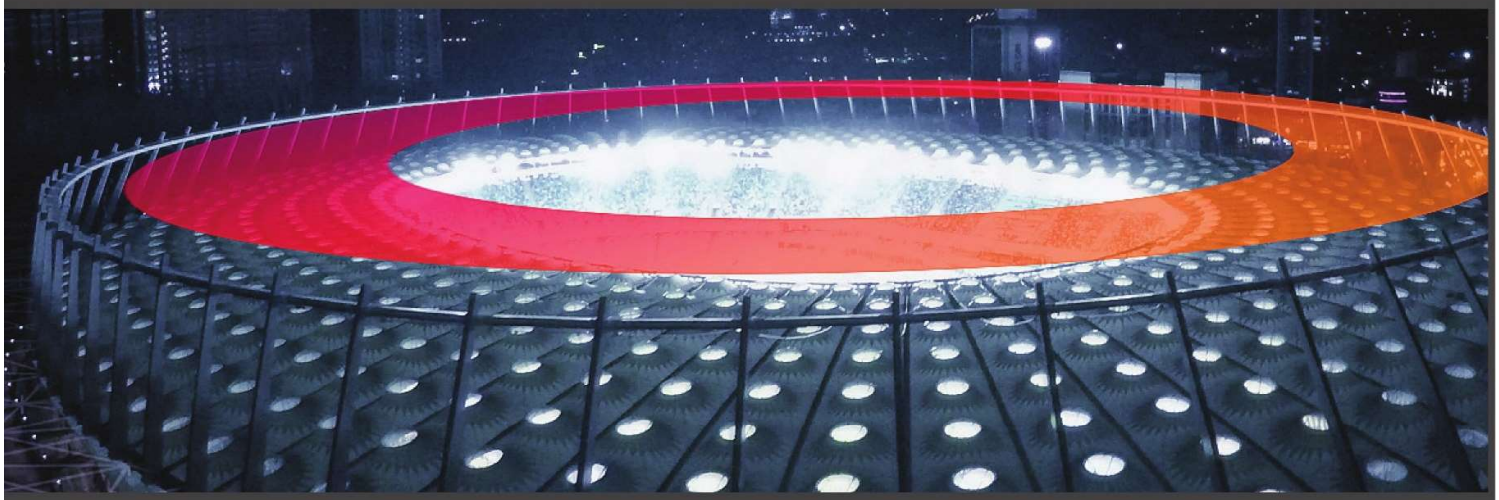
allot
See. Control. Secure.



Allot ACTI AWS
Deployment Guide

ACTI o 20.x

See. Control. Secure.

Version History

Each document has a version and a build number. The exact version and build of this document is found in the top row of the table below.

Document updates are released in electronic form from time to time and the most up to date version of this document will always be found on Allot's online Knowledge Base. To check for more recent versions:

1. **Log in** to the *support portal*.
2. **Navigate** to the *Knowledge Base*.
3. **Input** the *title* of this document in the search field.

Doc Rev	Internal Build	Product Version	Publisher	Summary of Changes
1	20.X.X		Tal Gindi / Michael Benattar	Created a brand-new ACTI AWS installation guide
2	20.X.X		Tal G / Sagi / Reddy	Enhanced Rev 1

Contents

VERSION HISTORY ii
CONTENTS iii
1 INTRODUCTION 1
1.1 EXPECTED EXECUTION TIME 1
1.2 ACRONYMS 1
1.3 DISCLAIMER 2
2 ACTI IN ENTERPRISE PUBLIC CLOUD ENVIRONMENTS 3
2.1 ALLOT CUSTOMER TYPES 3
2.2 ALLOT ACTI PUBLIC CLOUD DEPLOYMENT 4
2.3 SYSTEM OVERVIEW 8
2.4 INTERNAL ARCHITECTURE DIAGRAMS: 8
3 REQUIREMENTS AND PREREQUISITES 9
3.1 INFRASTRUCTURE: 9
3.2 ADDITIONAL SOFTWARE INFRASTRUCTURE ITEMS 9
3.2.1 USER PLANE & MANAGEMENT PLANE 9
3.3 PERMISSIONS 10
3.4 IMAGE TO AMI 10
4 ACTI V&C CLOUDFORMATION DEPLOYMENT VERIFICATION 11
4.1 METADATA AND PARAMETER GROUPING 11
STEP 1: VERIFY PARAMETER GROUPS IN THE AWS CONSOLE TO ENSURE CLARITY DURING STACK CREATION. 11
4.2 PARAMETERS DEFINE CUSTOMIZABLE INPUTS FOR STACK DEPLOYMENT. 12
STEP 2: INPUT THE FOLLOWING PARAMETERS DURING STACK CREATION: 12
4.3 MAPPINGS MAPS CIDR PREFIX LENGTHS TO BIT VALUES FOR SUBNET CALCULATIONS. 12
STEP 3: VERIFY THAT THE VPC CIDR CAN ACCOMMODATE THE DEFINED SUBNETS. 12
4.4 CONDITIONS DEFINES CONDITIONS TO CONTROL RESOURCE CREATION BASED ON PARAMETERS. 12
STEP 4: REVIEW AND ADJUST CONDITIONS BASED ON DEPLOYMENT NEEDS. 13
4.5 RESOURCES DEFINES ALL AWS RESOURCES TO BE CREATED. 13
STEP 5: ENSURE KEY PAIRS EXIST OR ARE GENERATED AUTOMATICALLY. 13
STEP 6: CONFIRM SUBNET ALLOCATION IN THE VPC DASHBOARD. 13
STEP 7: VALIDATE SECURITY GROUP RULES IN THE EC2 DASHBOARD. 13
STEP 8: ENSURE THE GWLB AND ENDPOINT SERVICE ARE OPERATIONAL. 13
STEP 9: VERIFY LAMBDA FUNCTION DEPLOYMENTS AND PERMISSIONS. 14

STEP 10: CHECK AUTO SCALING CONFIGURATIONS AND ENSURE CORRECT INSTANCE TYPES. 14
STEP 11: VALIDATE TARGET GROUP HEALTH CHECKS AND LISTENER CONFIGURATIONS. 14
STEP 12: CONFIRM ROUTING CONFIGURATIONS IN THE VPC DASHBOARD. 14
STEP 13: VERIFY NETWORK INTERFACE ATTACHMENTS AND CONFIGURATIONS. 14
STEP 14: TEST ALARMS AND ENSURE PROPER NOTIFICATION TRIGGERS. 15
4.6 OUTPUTS PROVIDE INFORMATION ABOUT THE CREATED RESOURCES. 15
5 ACTI V&C CLOUDFORMATION DEPLOYMENT 16
5.1 CREATE A CLOUDFORMATION STACK 16
5.2 LOADING THE TEMPLATE 16
5.3 SPECIFYING STACK PARAMETERS 17
5.4 DEFINING ALLOWED TRAFFIC SUBNETS WITHIN THE SGVES (NHR) 18
5.5 DEPLOYING THE STACK 19
6 DEFINING GWLBE ON CUSTOMER'S VPC (OPTIONAL) 20
6.1 GET THE GWLB NAME 20
6.2 CREATE THE GWLBE 20
6.3 DEFINING ROUTING TABLE IN INGRESS VPC 22
7 ROUTING GUIDANCE FOR INGRESS TRAFFIC INSPECTION ARCHITECTURE 23
7.1 SINGLE INSPECTION SETUP 23
7.2 DUAL INSPECTION SETUP 24
8 SUPPORT SERVICES 25
8.1 SUPPORT PLAN SUMMARY 26
8.1.1 INCIDENT LEVEL DEFINITIONS SUMMARY 26

1 Introduction

This guide provides step by step instructions for deploying Allot's solution in an Enterprise AWS account – as a dedicated **Inspection VPC used by Allot** only.

The below diagram depicts the network architecture of the system to be instantiated with this guide. The NX and DSC are management servers and the SGVE serves as Visibility & Control device, as well as the sensor device. The SGVE is deployed in the dedicated **Allot Inspection VPC** within the Enterprise customer's account. The overall solution is automatically deployed, using AWS CloudFormation, with SGVE High-Availability supported. The traffic is steered using GWLBe endpoint, from the Ingress / Egress VPC Hubs, to the Allot Inspection VPC, where the SGVE delivers Visibility & Control capabilities on ALL Enterprise Cloud traffic – both incoming and outgoing – to sustain a good user experience while consuming Public Cloud Apps & services.

