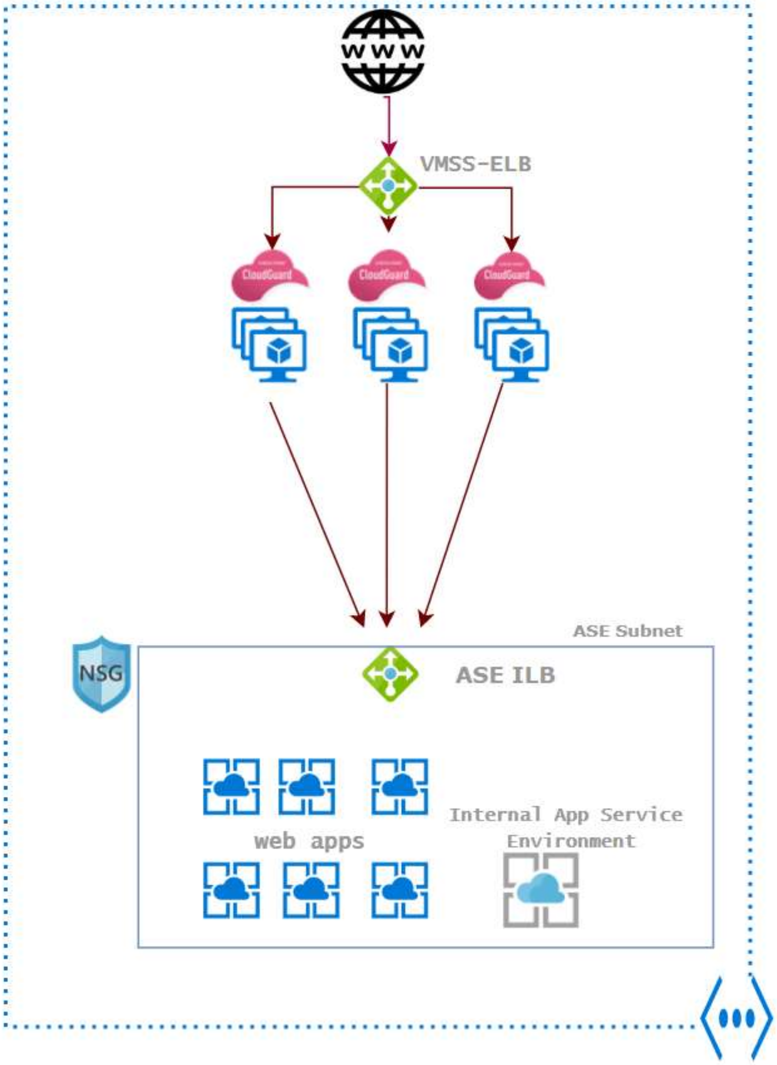
EXPOSING & PROTECTING AZURE WEB APPS WITH CLOUDGUARD IAAS VMSS

Created by: Eugene Tcheby – Cloud Security Architect Canada.
Date: 04/11/2020
Version: 1.0

This document shows how to expose and protect your Web Apps from an Internal App Service Environment in Microsoft Azure with Check Point CloudGuard IaaS as your NVA. In this whitepaper, we will leverage Check Point CloudGuard VMSS deployment with External Load Balancer only.
We are using a simple architecture with both the VMSS and Internal App Service Environment on the same VNET. You can also have App Service Environments spread across multiple VNETs, which can be peered with your security HUB.



In this whitepaper, we are assuming that:

a- You’re familiar with Check Point VMSS deployment and the CME automation for the gateways auto provisioning using autoprov_cfg commands on Check Point Management Server

b- You already went through the deployment steps of both CloudGuard VMSS and Management Server with the latest version of the CME.

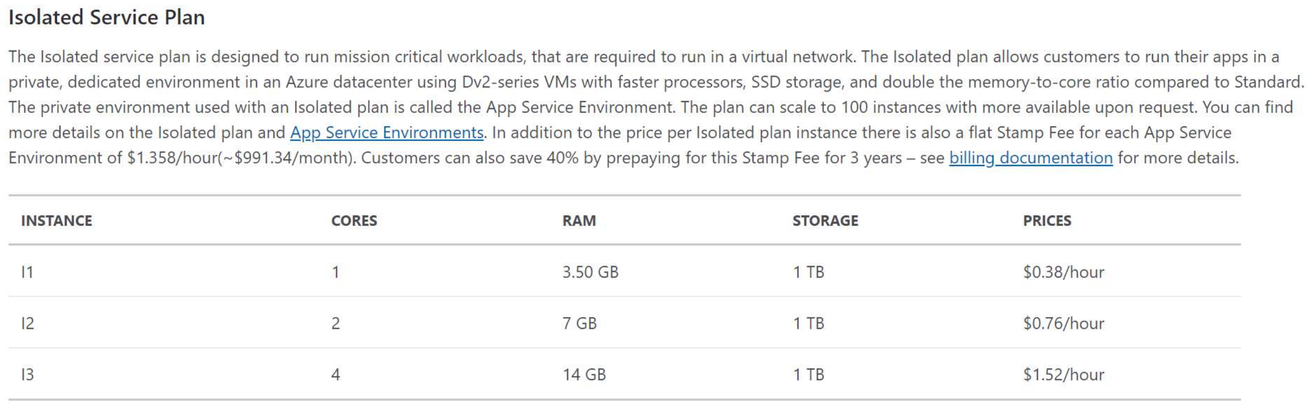
Cloud Management Extension (CME) Admin Guide
https://sc1.checkpoint.com/documents/IaaS/WebAdminGuides/EN/CP_CME/Content/Topics-Cloud_Management_Extension_CME/CME_Structure_and_Configurations.htm?tocpath=____5

CloudGuard VMSS deployment Guide
https://sc1.checkpoint.com/documents/IaaS/WebAdminGuides/EN/CP_VMSS_for_Azure/Content/Topics/Overview.htm?topic=documents/IaaS/WebAdminGuides/EN/CP_VMSS_for_Azure/216060

c- Your VMSS CloudGuard gateways belong to Frontend and Backend subnets of your VNET for their respective external interface eth0 and internal interface eth1.

d- You are familiar with the Azure Standard Load Balancer concepts such as Load Balancer Rules, Health Probes.

e- You are familiar with App Service Plans. We will use Isolated Plan for our app service.
https://azure.microsoft.com/en-us/pricing/details/app-service/linux/



Isolated Service Plan

The Isolated service plan is designed to run mission critical workloads, that are required to run in a virtual network. The Isolated plan allows customers to run their apps in a private, dedicated environment in an Azure datacenter using Dv2-series VMs with faster processors, SSD storage, and double the memory-to-core ratio compared to Standard. The private environment used with an Isolated plan is called the App Service Environment. The plan can scale to 100 instances with more available upon request. You can find more details on the Isolated plan and App Service Environments. In addition to the price per Isolated plan instance there is also a flat Stamp Fee for each App Service Environment of $1.358/hour(~$991.34/month). Customers can also save 40% by prepaying for this Stamp Fee for 3 years – see billing documentation for more details.

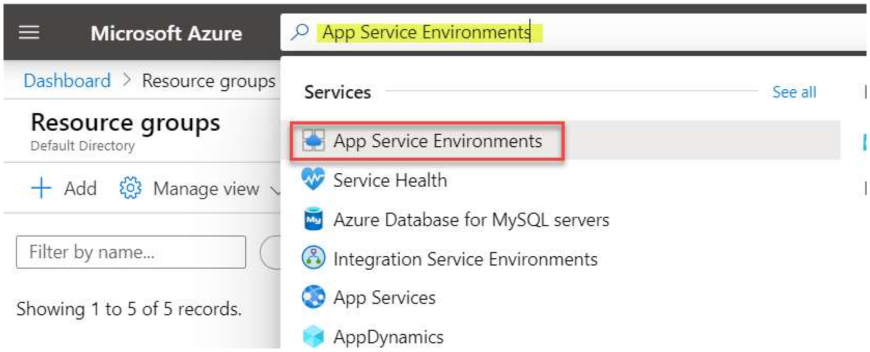
INSTANCE	CORES	RAM	STORAGE	PRICES
I1	1	3.50 GB	1 TB	$0.38/hour
I2	2	7 GB	1 TB	$0.76/hour
I3	4	14 GB	1 TB	$1.52/hour

f- You have a valid domain name.

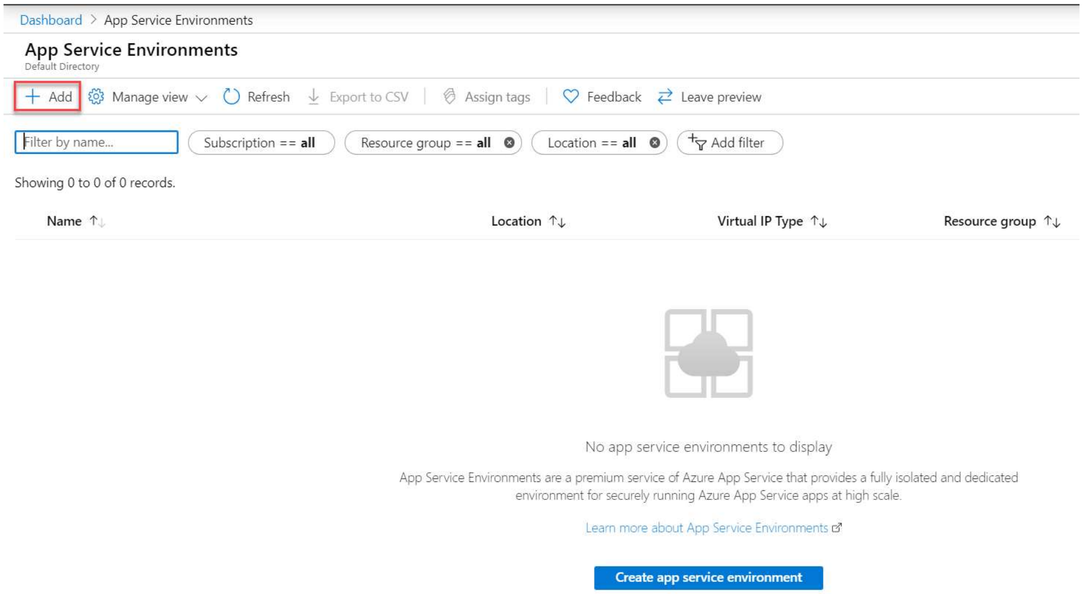
g- You have a valid SSL certificate for https testing purposes (ideal, but optional). I will not be using one, but your browser will generate certificate warnings matching the default Microsoft SSL certificate associate to your web app.

