



CLOUDGUARD

29 May 2024

**CLOUDGUARD  
NETWORK FOR  
AVIATRIX**

Deployment Guide



# Check Point Copyright Notice

© 2021 - 2024 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

## RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

## TRADEMARKS:

Refer to the [Copyright page](#) for a list of our trademarks.

Refer to the [Third Party copyright notices](#) for a list of relevant copyrights and third-party licenses.

# Important Information



## Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



## Certifications

For third party independent certification of Check Point products, see the [Check Point Certifications page](#).



## Check Point CloudGuard Network for Aviatrix Deployment Guide



## Latest Version of this Document in English

Open the latest version of this [document in a Web browser](#).  
Download the latest version of this [document in PDF format](#).



## Feedback

Check Point is engaged in a continuous effort to improve its documentation. [Please help us by sending your comments](#).

## Revision History

Date	Description
27 October 2022	Replaced icons
07 December 2021	First release of this document

# Table of Contents

---

<b>Introduction</b> .....	<b>5</b>
Prerequisites .....	5
Architecture Overview .....	5
Context Aware Service Insertion .....	7
Ingress Traffic Flow .....	7
<b>Deploying Check Point Gateways</b> .....	<b>8</b>
Step 1: Required Information .....	8
Step 2: Deploy the Check Point Gateways .....	9
<b>Adding Gateways to the Management Console</b> .....	<b>12</b>
<b>Configuring Egress Routing</b> .....	<b>14</b>
<b>Configuring Ingress Routing</b> .....	<b>16</b>
Step 1: Create a Target Group .....	16
Step 2: Create an Internal Load Balancer .....	16
Step 3: Configure the Security Settings .....	17
Step 4: Configure the External Load Balancer .....	17
Step 5: Configure the Security Policy to Allow Ingress Traffic .....	19

# Introduction

Check Point and Aviatrix have partnered to deliver a best-in-class experience for customers that want to extend advanced security protections and drastically simplifying their multi-cloud network architecture.

Aviatrix cloud networking software delivers a single, common platform for multi-cloud networking, regardless of public cloud providers used. Aviatrix delivers the simplicity and automation enterprises expected in the cloud with the necessary visibility and control.

This document provides instructions about how to configure and deploy Check Point Firewalls from the Aviatrix Controller.

