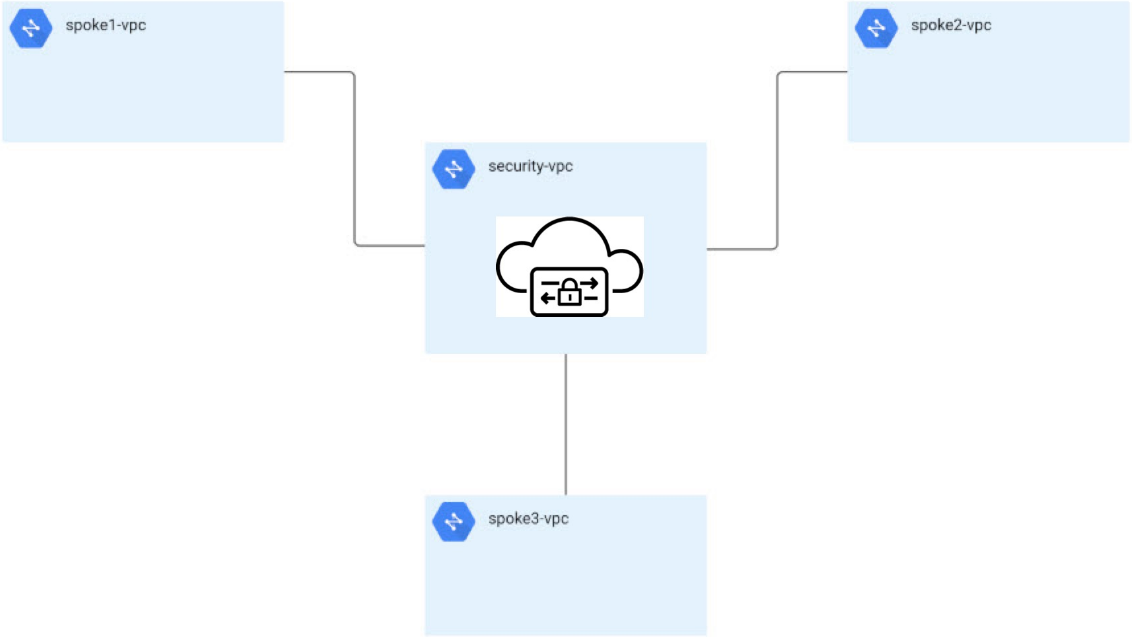
GCP

Service GCP

GCP Service VPC

For the Centralized deployment, Multicloud Defense Gateway is deployed in a new VPC. This VPC is called a Service VPC and peer with other Spoke (application) VPC to create a Hub-and-Spoke model as shown below:



Multicloud Defense orchestrates the creation of the Service VPC and the peering with the Spoke VPCs. Multicloud Defense also provides the ability to update the routing tables in Spoke VPCs to route traffic to

Service VPC for inspection. For instructions on how to make routing changes with Multicloud Defense in Spoke VPC, see Manage (Protect) Spoke VPCs in Hub Mode.

Create Service VPC

Step 1 Click **Manage** > **Gateways** > **Service VPCs/VNets**.

Step 2 Click **Create Service VPC/VNet**.

Step 3 Input parameter values:

Parameter	Description
Name	Assign a name to the Service VPC.
CSP Account	Select the GCP project to create the Service VPC.
Region	GCP region to deploy the Service VPC.
Datapath CIDR Block	The CIDR Block for the Multicloud Defense Gateway datapath Service VPC. This CIDR block must not overlap with address ranges in your Spoke (application) VPCs.
Management CIDR Block	The CIDR Block for the Multicloud Defense Gateway management Service VPC. This CIDR block must not overlap with address ranges in your Spoke (application) VPCs.
Availability Zones	Multicloud Defense recommends to select at least two (2) availability zones for resiliency.

