual machine

Search (Ctrl+ /)

«

Attach network interface

Detach network interface

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

CPSingleGateway-eth0

CPSingleGateway-eth1

**Network Interface:** CPSingleGateway-eth0 Effective

Virtual network/subnet: IL-Vnet/Frontend NIC Public IP: 137.

Inbound port rules

Outbound port rules

Application s

This network interface does not contain network security gro

## 2. Go to IP config. Add

CPSingleGateway-eth0 - IP configurations

Network interface

Search (Ctrl+ /)

«

+ Add

Save

Discard

Overview

Activity log

Access control (IAM)

Tags

Settings

IP configurations

DNS servers

Network security group

Properties

IP forwarding settings

IP forwarding

Virtual network

IP configurations

\* Subnet

Search IP configurations

| NAME      | IP VERSION |
|-----------|------------|
| ipconfig1 | IPv4       |

## 3. Add new IP 10.0.0.6 & 10.0.0.7 and give static public IP to each private IP made.

Add IP configuration

CPSingleGateway-eth0

\* Name

ipcnfig2

Type

Primary

Secondary

Primary IP configuration already exists

Private IP address settings

Allocation

Dynamic

Static

\* IP address

10.0.0.6

Public IP address

Disabled

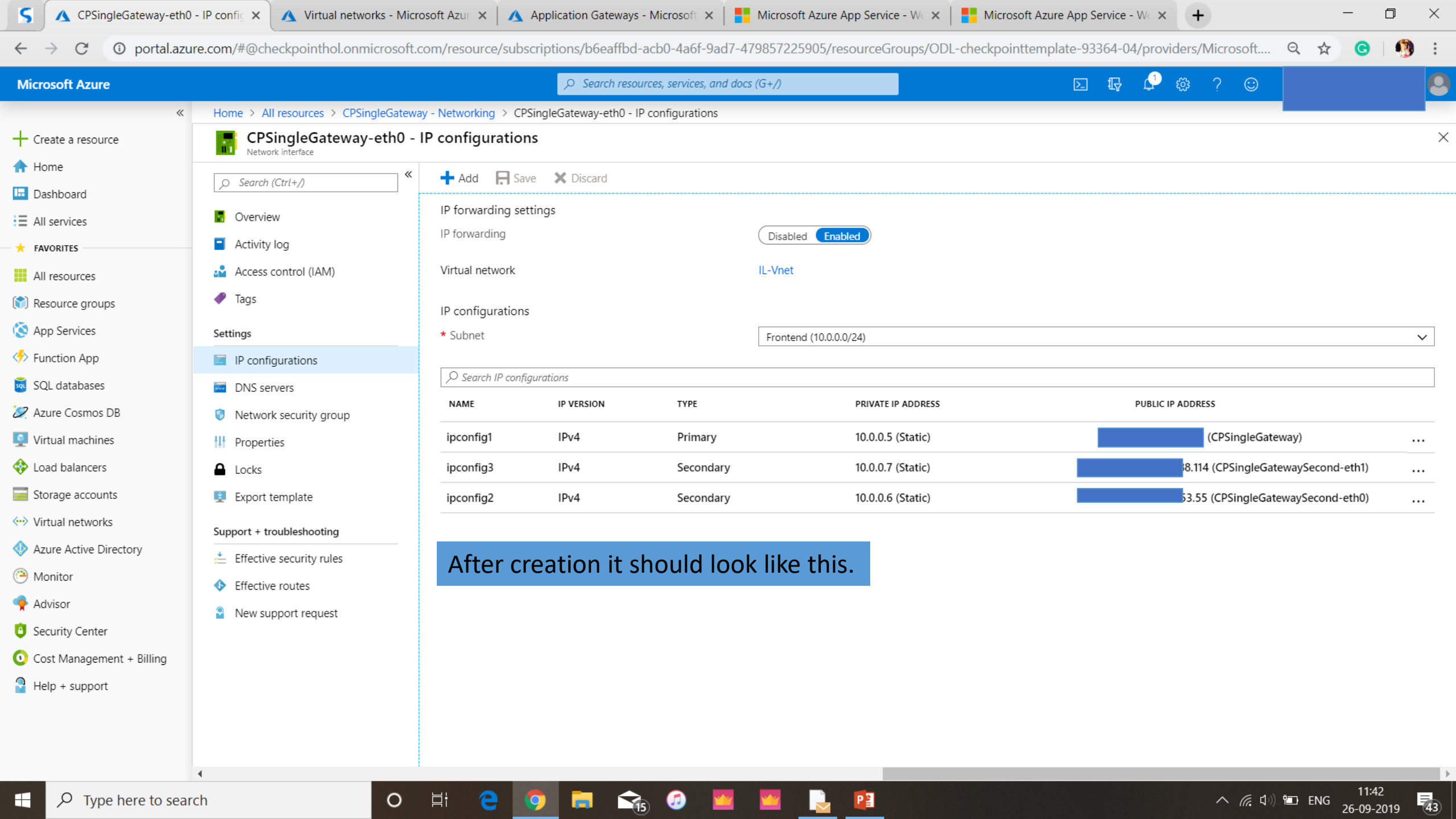
Enabled

\* IP address

Configure required settings

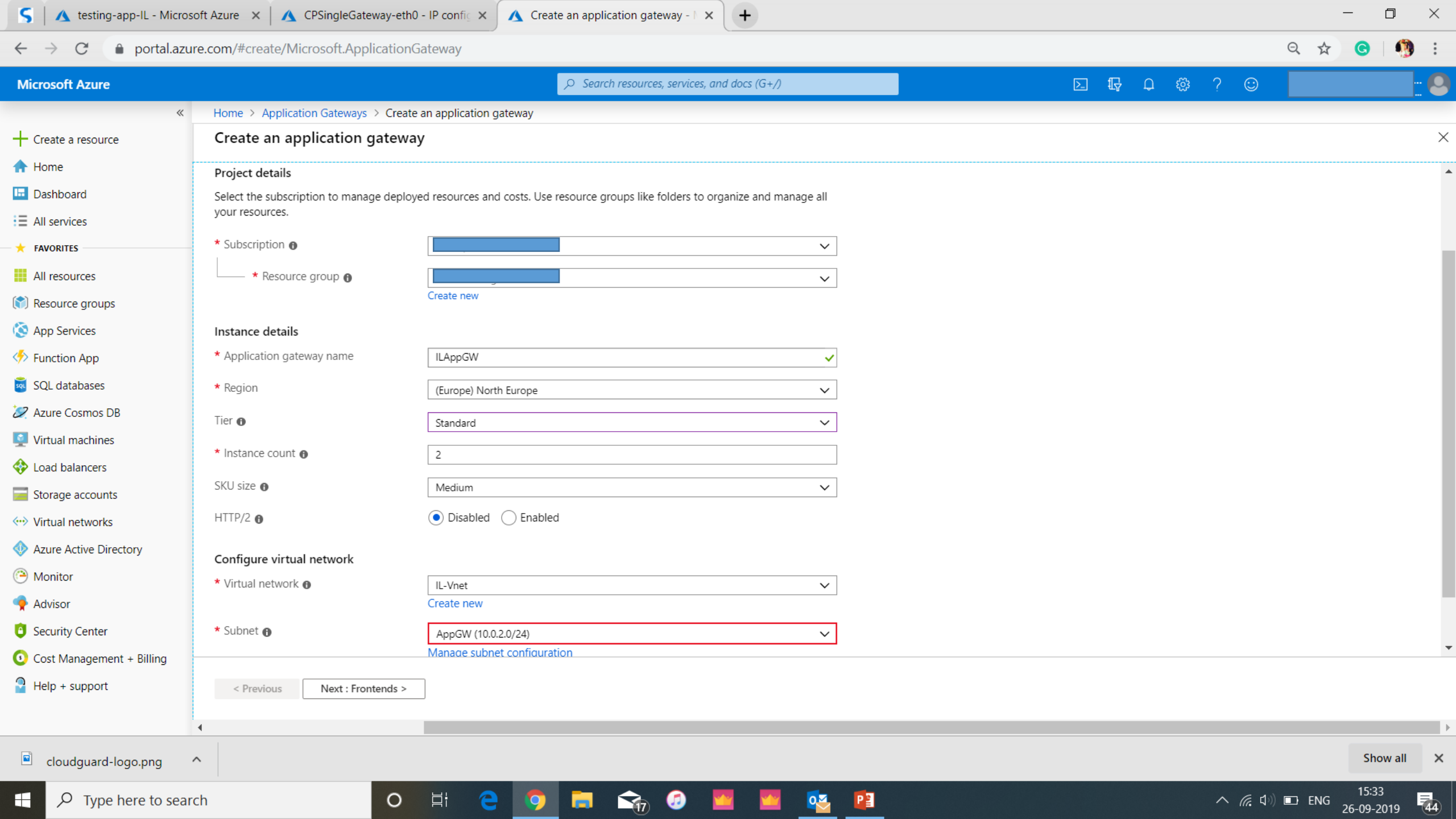
OK





# Configure Application Gateway







Home > Application Gateways > Create an application gateway

