

# CheckPoint CloudGuard PaaS Solution for Application Services in Azure

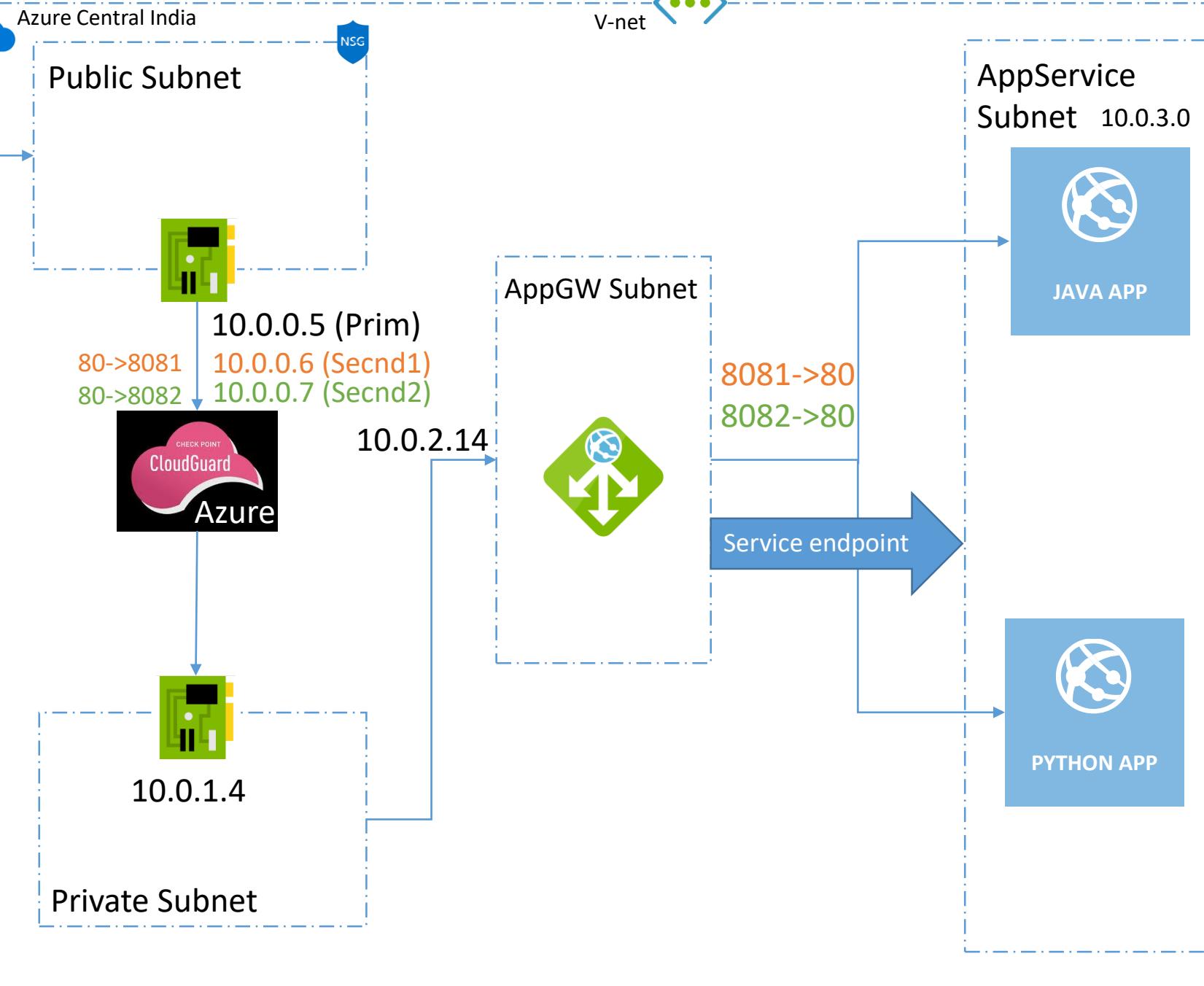


Solution found by:-  
Shalini Vishwakarma  
Amarpreet Singh

# Architecture

1.137.135.188.114  
2.137.135.253.55

Internet Users



# Log into Microsoft Azure cloud portal



portal.azure.com/#blade/HubsExtension/BrowseResourceBlade/resourceType/Microsoft.Network%2FvirtualNetworks

Microsoft Azure

Microsoft Azure

Search resources, services, and docs (G+)

Home > Virtual networks

Create a resource

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

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

...

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

Type here to search

O E G 15 M P

11:33 26-09-2019

43

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+)

Home > Virtual networks > IL-Vnet - Subnets

### IL-Vnet - Subnets

Virtual network

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

Subnet

Gateway subnet

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peering

Service endpoints

Properties

Locks

Export template

Monitoring

Diagnostic settings

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	-	-

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

## Microsoft Azure

Search resources, services, and docs (G+)

Home > Virtual networks > IL-Vnet - Service endpoints

### IL-Vnet - Service endpoints

Virtual network

Add

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

Diagnostic settings

Service	Subnet	Status	Locations
Microsoft.Web	1	Succeeded	*
	AppGW		

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



Type here to search



ENG

11:34  
26-09-2019

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+)

IL-Vnet

Virtual network

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

DNS servers

Peering

Service endpoints

Properties

Locks

Export template

Monitoring

Diagnostic 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

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

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



portal.azure.com/#blade/HubsExtension/BrowseResourceBlade/resourceType/Microsoft.Web%2Fsites

Microsoft Azure

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

<input type="checkbox"/> NAME ↑↓	STATUS	APP TYPE	APP SERVICE PLAN	LOCATION ↑↓	SUBSCRIPTION ↑↓
<input type="checkbox"/> ILAppJava	Running	Web App	ASP.NET Core	North Europe	Check Point Software Technologies Inc.
<input type="checkbox"/> ILAppPython	Running	Web App	ASP.NET Core	North Europe	Check Point Software Technologies Inc.
<input type="checkbox"/> testing-app-IL	Running	Web App	ASP.NET Core	North Europe	Check Point Software Technologies Inc.