1.1 Expected Execution Time

Assuming all prerequisites are in place and verified, and the customer account is alive and running, including the already deployed Ingress / Egress Hub VPC in AWS, and that, all the Allot Software Images are already uploaded, as well as the Allot CloudFormation script file to setup the Allot Inspection VPC, then this guide will take about 2 hours to complete (with the exception of ClearSee).

1.2 Acronyms

AMI	Amazon Machine Images
AOS	Allot Operating System
AWS	Amazon Web Services
CLI	Command Line Interface
COMPONENTS	Containerized Network Function
DPDK	Data Plane Development Kit
DSC	DDoS Secure Controller (out of current phase)
EC2	Amazon Elastic Compute Cloud
HW	Hardware
MOP	Method of Procedure
NAM	North America
NHR	Next Hop Router
NIC	Network Interface Controller
NUMA	Non-Uniform Memory Access
NX	NetXplorer - Allot NMS
SGVE	Service Gateway Containerized Edition

SRIOV	Single Root Input/Output Virtualization
SSH	Secure Shell
STC/LTC	Short Term Collector Long Term Collector
VM	Virtual Machine
VR	Virtual Router
VPC	Virtual Private Cloud
VF	Virtual Function.
COMPONENTS	Cloud-Native Network Function
VNF	Virtualized Network Function
ClearSee	Allot's Analytics Plane Function. Delivers advanced Application-based insights, dashboards and graphs - (out of current phase)
DM	Allot Data Mediator function - (out of current phase)
SMP	Allot Subscriber Management Platform - (out of current phase)

1.3 Disclaimer

The Implementation of Allot ACTI solution using this guide, requires the performing engineers to have experience and skills in the following areas:

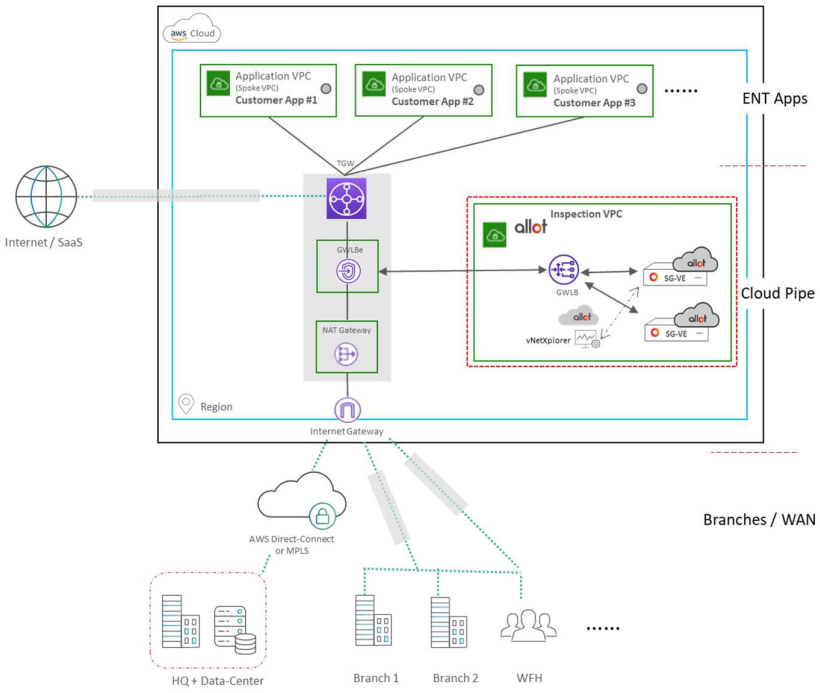
- AWS admin
- Highly knowledgeable in automated VPC deployment, using CloudFormation or Terraform.
- Configuring AWS Networking Elements (GWLBe, GWLB, Internet/NAT Gateway, TGW/VGW)
- Linux admin
- Basic understanding of Computer networking
- Production names and IP addresses will be differed then the Document and will be per LLD.

Please note that, as of today, Allot SMART is *not yet* a "Plug & Play" feature in AWS (e.g like the AWS marketplace) but rather a solution that needs to be designed, sized and approved by Allot for each individual deployment.

2 ACTI in Enterprise Public Cloud Environments

Typical Enterprise Public Cloud environments are following a rather standard architecture - the diagrams below provides an typical view, of the 2 types of Enterprises "classic" Public Cloud environment deployment architecture.

ENT environment architecture, with a ***single*** **Ingress / Egress VPC Hub**



In essence, Allot Inspection VPC includes both the Allot User-Plane (SGVE) as well as the Allot Control Plane (NetXplorer) elements – to ease on the reader understanding, the Allot product-set represented in the above diagrams, is the basic product-set required to achieve the ACTI Visibility & Control use-cases.

2.1 Allot Customer Types

Allot targets various customer-types – but for the sake of simplicity of this document, we will focus on the Enterprise Large customers – which are the mainstay of Allot's Enterprise customers.

There are multiple types of Enterprise customers – which are all using Allot's SW solutions – but to broadly paint the customers types, the below segments provides a :

1. **BFSI** – Banking Financial and Insurance
2. **Technological Customers** – from chip manufacturers, up to High-Tech Online Gaming companies
3. **Food & Beverage** – large F&B multinationals
4. **Transportation** – Large Transportation companies

5. **Governments**
6. **Universities & Education**

The bulk of the demand for Allot Public Cloud solution is coming from Large Enterprise (over 1000 users/employees) – which have more than 3-4 Cloud-migrated Applications, who are facing a major challenges with the below:

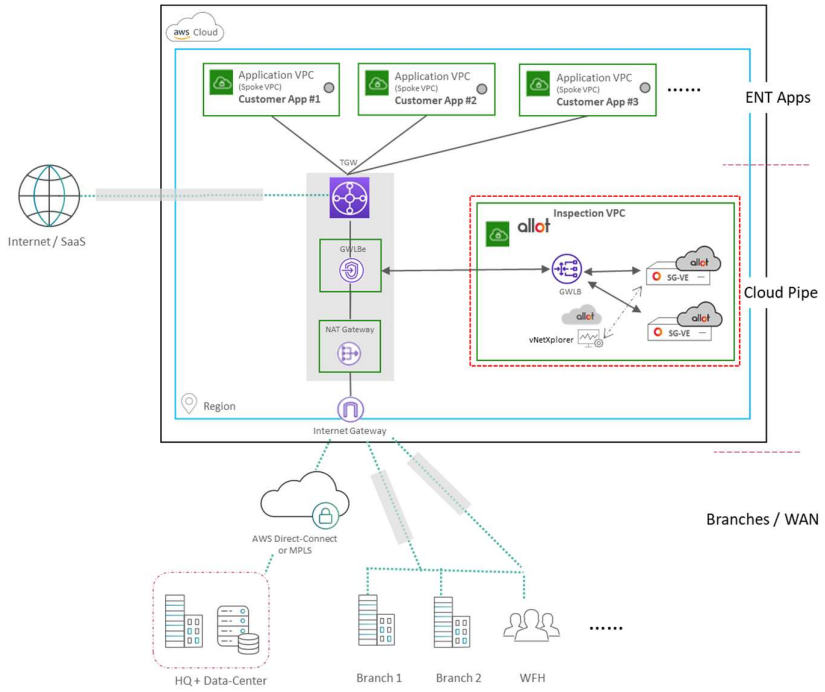
- Visibility and Control of their **corporate Applications** SLA
- Digital Experience Management (DEM) of their Online Services (websites, APIs, payment gateways…)
- Delivering App-aware, granular, DDoS and Volumetric Floods on Cloud environments, while assuring QoE SLA under attack

2.2 Allot ACTI Public Cloud Deployment

The solution can be deployed in any AWS Region.

The below diagrams provides a simplified overview of the Allot ACTI Inspection VPC in typical Enterprise AWS environment / account blueprint.