## Create an application gateway

### Project details


Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

\* Subscription 


\* Resource group 


[Create new](#)


### Instance details


\* Application gateway name  

\* Region


Tier 

\* Instance count 


SKU size 

HTTP/2  ☒ Disabled ☐ Enabled

### Configure virtual network

\* Virtual network 

[Create new](#)

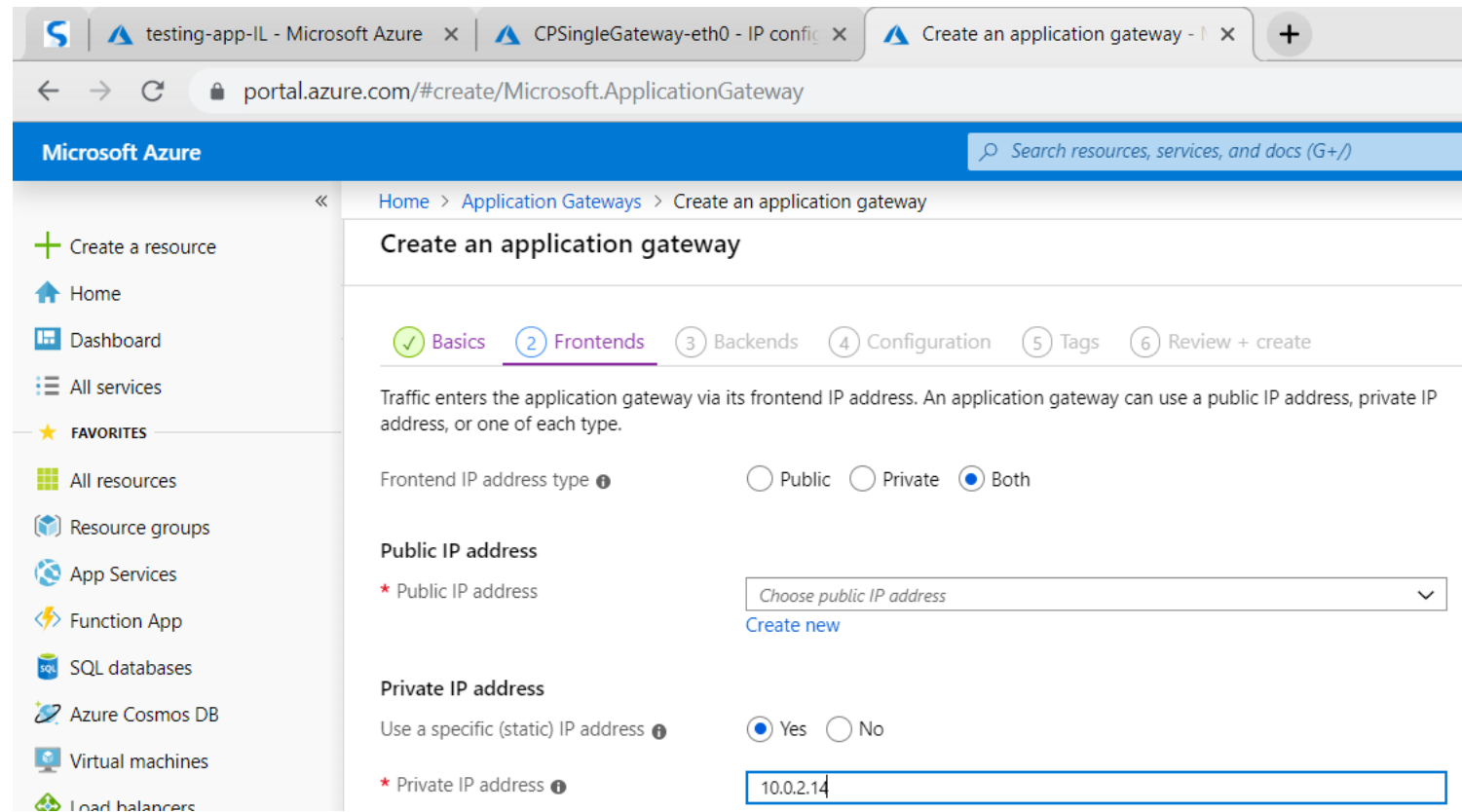
\* Subnet 

[Manage subnet configuration](#)

< Previous

Next : Frontends >

Create with both private and public IP  
Create a new public IP for AppGW



Microsoft Azure

Home > Application Gateways > Create an application gateway

### Create an application gateway

1 Basics 2 Frontends 3 Backends 4 Configuration 5 Tags 6 Review + create

Traffic enters the application gateway via its frontend IP address. An application gateway can use a public IP address, private IP address, or one of each type.

Frontend IP address type ☐ Public ☐ Private ☒ Both

**Public IP address**

\* Public IP address  [Create new](#)

**Private IP address**

Use a specific (static) IP address ☒ Yes ☐ No

\* Private IP address



Microsoft Azure

Search resources, services, and docs (G+)

Home > Application Gateways > Create an application gateway

Create an application gateway

Basics

Frontends

Backends

Configuration

Tags

Review + create

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, IP addresses, or fully qualified domain names (FQDN).