Type here to search

O E G 15 M P 11:35 26-09-2019 ENG 43

portal.azure.com/#@checkpoinalonmicrosoft.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

ILAppJava - Networking

Search (Ctrl+ /)

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

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

Settings

Configuration

Authentication / Authorization

Application Insights

Identity

Backups

Custom domains

TLS/SSL settings

Access Restrictions

Define and manage rules that control access to your application.

Learn More

Configure Access Restrictions



Type here to search



11:35

26-09-2019



## Microsoft Azure

Search resources, services, and docs (G+)



Home &gt; App Services &gt; ILAppJava - Networking &gt; Access Restrictions

## Access Restrictions

Remove Refresh



### Access Restrictions

Access restrictions allow you to define lists of allow/deny rules to control traffic to your app. Rules are evaluated in priority order. If there are no rules defined then your app will accept traffic from any address. [Learn more](#)

ilappjava.azurewebsites.net

ilappjava.scm.azurewebsites.net

Add rule

PRIORITY	NAME	SOURCE	ENDPOINT STATUS	ACTION	...
300	Test1	IL-Vnet/AppGW	Enabled	Allow	
2147483647	Deny all	Any		Deny	

For first App

- 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



Type here to search

11:35  
26-09-2019  
 ENG  
43

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

### Access Restrictions

Remove Refresh

### Access Restrictions

Access restrictions allow you to define lists of allow/deny rules to control traffic to your app. Rules are evaluated in priority order. If there are no rules defined then your app will accept traffic from any address. [Learn more](#)

PRIORITY	NAME	SOURCE	ENDPOINT STATUS	ACTION
300	Test2	IL-Vnet/AppGW	Enabled	<input checked="" type="checkbox"/> Allow
2147483647	Deny all	Any		<input type="checkbox"/> Deny

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.

Documentation

+ Add Refresh Start Stop

**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+/  
 Activity log Access control (IAM) Tags Diagnose and solve problems Security

Overview

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 ( <a href="#">change</a> ) : [REDACTED]	URL : <a href="https://testing-app-il.azurewebsites.net">https://testing-app-il.azurewebsites.net</a>
Status : Running	App Service Plan : ASP-ODLcheckpointtemplate9336401-8712 (S1: 1)
Location : North Europe	FTP/deployment userna... : No FTP/deployment user set
Subscription ( <a href="#">change</a> ) : [REDACTED]	FTP hostname : ftp://waws-prod-db3-137.ftp.azurewebsites.windows.net
Subscription ID : b6eaffbd-acb0-4a6f-9ad7-479857225905	FTPS hostname : ftps://waws-prod-db3-137.ftp.azurewebsites.windows.net
Tags ( <a href="#">change</a> ) : Click here to add tags	

# Deploying CheckPoint CloudGuard Security Management & Single Gateway



portal.azure.com/#create/hub

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 > 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

Go to create a resource on the left hand pane side type  
➤ Checkpoint IaaS  
➤ Press Enter  
➤ Choose sec mgmt

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](#)

Type here to search

11:41 26-09-2019

portal.azure.com/#create/hub

Microsoft Azure

Search resources, services, and docs (G+)

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

Create CloudGuard IaaS - Fire... 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 >

Server Name

Authentication type  Password  SSH public key

Password

Confirm password

Subscription

Resource group

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 43

portal.azure.com/#create/hub

Microsoft Azure

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

Search resources, services, and docs (G+)

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 Gateway
- Check Point CloudGuard IaaS R80.10 Cluster
- Check Point CloudGuard IaaS Scale Set
- Check Point CloudGuard IaaS Single Gateway

Overview Plans

Check Point CloudGuard IaaS Single Gateway

As a Microsoft Azure

CloudGuard IaaS High Availability

multi-layered threat prevention to protect customer assets in Azure from malware and sophisticated threats. You can 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

portal.azure.com/#create/hub

Microsoft Azure

Search resources, services, and docs (G+)

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

Create CloudGuard IaaS - Fire... Basics

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 >

VM Name

Authentication type  Password  SSH public key

Password

Confirm password

Subscription

Resource group

Location

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



11:42  
26-09-2019  
ENG  
43

# After the creation of security management & Single GW

## 1. Go to NIC under Settings

CPSingleGateway - Networking

Search (Ctrl+ /)

Attach network interface   Detach network interface

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

Settings   Networking

**Network Interface:** CPSingleGateway-eth0   Effectiv  
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

Search (Ctrl+ /)

Add   Save   Discard

Overview   Activity log   Access control (IAM)   Tags

Settings   IP configurations

IP configurations   Subnet

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



portal.azure.com/#@checkpoinalonmicrosoft.com/resource/subscriptions/b6eaffbd-acb0-4a6f-9ad7-479857225905/resourceGroups/ODL-checkpointtemplate-93364-04/providers/Microsoft...

**CPSingleGateway-eth0 - IP configurations**

**IP forwarding settings**

IP forwarding **Enabled**

**Virtual network** IL-Vnet

**IP configurations**

\* Subnet Frontend (10.0.0.0/24)

**Search IP configurations**

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
ipconfig1	IPv4	Primary	10.0.0.5 (Static)	[REDACTED] (CPSingleGateway) ...
ipconfig3	IPv4	Secondary	10.0.0.7 (Static)	[REDACTED] 8.114 (CPSingleGatewaySecond-eth1) ...
ipconfig2	IPv4	Secondary	10.0.0.6 (Static)	[REDACTED] 63.55 (CPSingleGatewaySecond-eth0) ...