ENT architecture type: ***single*** **Ingress / Egress VPC Hub**



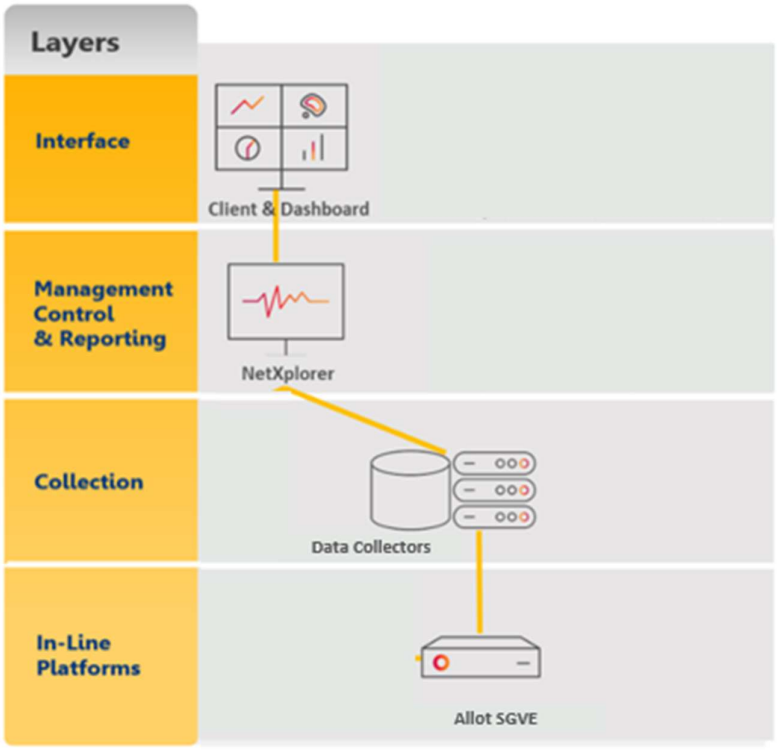
As explained, although there are several Enterprise architectural options – deploying Allot in the Enterprise customers always boils down the same boiler-plate deployment single step: deploying the Allot Inspection VPC in Enterprise customer AWS environment.

Allot Inspection VPC functionality - per components:

The below sections describe the additional Allot Control Plane components that can be deployed within the Allot Inspection VPC, to enhance the Allot capabilities and functionality offered to customers.

These components, can be deployed as AMI-formatted Virtual Machines (VMs), within the Allot Inspection VPC – the below section describes these components, their roles, their deployment architecture and their expected deployment time, on top of the basic Allot inspection VPC.

The below drawing provides a *logical view* of the various Allot components, and the layered interaction between these components:



The Interface Layer - provides multiple levels of access and operation including open interfaces for **integration with external systems** (such as: IaaS). As well as the Allot **ClearSee** Analytics Plane (with preset reporting dashboards plus dedicated self-service modules)

The Mgt Control & Reporting (or Control Plane) Layer - centralizes reporting, policy provisioning, and management of network traffic, configuration of all managed platforms, and notification/ mitigation of network attacks. This layer includes **Allot NetXplorer (NX)** and **Allot Subscriber Management Platform (SMP)**

The Collection Layer provides an efficient collection point for application, subscriber, and network usage statistics that are used in real-time and long-term reporting functions, as well as charging functions – it is instantiated through the Allot **Data Mediator (DM)**

The In-Line Platform (or User-Plane) Layer monitors network traffic in real time and dynamically enforces control for each application and for each user. This layer is always active and fully functional, even when

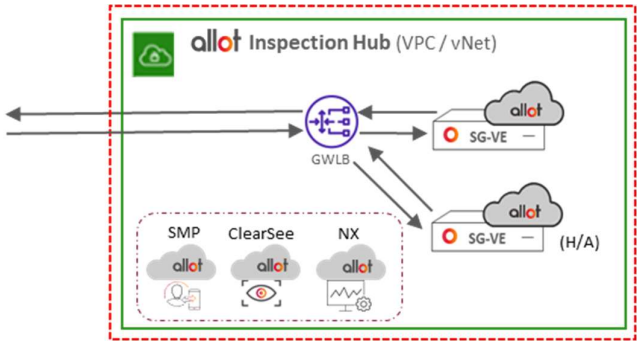
other layers might be temporarily unavailable. The inline Platform Layer, who comprises Allot **Service Gateway Virtual Edition**.

Allot COMPONENTSs roles and responsibilities (R&R)

The below table describes the Allot's COMPONENTS R&R (current deployment scope):

Component	Roles and Responsibilities
NetXplorer / NX	Supplies the network intelligence essential for Traffic and/or Service Optimization in Public Cloud Networks. It enables Enterprise Customers to: - understand how bandwidth resources are consumed by applications and users, and - define traffic management policies that link service and performance parameters to business goals and user expectations. - gain visibility of real-time as well as long-term reporting capabilities
AOS / SCGE	high-performance User-Plane (UP) Virtualized software, fully scalable, and able to meet any network capacity – the SGVE instances are centrally managed by the Allot NX management

The below diagram provides an example of Allot inspection VPC enhanced with a *sample* set of **additional Allot Control-Plane components** deployed within:



Deploying the Allot Inspection VPC – sizing guidelines:

The below table provides a sizing guidelines for each of the Allot components – enabling to pick the proper compute nodes (EC2):

Products		**Virtual Template Sizing**		
		vCPU	**vRAM (GB)**	**vDISK (GB) System + DB and Application**
Data-Plane (SG-VE)	SG-VE-04	**4**	**10**	**120**
	SG-VE-08	**8**	**20**	**120**
	SG-VE-16	**16**	**40**	**120**
	SG-VE-32	**32**	**80**	**120**
Control-Plane	NX	**8**	**16**	**120**

The below table provides the typical Allot Software image size, to be deployed:

Allot SW Products		AWS AMI
SG-VE	SG-VE-04	4.2GB
	SG-VE-08	
	SG-VE-16	
	SG-VE-32	
Control-Plane	NX	9.4GB

2.3 System Overview

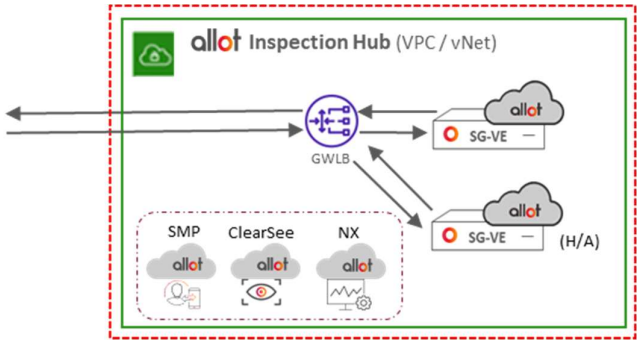
The following Allot components are included in the repository and will be deployed as COMPONENTSs:

- SGVE
- NetXplorer - including STC/LTC (Short-Time Collector / Long-Term Collector)

2.4 Internal Architecture Diagrams:

This section provides the reader with a high-level understanding, of the Allot Inspection Hub VPC internals & VPC connectivity:

- The AWS Network configuration (VPCs, subnets, etc.) – described in the installation steps section
- The AWS services running: GWLBe (endpoint) and GWLB (load-balancer) – same as above
- The Allot components deployed in each AWS account – described in this section



First, the Allot ACTI Control-Plane components deployment architecture:

- Allot SGVE (VM) user-plane element:
  - deployed in an H/A mode to avoid blackholing of the customer's traffic or applications
  - current H/A mode is active-standby
  - H/A is assured by a Serverless (Lambda) script, that constantly polls the active SGVE state
- Allot NX (NetXplorer) control plane element:
  - deployed as a standalone VM
  - controls the SGVE policy rules, configuration, and provides reporting/dashboarding
  - built as a Client-Server responsive Application
- Additional control plane elements – out of scope - will NOT be described here

Despite the single Inspection VPC, Allot has applied a logical separation between the control and the user planes. The logical separation focuses allows to have a separate and distinct scalability: where, the Allot User-Plane component (SGVE) deals with the actual Traffic Control and manipulation, while the Allot Control-Plane components (NX) provides the Cloud Networking Observability – through Real-Time Reporting, Alarms, Notification, and Dashboarding. As well as Allot Policy definition, elements management system, and configuration.

3 Requirements and Prerequisites

The following section lists all implementation prerequisites that shall be ready prior to starting to instantiate the Allot ACTI Inspection VPC.

The project repository contains the Allot Virtual Machine AMI Images which are to be deployed. All the repositories contain README files with detailed explanations.

The Enterprise customer environment access-rights have been properly granted, in order to allow for running the CloudFormation (or Terraform) script file.

3.1 Infrastructure:

- All Nodes created for the cluster **Must be** Synchronized to the following NTP server using **chronyc**: 169.254.169.123
- EC2 instances are composed as per the below table - Compute resources, with ENA on local zone

Component / COMPONENTS	AWS Instance type	vCPUs	Memory [GB]	Storage [GB]	Comments
NX	c6i.2xlarge	16	8	1850	Including internal STC, LTC
AOS / SGVE	m6in.4xlarge	16	64	120	Recommended that all vCPUs are mapped to a single NUMA

SGVE specific guidelines:

- An SGVE cluster, with the below:
  - 2 SGVE components for H/A
  - a single *dedicated EC2 compute node for each SGVE*
- The SGVE compute node will be run the Virtual Machine AMI image supplied by Allot.
- Data interfaces mapping on the SGVE worker node should be persistent in terms of names and interfaces, per the following example:
  - **Internal1 (data) Interface – ens20**
- Clusters should have proper Security Group policy configured to allow connectivity between each other

3.2 Additional Software Infrastructure Items

3.2.1 User Plane & Management Plane

- SRIOV and DPDK -enabled EC2 instances are selected.
- Allot Images – Please make sure you have access to the CICD AWS FTR Market place and can access the Allot Images.
- awscli is installed on a jump server.
- Logs – Allot recommends keeping logs duration of 8 min days before allowing a rollover.

