Manage Multicloud Defense Gateways

Overview

Multicloud Defense Gateway is a network-based security platform comprised of a network load balancer with a cluster of Multicloud Defense Gateway instances. It is an auto-scaling and self-healing cluster that scales out and in depending on the traffic load. Multicloud Defense Controller and gateway instances exchange constant and continuous information about the state, health and telemetry. The Multicloud Defense Controller makes the decision to scale out/in by measuring the telemetry data received from the gateway instances. The gateways can be configured to run in multiple availability zones for a highly available, resilient architecture. This ensures that a single availability zones failure from a cloud service provider does not compromise the security posture for running applications.

Once you have configured a gateway and any corresponding VPCs or VNets, you can use the **Gateway Details** page in the Multicloud Defense Controller to view and manage the state of them.

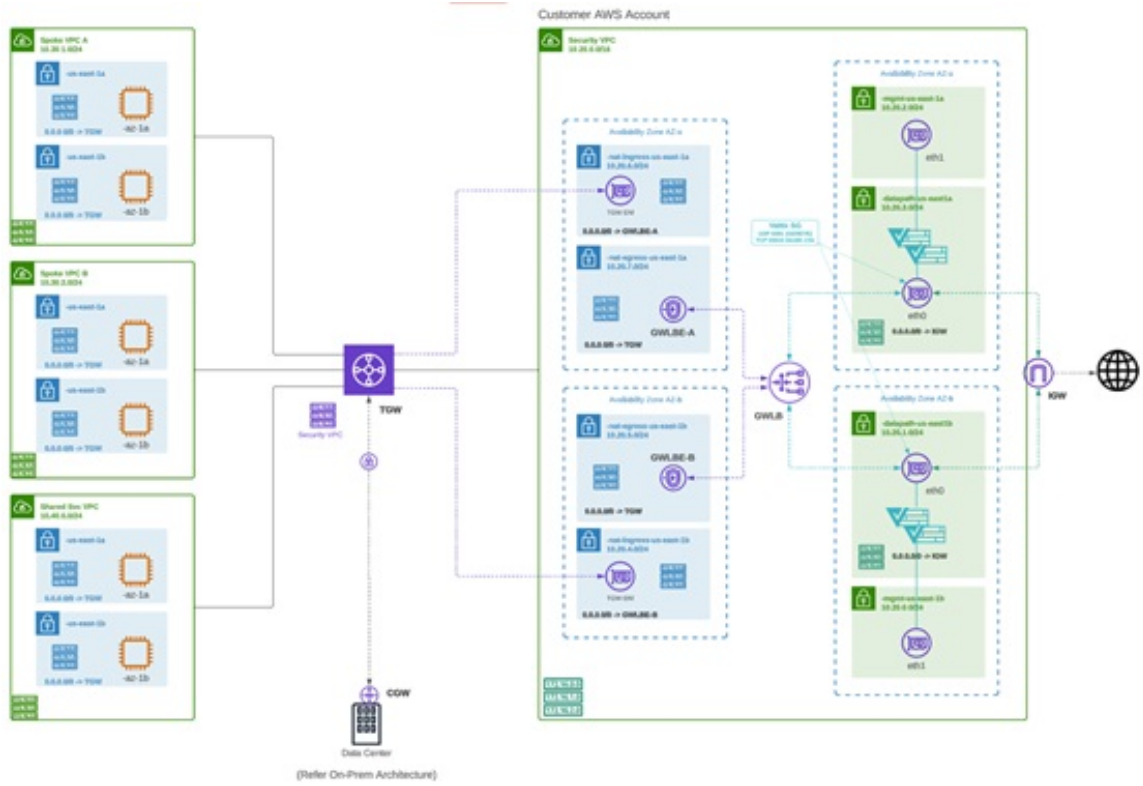
Multicloud Defense Gateways can be deployed in two ways; **Hub** mode and **Edge** mode.

Supported Gateway Use Cases

Egress

Deploying an Egress/East-West gateway to protect traffic leaving their public cloud networks. The egress gateway functions as a transparent forward proxy, performing full decryption and embedding advanced security features like intrusion prevention, antimalware, data loss prevention, and full-path URL filtering. Optionally, it can also operate in a forwarding mode, where it doesn't proxy or decrypt traffic but still applies security functionalities like malicious IP blocking and FQDN filtering.