**After creation it should look like this.**

# Configure Application Gateway



testing-app-IL - Microsoft Azure | CPSingleGateway-eth0 - IP config | Create an application gateway - Microsoft Azure

portal.azure.com/#create/Microsoft.ApplicationGateway

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 > 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: [dropdown menu]

\* Resource group: [dropdown menu] [Create new](#)

**Instance details**

\* Application gateway name: ILAppGW

\* Region: (Europe) North Europe

Tier: Standard

\* Instance count: 2

SKU size: Medium

HTTP/2:  Disabled  Enabled

**Configure virtual network**

\* Virtual network: IL-Vnet [Create new](#)

\* Subnet: AppGW (10.0.2.0/24) [Manage subnet configuration](#)

< Previous [Next : Frontends >](#)

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

testing-app-IL - Microsoft Azure | CPSingleGateway-eth0 - IP config | Create an application gateway +

portal.azure.com/#create/Microsoft.ApplicationGateway

Microsoft Azure

Home > Application Gateways > Create an application 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

Create an application gateway

Basics ✓ Frontends Backends Configuration Tags 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

Private IP address

Use a specific (static) IP address  Yes  No

\* Private IP address



testing-app-IL - Microsoft Azure | CPSingleGateway-eth0 - IP config | Add a backend pool - Microsoft / +

portal.azure.com/#create/Microsoft.ApplicationGateway

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 > 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

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 Yes No

Backend targets 1 item

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

Add Cancel



## 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

ILAppGWRule1

\* 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

ILAppGWListener1

\* Frontend IP

Private

( HTTP) ( HTTPS)

\* Port

8081

### Additional settings

Listener type

( Basic) ( Multi)

Error page url

( Yes) ( No)

Add

Cancel

Routing rules



Add a rule



## Repeat for second routing rule

## Add an HTTP setting

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

\* HTTP setting name

http1

( HTTP) ( HTTPS)

\* Backend port

80

### Additional settings

Cookie-based affinity

( Enable) ( Disable)

Connection draining

( Enable) ( Disable)

\* Request time-out  
(seconds)

20

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

testing-app-IL - Microsoft Azure | CPSingleGateway-eth0 - IP config | ILAppGWHttp1 - Microsoft Azure +

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

Microsoft Azure

Search resources, services, and docs (G+)

Home > Application Gateways > ILAppGW - Rules > ILAppGWRule1 > ILAppGWHttp1

ILAppGWHttp1

Save Discard Delete

Name: ILAppGWHttp1

\* Cookie based affinity:  Disabled  Enabled

\* Connection draining:  Disabled  Enabled

\* Protocol:  HTTP  HTTPS

Use for App service

Note: IMP

80

\* Request timeout (seconds): 20

Override backend path:

Use custom probe

\* Custom probe: ILAppGWHttp1a61f2786-b364-4298-9766-2f495ed39002

Pick host name from backend address

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

clouguard-logo.png

# **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.

CPMgmt  
Virtual machine

Search (Ctrl+ /)

Connect Start Restart Stop Capture Delete Refresh

Overview

Advisor (1 of 1): Use availability sets for improved fault tolerance →

Resource group (change)	[REDACTED] 3	Computer name	:	cpmgmt
Status	:	Operating system	:	Linux (gaia 101.450)
Location	:	Size	:	Standard D3 v2 (4 vCPUs, 11 GiB memory)
Subscription (change)	[REDACTED]	Ephemeral OS disk	:	N/A
Subscription ID	b6eaffbd-acb0-4a6f-9ad7-479857225905	Public IP address	:	168.63
		Private IP address	:	10.0.0.4
		Virtual network/subnet	:	IL-Vnet/Frontend

Activity log Access control (IAM) Tags Diagnose and solve problems Settings Networking

Download smart console from the link provided.