3.3 Permissions

- Customer's AWS Account Access
- Permissions to –
  - Create CloudFormation Stack
  - Create VPCs + Resources allocation

3.4 Image to AMI

- Could either be taken from –
  - Allot's Account AMIs (One for NX, One for SGVE)
  - Give the relevant QCOW2 / VMDK to customer to have AMI on his AWS account

4 ACTI V&C CloudFormation Deployment Verification

CloudFormation AWS native script automates the creation of robust architecture with high availability (HA) features. It provisions resources for traffic inspection, auto-scaling, and endpoint services and integrates Lambda functions for health monitoring.
The CloudFormation automation script, also creates the NX Management Server element.

The CloudFormation script is built to allow for horizontal as well as vertical scalability.

- In horizontal scalability (scale-out) – the script allows SGVE to use auto-scaling to add more units in case of burst
- In vertical scalability (scale-up) - the script allows the 2 SGVE H/A instances, to be deployed over a set of increasingly stronger AWS instance-types, spanning 4 capacity- ranges.
    - The SGVE capacity ranges:
        - 1<>4 Gbps
        - 4<>8 Gbps
        - 8<>16 Gbps
        - 16<>32 Gbps
    - For the sake of simplicity this document covers ONLY the 1<>4 Gbps case

4.1 Metadata and Parameter Grouping

- Metadata: Groups parameters for better readability in the AWS Console.

Step 1: Verify parameter groups in the AWS Console to ensure clarity during stack creation.

- **VPC Configuration:** Defines VPC and subnet settings.
- **Instance Configuration:** Specifies AMI IDs and instance types.
- **Health Check Configuration:** Configures health check parameters.
- **Security Configuration:** Defines administrative access controls.
- **Endpoint Service Configuration:** Manages endpoint service settings.
- **Management Server Configuration:** Parameters for creating a management server.
- **Consumer Network Configuration:** Specifies consumer network subnets.

4.2 Parameters Define customizable inputs for stack deployment.

Step 2: Input the following parameters during stack creation:

- pVpcCidr: Define the CIDR block for the VPC.
- pSubnetCidrPrefix: Set the prefix length for subnets (default: 27).
- pAmiId: Provide the AMI ID for the instances.
- pInstanceType: Specify the EC2 instance type (default: c5n.4xlarge).
- pKeyPairSgveServer: Select or create a key pair for SGVE server access.
- pAdminMgmtCidr: Define the CIDR for administrative access (default: 0.0.0.0/0).
- Health check parameters: pHealthCheckPort, pHealthCheckPath, etc.
- Endpoint service parameters: pAcceptanceRequired, pPrincipalIds.
- Management server and consumer network configurations as required.

4.3 Mappings Maps CIDR prefix lengths to bit values for subnet calculations.

- mCidrPrefixToBits: Maps prefixes (e.g., 24, 25) to bit counts.

Step 3: Verify that the VPC CIDR can accommodate the defined subnets.

4.4 Conditions Defines conditions to control resource creation based on parameters.

- cAcceptanceRequired: True if endpoint service acceptance is required.
- cCreateManagementServer: True as a management server should be created.
- cCreateManagementServerKeyPair: Checks for management server key pair creation.
- cCreateSgveKeyPair: Checks for SGVE server key pair creation.

Step 4: Review and adjust conditions based on deployment needs.

4.5 Resources Defines all AWS resources to be created.

Key Pairs

- rSgveKeyPair, rMgmtKeyPair: Create EC2 key pairs for SGVE and management servers.

Step 5: Ensure key pairs exist or are generated automatically.

VPC and Subnets

- rVpc: Creates a new VPC with DNS support.
- rMgmtSubnetAz1, rMgmtSubnetAz2: Management subnets in different AZs.
- rData1SubnetAz1, rData1SubnetAz2: Primary data subnets.
- rData2SubnetAz1, rData2SubnetAz2: Secondary data subnets for redundancy.

Step 6: Confirm subnet allocation in the VPC Dashboard.

Security Groups

- rDataSecurityGroup: Allows GENEVE and health check traffic.
- rMgmtSecurityGroup: Permits SSH, HTTPS, and SNMP traffic.

Step 7: Validate security group rules in the EC2 Dashboard.

Gateway Load Balancer

- rGatewayLoadBalancer: Provisions the GWLB.
- rEndpointService: Creates a VPC Endpoint Service for GWLB.
- rEndpointServicePermissions: Configures permissions if acceptance is required.

Step 8: Ensure the GWLB and endpoint service are operational.

Lambda Functions and Roles

- rLambdaUserDataInitRole, rLambdaUserDataInit: Initializes network interface configurations.
- rAlarmNotificationLambdaRole, rAlarmNotificationLambda: Manages CloudWatch alarms for unhealthy targets.

Step 9: Verify Lambda function deployments and permissions.

EC2 Launch and Auto Scaling

- rLaunchTemplateAz1, rLaunchTemplateAz2: Launch templates for instances in different AZs.
- rAutoScalingGroupAz1, rAutoScalingGroupAz2: Auto Scaling Groups maintain active-standby instances.

Step 10: Check Auto Scaling configurations and ensure correct instance types.

Target Groups and Listeners

- rGatewayLoadBalancerTargetGroup: Configures target groups with health checks.
- rGatewayLoadBalancerListener: Sets up listeners to forward traffic.

Step 11: Validate target group health checks and listener configurations.

Route Tables and Associations

- rMgmtRouteTable, rDataRouteTable: Create route tables for management and data traffic.
- rMgmtRouteTableAssociationAz1, rMgmtRouteTableAssociationAz2: Associate management subnets with the route table.
- rData1RouteTableAssociationAz1, rData1RouteTableAssociationAz2: Associate data subnets with the route table.

Step 12: Confirm routing configurations in the VPC Dashboard.

Network Interfaces

- rDataNetworkInterface1Az1, rDataNetworkInterface2Az1: Data interfaces for AZ1.
- rDataNetworkInterface1Az2, rDataNetworkInterface2Az2: Data interfaces for AZ2.
- rMgmtNetworkInterfaceAz1, rMgmtNetworkInterfaceAz2: Management interfaces.

Step 13: Verify network interface attachments and configurations.

CloudWatch Alarms

- rTargetGroupHealthAlarm: Monitors unhealthy targets in the GWLB target group.
- rLambdaInvokePermissionForAlarm: Grants CloudWatch permission to invoke Lambda functions.

Step 14: Test alarms and ensure proper notification triggers.