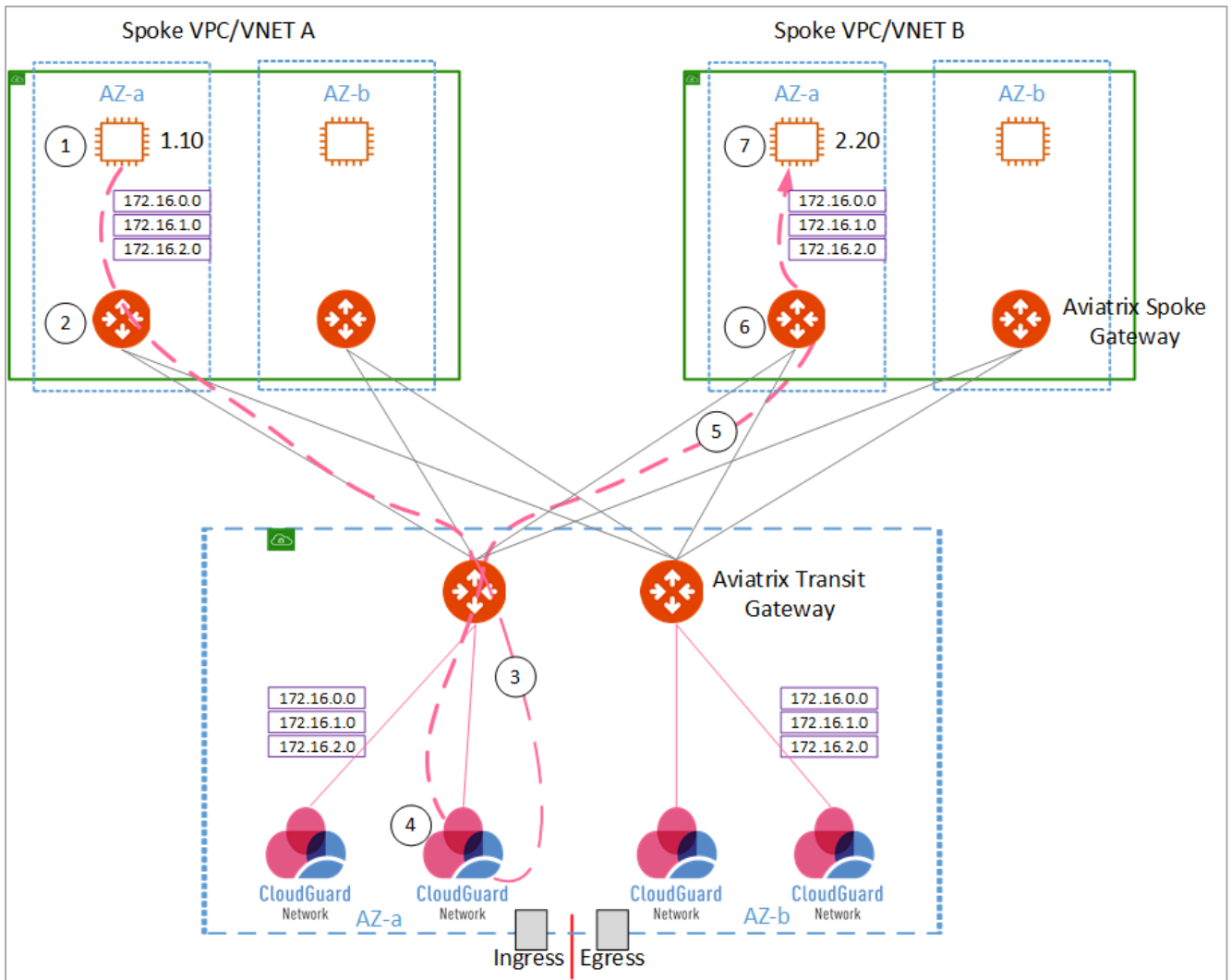
## Prerequisites

- Already configured Aviatrix Controller and Aviatrix Gateways
- All Security Domains are defined in the Aviatrix Controller
- Basic operation knowledge of Aviatrix and Check Point software

## Architecture Overview

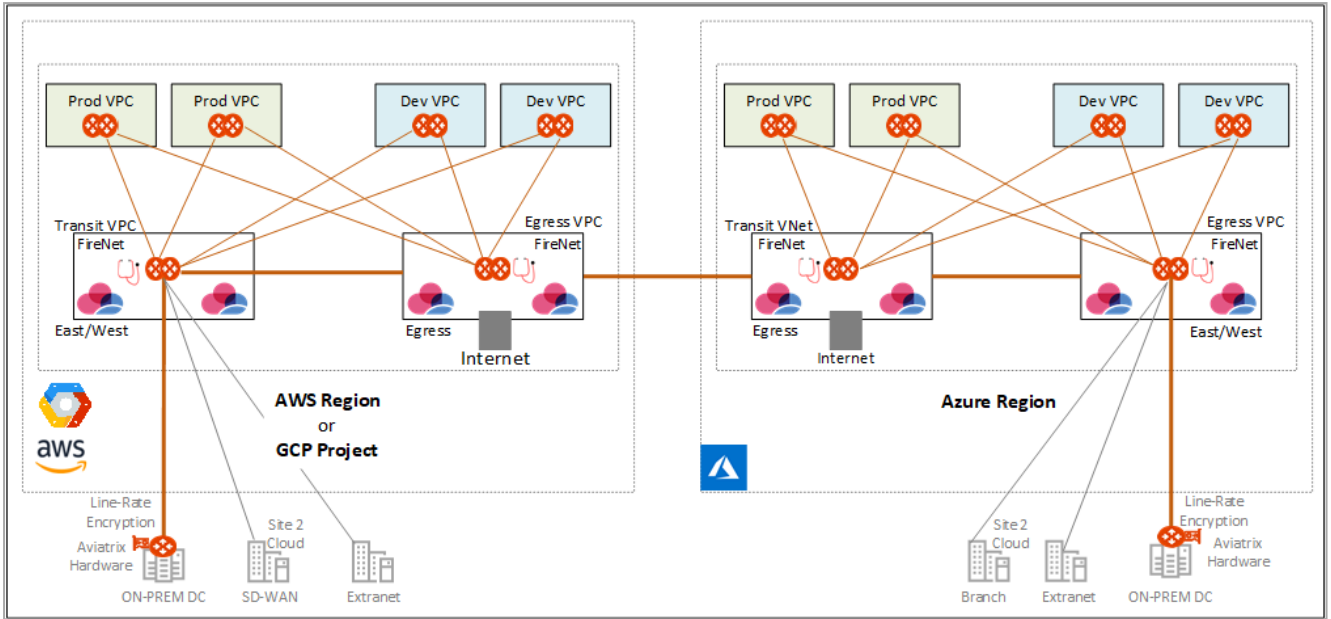
This section provides an overview of a standard design pattern for East-West, Ingress, and Egress traffic inspection with Check Point Security Gateways. To deploy a dedicated ingress zone, see the [Check Point Cloud Security Blueprint 2.0](#).