CHECK POINT  
CloudGuard™

Not secure | 168.63 [REDACTED] 174b9500adceec16ef504385b7/cgi-bin/home.tcl

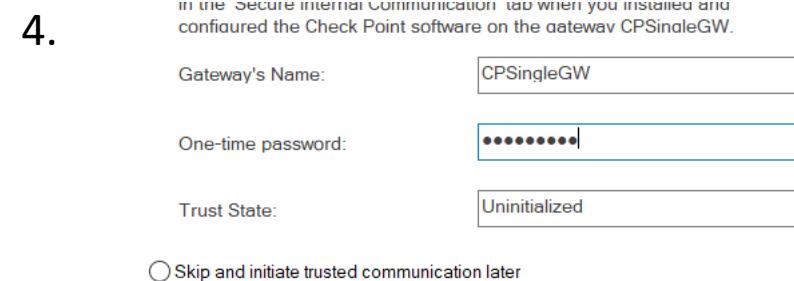
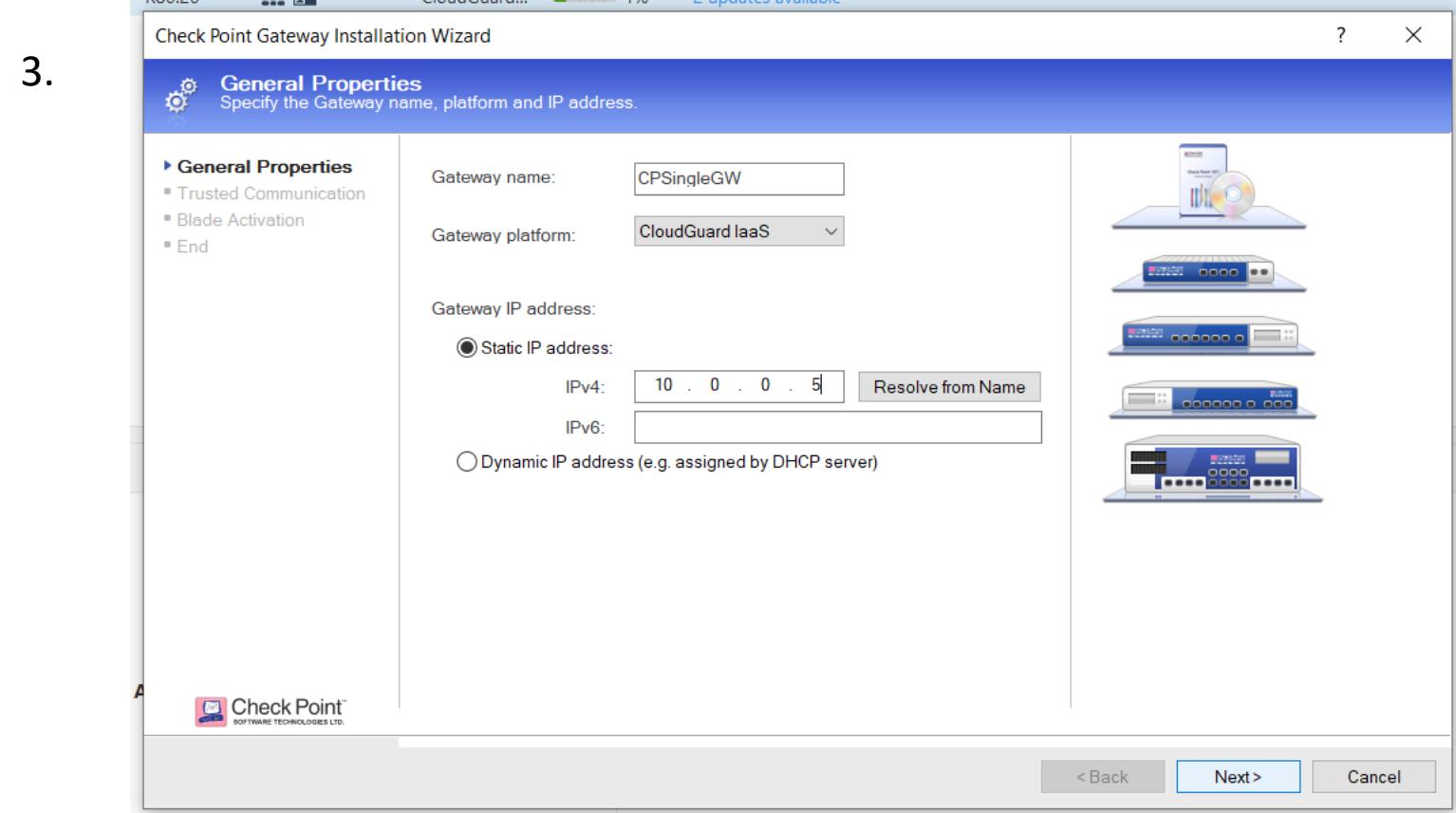
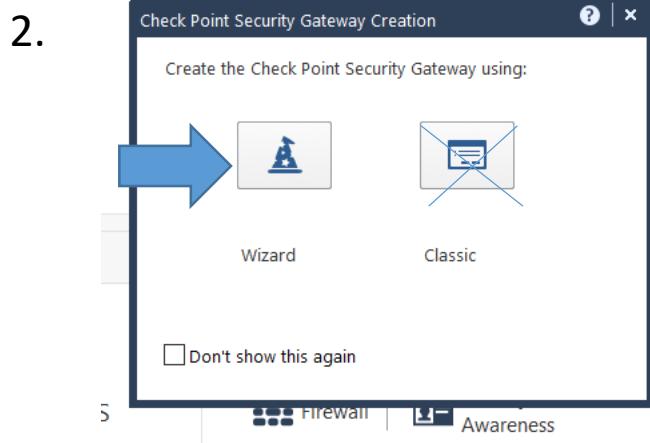
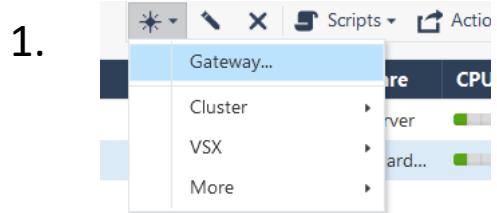
Search

Manage Software Blades using SmartConsole [Download Now!](#)

Advanced System Overview Blades

## 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

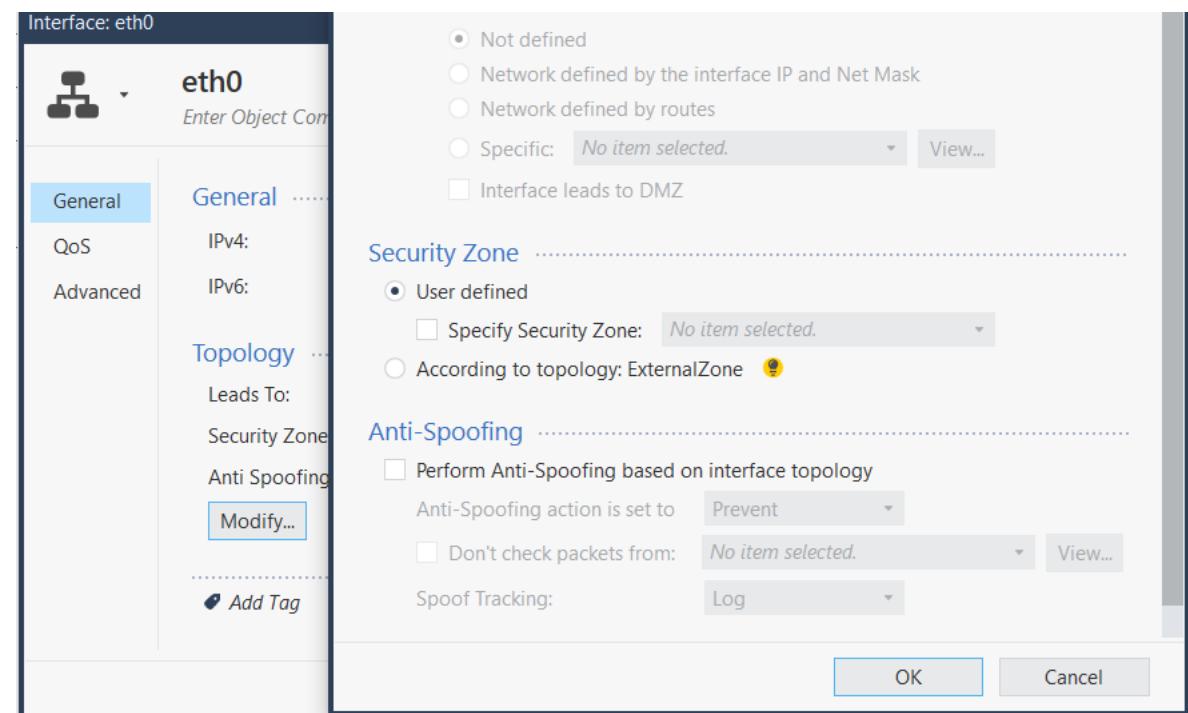


After creating gateway go to gateway properties and under network management do the following for each Ethernet

1.