Note

- Service VPC consist of the following:
  - Two (2) VPC - one for management and one for datapath
  - Four (4) firewall rules - 2 for management and 2 for datapath (ingress and egress)
- Service VPC CIDR must not overlap with Spoke VPC

Manage (Protect) Spoke VPCs in Hub Mode

Multicloud Defense will orchestration the creation of Service VPC, and also create VPC peering to your Spoke VPCs. Multicloud Defense can be made to make route table changes to your Spoke VPCs, so that traffic is routed to the Multicloud Defense Gateway for inspection. This Multicloud Defense orchestration makes it very easy to deploy and secure workloads.

Note Please wait a few minutes for the Service VPC to be created, and state to become **ACTIVE** before proceeding with the following steps:

To protect Spoke VPCs, we need to create VPC peering between Spoke VPCs and Service VPC. This allows Multicloud Defense to orchestrate the routing change in the Spoke VPCs so that traffic will be sent to the Multicloud Defense Gateway for inspection.

When enabling Protected VPCs, Multicloud Defense Controller orchestrates the following:

- Create VPC peering between Multicloud Defense Service VPC (datapath) and Spoke VPC
- Add/Update default route to redirect spoke traffic to Multicloud Defense Gateway

There are two ways to make this configuration:

- Add Spoke VPCs from Service VPC Menu, on page 3
- Add Spoke VPCs from Inventory Menu, on page 3

Add Spoke VPCs from Service VPC Menu

Step 1 Navigate to **Manage** > **Service VPCs/VNets**.

Step 2 Select Service VPC and click on **Actions** > **Manage Spoke VPC/VNet**.

Step 3 Add all Spoke VPCs to protect to the Spoke table.

Step 4 Click on View/Edit link under the Route Tables column.

Step 5 Checkbox **Send Traffic via Multicloud Defense Gateway** to update default route to point to Multicloud Defense Gateway for inspection.

Step 6 Click **Update routes**.

Step 7 Click **Save**.

Add Spoke VPCs from Inventory Menu

Step 1 Navigate to **Manage** > **Cloud Accounts** > **Inventory**.

Step 2 Click on VPCs/VNets. This will list all the VPCs in your cloud accounts.

Step 3 Click on the **Secure** button to secureVPC.

Step 4 Select Service VPC.

Step 5 Checkbox "**Send Traffic via Multicloud Defense Gateway** ". This will configure default route for spoke VPC to Multicloud Defense.

Step 6 Click **Save**.

GCP Centralized Ingress Protection

The Multicloud Defense Gateway is deployed in to a VPC to protect your applications by acting as a **Reverse Proxy**. Users access the application via the Multicloud Defense Gateway. The backend applications are configured on ther Multicloud Defense Gateway as a proxy targets. The reverse proxy function requires

Multicloud Defense to decrypt TLS traffic and perform deep packet inspection. The proxied traffic to the backend/target can be sent as plain text HTTP, HTTPS, TCP or TLS.

Step 1 Navigate to **Manage** > **Gateways** > **Gateways**.

Step 2 Click **Add Gateway**.

Step 3 Select the account you previously created.

Step 4 Enter the gateway information where appropriate:

- **Instance Type** - Choose the type of cloud service provider. Note that there may be multiple variations of instances depending on which cloud service provider you are using.
- **Minimum Instances** - Select the minimum number of instances that you plan to deploy.
- **Maximum Instances** - Select the maximum number instances that you plan to deploy. This is the maximum number that is used for auto-scaling in each availability zone.
- **HealthCheck Port** - Default is 65534. The port number used by Multicloud Defense load balancer to check the health of the instances. Datapath security groups assigned to the instance(s) must allow traffic on this port.
- (Optional) **Packet Capture Profile** - Packet Capture Profile for threat and flow PCAPs.
- (Optional) **Diagnostics Profile** - Diagnostics Profile used to store Technical Support information.
- (Optional) **Log Profile** - Log Forwarding Profile used to forward Events/Logs to a SIEM.
- (Optional) **Disk Encryption** - Select either **GCPmanaged encryption** or **Customermanaged encryption key**. For customer managed encryption key, the user will need to input the resource ID of the encryption key.

Step 5

Step 6 Click **Next**.

Step 7 Enter the following paramters:

- **Type** - Ingress.