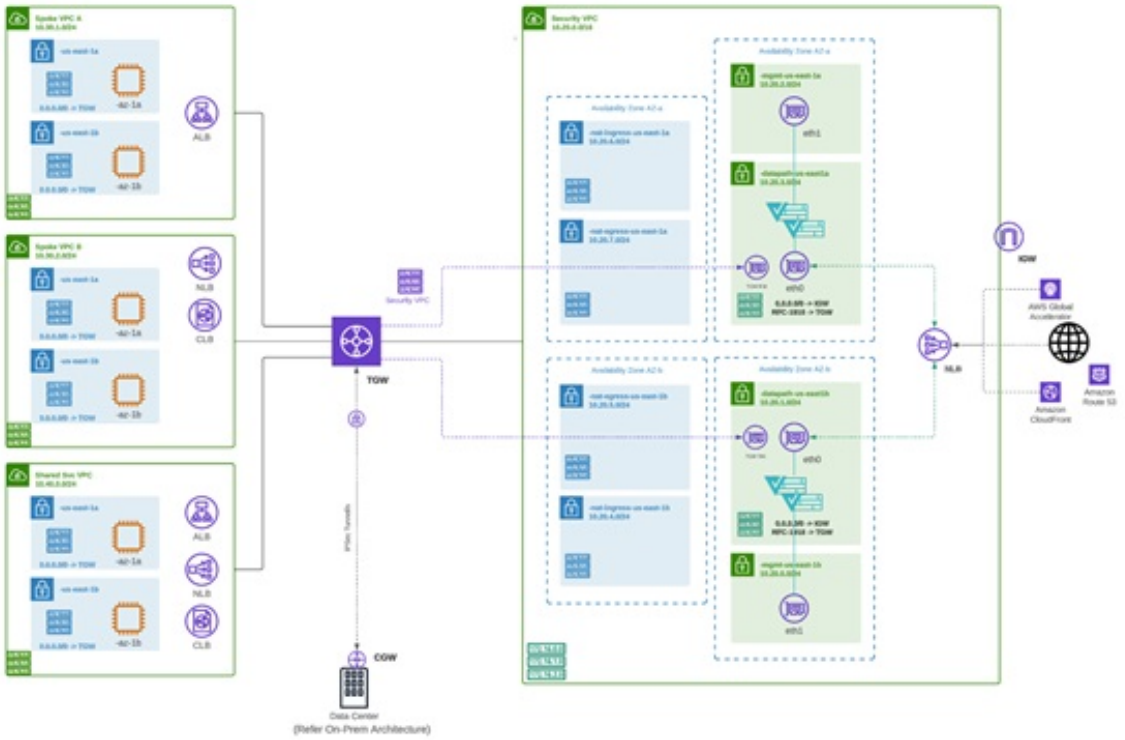
The following diagram is an example of an AWS account with an egress gateway in a centralized mode:



Ingress

Deploying an Ingress gateway protects our public-facing applications. The Ingress gateway acts as a reverse proxy that carries out full decryption and applies advanced security functionalities such as intrusion prevention, antimalware, web application firewall (WAF), and full-path URL filtering.