+Add a backend pool

| BACKEND POOL | TARGETS |
|--------------|---------|
| No results   |         |

Make one for ILAppJava

Make another for ALAppPython

Note: Do not add under same target make two different backend pool ILBackendPool1 & ILBackendPool2 for each app services

< Previous

Next : Configuration >

Add a backend pool

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, IP addresses, or a valid Internet hostname.

Name

ILBackendPool1

Add backend pool without targets

YesNo

Backend targets

1 item

| TARGET TYPE            | TARGET         |
|------------------------|----------------|
| App Services           | testing-app-IL |
| IP address or hostname | ILAppJava      |
|                        | ILAppPython    |

Add

Cancel

cloudguard-logo.png

Type here to search

17

44

15:36

26-09-2019



## Add a routing rule

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

\* Rule name

\* [Listener](#) \* [Backend targets](#)

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

\* Listener name

\* Frontend IP

Protocol ☒ HTTP ☐ HTTPS

\* Port

### Additional settings

Listener type ☒ Basic ☐ Multi

Error page url ☐ Yes ☒ No

## Add a routing rule

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

\* Rule name

\* [Listener](#) \* [Backend targets](#)

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of HTTP settings that define the behavior of the routing rule.

\* Backend target

[Create new](#)

\* HTTP setting

[Create new](#)

### Path-based routing

You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of HTTP settings based on the URL path.

| PATH | PATH RULE NAME | HTTP SETTING | BACKEND POOL |
|------|----------------|--------------|--------------|
|------|----------------|--------------|--------------|

No additional targets to display

[Add multiple targets to create a path-based rule](#)

Repeat for second routing rule

## Add an HTTP setting

[← Save changes and go back to routing rules](#)

\* HTTP setting name

Backend protocol ☒ HTTP ☐ HTTPS

\* Backend port

### Additional settings

Cookie-based affinity ☐ Enable ☒ Disable

Connection draining ☐ Enable ☒ Disable

\* Request time-out (seconds)

Override backend path

### Host name

By default, Application Gateway does not change the incoming HTTP host header from the client and sends the header unaltered to the backend. Multi-tenant services like App service or API management rely on a specific host header or SNI extension to resolve to the correct endpoint. Change these settings to overwrite the incoming HTTP host header.

Override with new host name ☐ Yes ☒ No

Host name override ☐ Pick host name from backend target ☒ Override with specific domain name

Add

Cancel

nd frontend IP configuration if you haven't



Add a rule



testing-app-IL - Microsoft Azure

CPSingleGateway-eth0 - IP config

ILAppGWHttp1 - Microsoft Azure

portal.azure.com/#@checkpointhol.onmicrosoft.com/resource/subscriptions/b6eaffbd-acb0-4a6f-9ad7-479857225905/resourceGroups/ODL-checkpointtemplate-93364-01/providers/Microsoft...

Microsoft Azure

Search resources, services, and docs (G+)

Create a resource

Home

Dashboard

All services

FAVORITES

All resources

Resource groups

App Services

Function App

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Security Center

Cost Management + Billing

Help + support

ILAppGWHttp1

ILAppGW

Save Discard Delete

Name

ILAppGWHttp1

Cookie based affinity

Disabled Enabled

Connection draining

Disabled Enabled

Protocol

HTTP HTTPS

☒ Use for App service

80

Request timeout (seconds)

20

Override backend path

☒ Use custom probe

Custom probe

ILAppGWHttp1a61f2786-b364-4298-9766-2f495ed39002

☒ Pick host name from backend address

Note: IMP

cloudguard-logo.png

Type here to search

17

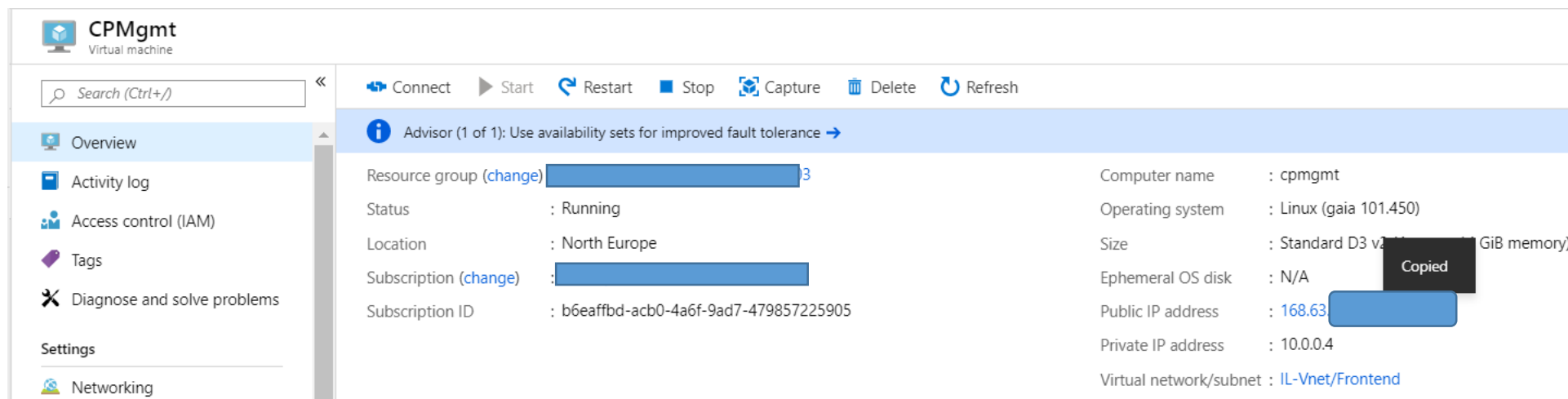
44

15:44  
26-09-2019

# Configuration on CheckPoint Smart Console

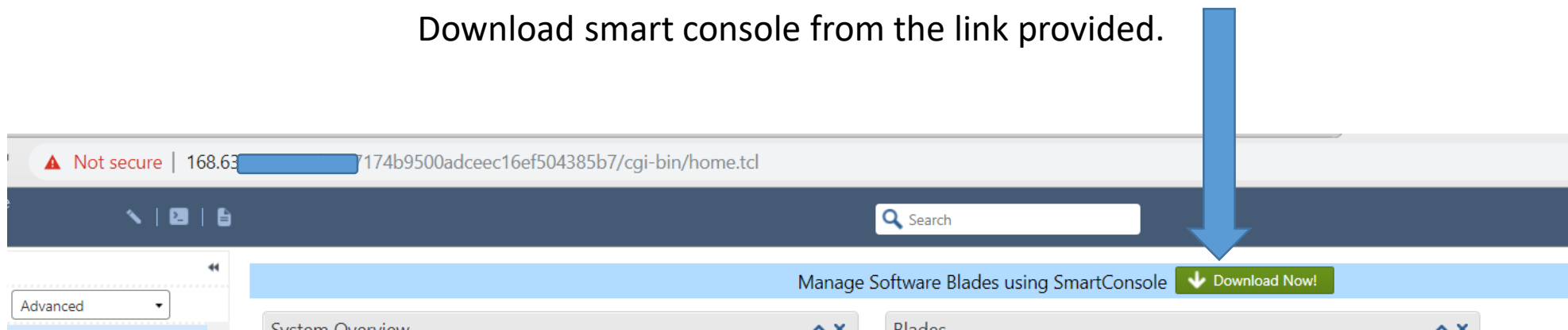


Copy Public IP of CP Mgmt and open <https://cpmgmtpublicip> Gaia portal will get opened use Credentials (provided by you while configuring checkpoint management virtual machine in azure portal) to log in into cpmgmt.