STEP 1: CREATE AN ILB APP SERVICE ENVIRONMENT

From the Azure Portal search “**App Service Environments**”



On the App Service Environment, click **“Add”**

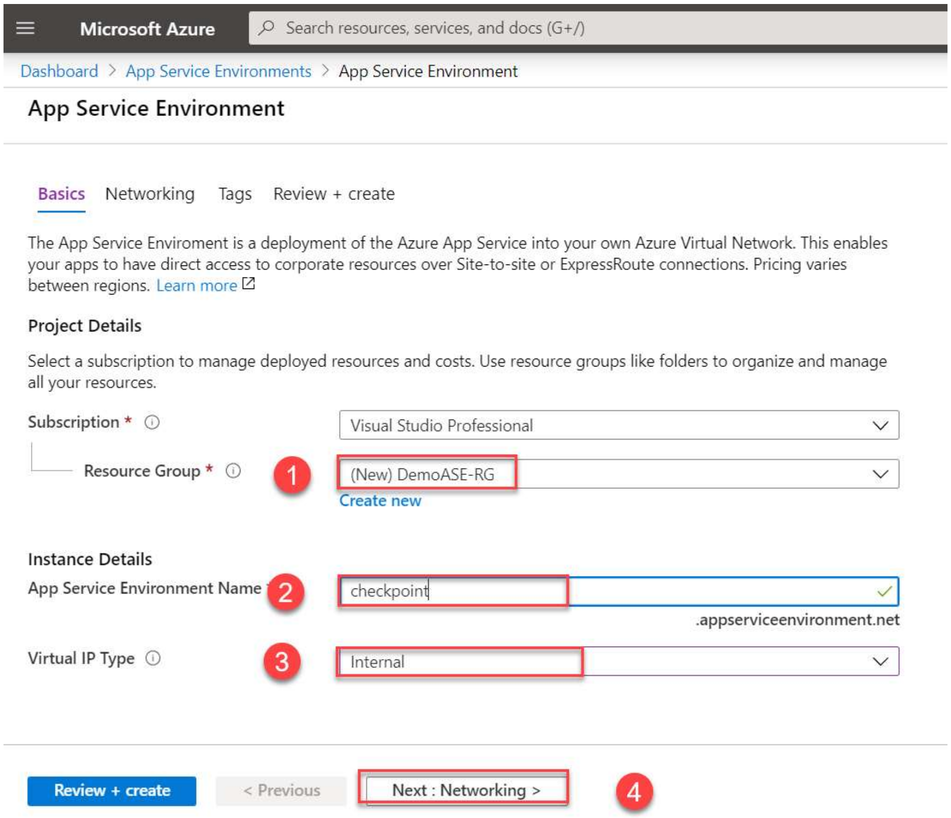


No app service environments to display

App Service Environments are a premium service of Azure App Service that provides a fully isolated and dedicated environment for securely running Azure App Service apps at high scale.

Under Basics Tab

1- Create a new resource group for your App Service Environment.
2- Select a unique App Service Environment Name
3- ***Virtual IP***: Select Internal
4- Once done with above, ***click Next : Networking***


Microsoft Azure
Search resources, services, and docs (G+/)
Dashboard > App Service Environments > App Service Environment

App Service Environment

Basics Networking Tags Review + create

The App Service Enviroment is a deployment of the Azure App Service into your own Azure Virtual Network. This enables your apps to have direct access to corporate resources over Site-to-site or ExpressRoute connections. Pricing varies between regions. Learn more

Project Details

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

Subscription * : Visual Studio Professional

Resource Group * : 1 (New) DemoASE-RG — Create new

Instance Details

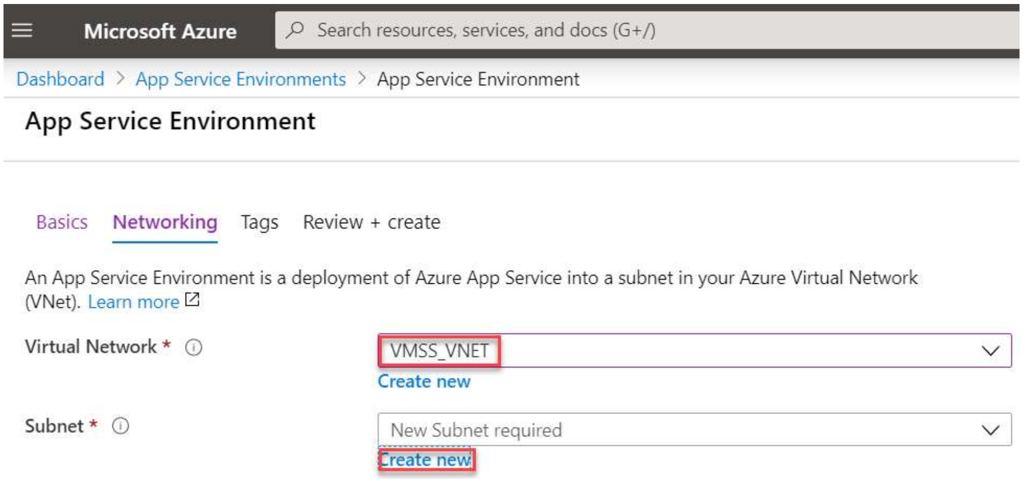
App Service Environment Name : 2 checkpoint .appserviceenvironment.net

Virtual IP Type : 3 Internal

Under the **Networking Tab**,

Virtual Network – From the dropdown, select the existing VNET of the Check Point VMMS solution.

Subnet - Click on **"Create New"**


Microsoft Azure
Search resources, services, and docs (G+/)
Dashboard > App Service Environments > App Service Environment

App Service Environment

Basics Networking Tags Review + create

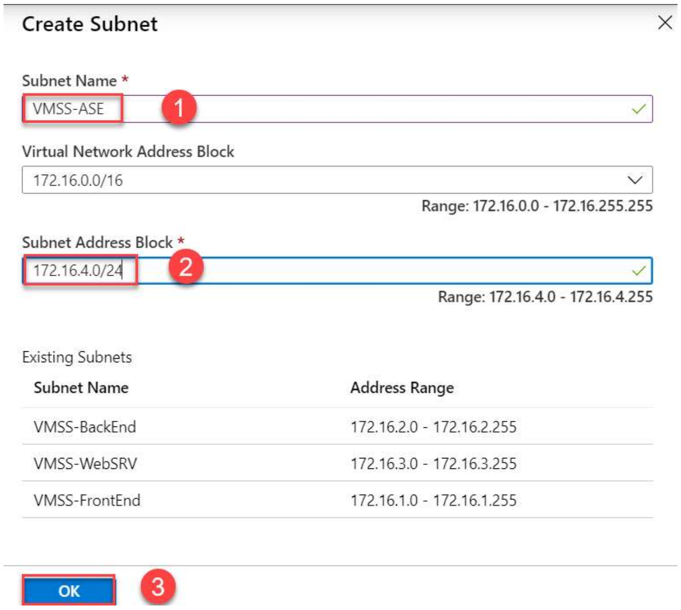
An App Service Environment is a deployment of Azure App Service into a subnet in your Azure Virtual Network (VNet). Learn more

Virtual Network * : VMSS_VNET — Create new

Subnet * : New Subnet required — Create new

Subnet Name: VMSS-ASE (you can use any subnet name of your choice).

Subnet Address Block: 172.16.4.0/24 – (you can create any CIDR block for your subnet based on your VNET configuration).
Once done, click OK



Create Subnet

Subnet Name *
VMSS-ASE

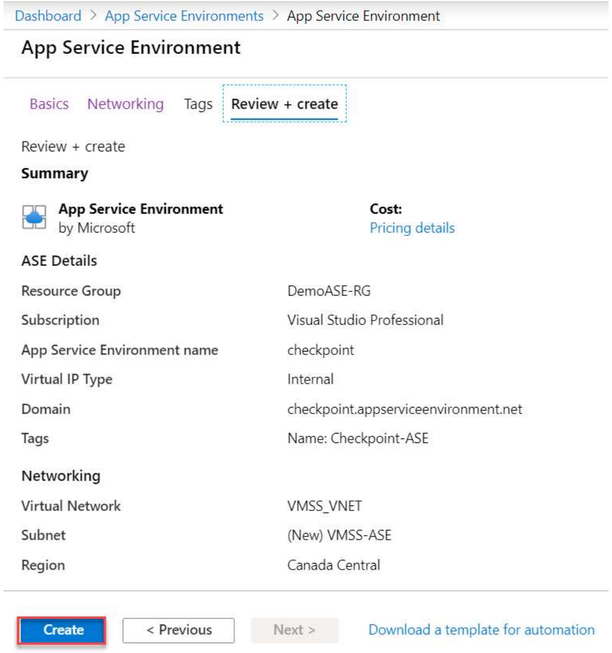
Virtual Network Address Block
172.16.0.0/16
Range: 172.16.0.0 - 172.16.255.255