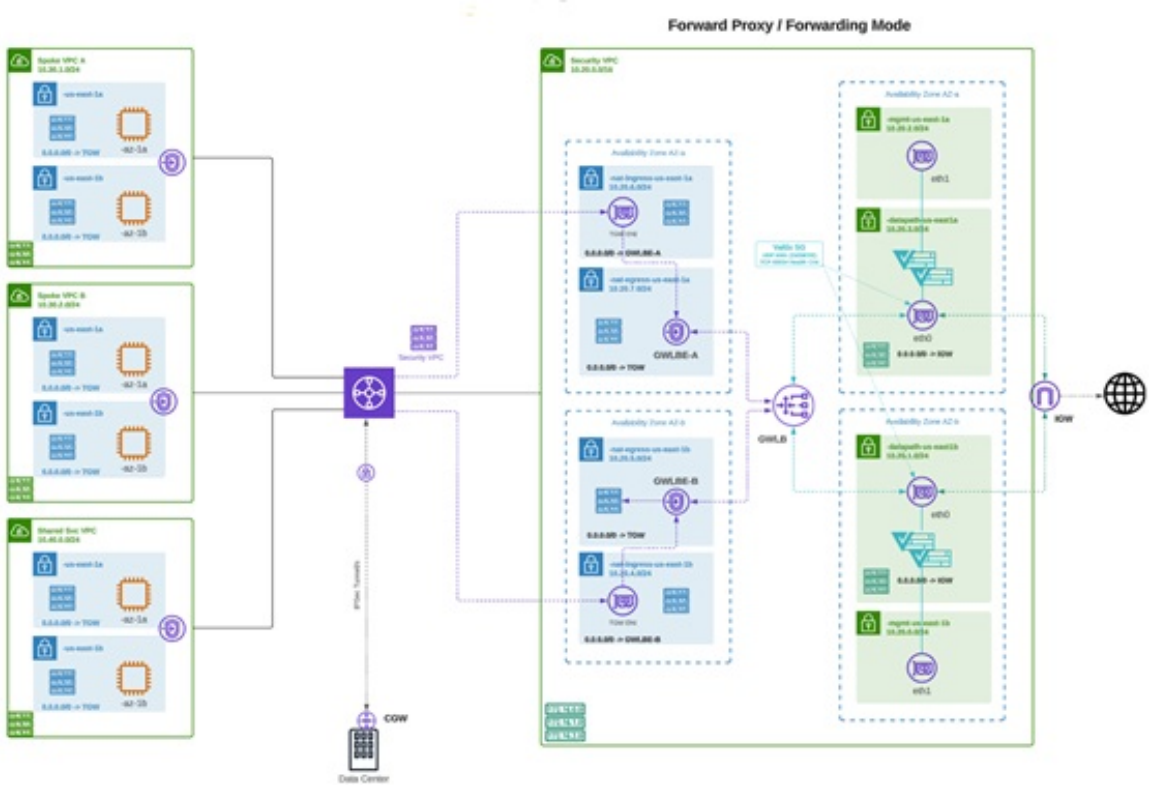
The following diagram is an example of an AWS account with an ingress gateway in a centralized mode:



East-West

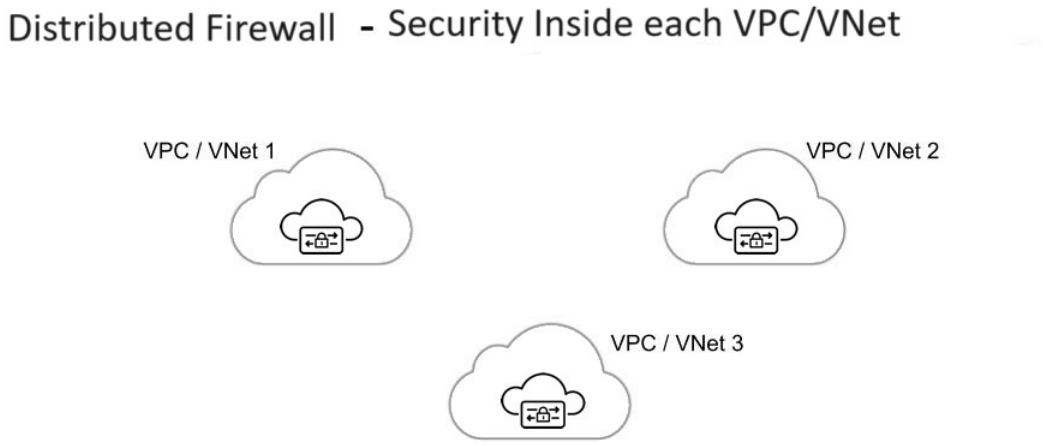
An Egress/East-West gateway deployment implements East-West L4 segmentation between subnets or VPCs/Vnets within their public cloud environments. The gateway functions in a forwarding mode with L4 firewall rules, allowing or denying traffic based on set parameters, with optional logging enabled.

The following diagram is an example of an AWS account with an east-west gateway in a centralized mode:



Distributed

You have applications running in multiple VPC/VNets. Deploy a Multicloud Defense Gateway in each of the VPCs/VNets.



Centralized / Hub

You have applications running in multiple VPCs/VNet. You would like to secure all the applications through a centralized security services VPC/VNet. This model deploys the Multicloud Defense Gateway in a service VPC. You attach all the application VPCs (Spoke VPCs) and the Services VPC to the AWS Transit Gateway or VNet/VPC peering in Azure and GCP. Multicloud Defense provides an option to orchestrate the AWS Transit Gateway, Services VPC and the Spoke VPC Attachments. This is the recommended solution for ease of deployment, removing the complexity of multiple route tables and Transit Gateway attachments.