  -
-
- **Gateway Image** - Image to be deployed.
- **Policy Ruleset** - Select the policy ruleset to associate with this gateway.
- **Region** - Select the region this gateway will be deployed into.
- **Gateway Service Account Email** - Enter the Multicloud Defense Gateway service account email. Ensure that the service account has the necessary IAM roles: `Secret Manager Secret Accessor` and `Storage Object Creator`.
- **Datapath VPC** - Select the VPC to associate with the datapath interface of the Gateway.
- **Datapath Network Tag** - The tag assigned to the network interface of the Gateway in the datapath VPC.
- **Management VPC** - Select the VPC to associate with the management interface of the Gateway.
- **Management Network Tag** - The tag assigned to the network interface of the Gateway in the management VPC.

Step 8 Select the **Availability Zone**, the **Mgmt Subnet** and the **Datapath Subnet**. The available subnets will be based on the VNet selected above. For high availabilty purposes the gateway instances can be deployed in multiple availability zones. Click the plus button to add a new availability zone and select the parameters for the selected zones.

Step 9 The Multicloud Defense Gateway deployment takes a few minutes to reach an **Active** state.

GCP Centralized Egress / East-West Protection

The Multicloud Defense Gateway is deployed in to a VPC to protect outbound and East-West traffic inside your VPCs. For HTTP or TLS applications with SNI extension header, the Multicloud Defense Gateway can act as a transparent forward proxy. Multicloud Defense will terminate outbound sessions, and proxy the request on behalf of the client inside the VPC. For this decryption/encryption operation to function, trusted root/intermediate certificates need to be installed on the Multicloud Defense Gateway and the client application instances.

Step 1 Navigate to **Manage** > **Gateways** > **Gateways**.

Step 2 Click **Add Gateway**.

Step 3 Select the account you previously created.

Step 4 Click **Next**.

- **Instance Type** - Choose the type of cloud service provider. Note that there may be multiple variations of instances depending on which cloud service provider you are using.
- **Minimum Instances** - Select the minimum number of instances that you plan to deploy.
- **Maximum Instances** - Select the maximum number instances that you plan to deploy. This is the maximum number that is used for auto-scaling in each availability zone.
- **HealthCheck Port** - Default is 65534. The port number used by Multicloud Defense load balancer to check the health of the instances. Datapath security groups assigned to the instance(s) must allow traffic on this port.
- (Optional) **Packet Capture Profile** - Packet Capture Profile for threat and flow PCAPs.
- (Optional) **Diagnostics Profile** - Diagnostics Profile used to store Technical Support information.
- (Optional) **Log Profile** - Log Forwarding Profile used to forward Events/Logs to a SIEM.
- **Disk Encryption** - Select either **GCPmanaged encryption** or **Customermanaged encryption key**. For customer managed encryption key, the user will need to input the resource ID of the encryption key.

Step 5 Click **Next**.

Step 6 Provide the following parameters:

- **Type** - Ingress.

  -
- **Gateway Image** - Image to be deployed.
- **Policy Ruleset** - Select the policy ruleset to associate with this gateway.
- **Region** - Select the region this gateway will be deployed into.

- **Gateway Service Account Email** - Enter the Multicloud Defense Gateway service account email. Ensure that the service account has the necessary IAM roles: `Secret Manager Secret Accessor` and `Storage Object Creator`.
- **Datapath VPC** - Select the VPC to associate with the datapath interface of the Gateway.
- **Datapath Network Tag** - The tag assigned to the network interface of the Gateway in the datapath VPC.
- **Management VPC** - Select the VPC to associate with the management interface of the Gateway.
- **Management Network Tag** - The tag assigned to the network interface of the Gateway in the management VPC.

Step 7 Select the **Availability Zone**, the **Mgmt Subnet** and the **Datapath Subnet**. The available subnets will be based on the VNet selected above. For high availabilty purposes the gateway instances can be deployed in multiple availability zones. Click the plus button to add a new availability zone and select the parameters for the selected zones.

Step 8 The Gateway deployment takes a few minutes to reach an **Active** state.