Subnet Address Block *
172.16.4.0/24
Range: 172.16.4.0 - 172.16.4.255

Existing Subnets

Subnet Name	Address Range
VMSS-BackEnd	172.16.2.0 - 172.16.2.255
VMSS-WebSRV	172.16.3.0 - 172.16.3.255
VMSS-FrontEnd	172.16.1.0 - 172.16.1.255

Skip the Tags tab. Under the **"Review + Create" Tab** check your ASE configuration details and click **"Create"**



Dashboard > App Service Environments > App Service Environment

App Service Environment

Review + create

Summary

App Service Environment
by Microsoft

Cost:
Pricing details

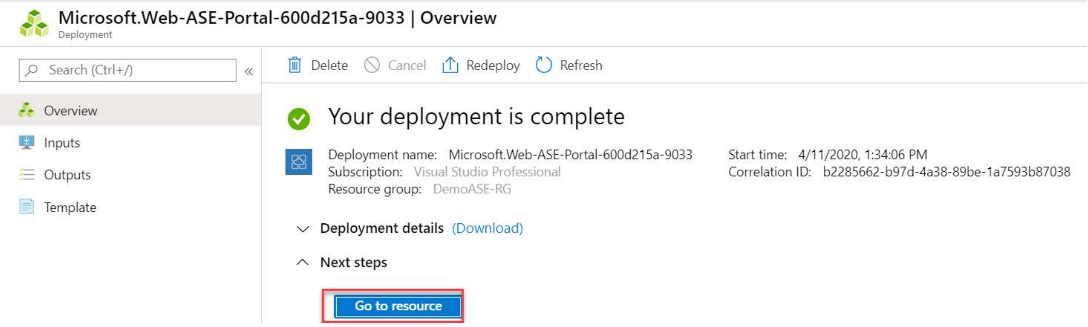
ASE Details

Resource Group	DemoASE-RG
Subscription	Visual Studio Professional
App Service Environment name	checkpoint
Virtual IP Type	Internal
Domain	checkpoint.appserviceenvironment.net
Tags	Name: Checkpoint-ASE

Networking

Virtual Network	VMSS_VNET
Subnet	(New) VMSS-ASE
Region	Canada Central

Please note this deployment takes up to 2 hours. It also creates a route table for the Checkpoint App Service Environment subnet, and a NSG for the ASE subnet.
Once deployment is completed, click **"Go to Resource"**



Your deployment is complete

Deployment name: Microsoft.Web-ASE-Portal-600d215a-9033
Subscription: Visual Studio Professional
Resource group: DemoASE-RG

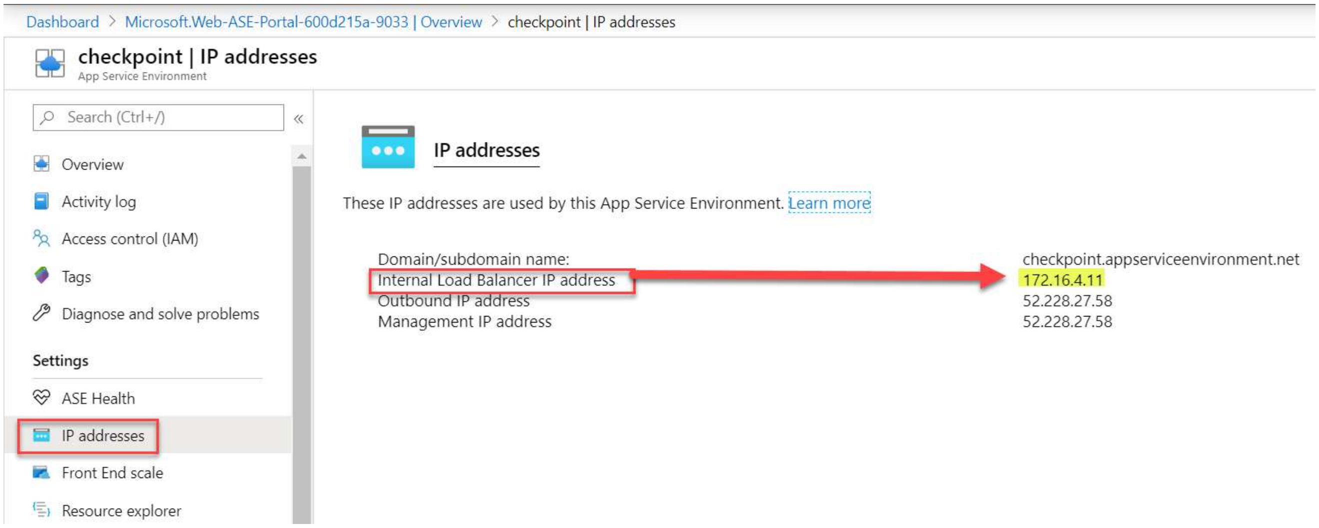
Start time: 4/11/2020, 1:34:06 PM
Correlation ID: b2285662-b97d-4a38-89be-1a7593b87038

Deployment details (Download)

Next steps

Under Settings, select IP addresses, and notice the Internal Load Balancer IP address – The Checkpoint VMSS gateways will forward allowed inbound HTTP(s) connection to the ILB private IP by performing a D-NAT (we will review it later in the Checkpoint Access Control & NAT rules configuration) .
PS: The Management & Outbound public IP are only for your web apps and system to make calls to resources the internet. However, access to the App Service Environment is only accessible via its private endpoint, which the ILB is.

For more information on ILB-ASE Networking, refer to Microsoft Documentation
https://docs.microsoft.com/en-us/azure/app-service/environment/network-info

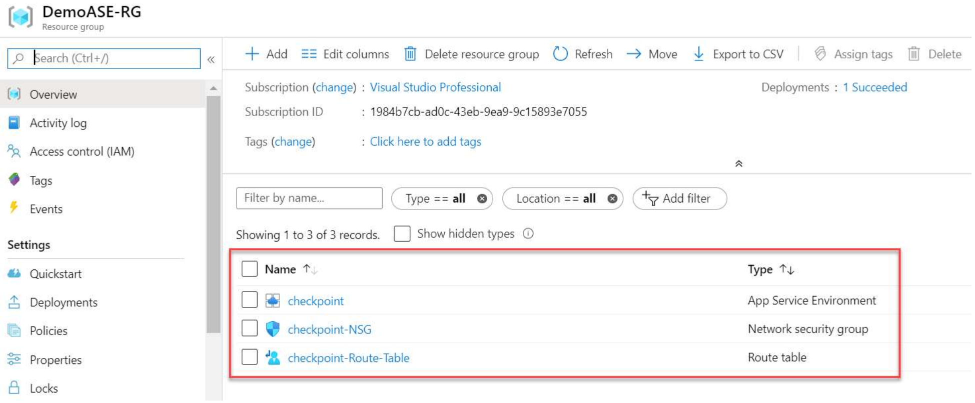


IP addresses

These IP addresses are used by this App Service Environment. Learn more

Domain/subdomain name:	checkpoint.appserviceenvironment.net
Internal Load Balancer IP address	172.16.4.11
Outbound IP address	52.228.27.58
Management IP address	52.228.27.58

From Azure Portal, select Resource Groups. Review the resource created by the ASE deployment.



Subscription (change) : Visual Studio Professional
Subscription ID : 1984b7cb-ad0c-43eb-9ea9-9c15893e7055
Tags (change) : Click here to add tags

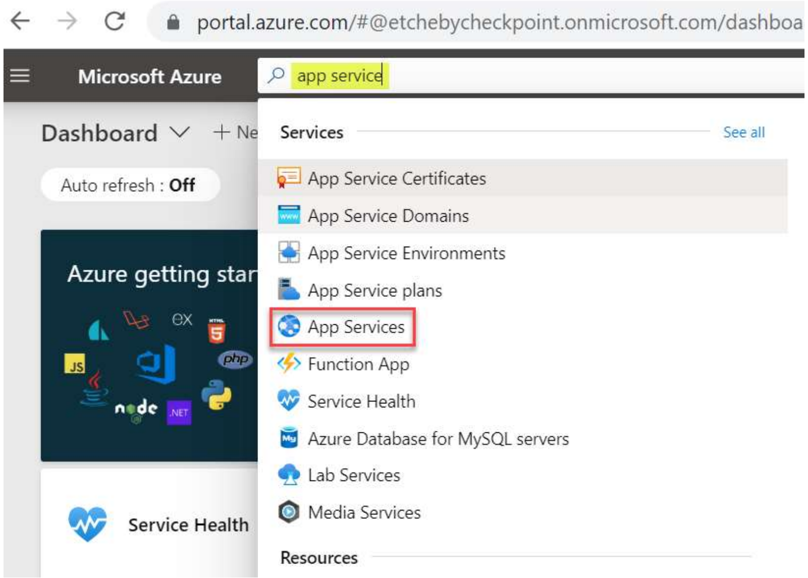
Deployments : 1 Succeeded

Showing 1 to 3 of 3 records. □ Show hidden types

Name ↑↓	Type ↑↓
checkpoint	App Service Environment
checkpoint-NSG	Network security group
checkpoint-Route-Table	Route table