**Example - East-West Packet Walk for AWS, Azure, and Google (GCP):**



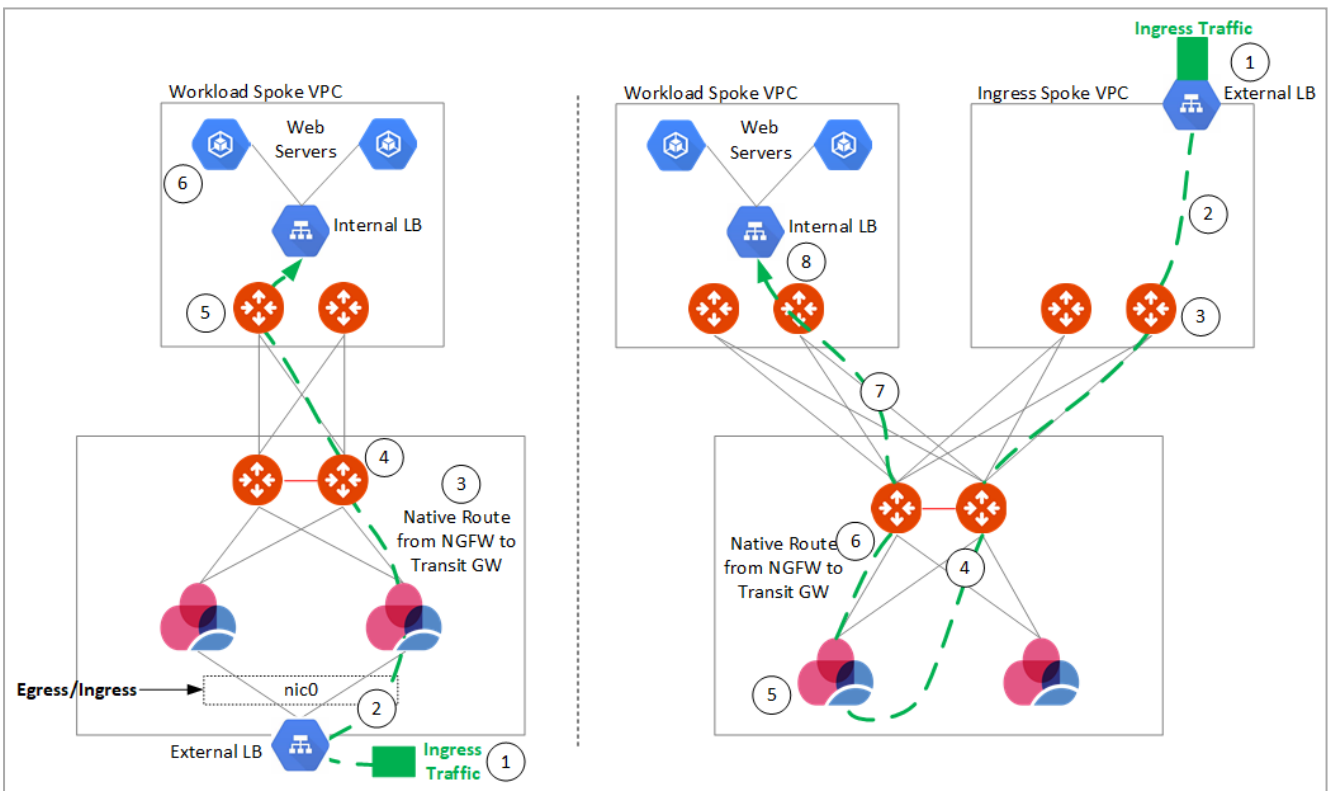
1. Aviatrix programs the local VPC/VNET route table that pointed to the Aviatrix Spoke Gateway.
2. Aviatrix Spoke Gateway sends traffic to one of the Aviatrix Transit Gateways.
3. Aviatrix Transit Gateway PBR rules to determine if either source or destination requires FireNet. If there is a match, then traffic is redirected to the one of the available CloudGuard Security Gateways.
4. CloudGuard processes the packet and sends the traffic back to the Aviatrix Transit Gateway.
5. Aviatrix Transit Gateway receives packet from the CloudGuard Security Gateway and sends the packer to the destination Aviatrix Spoke Gateway.
6. Aviatrix Spoke Gateway routes traffic to the VPC/VNET route table.
7. EC2/VM see this as an native VPC communication flow.