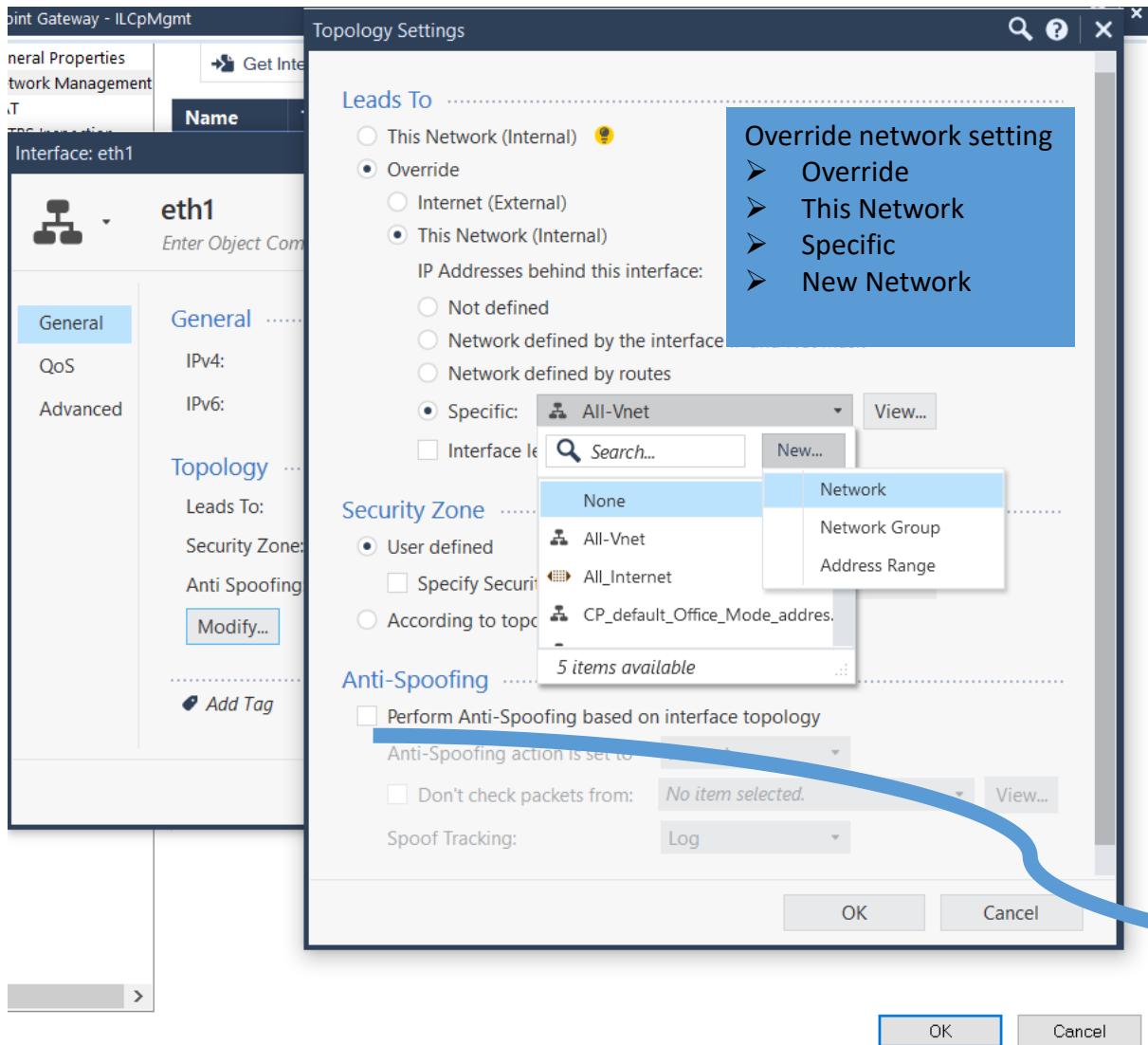
Name	Topology	IP	Comments
eth0	External	10.0.0.5/24	
eth1	All-Vnet	10.0.1.4/24	

2. Untick Anti-spoofing for eth0

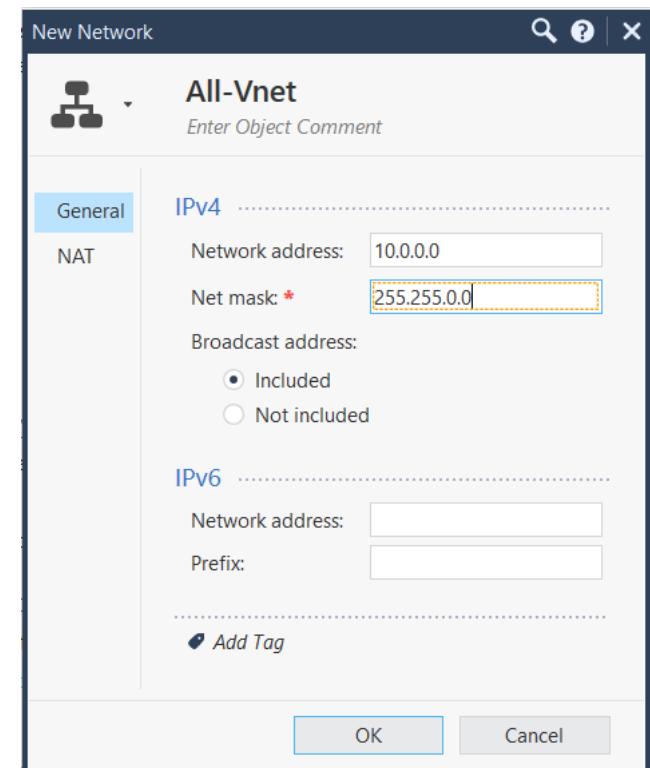


## For eth1

3.