STEP 2: CREATE A WEB APP – USING AZURE APP SERVICES

From the Azure Portal, search **"App Service"**. Select **"App Services"**



portal.azure.com/#@etchebycheckpoint.onmicrosoft.com/dashboa

Microsoft Azure | app service

Dashboard | + Ne

Auto refresh : Off

Azure getting star

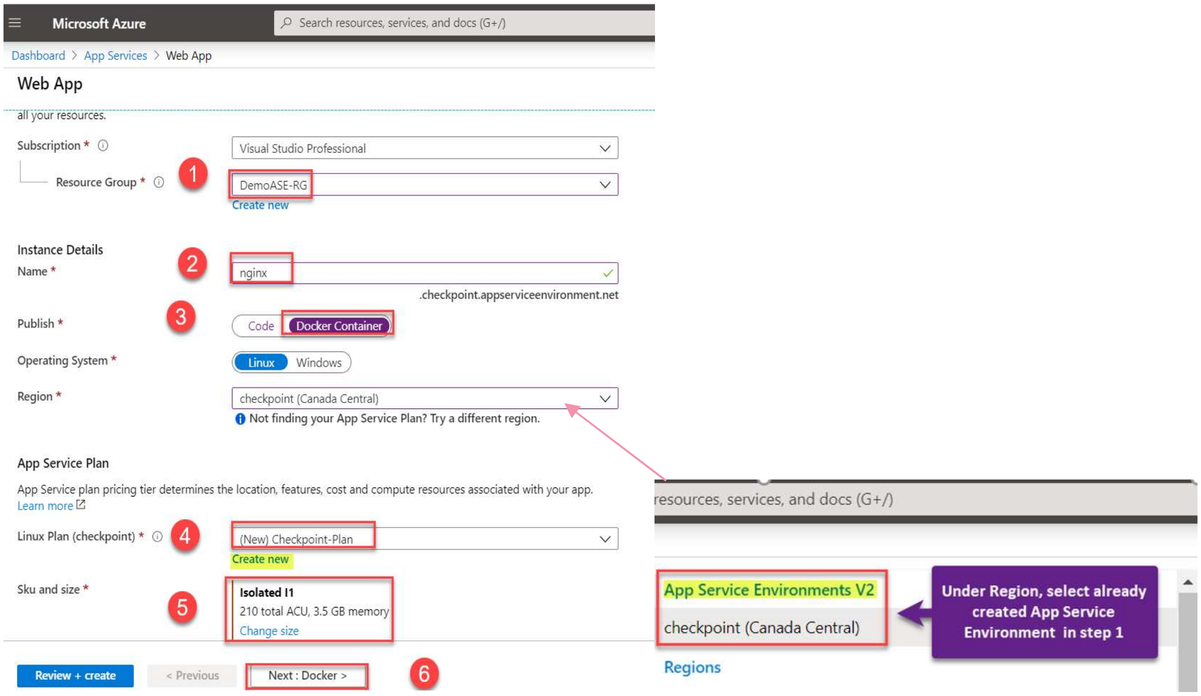
Service Health

Services | See all

- App Service Certificates
- App Service Domains
- App Service Environments
- App Service plans
- App Services
- Function App
- Service Health
- Azure Database for MySQL servers
- Lab Services
- Media Services

Resources

Resource Group: Select same resource as the one you created for the ILB-ASE.
Instance Name: nginx - we are deploying a simple nginx web app. could be any
Publish: Select "Docker Container"
Operating System: Linux
Region: **Select your App Service Environment created in Step 1**
Linux Plan: Create New – Example: Checkpoint-Plan
SKU and Size: Leave default – Isolated I1 (do not change to different SKU and size)
Click ***Next: Docker***



Microsoft Azure | Search resources, services, and docs (G+/)

Dashboard > App Services > Web App

Web App

all your resources.

Subscription * : Visual Studio Professional

1 Resource Group * : DemoASE-RG (Create new)

Instance Details

2 Name * : nginx .checkpoint.appserviceenvironment.net

3 Publish * : Code | Docker Container

Operating System * : Linux | Windows

Region * : checkpoint (Canada Central)

Not finding your App Service Plan? Try a different region.

App Service Plan

App Service plan pricing tier determines the location, features, cost and compute resources associated with your app. Learn more

4 Linux Plan (checkpoint) * : (New) Checkpoint-Plan (Create new)

5 Sku and size * : Isolated I1 — 210 total ACU, 3.5 GB memory — Change size

Review + create | < Previous | 6 Next : Docker >

resources, services, and docs (G+/)

App Service Environments V2

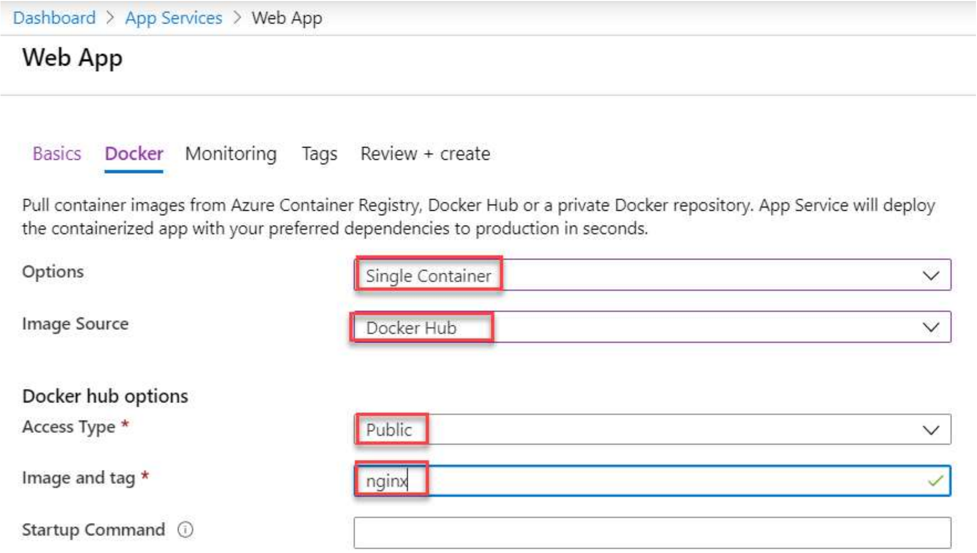
checkpoint (Canada Central)

Regions

Under Region, select already created App Service Environment in step 1

Under Docker Tab, we will configure a single Docker container with the nginx container image from Docker Hub public registry (https://hub.docker.com)

PS: You could also pull any images from your private Azure Container Registry if you have one.
Options: Single Container
Image Source: Docker Hub
Access Type: Public
Image and tag: nginx



Pull container images from Azure Container Registry, Docker Hub or a private Docker repository. App Service will deploy the containerized app with your preferred dependencies to production in seconds.

Options: Single Container

Image Source: Docker Hub

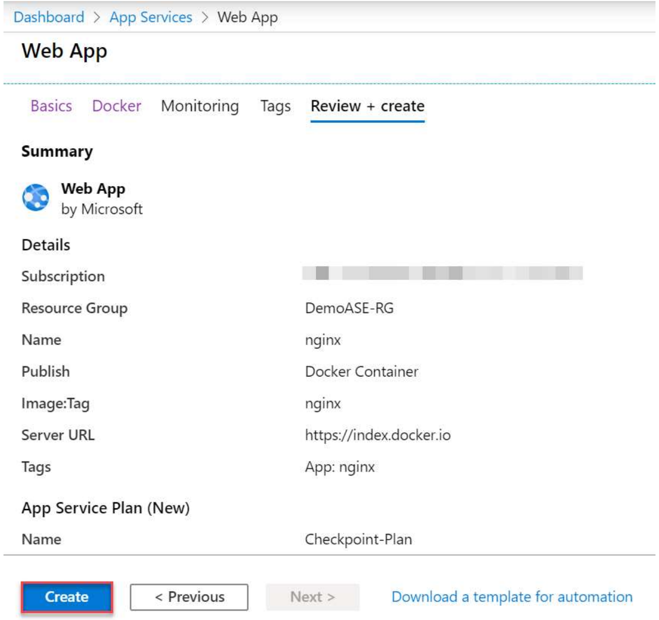
Docker hub options

Access Type *: Public

Image and tag *: nginx

Startup Command

Skip Monitoring & Tags tabs. Under ***Review + Create***, check your web app and container configuration and click **"create"**



Summary

Web App
by Microsoft

Details

Subscription	
Resource Group	DemoASE-RG
Name	nginx
Publish	Docker Container
Image:Tag	nginx
Server URL	https://index.docker.io
Tags	App: nginx

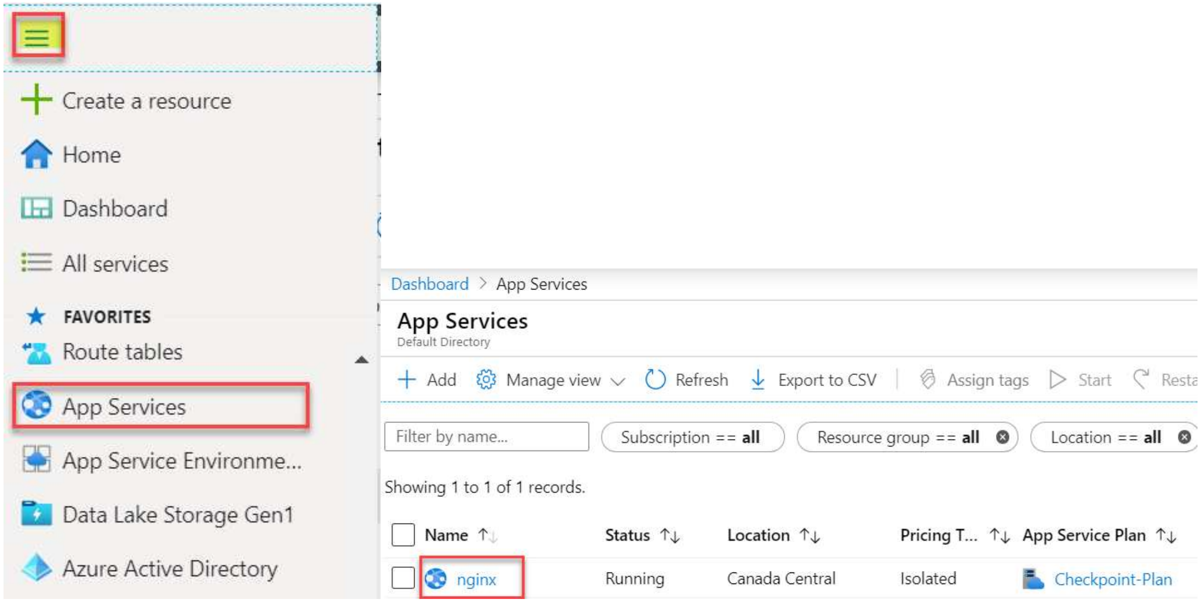
App Service Plan (New)

Name	Checkpoint-Plan

Your web app should be ready and running within a few seconds.