The screenshot shows the Azure portal interface for a virtual machine named 'CPMgmt'. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, and Networking. The main area displays the VM's status as 'Running' and provides details such as Resource group, Location (North Europe), Subscription ID, Computer name (cpmgmt), Operating system (Linux (gaia 101.450)), Size (Standard D3 v2), Ephemeral OS disk (N/A), Public IP address (168.63...), Private IP address (10.0.0.4), and Virtual network/subnet (IL-Vnet/Frontend). A 'Copied' tooltip is visible over the Public IP address field.

Download smart console from the link provided.



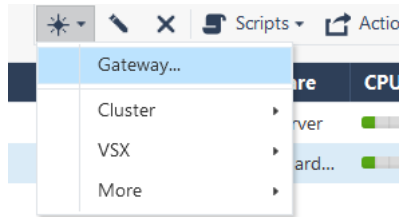
The screenshot shows the Gaia portal interface. The address bar displays the URL '168.63...174b9500adceec16ef504385b7/cgi-bin/home.tcl'. The main content area features a banner for 'Manage Software Blades using SmartConsole' with a prominent green 'Download Now!' button. A large blue arrow points from the text 'Download smart console from the link provided.' to this button. The interface also includes a search bar and a 'System Overview' tab.



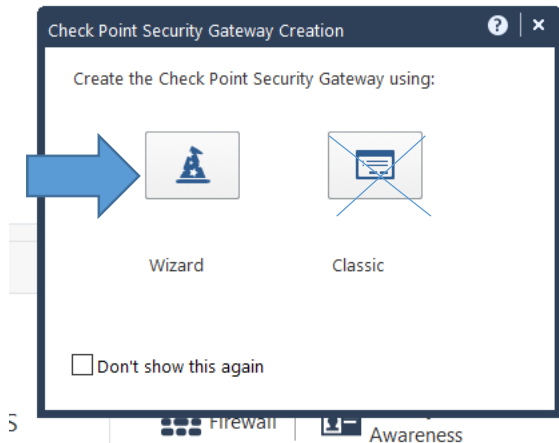
## Configuration for deploying CheckPoint CloudGuard Single Gateway on Smart Console

Note: we need to create single gateway only as management is already there. No need to do for secondary IP's

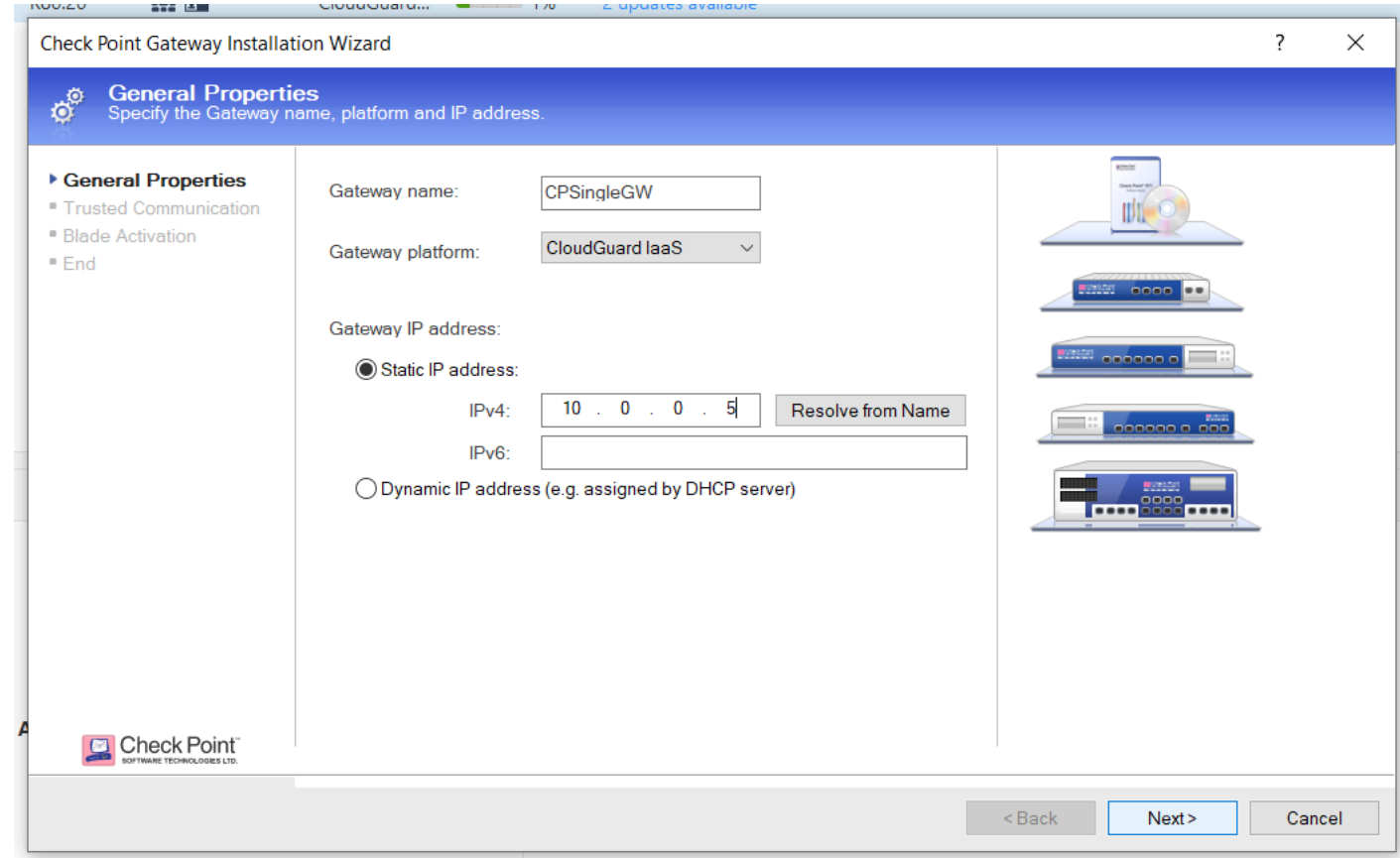
1.



2.



3.