4.



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

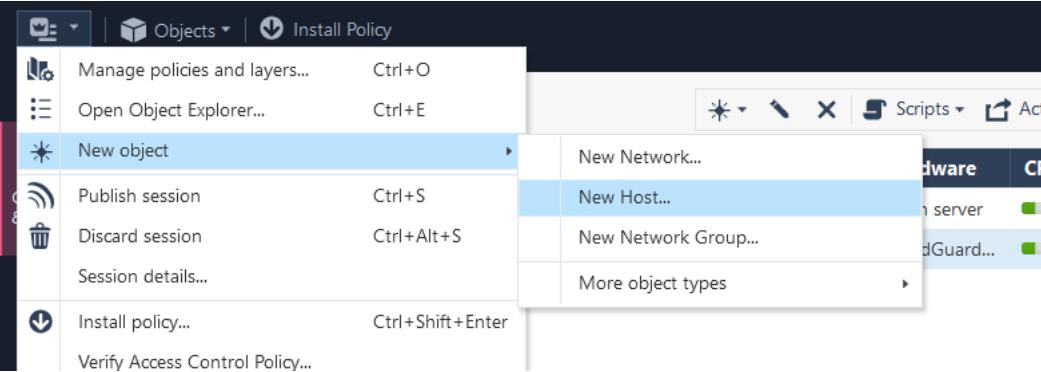


## 1. Go to top left corner

➤ New Object

➤ New Host

Create these all host for use.



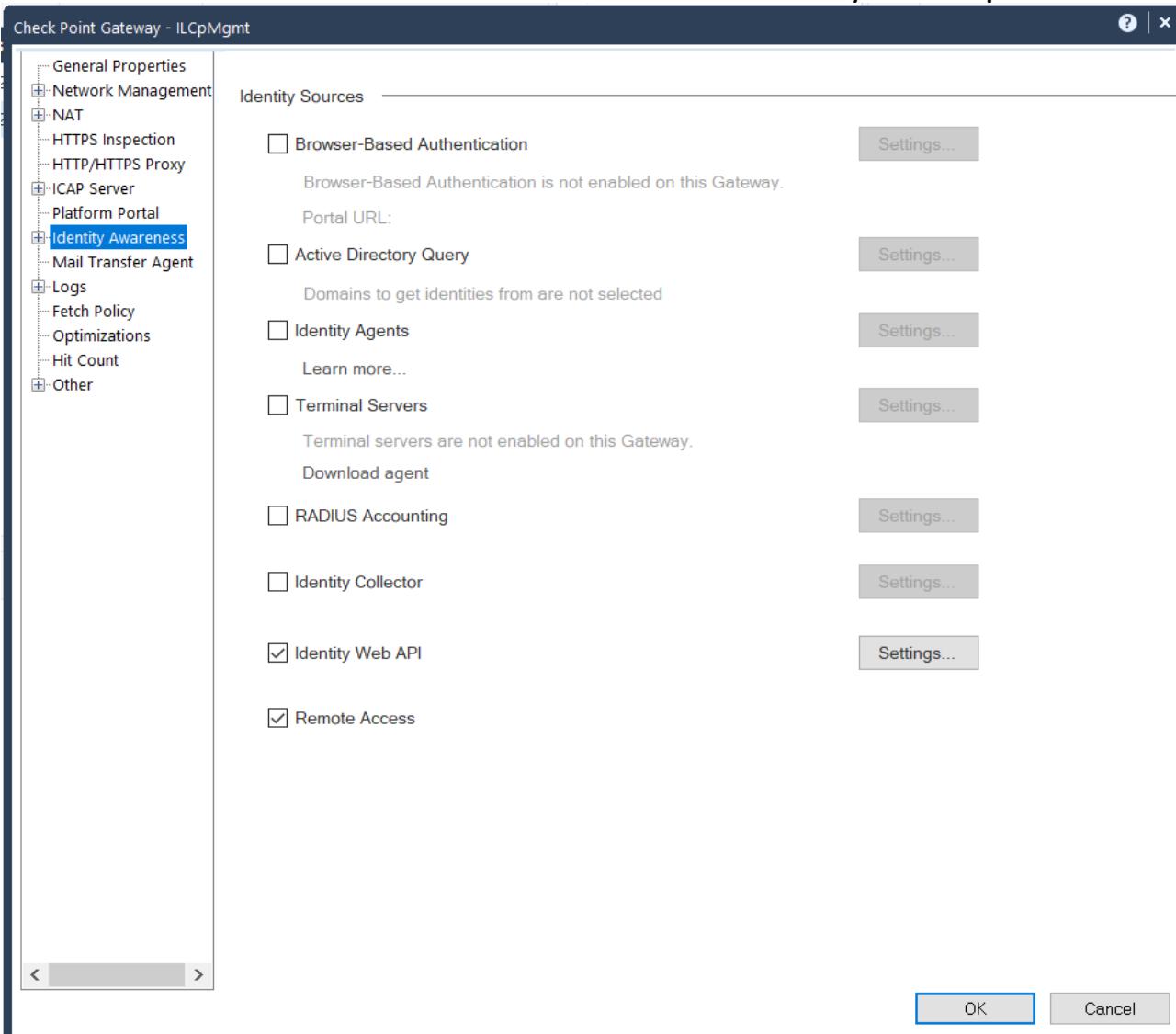
The screenshot displays five separate 'Host' configuration dialog boxes, each with tabs for General, Network Management, NAT, Advanced, and Servers. The 'General' tab is selected in all dialogs.