STEP 3 – CONFIGURE YOUR WEB APP CUSTOM DOMAIN WITH YOUR DOMAIN NAME

From the Azure Portal, click on three stripes on top left. Click ***"App Services".***



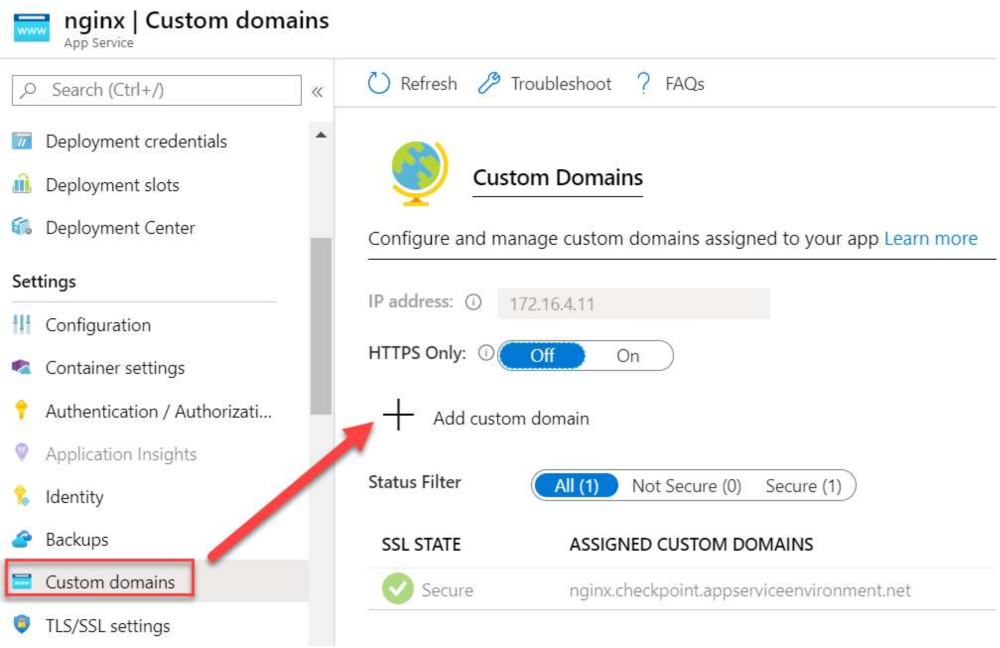
Subscription == all | Resource group == all | Location == all

Showing 1 to 1 of 1 records.

Name	Status	Location	Pricing T...	App Service Plan
nginx	Running	Canada Central	Isolated	Checkpoint-Plan

Then select nginx to open web app we created on step 2.

From the nginx web app menu, select ***Custom Domains > Add custom domain.***
Turn "HTTPS Only" ON if you have a valid SSL certificate. I am not using one in this demo.



Configure and manage custom domains assigned to your app Learn more

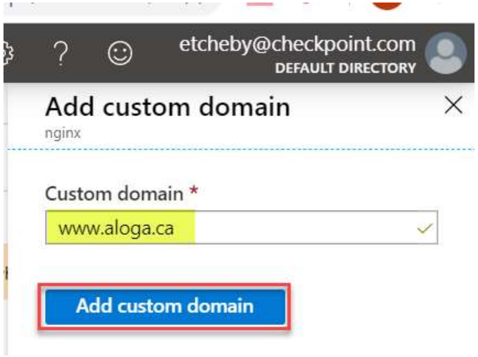
IP address: 172.16.4.11

HTTPS Only: Off On

Status Filter: All (1) Not Secure (0) Secure (1)

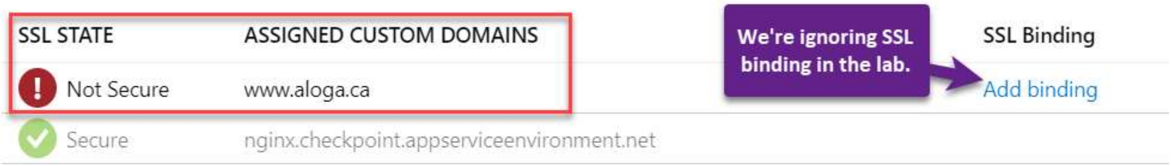
SSL STATE	ASSIGNED CUSTOM DOMAINS
Secure	nginx.checkpoint.appserviceenvironment.net

Under ***Add custom domain***, enter your domain name (below depicts my own domain name)



Custom domain *: www.aloga.ca

After adding your custom domain, it should appear under ***Assigned Custom Domains.***

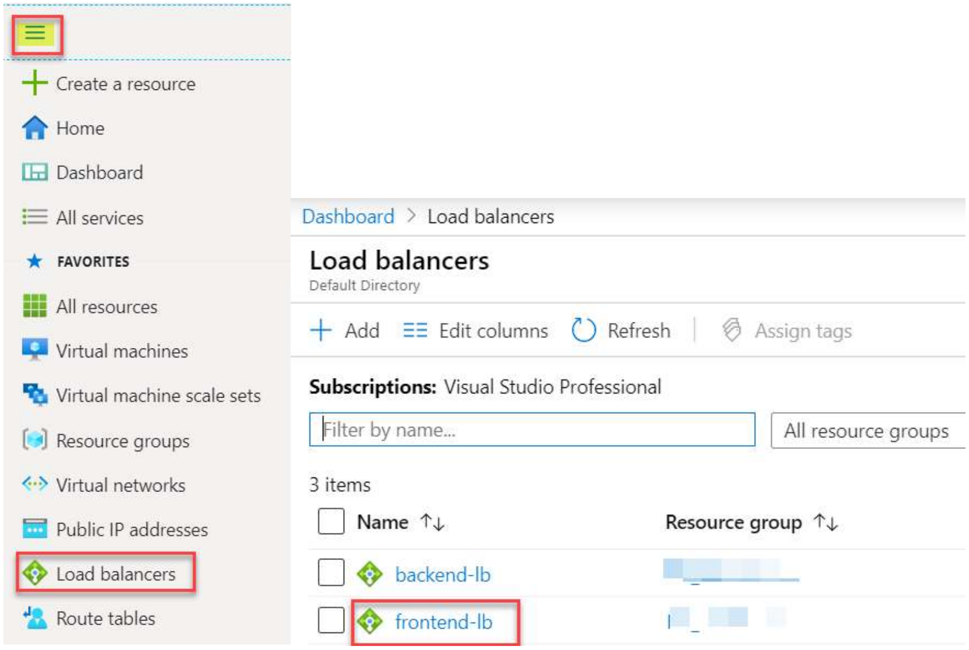


SSL STATE	ASSIGNED CUSTOM DOMAINS	SSL Binding
Not Secure	www.aloga.ca	Add binding
Secure	nginx.checkpoint.appserviceenvironment.net	

We're ignoring SSL binding in the lab.

STEP4 – CHECKPOINT VMSS EXTERNAL LOAD BALANCER & DNS MANAGER CONFIGURATION

From the Azure Portal, select three stripes on top left, click on ***Load Balancers***. By default, the CloudGuard VMSS deployment creates two Load Balancers: Frontend & Backend. Select ***frontend-lb.*** It represents the external LB associated to Public IP (s) to expose our web app.
PS: You could also use a L7 – Azure Application Gateway in front of the Checkpoint VMSS for inbound HTTP(s) host-based redirection rules and SSL offloading.

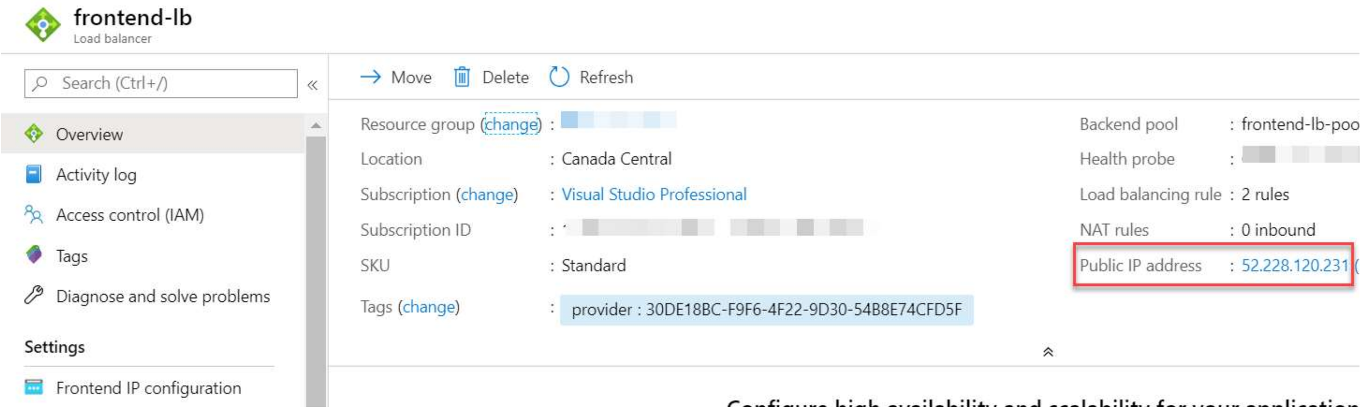


Subscriptions: Visual Studio Professional

3 items

Name	Resource group
backend-lb	[redacted]
frontend-lb	[redacted]

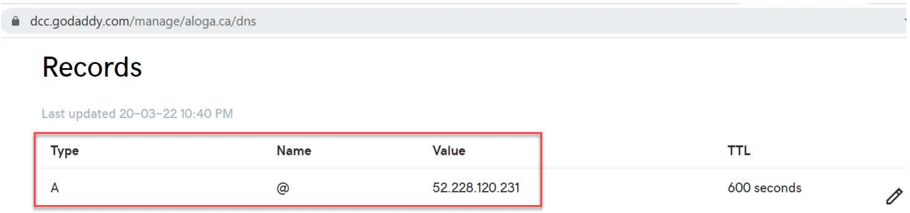
From the frontend-lb overview, obtain the public IP associated to it. It is also possible to get it from the Frontend IP configuration menu.