4.6 Outputs Provide information about the created resources.

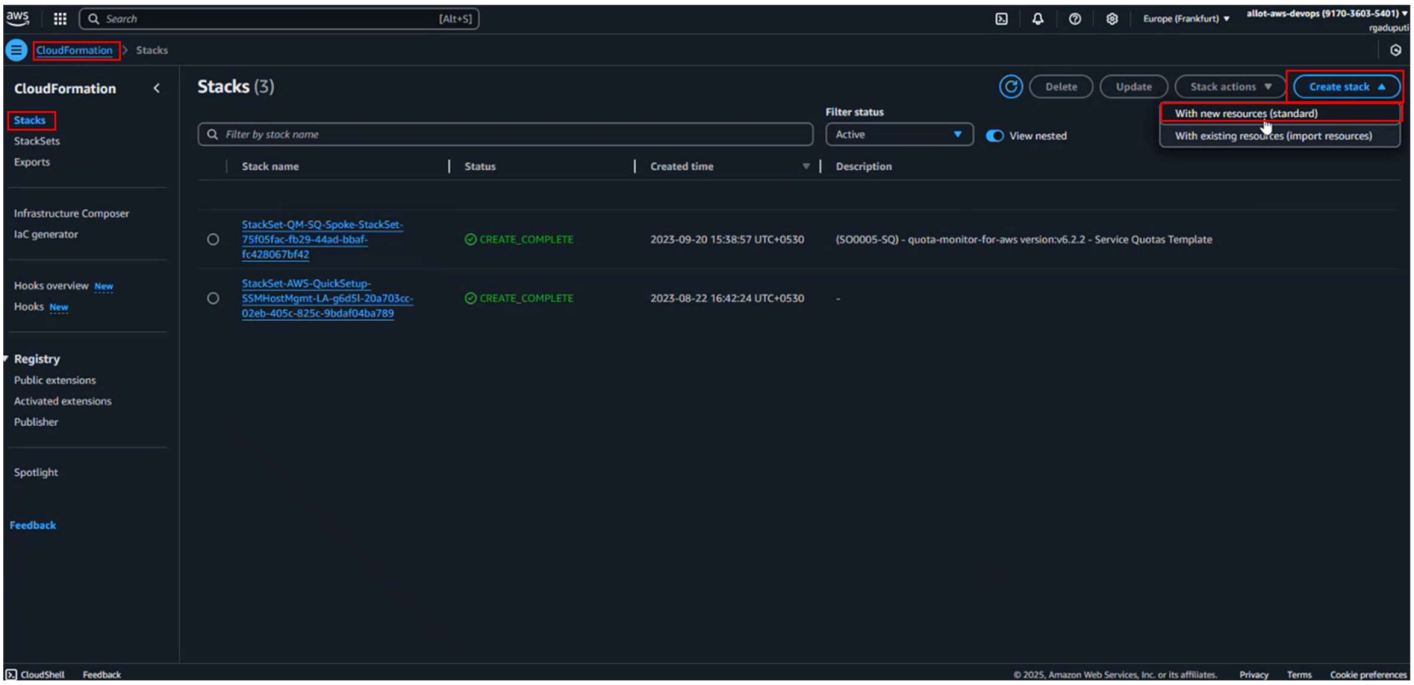
- oMgmtSubnetCidrs, oData1SubnetCidrs, oData2SubnetCidrs: Output CIDR blocks.
- oEndpointServiceId: Output the endpoint service ID.
- oMgmtServerIP: Output the private IP of the management server if created.

5 ACTI V&C CloudFormation Deployment

5.1 Create a CloudFormation Stack

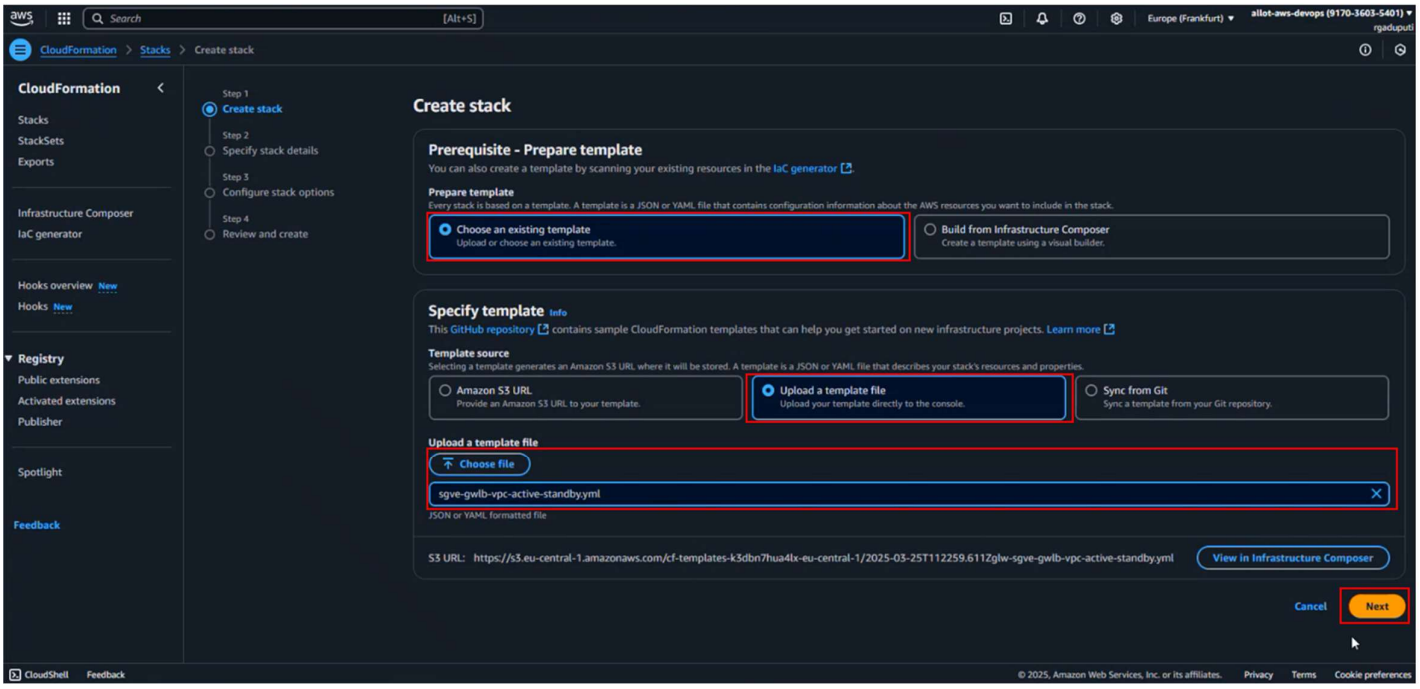
In the AWS GUI –

Click on CloudFormation --> Stacks --> Create Stack --> "With new resources"



5.2 Loading the Template

Choose an existing Template --> Upload a template file --> Choose file, use the provided template to deploy 2 x SGVEs (Active-Standby) & NX Mgmt. --> Click "Next"



5.3 Specifying Stack Parameters

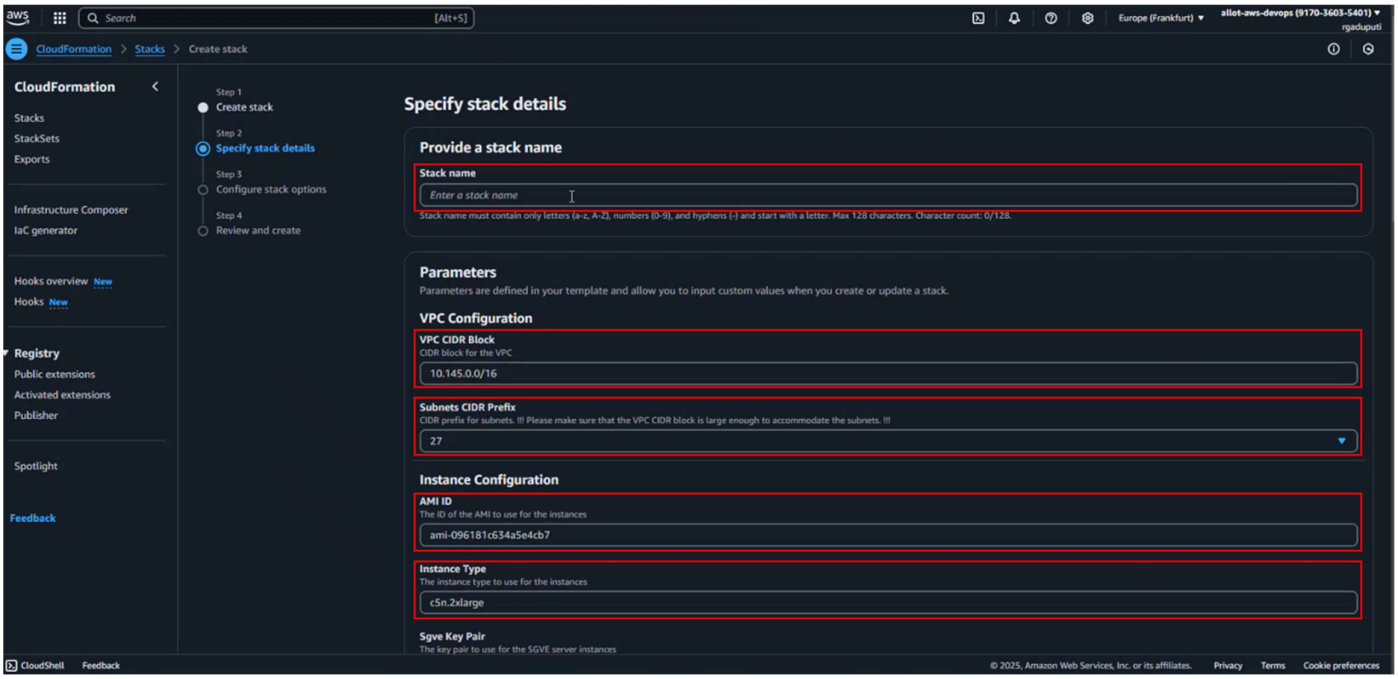
The YAML already have some default values that should not be changed.