# Context Aware Service Insertion




# Ingress Traffic Flow

Ingress Designs and Packet Walk for AWS, Azure, and Google (GCP)



# Deploying Check Point Gateways

This sections explains step-by-step how to provision two Check Point Gateway (one gateway behind each Aviatrix gateway).

 **Note** - There is an option for customers to deploy more than two Check Point gateways.

## Step 1: Required Information

This table gives the required information to deploy a Check Point Security Gateway.

Device Information	IP Address	Credentials
Aviatrix Cloud Controller		
Check Point SMS		
Check Point SIC Key	N/A	<sic key>
Check Point Gateway Names		<host1/host2...>
GW01 internal router IP		N/A
GW02 internal router IP		N/A
Firewall Interface IP	FW01: External IP FW01: Internal IP	FW02: External IP FW02: Internal IP
Internal Test Server		

For the Internal Router IP, we recommend that you add three return routes, each for a RFC1918 address that points back to the VPC router of the subnet `aviatrix*dmz-firewall` and or `aviatrix*hagw-dmz firewall`, if you attach the instance to the back up gateway.

To do this, navigate to the **AWS Management Console > VPC > Subnets** and filter by "**dmz-firewall**". This allows you to control the VPC router IP, which is the first host for each subnet.

Example:

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4
aviatrix-FireNet-GW-dmz-firewall	subnet-0da5...	available	vpc-02dc5b...	172.22.0.128/28	8
aviatrix-FireNet-GW-hagw-dmz-firewall	subnet-0ebe...	available	vpc-02dc5b...	172.22.0.160/28	9

## Step 2: Deploy the Check Point Gateways

These describe how to deploy Check Point Security Gateways from the Aviatrix Controller.

To deploy a Check Point Gateway:

1. Log in to the Aviatrix Controller.
2. Navigate to Firewall **Network** > **Setup** > **Launch & Associate Firewall Instance**.
3. For each field, enter the required information:
  - **VPC ID** - The Aviatrix Firewall VPC, for a new deployment use only one VPC ID.
  - **Gateway Name** - The Aviatrix Gateway in which this Check Point Firewall is provisioned for. An Aviatrix best practice is to deploy two Aviatrix Gateways, for which it is necessary to deploy two Check Point Firewalls behind each one.
  - Select these options:
    - **Firewall Instance Name**
    - **Firewall Image Version** (If more than two versions are listed, always select the latest one)
    - **Firewall Instance Size**
  - **Egress Interface Subnet**
    - Select the subnet that pertains to the Aviatrix Gateway above
    - Always select the public **fw ingress-egress** subnet
  - **Key Pair Name** (Optional) - You can use an existing key from AWS, or a new key is issued after the gateway is deployed.

### ■ Bootstrap details:

- Username: "admin", password "Aviatrix123#", sic "Aviatrix123"
- Router IP address are different between Primary and Secondary gateways because they are located in different AZs.

4. Verify that each field is correct > click **Launch**. Aviatrix also verifies if the subnet information is correct for the selected Aviatrix Gateway.

5. Keep this window open until the gateway provisioning finishes:

6. Deploy the second Check Point Gateway.

7. Note that a change in these fields to reflect the second Aviatrix Gateway.

- **Gateway Name:** (such as FireNet-GW-hagw)
- **Firewall Instance Name:**
- **Egress Interface Subnet:** (as in us-west-2b)