Resource group (change) : [redacted]
Location : Canada Central
Subscription (change) : Visual Studio Professional
Subscription ID : [redacted]
SKU : Standard
Tags (change) : provider : 30DE18BC-F9F6-4F22-9D30-54B8E74CFD5F

Backend pool : frontend-lb-poo
Health probe : [redacted]
Load balancing rule : 2 rules
NAT rules : 0 inbound
Public IP address : 52.228.120.231

From your DNS Manager, create an A-Record. Your domain name should be matching the Checkpoint VMSS frontend-lb public IP from your load balancer overview or IP configuration,

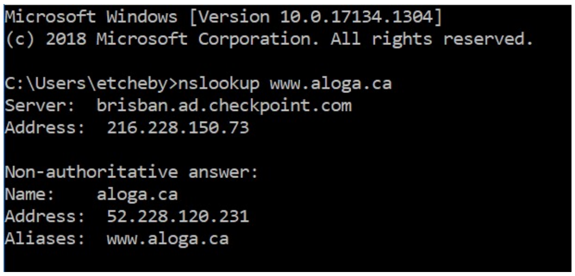

dcc.godaddy.com/manage/aloga.ca/dns

Records

Last updated 20-03-22 10:40 PM

Type	Name	Value	TTL
A	@	52.228.120.231	600 seconds

To make sure your entry was recorded, perform nslookup against your domain name and check if it resolves to your frontend-lb public IP.

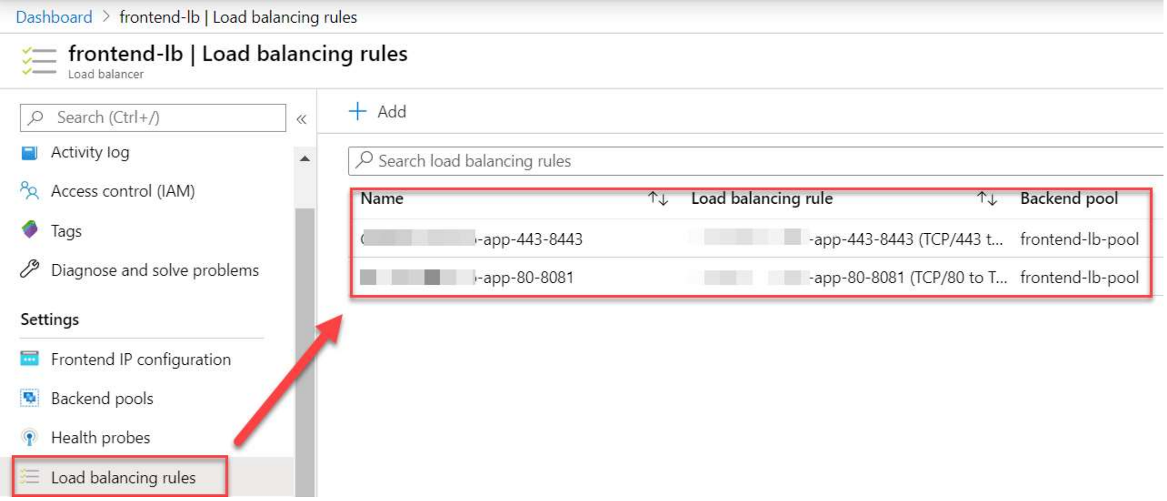

```
Microsoft Windows [Version 10.0.17134.1304]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\etcheby>nslookup www.aloga.ca
Server:  brisban.ad.checkpoint.com
Address:  216.228.150.73

Non-authoritative answer:
Name:    aloga.ca
Address:  52.228.120.231
Aliases:  www.aloga.ca
```

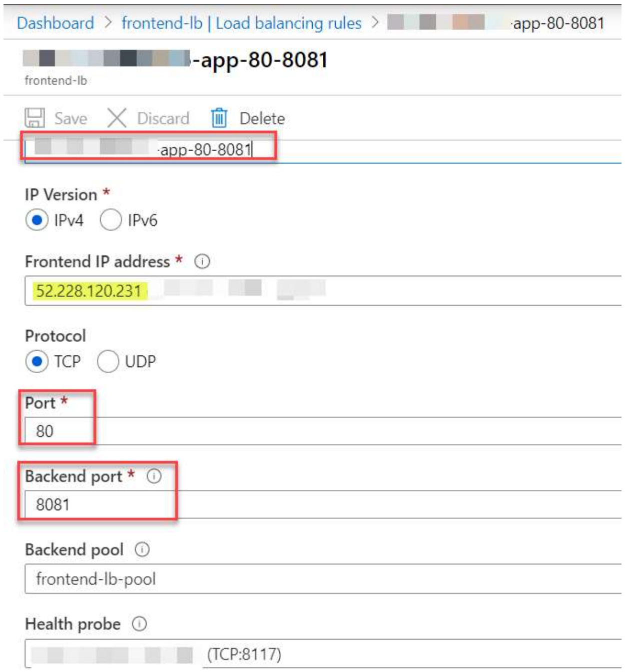
Ensure you have load balancer rules on your frontend-lb to listen on standard ports 80 & 443 (if you are using SSL certificate) to listen on TCP high ports. The Checkpoint VMSS gateways will listen on the defined high ports in the Load Balancer rules.

From the frontend-lb page on Azure Portal, review your load balancing rules


Dashboard > frontend-lb | Load balancing rules
frontend-lb | Load balancing rules
Load balancer
Search (Ctrl+/)
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Frontend IP configuration
Backend pools
Health probes
Load balancing rules
+ Add
Search load balancing rules

Name	Load balancing rule	Backend pool
[redacted]-app-443-8443	[redacted]-app-443-8443 (TCP/443 t...	frontend-lb-pool
[redacted]-app-80-8081	[redacted]-app-80-8081 (TCP/80 to T...	frontend-lb-pool

In the example below, we are using 8081 and 8443 as high ports in the load balancing rules for ports 80 and 443 respectively.


Dashboard > frontend-lb | Load balancing rules > [redacted]app-80-8081
Save
Discard
Delete

[redacted]-app-80-8081

frontend-lb

[redacted]app-80-8081

IP Version *
● IPv4 ○ IPv6

Frontend IP address *
52.228.120.231 [redacted]

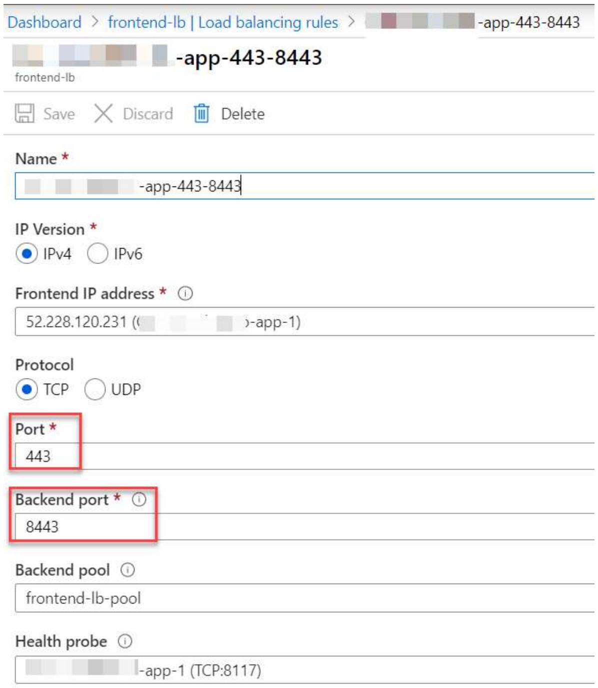
Protocol
● TCP ○ UDP

Port *
80

Backend port *
8081

Backend pool
frontend-lb-pool

Health probe
[redacted] (TCP:8117)


Dashboard > frontend-lb | Load balancing rules > [redacted]-app-443-8443
Save
Discard
Delete

[redacted]-app-443-8443

frontend-lb

Name *
[redacted]-app-443-8443

IP Version *
● IPv4 ○ IPv6

Frontend IP address *
52.228.120.231 ([redacted]-app-1)

Protocol
● TCP ○ UDP

Port *
443

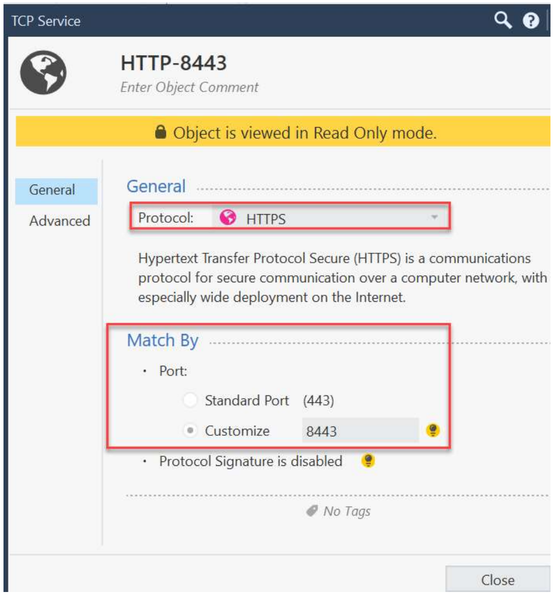
Backend port *
8443

Backend pool
frontend-lb-pool

Health probe
[redacted]-app-1 (TCP:8117)

STEP 5 – ACCESS CONTROL AND NAT RULES CONFIGURATION

Create custom TCP object that represents the high ports the Cloudguard VMSS instances listen on. Based on your frontend-lb load balancing rules.