The main parameters that needs to be modified between one customer to another are –

- CIDR Block – Customer to define a subnet of IPs within his AWS account to be associated with Allot Products within the Inspection VPC –
  - SGVEs Mgmt
  - SGVEs Interfaces (NHR Mode)
  - NX Mgmt
  - GWLB

- Subnet CIDR Prefix –
  - /27 would suffice

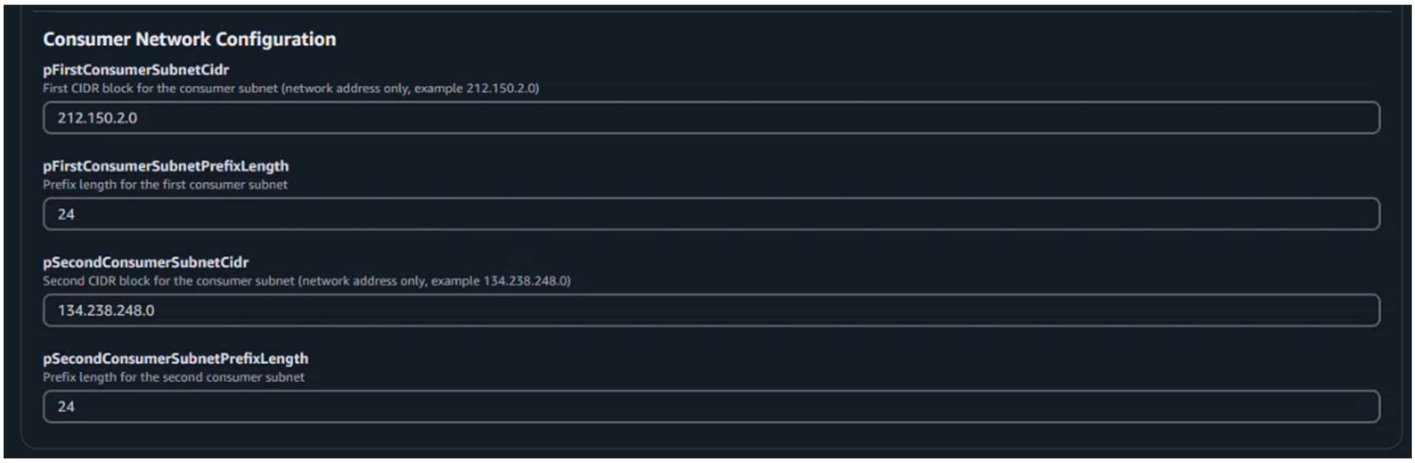
- AMI ID –
  - Could either be taken from –
    - Allot's Account AMIs (One for NX, One for SGVE)
    - Give the relevant QCOW2 / VMDK to customer to have AMI on his AWS account
- Instance type –
  Depends on the SGVE's size – would be defined by RnD



- Security Access-list (Optional)
- Same configurations to the Mgmt server (NX) –
    - Create Management Server MUST be set to "TRUE".

5.4 Defining allowed traffic subnets within the SGVEs (NHR)

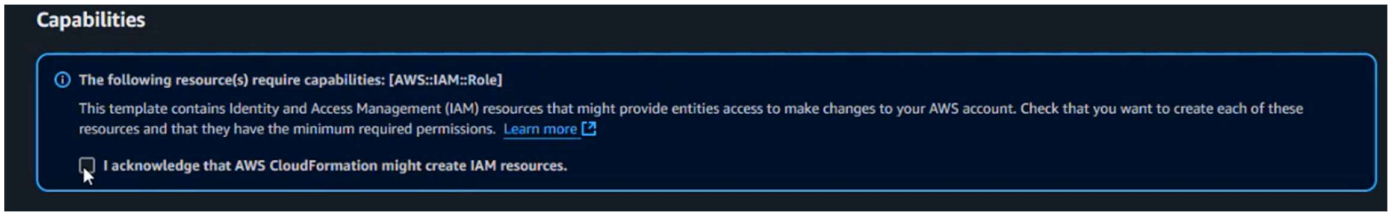
As for now we are supporting up to two allowed subnets, this would be expanded soon



Click "Next"

5.5 Deploying the Stack

In the next screen, scroll down and acknowledge.



Click "Next" --> Review the parameters & Submit Stack creation.

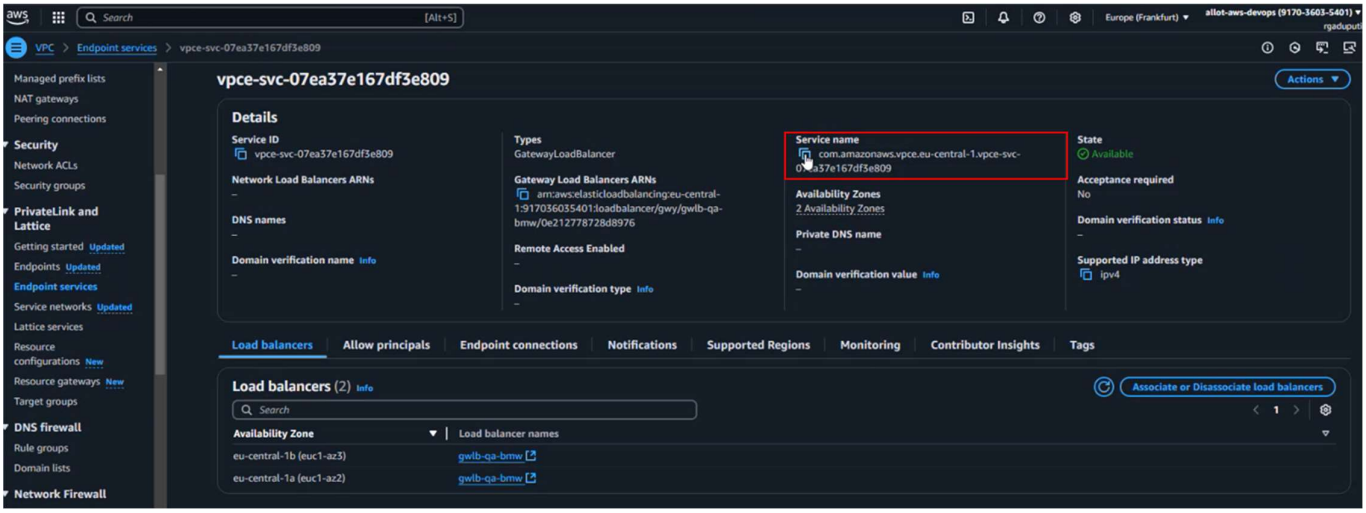
6 Defining GWLBe on customer's VPC (Optional)

In case the customer is asking for assistance with setting a route from his Ingress/Egress VPC to Allot's Inspection VPC –

6.1 Get the GWLB Name

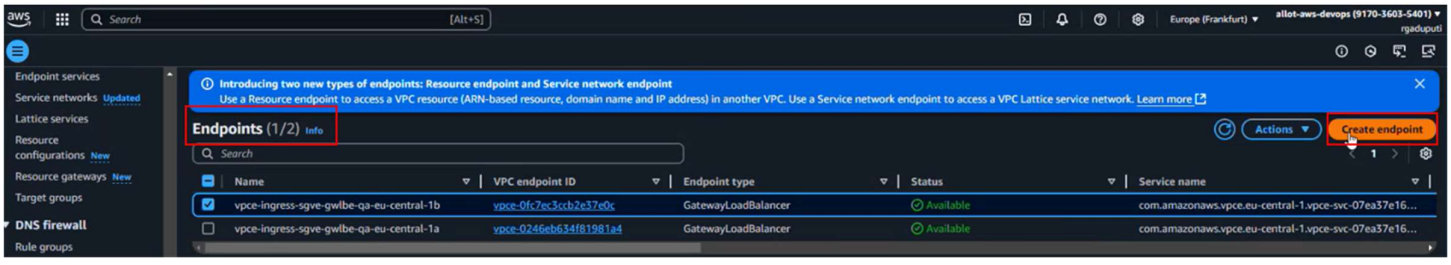
Within the AWS GUI --> VPC --> Your VPC --> Endpoint Services
Go inside the GateWayLoadBalancer type created –