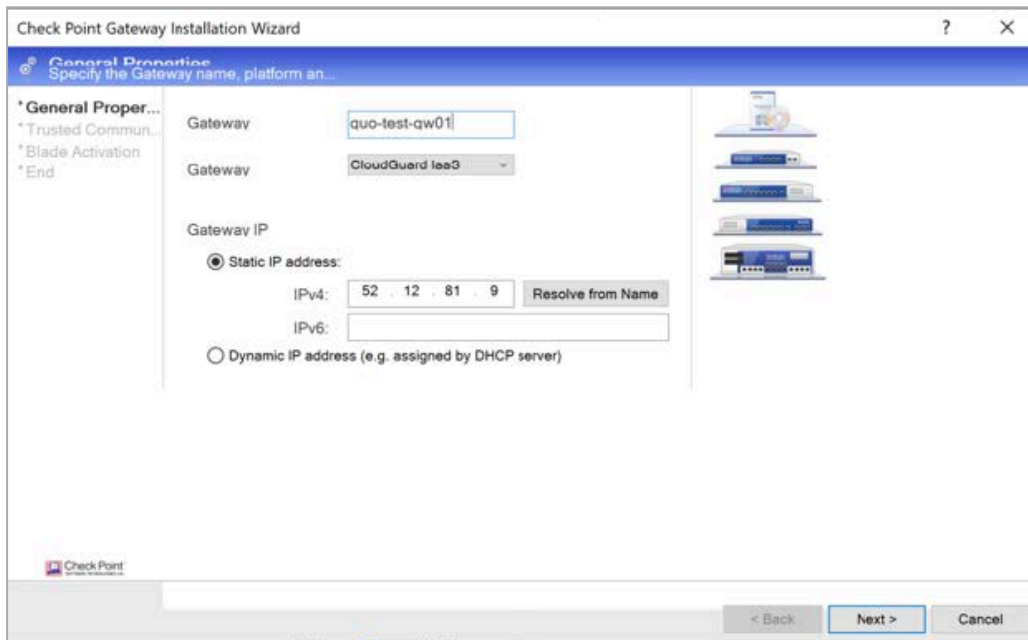
Do these steps again for each gateway.

# Adding Gateways to the Management Console

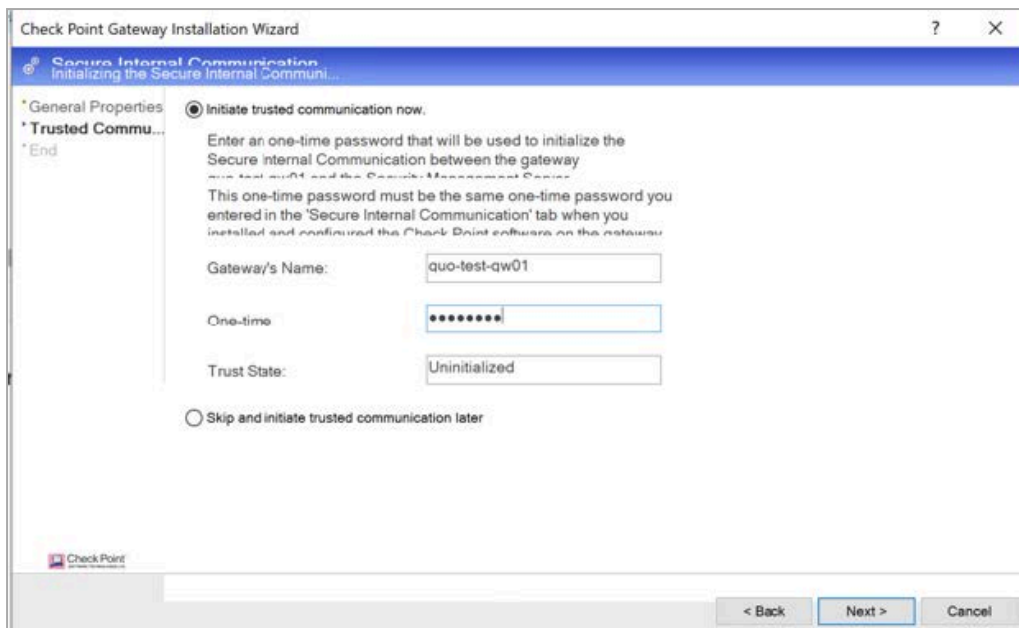
This step describes how to add a Security Gateway to Check Point's Security Management Server. A Security Gateway enforces Security Policies configured on the Security Management Server. To install Security Policies on the Security Gateway, configure the Security Gateway object in SmartConsole.

## To add gateways to the Management Console:

1. Log in to the Check Point Management Console.
2. Create a new single gateway, use the **Wizard** mode.



3. Enter the SIC\_Key used in "Bootstrap details. See ["Deploying Check Point Gateways" on page 8](#).



4. Accept the network values > click **Close**.
5. Stop the Anti-Spoofing Software Blade on the external interface.
  - a. Navigate to **Gateway Object > Network Management > eth0 (external) > Modify**.
  - b. Clear the checkbox **Perform Anti-Spoofing based on interface topology** > click **OK > OK**.
  - c. To close object, click **OK**.
6. Do these steps again for each gateway.

# Configuring Egress Routing

This section describes the necessary steps to configure egress routing.