4.

in the 'Secure Internal Communication' tab when you installed and configured the Check Point software on the gateway CPSingleGW.

|                    |               |
|--------------------|---------------|
| Gateway's Name:    | CPSingleGW    |
| One-time password: | .....         |
| Trust State:       | Uninitialized |

☐ Skip and initiate trusted communication later



1.

| Name | Topology | IP          | Comments |
|------|----------|-------------|----------|
| eth0 | External | 10.0.0.5/24 |          |
| eth1 | All-Vnet | 10.0.1.4/24 |          |

## 2. Untick Anti-spoofing for eth0



Interface: eth0

eth0

Enter Object Configuration

General

QoS

Advanced

General

Topology

Leads To:

Security Zone

Anti Spoofing

Modify...

Add Tag

☒ Not defined

☐ Network defined by the interface IP and Net Mask

☐ Network defined by routes

☐ Specific: 

No item selected.

View...

☐ Interface leads to DMZ

Security Zone

☒ User defined

☐ Specify Security Zone: 

No item selected.

☐ According to topology: ExternalZone

Anti-Spoofing

☐ Perform Anti-Spoofing based on interface topology

Anti-Spoofing action is set to 

Prevent

☐ Don't check packets from: 

No item selected.

View...

Spoof Tracking: 

Log

OK

Cancel

For eth1

3.

Topology Settings

Leads To

- ☐ This Network (Internal)
- ☒ Override
  - ☐ Internet (External)
  - ☒ This Network (Internal)
    - IP Addresses behind this interface:
      - ☐ Not defined
      - ☐ Network defined by the interface
      - ☐ Network defined by routes
      - ☒ Specific: All-Vnet View...

Security Zone

- ☒ User defined
  - ☐ Specify Security Zone
  - ☐ According to topology

Anti-Spoofing

- ☐ Perform Anti-Spoofing based on interface topology
  - Anti-Spoofing action is set to
  - ☐ Don't check packets from: No item selected. View...
  - Spoof Tracking: Log

Override network setting

- Override
- This Network
- Specific
- New Network

None

Network

Network Group

Address Range

5 items available

OK Cancel

4.

New Network

All-Vnet

Enter Object Comment

General

NAT

IPv4

Network address: 10.0.0.0

Net mask: \* 255.255.0.0

Broadcast address:

- ☒ Included
- ☐ Not included

IPv6

Network address:

Prefix:

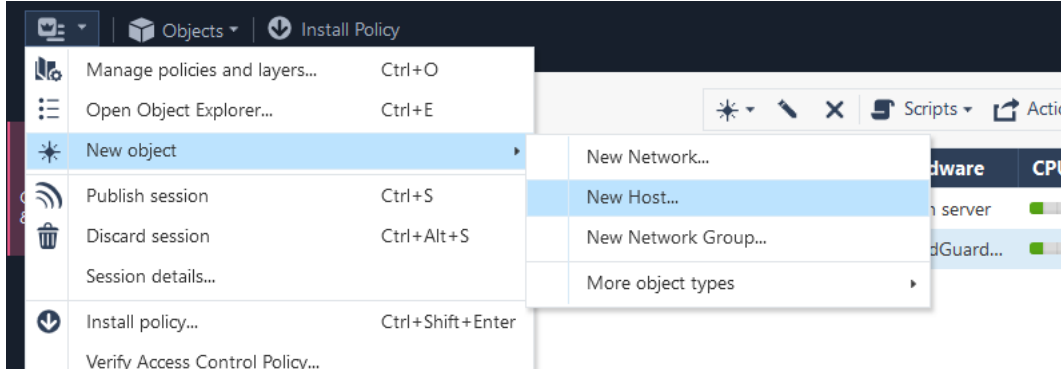
Add Tag

OK Cancel

5. Untick Anti-spoofing at the end for eth1.



1. Go to top left corner
  - New Object
  - New HostCreate these all host for use.



Host

**CPEExtGW**  
Enter Object Comment

General Machine

Network Management IPv4 address: 10.0.0.5

NAT IPv6 address:

Advanced

Servers

Add Tag

OK

Host

**CPEExtSecn1GW**  
Enter Object Comment

General Machine

Network Management IPv4 address: 10.0.0.6 Resolve from name

NAT IPv6 address:

Advanced

Servers

Add Tag

OK Cancel

New Host

**LoopBack**  
Enter Object Comment

General Machine

Network Management IPv4 address: 127.0.0.1 Resolve from name

NAT IPv6 address:

Advanced

Servers

Add Tag

OK Cancel

Host

**CPEExtSecn2GW**  
Enter Object Comment

General Machine

Network Management IPv4 address: 10.0.0.7

NAT IPv6 address:

Advanced

Servers

Add Tag

OK

Host

**CPGWInternalIP**  
Enter Object Comment

General Machine

Network Management IPv4 address: 10.0.1.4 Resolve from name

NAT IPv6 address:

Advanced

Servers

Add Tag

OK Cancel

Host

**AppGWPrivateIP**  
Enter Object Comment

General Machine

Network Management IPv4 address: 10.0.2.14 Resolve from name

NAT IPv6 address:

Advanced

Servers

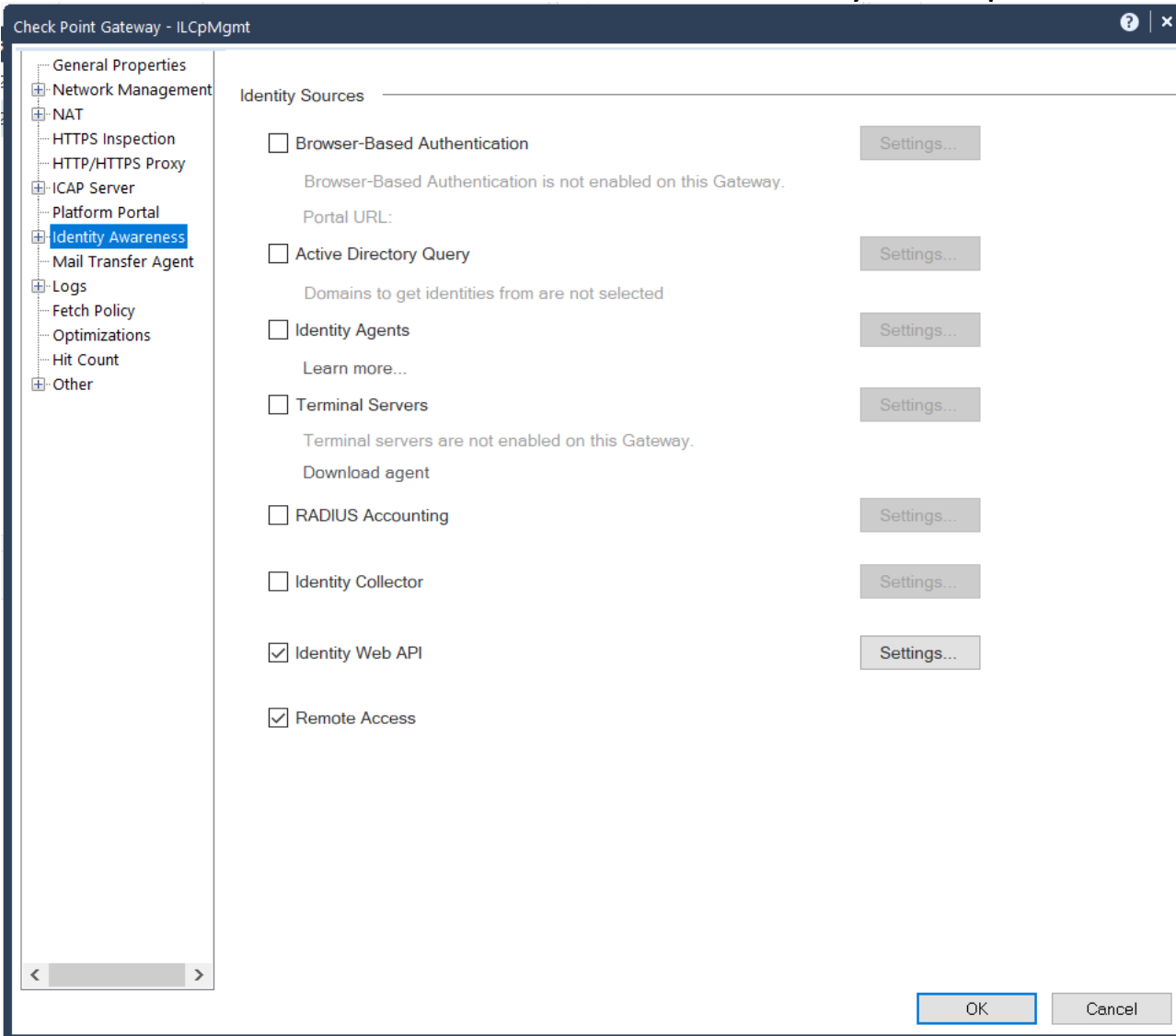
Add Tag

OK Cancel

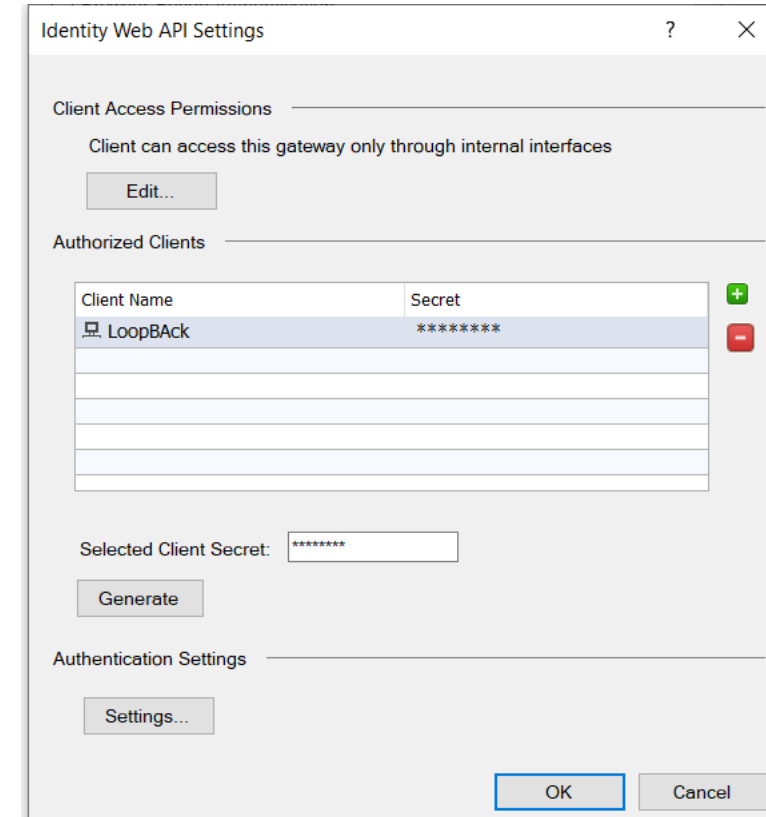


After enabling Identity awareness

- gateway general properties tab
- under Identity awareness
- Untick terminal services and choose identity web api



- Choose previously defined **Host LoopBack** Here and save Selected client secret id for future use.



Install policy after every changes did on Smart console

Go to top left portion of console

- find Install Policy Icon
- Publish & Install
- Untick Threat Prevention
- Install
- Wait for policy to install

The screenshot displays the Check Point SmartConsole interface. On the left, a sidebar contains navigation icons for Gateways & Servers, Security Policies, Logs & Monitor, and a gear icon for Settings. The main area is divided into two panels. The left panel, titled 'Standard', shows the 'Access Control' policy configuration. The right panel, titled 'Standard', shows the 'Threat Prevention' policy configuration. In the 'Threat Prevention' section, the 'Access Control' checkbox is checked, and the 'Threat Prevention' checkbox is unchecked. Below these checkboxes, it states 'Total changes from last installation (26-09-2019): 5 Changes from 1 sessions (by admin)'. The 'Install Policy' dialog box is open in the foreground, displaying the 'You have unpublished changes' message. It prompts the user to provide a session name before publishing changes. The 'Session name' field is filled with 'admin@9/26/2019'. The 'Description' field is empty. At the bottom of the dialog, it shows 'Total draft changes: 5' and buttons for 'Publish & Install' and 'Cancel'. The 'Install Mode' section at the bottom of the 'Standard' panel shows the 'Install on each selected gateway independently' option selected. Below this, there are two sub-options: 'For gateway clusters, if installation on a cluster member fails, do not install on that cluster.' (checked) and 'Install on all selected gateways. If installation on a gateway fails, do not install on all gateways of the same version.' (unchecked). At the bottom right of the 'Standard' panel, there are 'Install' and 'Cancel' buttons.

**Standard**

☒ Access Control

☐ Threat Prevention

Total changes from last installation (26-09-2019):  
5 Changes from 1 sessions (by admin)

**ILCpMgmt**

IP: 10.0.0.5 | Version: R80.20

[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.

**SmartConsole**

**You have unpublished changes**

You are required to provide a session name before you can publish your changes:

Session name: admin@9/26/2019

Description:

Total draft changes: 5

[Publish & Install](#) [Cancel](#)

**Standard**

[Install](#) [Cancel](#)



Install Policy

Discard

Session

1

Publish

Check Point SmartConsole

Columns: General

Scripts

Actions

Monitor

Search...

2

| Status | Name         | IP           | Version | Active Blades | Hardware      | CPU Usa...                | Recommended Updat... | Comme... |
|--------|--------------|--------------|---------|---------------|---------------|---------------------------|----------------------|----------|
| ✓      | cpmgmt       | 168.63.40.17 | R80.20  |               | Open server   | <div><div></div></div> 2% | 3 updates available  |          |
| ✓      | ILcpSingleGV | 10.0.0.5     | R80.20  |               | CloudGuard... | <div><div></div></div> 1% | 2 updates available  |          |

Install policy

Summary

Tasks

Errors

cpmgmt

IPv4 Address: 168.63.40.17

OS: Gaia

Version: R80.20

License Status: Not Activated

Open server

CPU:  2%

Memory:  24%

Device & License Information...