Copy the GWLB Service-Name –



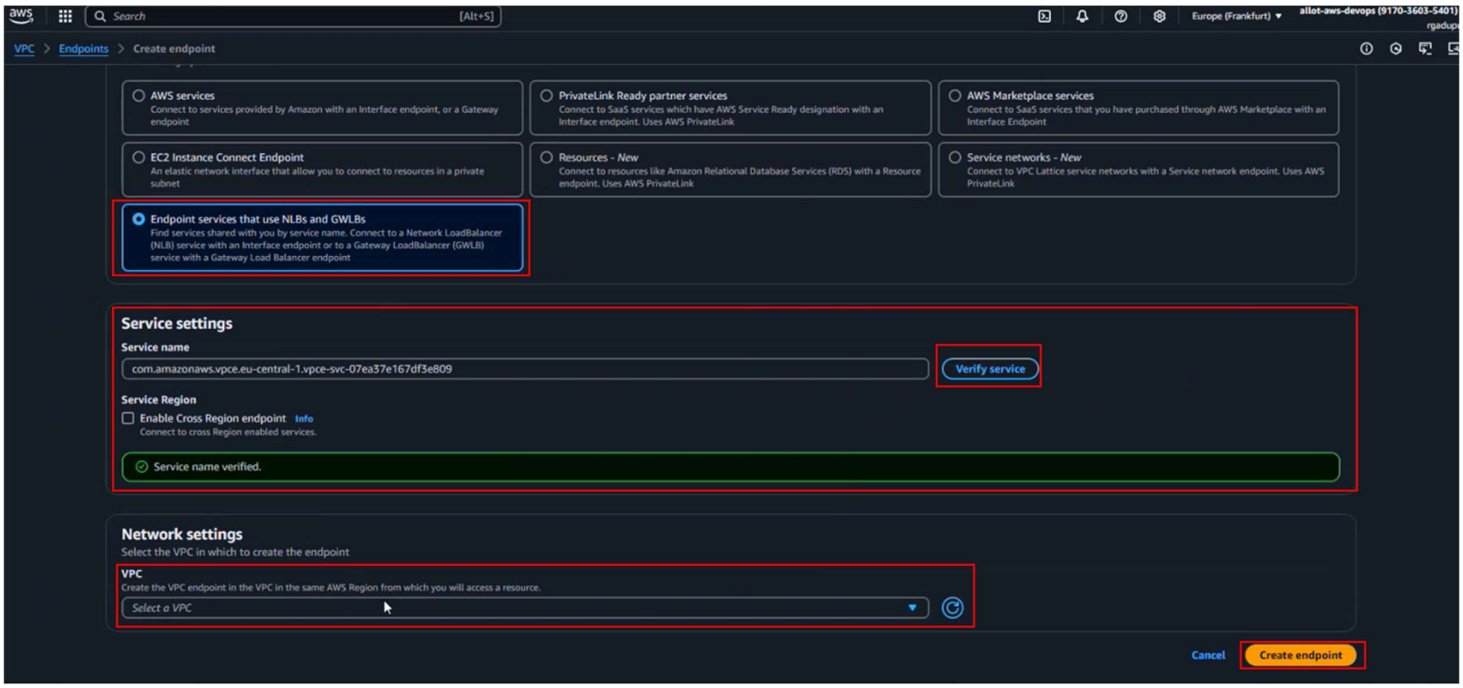
6.2 Create the GWLBe

Go to Endpoints --> Create Endpoint

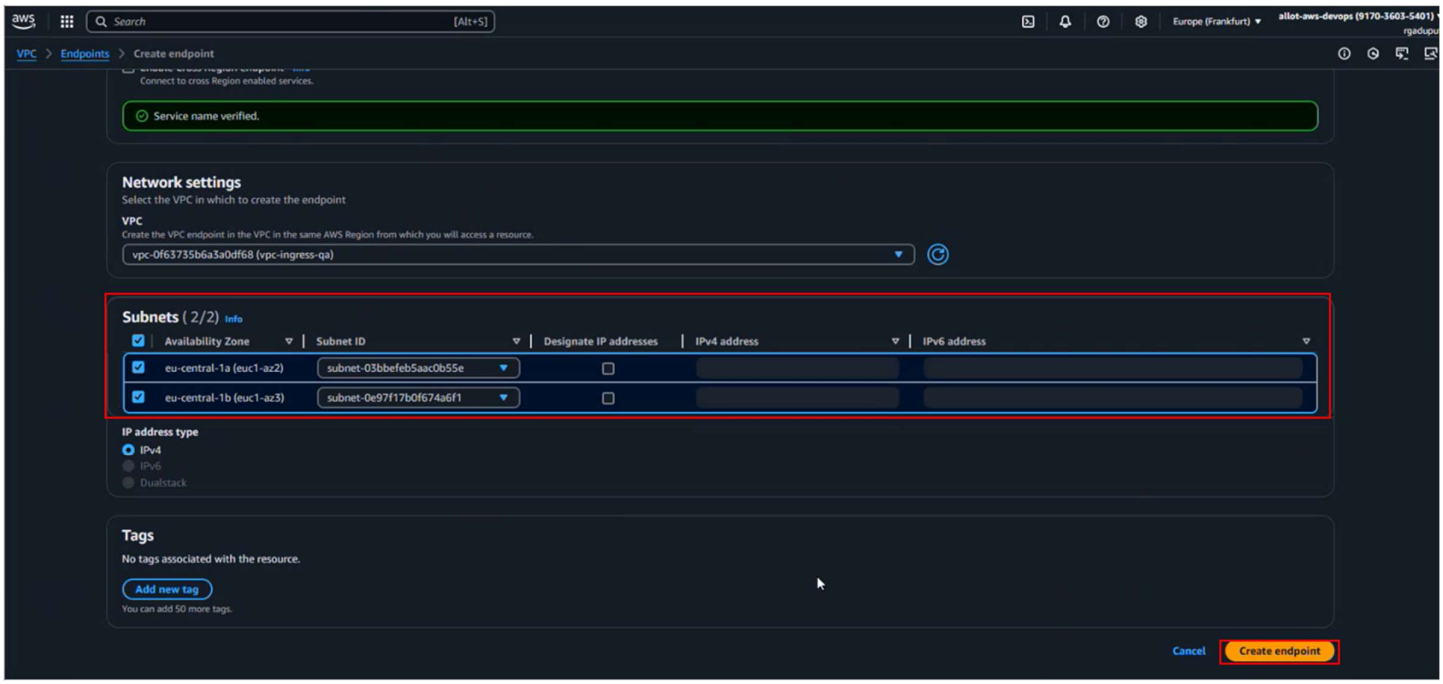


Choose " Endpoint services that use GWLBs" --> Paste the GWLB Name your copied and verify the service exists.

In "Network settings" Choose the customer's Ingress VPC –



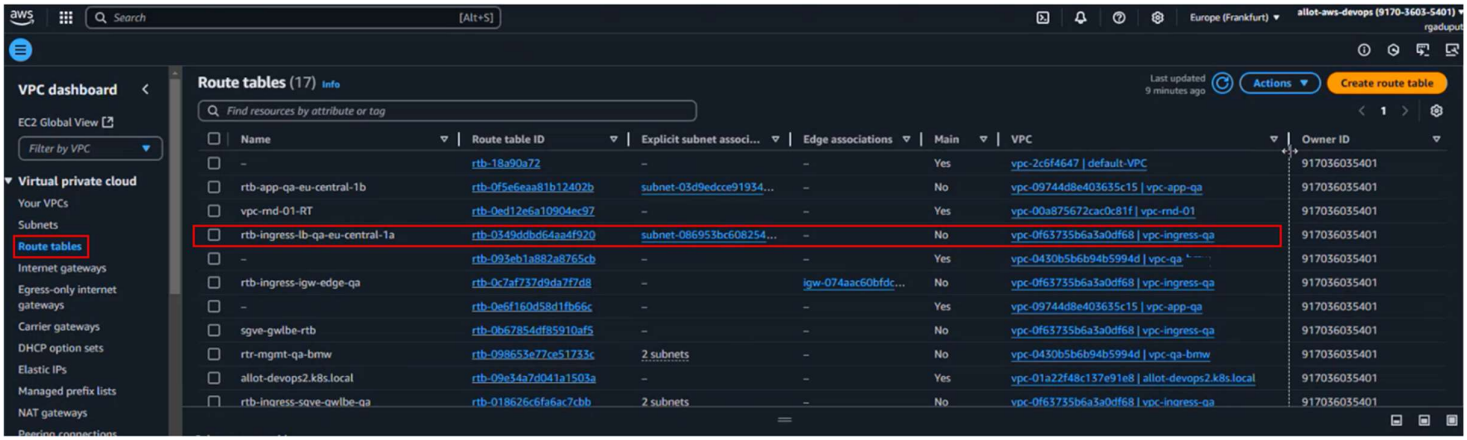
Choose the relevant Subnets for the defined AZs –