## To configure egress routing:

1. Configure the Security Policy to allow internal VPC networks to the Internet.

4		net_10.0.0.0_8	* Any	* Any	* Any	Accept	Log	* Policy Targets
5	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets

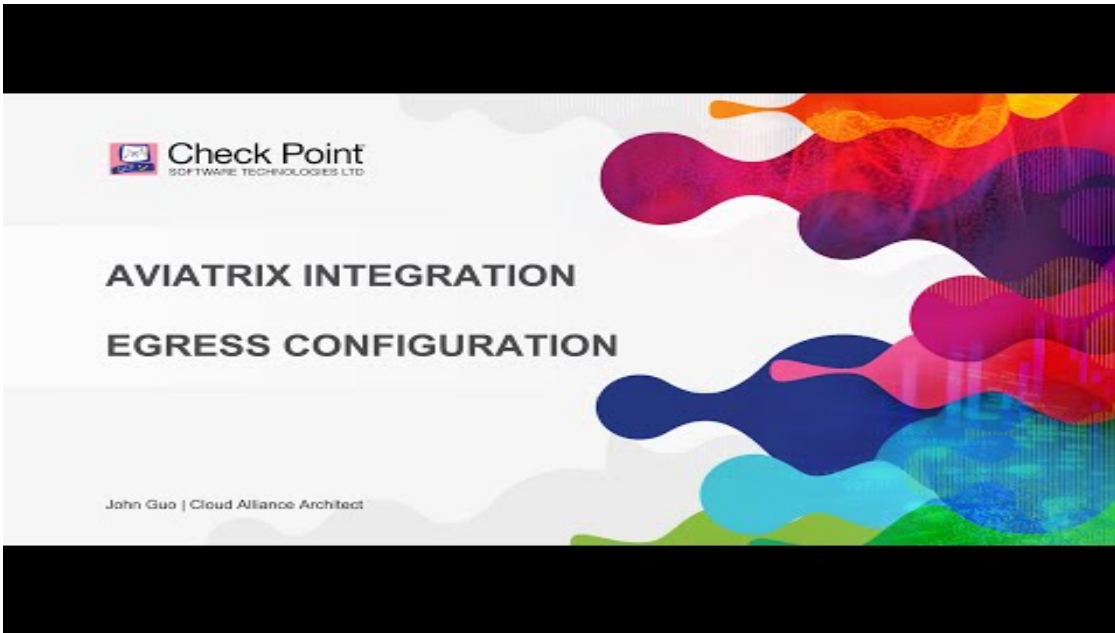
2. Makes sure there is a correct outbound NAT policy setup.

Manual Lower Rules (5-6)								
5	net_10.0.0.0_8	net_10.0.0.0_8	* Any	= Original	= Original	= Original	* Policy Targets	
6	All_Internet	* Any	* Any	All_Internet	= Original	= Original	* Policy Targets	

3. Push the Policy.
4. Use an internal to host to test the outbound connectivity.
  - a. Go to **SmartConsole** > navigate to **Logs & Monitor**.
  - b. Check that traffic is distributed between both Check Point Gateways. This is because traffic is load balanced by Aviatrix Gateways.

Time	Origin	Source	Destination	Service	Access Rule N...	Policy...	Description
Today, 2:38:01 PM	gwan-test-gw01	810.156.49.80 (10.156.49.80)	12.12.12.227	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:01 PM	gwan-test-gw01	810.156.49.80 (10.156.49.80)	12.12.12.236	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:01 PM	gwan-test-gw01	810.156.49.80 (10.156.49.80)	12.12.12.223	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:01 PM	gwan-test-gw01	810.156.49.80 (10.156.49.80)	12.12.12.225	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:02 PM	gwan-test-gw01	810.156.49.80 (10.156.49.80)	12.12.12.241	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:04 PM	gwan-test-gw02	810.156.49.80 (10.156.49.80)	12.12.12.0	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:04 PM	gwan-test-gw02	810.156.49.80 (10.156.49.80)	12.12.12.3	https (TCP/443)	4	Standard	https Traffic Accepted In...
Today, 2:38:04 PM	gwan-test-gw02	810.156.49.80 (10.156.49.80)	12.12.12.2	https (TCP/443)	4	Standard	https Traffic Accepted In...
Today, 2:38:04 PM	gwan-test-gw02	810.156.49.80 (10.156.49.80)	12.12.12.251	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:04 PM	gwan-test-gw02	810.156.49.80 (10.156.49.80)	12.12.12.253	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:04 PM	gwan-test-gw02	810.156.49.80 (10.156.49.80)	12.12.12.255	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:03 PM	gwan-test-gw01	810.156.49.80 (10.156.49.80)	12.12.12.232	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:03 PM	gwan-test-gw02	810.156.49.80 (10.156.49.80)	12.12.12.224	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:03 PM	gwan-test-gw02	810.156.49.80 (10.156.49.80)	12.12.12.229	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:03 PM	gwan-test-gw02	810.156.49.80 (10.156.49.80)	12.12.12.226	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:02 PM	gwan-test-gw02	810.156.49.80 (10.156.49.80)	12.12.12.246	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:02 PM	gwan-test-gw02	810.156.49.80 (10.156.49.80)	12.12.12.244	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:02 PM	gwan-test-gw01	810.156.49.80 (10.156.49.80)	12.12.12.248	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:02 PM	gwan-test-gw01	810.156.49.80 (10.156.49.80)	12.12.12.239	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:02 PM	gwan-test-gw01	810.156.49.80 (10.156.49.80)	12.12.12.237	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:02 PM	gwan-test-gw01	810.156.49.80 (10.156.49.80)	12.12.12.238	http (TCP/80)	4	Standard	http Traffic Accepted In...
Today, 2:38:02 PM	gwan-test-gw01	810.156.49.80 (10.156.49.80)	12.12.12.242	http (TCP/80)	4	Standard	http Traffic Accepted In...