TCP Service

HTTP-8443

Enter Object Comment

Object is viewed in Read Only mode.

General

Advanced

General

Protocol: HTTPS

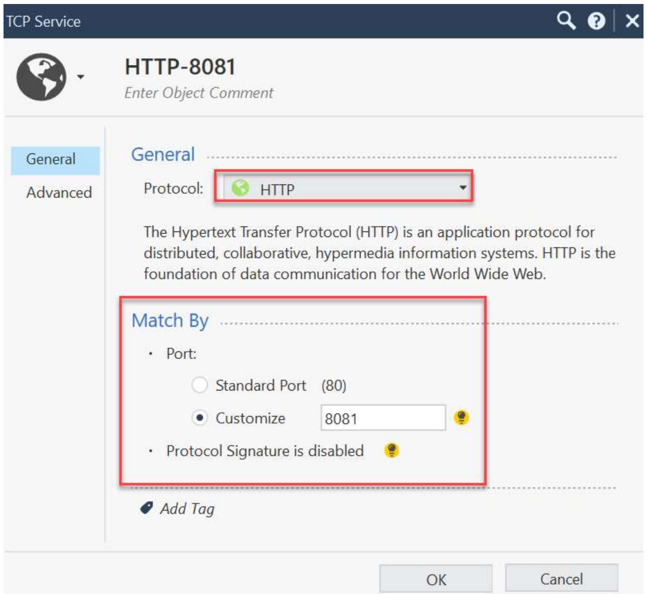
Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.

Match By

- Port:
  - ○ Standard Port (443)
  - ● Customize 8443
- Protocol Signature is disabled

No Tags

Close



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.

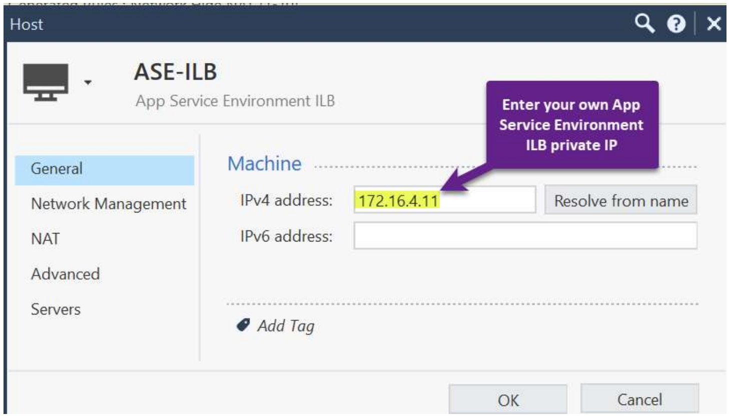
Match By

- Port:
  - ○ Standard Port (80)
  - ● Customize 8081
- Protocol Signature is disabled

Add Tag

OK Cancel

Create a host object that represents your **App Service Environment ILB**



Host

ASE-ILB

App Service Environment ILB

Enter your own App Service Environment ILB private IP

General

Network Management

NAT

Advanced

Servers

Machine

IPv4 address: 172.16.4.11

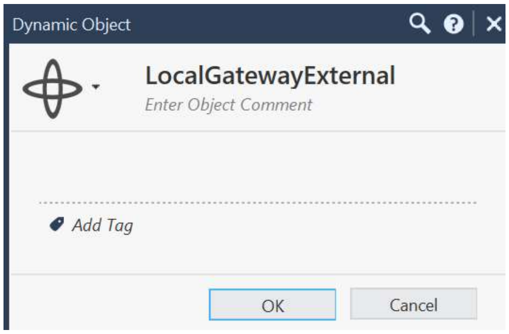
Resolve from name

IPv6 address:

Add Tag

OK Cancel

Create dynamic objects **LocalGatewayExternal & LocalGatewayInternal** that represents the external and internal private IP of the VMSS gateways



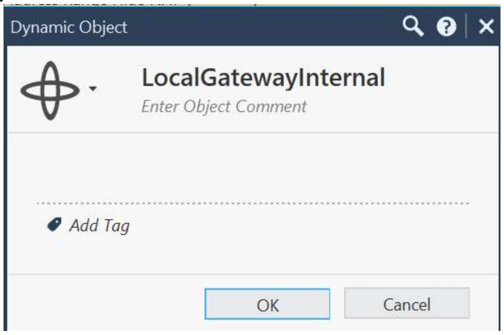
Dynamic Object

LocalGatewayExternal

Enter Object Comment

Add Tag

OK Cancel



Dynamic Object

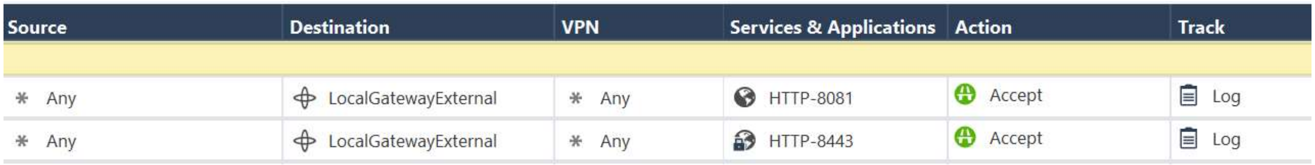
LocalGatewayInternal

Enter Object Comment

Add Tag

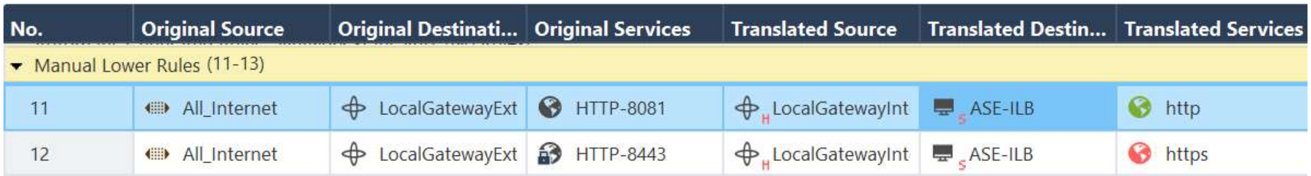
OK Cancel

Access Control Rules



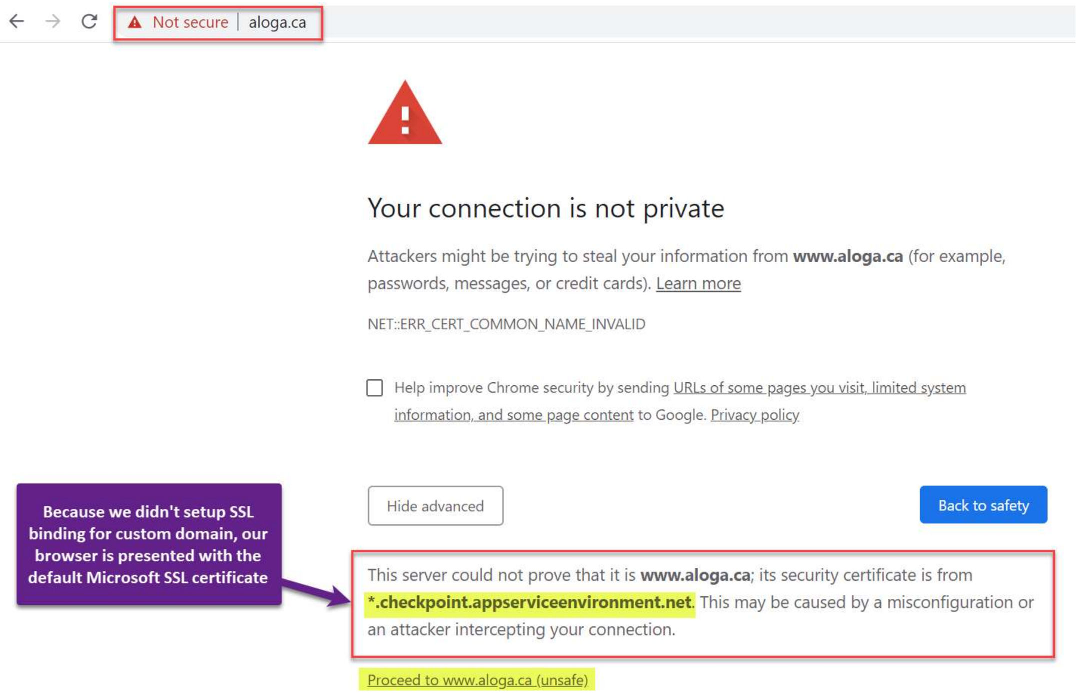
Source	Destination	VPN	Services & Applications	Action	Track
Any	LocalGatewayExternal	Any	HTTP-8081	Accept	Log
Any	LocalGatewayExternal	Any	HTTP-8443	Accept	Log

NAT Rules.