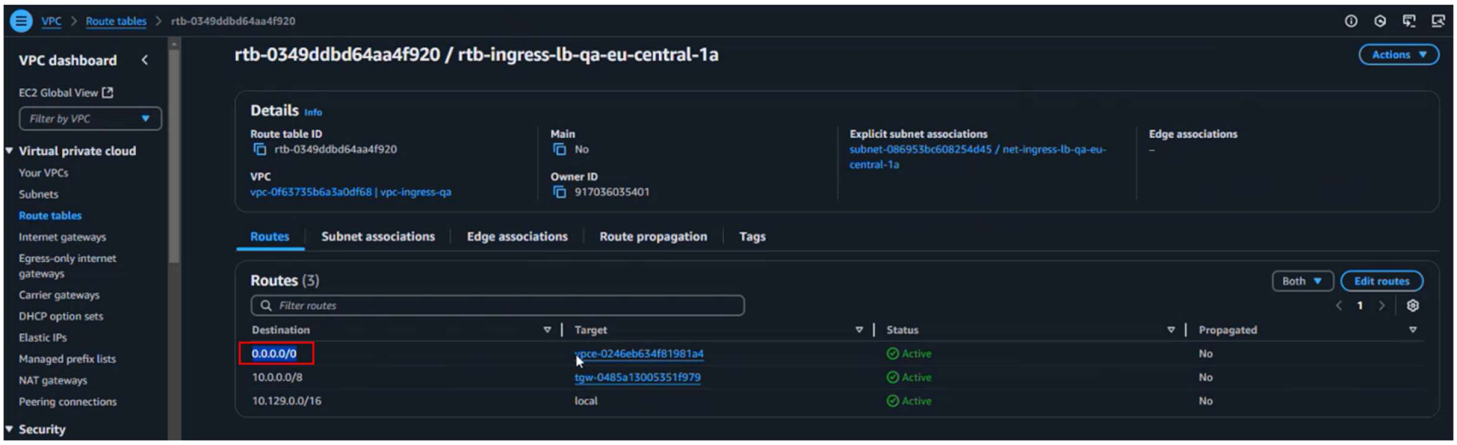
Click "Create Endpoint"

6.3 Defining Routing Table in Ingress VPC

Choose "Route Table" --> Choose the relevant "Ingress VPC"



In this example all traffic is routed from the Ingress VPC to Allot's Inspection VPC –



7 Routing Guidance for Ingress Traffic Inspection Architecture

7.1 Single Inspection Setup

To implement an ingress traffic inspection architecture for **Single Inspection**, you will need the following resources and configurations:

1. **Internet Gateway**: Provides internet access for the VPC.

2. **SGVE Gateway Load Balancer Endpoint (GWLBe) Subnets**:
    - Subnets dedicated to the SGVE GWLBe endpoints.

3. **Single SGVE GWLBe Routing Table**:
    - Contains a `0.0.0.0/0` route pointing to the Internet Gateway.

4. **Load Balancer Subnets**:
    - Subnets for the load balancer to route traffic.

5. **Multiple Load Balancer Routing Tables**:
    - Each availability zone (AZ) used must have its own routing table.

    - Routing tables should include:
        - Subnet-specific routes for destination subnets.
        - If a Transit Gateway is used, a global served CIDR can be applied.
        - A default (`0.0.0.0/0`) route pointing back to the SGVE GWLBe endpoints.
        - **Note**: A single GWLBe endpoint can support multiple AZs if the cross-AZ feature is enabled on the GWLB.

6. **Single Edge Routing Table**:
    - Contains routes pointing to the SGVE GWLBe endpoints in each AZ.
    - Includes load balancer subnet CIDRs as specific routes.
    - Has the Internet Gateway attached as the edge route.

7.2 Dual Inspection Setup

If **dual inspection** is required, the configuration steps will change as follows:

1. **Routing Table for Each SGVE GWLBe Subnet**:
    - Create a dedicated routing table for each SGVE GWLBe subnet.

2. **Each SGVE GWLBe Routing Table**:
    - Add a `0.0.0.0/0` route to the Internet Gateway (IGW).
    - Add specific routes per load balancer subnet pointing to the **customer's Firewall GWLB inspection endpoint**.

3. **Existing Customers Firewall GWLB Routing Tables**:
    - Modify routing tables to include the following:
        - Add/Change a `0.0.0.0/0` route pointing back to the SGVE GWLBe endpoint for each AZ.

8 Support Services

Allot support is primarily based on the Allot Support Center (ASC) operating in the customer's region, backed up by "follow-the-sun" process allowing continuous support 24 hours a day 365 days a year for critical issues. Any registered and trained End User personnel may contact the ASC. Allot ASCs are manned by expert engineers, well trained in both Allot productand networking in general, in order to ensure the most professional and high-level technical support to our End Users.

The most efficient and fastest communication with the ASC is by opening a Support Case at the Allot Support site (HTTPS://WWW.ALLOT.COM/SUPPORT-SERVICES/SUPPORT-CENTER/). Opening a case ensures all necessary information is provisioned at the generation of the Support Case. Other methods of contact include email to support@allot.com, or telephone calls to the ASC number listed.

Allot Support is provided based on the Serial Number of the product (hardware and/or software). The relevant Serial Number must be covered by a valid Support Contractat the time a supportcase is opened.

Upon receiving the support request, a Support Case will be opened in the Allot CRM system and the initiator of the support request will be informed of the Support Case Number. All further email communication pertaining to the support request should carry the Support Case Number and Reference ID in the subject line. Unless instructed otherwise by the ACS, all subsequent emails regarding the case must be directed to SUPPORT@ALLOT.COM.

An Allot ASC engineer will follow up the Case with the requestor and will resolve or escalate as needed. Updates will be posted to the Allot Support Case Online Portal. If required by the case or requested by the End User, responses may be sent by email.

To enhance the ability to provide the required assistance, it is important to provide the ASC as much information as possible when opening a Case. Mandatory information requirements are listed in the section relating to the opening of a Case set forth below.

The Allot Global Support Services (GSS) organization currently includes more than 100 carefully selected, highly professional Support Engineers. The GSS organization is divided into ASCs according to geographical location and professional expertise, providing expedient, high-quality, and reliable customersupport to the various Allot products acrossall time zones and in many cases in the local language.

The support framework is coordinated by collaborative round-the-world sharing of an extensive human and computing/network infrastructure, backed up by a fully committed R&D organization. The GSS is designed for the continuous treatment of requests (Case/Incident) for customer support until the Case is resolved, as well real time reporting on Case status. It is subject to periodic auditing.

8.1 Support Plan Summary

Plan Name	Gold Plan	Platinum Plan
Price (From Product List Price)	15%	18%
Hours of Coverage	24 x 7	24 x 7
Response Times (hours)		
Severity 1	4	1
Severity 2	4	2
Severity 3	4	4
Restoration Times*		
Severity 1	N/A	8 Hours
Severity 2	N/A	4 Days
Severity 3	N/A	N/A
Resolution Times		
Severity 1	N/A	8 Weeks
Severity 2	N/A	14 Weeks
Severity 3	N/A	Next SW version
Software Updates		
Error Corrections	√	√
Protocols Update	√	√
New Versions	√	√
Additional Services		
Advance RMA	√	√
Resident Engineer	Available at additional Charge	Available at additional Charge
Annual Network Audit	Available at additional Charge	Available at additional Charge
DDoS protection ERT service	Available at additional Charge	Available at additional Charge

1 All plans refer to support for T3 and above. T1/T2 remote support is available at additional charge.
2 All times are net-support times and are in effect while remote connectivity is provided.
3 New Versions may require the procurement by End User of additional hardware, related third party software and/or installation and configuration services.
4 New Versions eligibility is only for products or features purchased. Any additional features may be chargeable.
5 New Version eligibility does not include any Professional Services upgrade work. Such work must be done by a trained End User engineer or procured separately from Allot. defined release frequency.
6 RMA is Relevant only for Hardware provided by Allot.
7 Protocol updates SLA is in line with Allot
Protocol pack defined release frequency

8.1.1 Incident Level Definitions Summary

- Severity 1: An error or defect that has a critical service affecting impact on the network resulting in a major effect on more than 25% of users and requiring immediate corrective action in order to prevent material negative effects on revenue or data loss.
- Severity 2: An error that has some impact on business, system operations, maintenance, and administration affecting less than 25% of users and that does not significantly affect the operation or service quality of the system.

- Severity 3: A minor, non-service affecting defect that has minimal impact on business, maintenance, and administration such as in cases where the product is usable, however there is a minor impact on performance or reporting which does not affect the overall operation or service quality of the system. This level also includes any documentation issues and general measurement issues.