For more information, see this tutorial video.



# Configuring Ingress Routing

This section describes the necessary steps to configure ingress routing.

## Step 1: Create a Target Group

1. Log into the AWS Management Console.
2. Navigate to **Services > EC2 > Load Balancing > Target Groups > Create target group**.
3. Enter these details for the target group:
  - a. **Target Group Name:** guo-internal-80 and guo-internal-22
  - b. **Target type:** Instance
  - c. **Protocol:** TCP
  - d. **Port:** 80 and 22
  - e. **VPC:** <Where test server resides>
4. Click **Create**.
5. Register targets to the internal target group.
  - a. Below **Create target group**, in the **Name** column, select the target group > click **Targets > Edit**.
  - b. Select <**Test Server**> > **Add to registered > Save**.
  - c. For each Target group, repeat steps "a" and "b".

## Step 2: Create an Internal Load Balancer

1. Navigate to **Services > EC2 > Load Balancing > Load Balancer > Create Load Balancer > Create (Network Load Balancer)**.
2. Enter the required details:
  - **Name:** Enter a name
  - **Scheme:** Internal
  - **Listeners:** Ports 80 and 22
  - **VPC:** Where the server resides
  - **AZ:** Select each Availability Zone

## Step 3: Configure the Security Settings

1. Go to **Configure Security Settings > Configure Routing** and enter the necessary details.
2. Enter the required details:
  - **Target Group:** Existing
  - **Name:** guo-internal-22
  - **Next:** Register Targets > Review > Create.
  - **Listeners:** Edit the **listener** to match the associated port(s)

## Step 4: Configure the External Load Balancer

To configure the AWS External Load Balancer, do these steps:

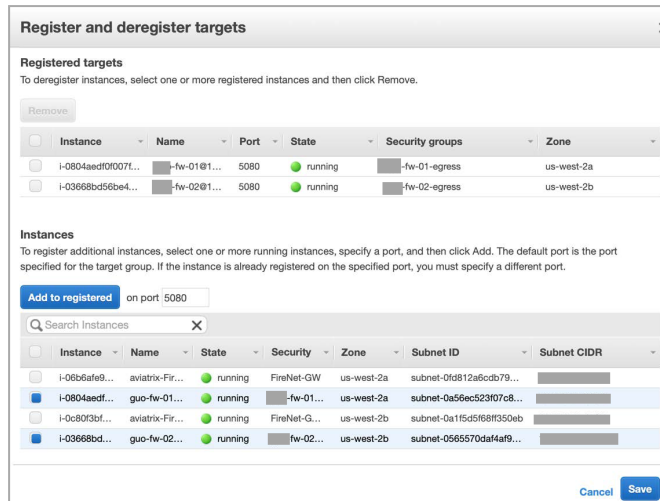
1. Log into the AWS Management Console
2. Navigate to **Services > EC2 > Load Balancing > Target Groups > Create target group.**
3. Create the target groups
  - a. Enter the necessary details:
    - **Target Group Name:** example-external-5080 and guo-internal-5022
    - **Target type:** Instance
    - **Port:** 5080 and 5022
    - **VPC:** <Where firewall resides>

The screenshot shows the 'Create target group' form in the AWS Management Console. The form includes the following fields and values:

- Target group name:** example-external-5080
- Target type:** Instance (selected with a radio button)
- Protocol:** TCP
- Port:** 5080
- VPC:** aviatr

- b. Click **Create**.
- c. Repeat steps 2 and 3 for each target group.