- CPExtGW:** IPv4 address: 10.0.0.5
- CPExtSecln1GW:** IPv4 address: 10.0.0.6
- LoopBack:** IPv4 address: 127.0.0.1
- CPExtSecln2GW:** IPv4 address: 10.0.0.7
- CPGWInternalIP:** IPv4 address: 10.0.1.4
- AppGWPrivateIP:** IPv4 address: 10.0.2.14

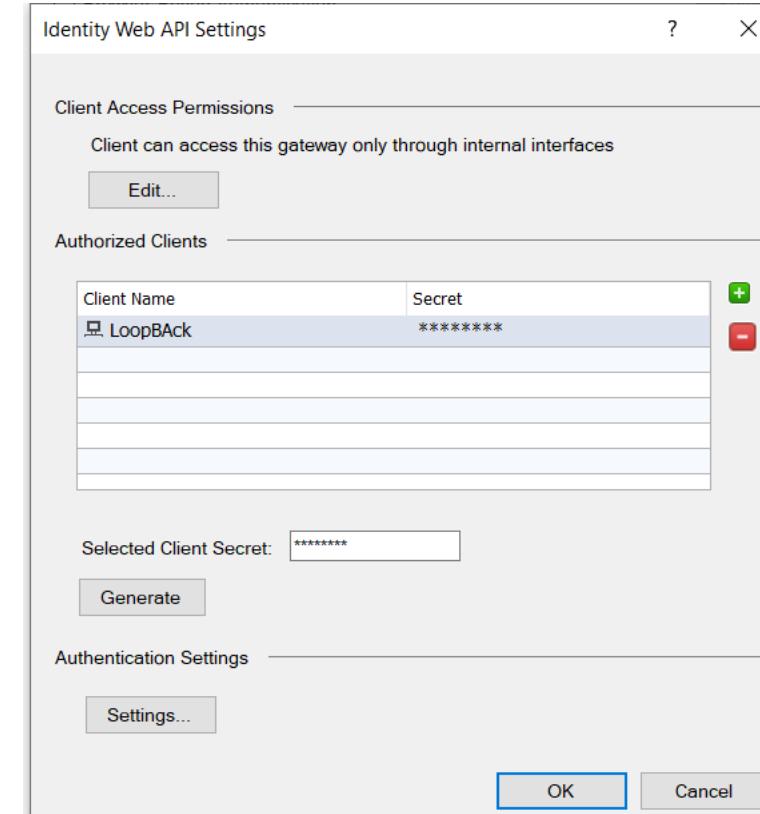
Each dialog box has an 'OK' button at the bottom right and an 'Add Tag' link under the 'Machine' section. The 'Network Management' tab contains a 'Resolve from name' checkbox. The 'Advanced' and 'Servers' tabs are currently empty.

## 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 shows the Check Point SmartConsole interface. On the left, there's a navigation sidebar with icons for Objects, GATEWAYS & SERVERS, SECURITY POLICIES, LOGS & MONITOR, Shared Policies, Geo Po, and Inspect. A large red CloudGuard logo is at the bottom left.

The main area has a title bar "Install Policy". Below it, a modal dialog box titled "SmartConsole" displays the message "You have unpublished changes". It contains fields for "Session name" (set to "admin@9/26/2019") and "Description", and a note "Total draft changes: 5". At the bottom are "Publish & Install" and "Cancel" buttons.

To the right of the dialog, the "Standard" policy page is visible. It shows a summary: "Total changes from last installation (26-09-2019): 5 Changes from 1 sessions (by admin)". Under "Access Control", a checkbox is checked. Under "Threat Prevention", a checkbox is unchecked. Below this, a section for "ILCpMgmt" is shown with IP: 10.0.0.5 | Version: R80.20, with links for "View changes" and "Policy Targets...".

At the bottom, an "Install Mode" section offers three options:

- 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.

Buttons for "Install" and "Cancel" are at the bottom right.

Objects | Install Policy | Discard | Session | 1 | Publish | Check Point SmartConsole

Columns: General | Scripts | Actions | Monitor | Search... | 2 ✓

GATEWAYS & SERVERS | SECURITY POLICIES | LOGS & MONITOR | MANAGE & SETTINGS | COMMAND LINE | WHAT'S NEW

Install policy

Status	Name	IP	Version	Active Blades	Hardware	CPU Usa...	Recommended Updat...	Comme...
✓	cpmgmt	168.63.40.17	R80.20	Network Policy Management	Open server	2%	3 updates available	
✓	ILcpSingleGV	10.0.0.5	R80.20	Logging & Status	CloudGuard...	1%	2 updates available	

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

Summary | Tasks | Errors

**cpmgmt**

IPv4 Address: 168.63.40.17 | OS: Gaia | Version: R80.20 | License Status: Not Activated

Open server

Management Blades

Network Policy Management | Logging & Status

CPU: 2% | Memory: 24%

Device & License Information... | Activate Blades...

No tasks in progress | 1 Draft change saved | admin

Type here to search | 12:01 | ENG | 26-09-2019 | 42

# Let us create TCP object

- One for 8081
- Other for 8082

The screenshot shows the Check Point CloudGuard interface. In the top-left, there's a context menu with options like 'Manage policies and layers...', 'Open Object Explorer...', 'New object' (which is highlighted), 'Publish session', 'Discard session', 'Session details...', 'Install policy...', and 'Verify Access Control Policy...'. Below this, a sub-menu for 'More object types' is open, showing 'Network Object', 'Service' (which is also highlighted), and 'Custom Application/Site'. To the right, there's a table with columns for 'destination...', 'Original Services', 'Translated Source', 'Translated Destination...', and 'Translated S...'. A row in the table shows 'Secn1GW' as the destination, 'http' as the original service, and 'CPGWInternalIP' as the translated source. The 'Translated Destination...' column has two entries: 'AppGWPrivateIP' and 'Http-8081'. The 'Translated S...' column has two entries: 'Http-8082' and 'Http-8081'. A search bar at the top right says 'Search for IP, object, action, ...'.