Management Blades

Network Policy Management

Logging & Status

Activate Blades...

Search...

New...

Object Categories

Network Objects

25

Services

515

Applications/Categories

7508

VPN Communities

2

Data Types

62

Users

1

Servers

1

Time Objects

3

UserCheck Interactions

13

Limit

4

No tasks in progress

168.63.40.17

1 Draft change saved

admin

Type here to search

15

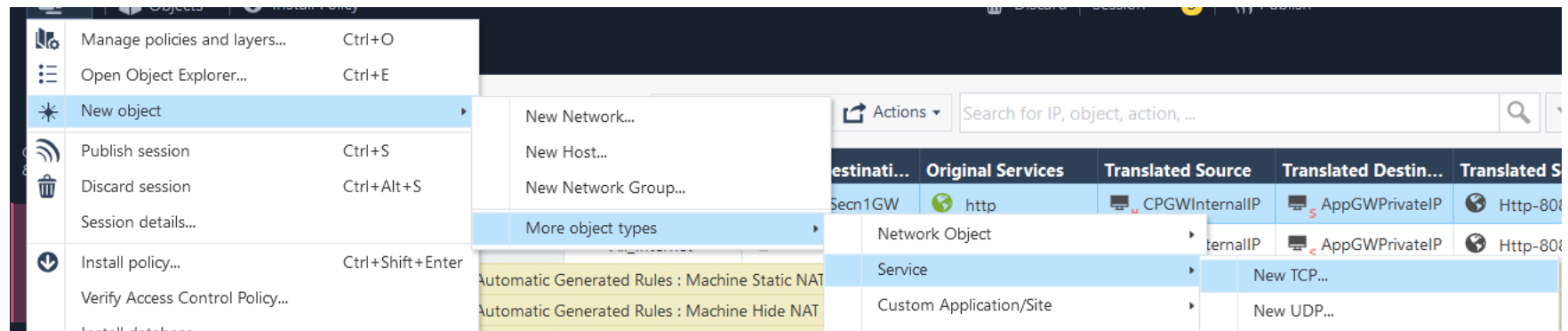
12:01

26-09-2019

42

Let us create TCP object

- One for 8081
- Other for 8082



New TCP Service

**Http-8081**  
Enter Object Comment

**General**  
Advanced

**General**

Protocol: HTTP

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

**Match By**

- Port:
  - ☐ Standard Port (80)
  - ☒ Customize 8081
- Protocol Signature is disabled

Add Tag

OK Cancel

New TCP Service

**Http-8082**  
Enter Object Comment

**General**  
Advanced

**General**

Protocol: HTTP

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

**Match By**

- Port:
  - ☐ Standard Port (80)
  - ☒ Customize 8082
- Protocol Signature is disabled

Add Tag

OK Cancel



# Create policy under Security Policies > Policy section

GATEWAYS & SERVERS

SECURITY POLICIES

LOGS & MONITOR

Access Control

Policy

NAT

Threat Prevention

Policy

Exceptions

Shared Policies

Geo Policy

Install Policy

Actions

Search for IP, object, action, ...

| No. | Name              | Source | Destination   | VPN   | Services & Applications | Action |
|-----|-------------------|--------|---------------|-------|-------------------------|--------|
| 1   | Gaia              | * Any  | CPEExtGW      | * Any | https                   | Accept |
| 2   | Inbound-to-Python | * Any  | CPEExtSecn1GW | * Any | http                    | Accept |
| 3   | Inbound-to-Java   | * Any  | CPEExtSecn2GW | * Any | http                    | Accept |
| 4   | Cleanup rule      | * Any  | * Any         | * Any | * Any                   | Drop   |

## Create 2 NAT under same section

GATEWAYS & SERVERS

SECURITY POLICIES

LOGS & MONITOR

Access Control

Policy

NAT

Threat Prevention

Policy

Exceptions

Shared Policies

Geo Policy

Inspection Settings

Actions

Search for IP, object, action, ...

| No.   | Original Source | Original Destinati... | Original Services | Translated Source | Translated Destin... | Translated Services | Install On       | Commer |
|---|-----------------|-----------------------|-------------------|-------------------|----------------------|---------------------|------------------|--------|
| 1   | All_Internet    | CPEExtSecn1GW         | http              | CPGWInternalIP    | AppGWPrivateIP       | Http-8081           | * Policy Targets |        |
| 2   | All_Internet    | CPEExtSecn2GW         | http              | CPGWInternalIP    | AppGWPrivateIP       | Http-8082           | * Policy Targets |        |
| Automatic Generated Rules : Machine Static NAT (No Rules)       |                 |                       |                   |                   |                      |                     |                  |        |
| Automatic Generated Rules : Machine Hide NAT (No Rules)         |                 |                       |                   |                   |                      |                     |                  |        |
| 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 (3-4)              |                 |                       |                   |                   |                      |                     |                  |        |
| 3   | Loading...      | Loading...            | * Any             | Loading...        | Loading...           | Loading...          | Loading...       |        |

Note: In Translated Source section remember to do the following for both the NAT (Hide behind NAT):-

CPGWInternalIP

AppGWPrivateIP

Http-8082

\* Poli

Replace...

NAT Method

Edit Object...

Remove

Edit

Cut

Copy

Paste

Where Used...

Static

Hide

Stateful NAT64

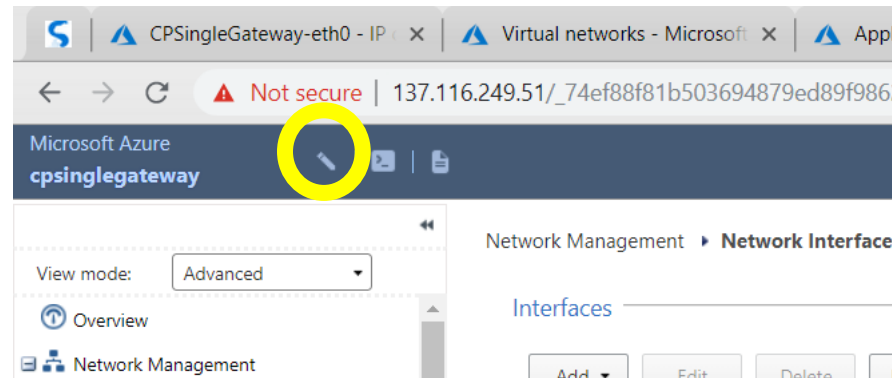
Stateless NAT46



Till here we are done with the smart console part  
Now we will add the secondary IP's made in azure portal into our firewall interface  
i.e we will make it learn the IP in order to work with them