No.	Original Source	Original Destinati...	Original Services	Translated Source	Translated Destin...	Translated Services
Manual Lower Rules (11-13)						
11	All_Internet	LocalGatewayExt	HTTP-8081	LocalGatewayInt	ASE-ILB	http
12	All_Internet	LocalGatewayExt	HTTP-8443	LocalGatewayInt	ASE-ILB	https

Testing of web app. https://www.yourdomain.com



Your connection is not private

Attackers might be trying to steal your information from **www.aloga.ca** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

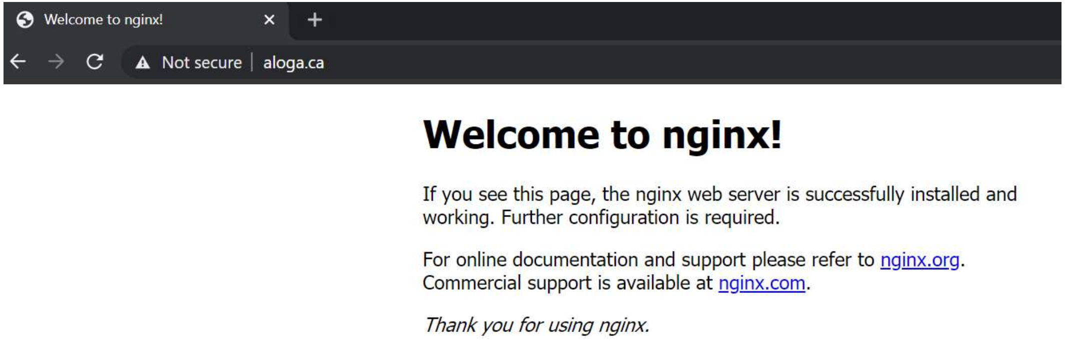
□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

Because we didn't setup SSL binding for custom domain, our browser is presented with the default Microsoft SSL certificate

This server could not prove that it is **www.aloga.ca**; its security certificate is from ***.checkpoint.appserviceenvironment.net**. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to www.aloga.ca (unsafe)

NGNIX test page successful.



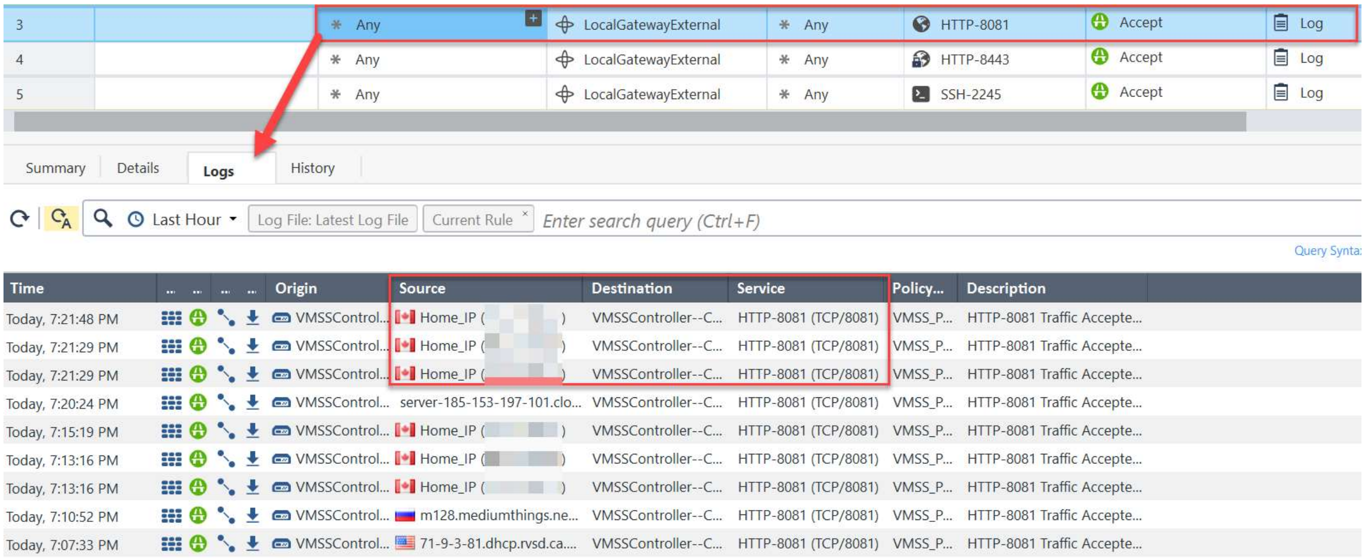
Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

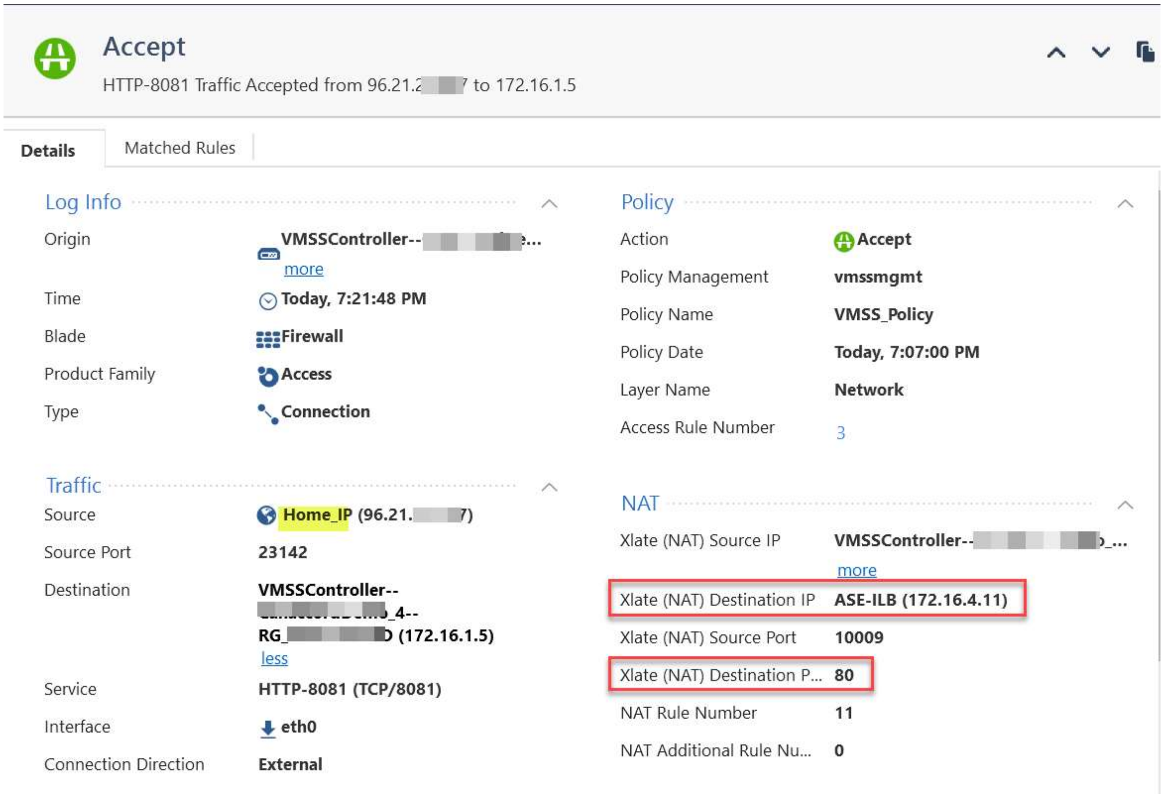
Thank you for using nginx.

Review of logs.



3		Any	LocalGatewayExternal	Any	HTTP-8081	Accept	Log
4		Any	LocalGatewayExternal	Any	HTTP-8443	Accept	Log
5		Any	LocalGatewayExternal	Any	SSH-2245	Accept	Log

Time	Origin	Source	Destination	Service	Policy...	Description
Today, 7:21:48 PM	VMSSControl...	Home_IP ([redacted])	VMSSController--C...	HTTP-8081 (TCP/8081)	VMSS_P...	HTTP-8081 Traffic Accepte...
Today, 7:21:29 PM	VMSSControl...	Home_IP ([redacted])	VMSSController--C...	HTTP-8081 (TCP/8081)	VMSS_P...	HTTP-8081 Traffic Accepte...
Today, 7:21:29 PM	VMSSControl...	Home_IP ([redacted])	VMSSController--C...	HTTP-8081 (TCP/8081)	VMSS_P...	HTTP-8081 Traffic Accepte...
Today, 7:20:24 PM	VMSSControl...	server-185-153-197-101.clo...	VMSSController--C...	HTTP-8081 (TCP/8081)	VMSS_P...	HTTP-8081 Traffic Accepte...
Today, 7:15:19 PM	VMSSControl...	Home_IP ([redacted])	VMSSController--C...	HTTP-8081 (TCP/8081)	VMSS_P...	HTTP-8081 Traffic Accepte...
Today, 7:13:16 PM	VMSSControl...	Home_IP ([redacted])	VMSSController--C...	HTTP-8081 (TCP/8081)	VMSS_P...	HTTP-8081 Traffic Accepte...
Today, 7:13:16 PM	VMSSControl...	Home_IP ([redacted])	VMSSController--C...	HTTP-8081 (TCP/8081)	VMSS_P...	HTTP-8081 Traffic Accepte...
Today, 7:10:52 PM	VMSSControl...	m128.mediumthings.ne...	VMSSController--C...	HTTP-8081 (TCP/8081)	VMSS_P...	HTTP-8081 Traffic Accepte...
Today, 7:07:33 PM	VMSSControl...	71-9-3-81.dhcp.rvsd.ca....	VMSSController--C...	HTTP-8081 (TCP/8081)	VMSS_P...	HTTP-8081 Traffic Accepte...



Accept

HTTP-8081 Traffic Accepted from 96.21.2[redacted]7 to 172.16.1.5

Log Info

Origin	VMSSController--[redacted]e... more
Time	Today, 7:21:48 PM
Blade	Firewall
Product Family	Access
Type	Connection

Traffic

Source	Home_IP (96.21.[redacted]7)
Source Port	23142
Destination	VMSSController--[redacted]_4--RG_[redacted]D (172.16.1.5) less
Service	HTTP-8081 (TCP/8081)
Interface	eth0
Connection Direction	External

Policy

Action	Accept
Policy Management	vmssmgmt
Policy Name	VMSS_Policy
Policy Date	Today, 7:07:00 PM
Layer Name	Network
Access Rule Number	3

NAT

Xlate (NAT) Source IP	VMSSController--[redacted]b_... more
Xlate (NAT) Destination IP	ASE-ILB (172.16.4.11)
Xlate (NAT) Source Port	10009
Xlate (NAT) Destination P...	80
NAT Rule Number	11
NAT Additional Rule Nu...	0