## d. Add firewalls to both external target groups.



## 4. Create an External Load Balancer.

a. Navigate to **Services > EC2 > Load Balancing > Load Balancer > Create Load Balancer > Create (Network Load Balancer)**.

## b. Enter the necessary details:

- **Name:**
- **Scheme:** internet-facing
- **Listeners:** 80 and 22
- **VPC:** Where server resides>
- **AZ:** Select each AZ

## 5. Configure the Security Settings:

a. Go to **Configure Security Settings > Configure Routing**, enter the necessary details:

- **Target Group:** Existing
- **Name:** example-external-5022

b. Click **Next > Register Target > Review**.c. Click **Create**.

## 6. Edit Listeners to match the associated port.

- a. Below Listeners, select Add listener.
- b. Select the checkboxes for **TCP : 22** and **TCP : 80**.

# Step 5: Configure the Security Policy to Allow Ingress Traffic

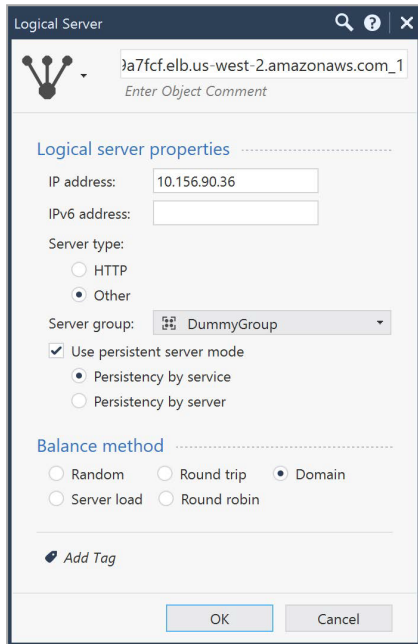
To allow ingress traffic, do these steps:

1. Log into SmartConsole.
2. Create a **Dynamic** object:
  - a. Go to **Object > New > More > Network Object > Dynamic Objects > Dynamic Objects**.
  - b. In the **Name** field, give the object this name: LocalGatewayInternal
  - c. Repeat steps "a" and "b" for the second Dynamic object.
3. Create a dummy host object:
  - a. Go to **Object > New > Host**.
  - b. Enter the necessary details:
    - Name: DummyHost
    - IP: 169.254.1.1
4. Create a dummy object group
  - a. Go to **Objects > New > Network Group**.
  - b. In the **Name** field, enter DummyGroup.
  - c. Add the DummyHost to this DummyGroup.
5. Create two Logical Servers.
  - a. Go to **Object > New > More > Network Object > More > Logical Server**.
  - b. In the **Name** field, enter the DNS name provided by the AWS Internal Load Balancer.

Example:

```
fw01 = internal-InternalELB-1087819072.us-east-1.elb.amazonaws.com_1)
fw02 = internal-InternalELB-1087819072.us-east-1.elb.amazonaws.com_2
```

- c. In the **IPv4 Address** field, enter the external IP address associated with the gateway instance.
- d. For **Server's type**, select **Other**. Note - Select **Other** even if you work with HTTP.
- e. Select the checkbox **Persistent server mode** and keep the default option **Persistency by service**.
- f. Below **Balance Method**, select **Domain**.
- g. Repeat steps "a" through "f" for each gateway. Remember, put "**\_<Number>**" at the end of the Logical server name, as in this example:



6. Create an Access Rule:

No.	Source	Destination	VPN	Services & Applica...	Action	Track	Inst
1	* Any	guo-internal-lb-311be751719a7fcf.elb.us-west-2.amazonaws.com_1 guo-internal-lb-311be751719a7fcf.elb.us-west-2.amazonaws.com_2	* Any	tcp_5022 tcp_5080	Accept	Log	*

7. Create a NAT rule:

No.	Original Source	Original Destination	Original Services	Translated Source	Translated Destin...	Translated Services	Install On
1	All_Internet	LocalGatewayExternal	tcp_5080	LocalGatewayInternal	Original	http	* Policy Targets
2	All_Internet	LocalGatewayExternal	tcp_5022	LocalGatewayInternal	Original	ssh	* Policy Targets

8. Push the policy.

9. Verify the connection

- a. Copy the DNS name of the External Load Balancer.
- b. Open a browser and paste the External Load Balancer's DNS name.

c. Verify the log entry.