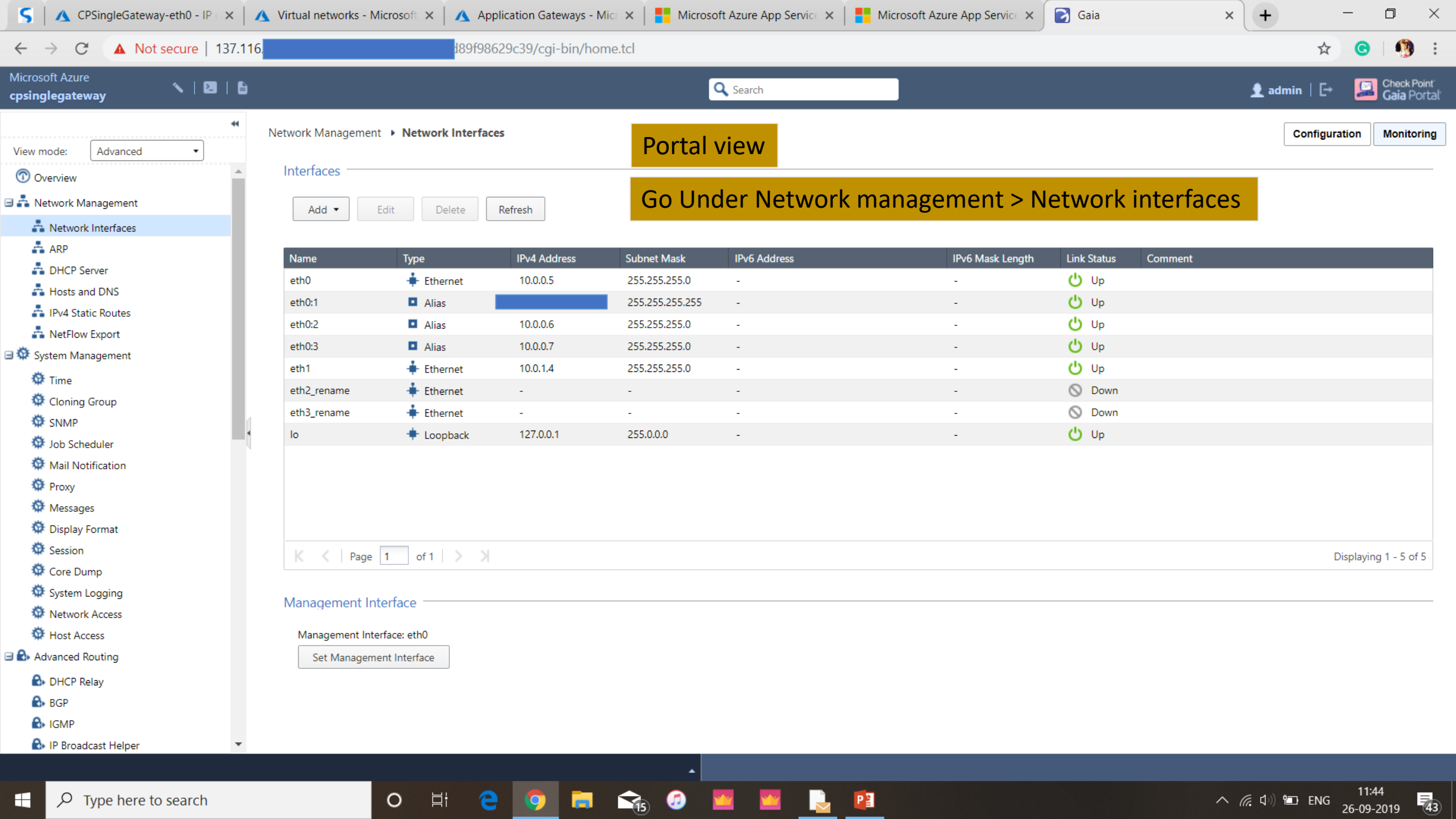
Log Into your Gaia portal using Single Management Public IP (Public IP corresponding to primary interface 10.0.0.5)  
Username as : admin  
Password as : password that you kept during Checkpoint CloudGuard setup(In Azure)

If a lock appears in the highlighted section shown below do click on it and acquire access to write permission



Follow rest as shown in picture





## Interfaces

1.

| Name        | Type     | IPv4 Address | Subnet Mask   | IPv6 Address | IPv6 Mask Length |
|-------------|----------|--------------|---------------|--------------|------------------|
| eth0        | Ethernet | 10.0.0.5     | 255.255.255.0 | -            | -                |
| eth0:1      | Alias    | 10.0.0.6     | 255.255.255.0 | -            | -                |
| eth0:2      | Alias    | 10.0.0.7     | 255.255.255.0 | -            | -                |
| eth0:3      | Alias    | 10.0.1.4     | 255.255.255.0 | -            | -                |
| eth1        | Ethernet | -            | -             | -            | -                |
| eth2_rename | Ethernet | -            | -             | -            | -                |
| eth3_rename | Ethernet | -            | -             | -            | -                |
| lo          | Loopback | 127.0.0.1    | 255.0.0.0     | -            | -                |

Page 1 of 1

## Interfaces

2.

| Name        | Type     | IPv4 Address | Subnet Mask | IPv6 Address |
|-------------|----------|--------------|-------------|--------------|
| eth0        | Ethernet |              |             |              |
| eth0:1      | Alias    |              |             |              |
| eth0:2      | Alias    |              |             |              |
| eth0:3      | Alias    |              |             |              |
| eth1        | Ethernet |              |             |              |
| eth2_rename | Ethernet |              |             |              |
| eth3_rename | Ethernet |              |             |              |
| lo          | Loopback |              |             |              |

Page 1 of 1

Add Alias

Type: ☒ Alias

Enable: ☒

Member Of:

eth0

eth1

eth2\_rename

eth3\_rename

OK Cancel

3.

Add Alias

Type: ☒ Alias

Enable: ☒

IPv4 IPv6 Alias

☐ Obtain IPv4 address automatically

☒ Use the following IPv4 address:

IPv4 address: 10 . 0 . 0 . 6

Subnet mask: 255 . 255 . 255 . 0

OK Cancel

4.

Add Alias

Type: ☒ Alias

Enable: ☒

IPv4 IPv6 Alias

☐ Obtain IPv4 address automatically

☒ Use the following IPv4 address:

IPv4 address: 10 . 0 . 0 . 7

Subnet mask: 255 . 255 . 255 . 0

OK Cancel



# Testing





<http://PublicIPMappedtoSecondaryIP1>  
you will be able to access the web app

## Hey, Java developers!

Your app service is up and running.

Time to take the next step and deploy your code.

Have your code ready?

Use deployment center to get code published from your client or setup continuous deployment.

Deployment Center

Don't have your code yet?

Follow our quickstart guide and you'll have a full app ready in 5 minutes or less.

Quickstart



### Technical Information

java.version: 11.0.2

java.home: /usr/lib/jvm/zulu-11-azure-jre-headless-tools\_11.29.3-11.0.2-linux\_musl\_x64



<http://PublicIPMappedtoSecondaryIP2>  
you will be able to access the web app

Hey, **Python** developers!

Your app service is up and running.

Time to take the next step and deploy your code.

Have your code ready?

Use deployment center to get code published from your client or setup continuous deployment.

Deployment Center

Don't have your code yet?

Follow our quickstart guide and you'll have a full app ready in 5 minutes or less.

Quickstart



**Thank You**