Figure 1: AWS - Using AWS Transit Gateway

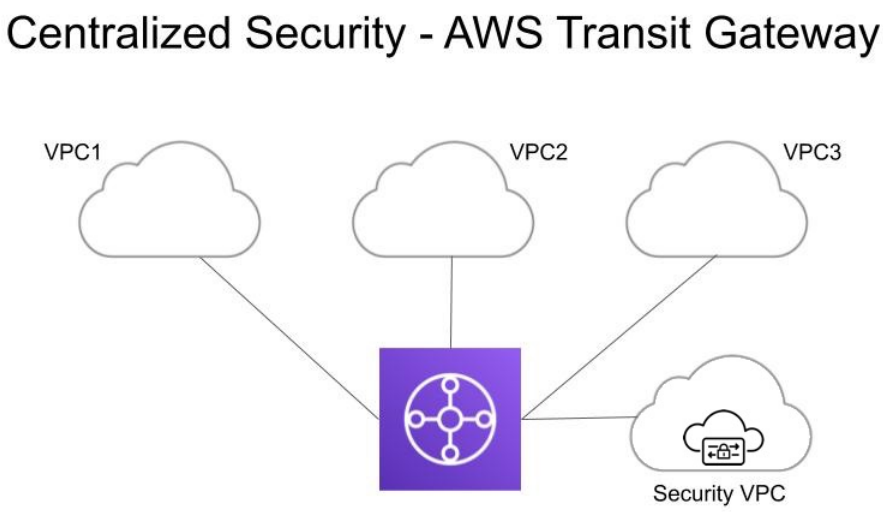


Figure 2: Azure - VNet Peering

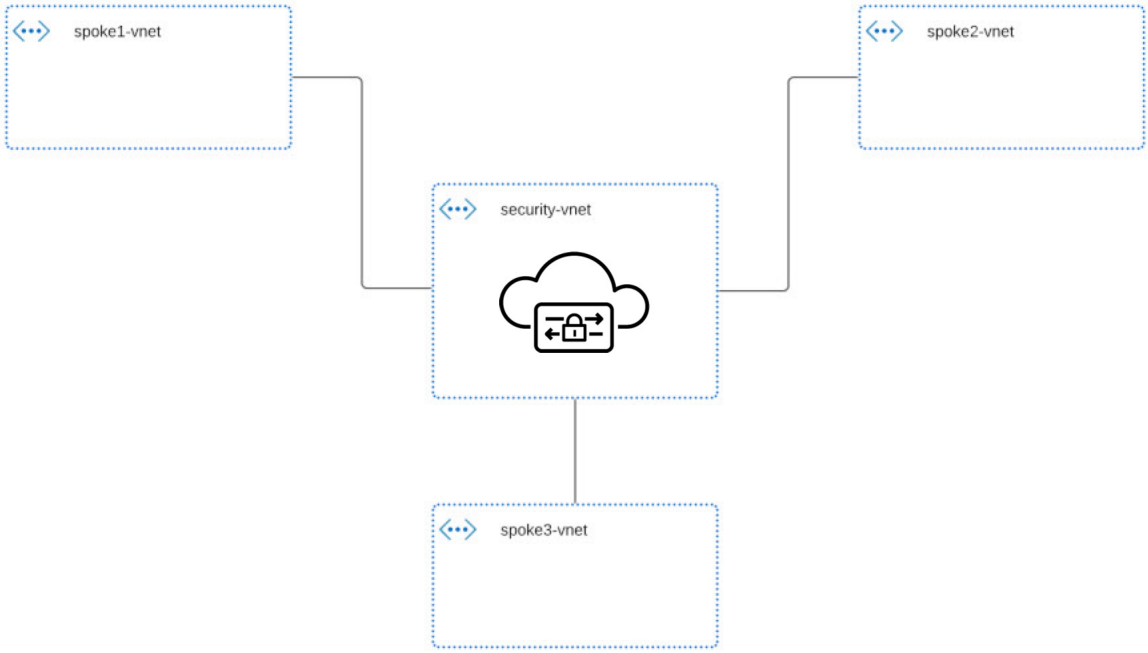
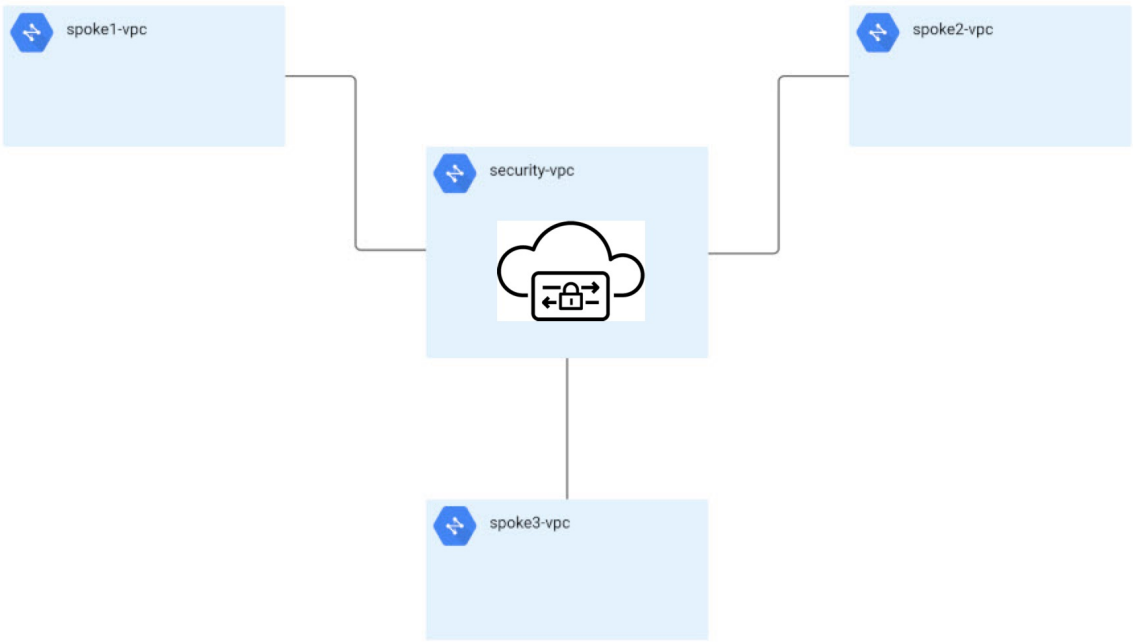