Two side-by-side windows titled 'New TCP Service'.  
Left window (Http-8081):  
- General tab selected.  
- Protocol: HTTP.  
- Description: '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
- Protocol Signature is disabled

  
Right window (Http-8082):  
- General tab selected.  
- Protocol: HTTP.  
- Description: '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
- Protocol Signature is disabled



## Create policy under Security Policies > Policy section

The screenshot shows the Check Point Management Console interface. On the left, there's a sidebar with icons for GATEWAYS & SERVERS, SECURITY POLICIES (selected), and LOGS & MONITOR. The main area is titled "Access Control" and contains a table of policies:

No.	Name	Source	Destination	VPN	Services & Applications	Action
1	Gaia	* Any	CPExtGW	* Any	https	Accept
2	Inbound-to-Python	* Any	CPExtSecn1GW	* Any	http	Accept
3	Inbound-to-Java	* Any	CPExtSecn2GW	* Any	http	Accept
4	Cleanup rule	* Any	* Any	* Any	* Any	Drop

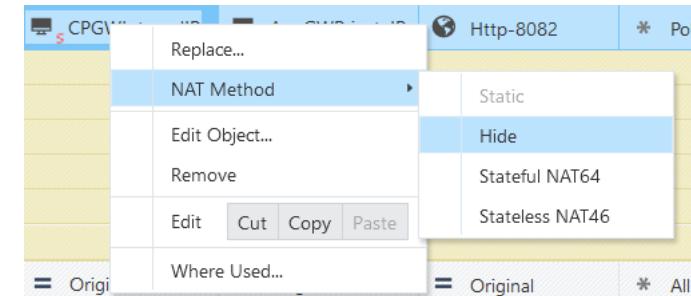
## Create 2 NAT under same section

The screenshot shows the Check Point Management Console interface. On the left, there's a sidebar with icons for GATEWAYS & SERVERS, SECURITY POLICIES (selected), and LOGS & MONITOR. The main area is titled "Access Control" and contains a table of NAT rules:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Install On	Comments
1	All_Internet	CPExtSecn1GW	http	CPGWInternalIP	AppGWPrivateIP	Http-8081	* Policy Targets	
2	All_Internet	CPExtSecn2GW	http	CPGWInternalIP	AppGWPrivateIP	Http-8082	* Policy Targets	

A blue box highlights the "Translated Source" column, and a blue arrow points down to a context menu on the "Translated Source" field of the third row.

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



Till here we are done with the smart console part

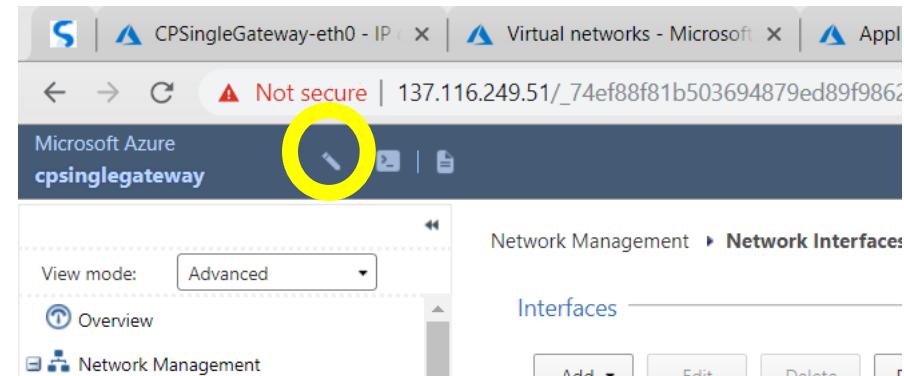
Now we will add the secondary IP's made in azure portal into our firewall interface  
i.e we will make it learn the IP in order to work with them

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



Not secure | 137.116.89f98629c39/cgi-bin/home.tcl

## Network Management > Network Interfaces

**Portal view**

**Go Under Network management > Network interfaces**

Name	Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length	Link Status	Comment
eth0	Ethernet	10.0.0.5	255.255.255.0	-	-		Up
eth0:1	Alias		255.255.255.255	-	-		Up
eth0:2	Alias	10.0.0.6	255.255.255.0	-	-		Up
eth0:3	Alias	10.0.0.7	255.255.255.0	-	-		Up
eth1	Ethernet	10.0.1.4	255.255.255.0	-	-		Up
eth2_rename	Ethernet	-	-	-	-		Down
eth3_rename	Ethernet	-	-	-	-		Down
lo	Loopback	127.0.0.1	255.0.0.0	-	-		Up

Page 1 of 1 | Displaying 1 - 5 of 5

### Management Interface

Management Interface: eth0

**Set Management Interface**

View mode: Advanced

Overview

Network Management

- Network Interfaces
- ARP
- DHCP Server
- Hosts and DNS
- IPv4 Static Routes
- NetFlow Export

System Management

- Time
- Cloning Group
- SNMP
- Job Scheduler
- Mail Notification
- Proxy
- Messages
- Display Format
- Session
- Core Dump
- System Logging
- Network Access
- Host Access

Advanced Routing

- DHCP Relay
- BGP
- IGMP
- IP Broadcast Helper

## Interfaces

	Add	Edit	Delete	Refresh
Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length
Ethernet	10.0.0.5	255.255.255.0	-	-
Alias		255.255.255.255	-	-
Ethernet	10.0.0.6	255.255.255.0	-	-
Alias	10.0.0.7	255.255.255.0	-	-
Ethernet	10.0.1.4	255.255.255.0	-	-
Ethernet	-	-	-	-
Ethernet	-	-	-	-
Loopback	127.0.0.1	255.0.0.0	-	-

1.

## Interfaces

Add	Edit	Delete	Refresh	
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			

Add Alias

Type:  Alias

Enable:

IPv4 IPv6 Alias

Member Of: Select... eth0 eth1 eth2\_rename eth3\_rename

2.

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

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

3.

Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length
Ethernet				
Alias				
Alias				
Alias				
Ethernet				
Ethernet				
Ethernet				
Loopback				

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

4.

# 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