Figure 3: GCP - VPC Peering



Advanced Use Cases

There may be additional prerequisites or post-prrcedure steps for some gateways. Consider the following environments:

AWS: Accelerator to the Ingress Gateway

Multicloud Defense can integrate with a set of one or more AWS global accelerators to use as an ingress point to load balance traffic across the Multicloud Defense Gateway instances. This is similar to the AWS network load balancer that is created and managed by Multicloud Defense when an ingress gateway is deployed, but offers an alternative ingress point for the ingress gateway to protect applications and workloads.

Accelerator, it will manage the global accelerators' listener endpoint group to ensure the endpoint group has the active set of gateway onstances. Client IP addresses will be preserved as they pass through the global accelerator to the Multicloud Defense ingress gateway.

In order to integrate Multicloud Defense with a global accelerator, the user must have first created the global accelerator within AWS, defined a desired listener and created an empty endpoint group (or an endpoint group that contains the existing Multicloud Defense ingress gateway instances). Once the AWS resources exist, then the Multicloud Defense ingress gateway can be configured to integrate with the global accelerator.

Gateways Details

To view the **Gateway Details** page for already established gateways are available in **Manage** > **Gateways**. You can add and manage all gateways from this page. Managing a gateway allows you to edit, upgrade, enable, disable, export, or delete the instance. You must click the checkbox of the gateway you want to modify prior to making any changes.

Note You **must** be an Admin or SuperAdmin for these actions.

To filter and search the list of gateways, use the following criteria can be any of the following items:

- **Name** - The name of the gateway.
- **CSP Account** - The cloud service provider account that is associated with the gateway.
- **CSP Type** - The type of cloud service provider account.
- **Region** - The region of the cloud service provider that is associated with the gateway you are searching for.
- **State** - The current state of the gateway. Gateways can be active or inactive, or pending active or pending inactive.
- **Instance Type** - Each cloud service provider supports a number of instance types.
- **Mode** - Multicloud Defense Gateway instances can be depoyed in hub or edge mode.

Click **Switch to Advanced Search** to construct your own search. Use the drop-down option within the search bar to utilize some of the auto-generated search criteria if needed. For searches that have to repeated, you can **copy** or even **save** searches for future use.

Configure Multicloud Defense Gateway and VPC/VNets

Before You Begin

The supported cloud service providers are separate entities that use their own vocabulary and gateway environment. Not every option available in the Multicloud Defense Controller is compatible with your cloud service provider. For example, AWS uses its own Transit Gateway and you can add VPCs to it while Azure utilizes a load- balancer to manage web traffic and applications and you can add VNets to it. Keep this in mind when proceeding.

Note For AWS environments, when securing spoke VPCs in centralized mode, Multicloud Defense attaches VPCs to the Transit Gateway that is associated to the service VPC. By default, Multicloud Defense will randomly select a subnet in each availability zone for Transit Gateway attachment. You can change this option when you add a VPC or you can modify a VPC that is already assigned to the gateway.

You can also orchestrate a transit gateway through the Multicloud Defense Gateway or attach an existing Transit Gateway.

Resources Created by Multicloud Defense

The following resources are created by Multicloud Defense when you create a gateway, VPC, or VNet. These are created as part of the process and do not require any additional actions from the user. Note that difference resources are created per each cloud service provider requirements.

GCP Resources

Multicloud Defense creates two service VPCs and four firewalls. See the following for the exact resource allocation:

Service VPC

- Management
- Datapath

Firewall Rules

- Management (ingress)
- MAnagement (egress)
- Datapath (egress)
- Datapath (egress)

Note The Service VPC CIDR **cannot** overlap with the Spoke VPC.

AWS Resources

Multicloud Defense creates three service VPCs to address the supported use cases (ingress, egress/ east-west). Created and affiliated with each of these VPCs is the following:

- Four subnets in each availability zone.
- One route table for each of the subnets.
- Two security-groups: management and datapath.
- One Transit Gateway.

Note This Transit Gateway is created and attached to the gateway during the creation of the service VPC. This gateway can be reused with other service VPCs.

- A Transit Gateway route table.

Note The route table is attache to the Service VPC as part of the creation process.

Note The AWS Gateway Load Balancer (GWLB) does not support add/remove of availability zones after initial deployment of a GWLB. You will need to redeploy the service VPC if you need to change availability zones. See AWS documentation for more information.

Azure Resources

Multicloud Defense created one Service VNet with the following resources:

- One VNet.
- Two network security groups.

The Service VNet CIDR value must not overlap with spoke VNet.

Create a Service VPC or VNet

Use the following procedure to create a Service VPC or Service VNet, depending on the gateway you are creating this for. Note the options that are specific to your cloud service provider.

Step 1 From the Multicloud Defense Controller, navigate to **Manage** > **Service VPCs/VNets**.

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

Step 3 Input parameter values:

- **Name** - Assign a name to the Service VPC/VNet.
- **CSP Account** - Select the CSP account to create the Service VPC/VNet.

- **Region** - Select the region the Service VPC will be deployed to.
- (Azure only) **CIDR Block** – The CIDR Block for Service VNet. This must not overlap with your Spoke(application) VNets.
- (AWS/GCP only) **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.
- (AWS/GCP only) **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** - If you are creating a VPC, you **must** configure **one** availabilitliy zone only. For a VNet, Multicloud Defense recommends to select at least two availability zones for resiliency.
- (Azure only) **Resource Group** - The Resource Group to deploy Service VNet.
- (AWS only)**Transit Gateway** - The Transit Gateway connects virtual private cloud and on-premises networks through a central hub. Use the drop-down menu to select an existing gateway for this VPC. If there is no pre-existing gateway for you to select, choose **Create_new**. This option allows Multicloud Defense to create one as part of the VPC creation process.
- (AWS only) **Transit Gateway Name** - If you opted to create a new Transit Gateway, enter a name for the gateway in this field.
- (AWS only) **Auto accept shared attachments** - If you opted ot create a new Transit Gateway and intend to use this VPC for a multi-account hub gateway deployment, check this option.
- **Use NAT Gateway** - Enable this option if you want all egress traffic will go through NAT Gateway.

Caution Do **not** enable this NAT Gateway option if you intend to deploy this Service VPC to deploy a Multicloud Defense VPN gateway in AWS.

What to do next

Add a Multicloud Defense Gateway.

Add a Multicloud Defense Gateway

Use the following procedure to add a Multicloud Defense Gateway for your cloud service provider:

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

Step 2 Click **Add Gateway**.

Step 3 Select the cloud service provider you want to add the gateway to.

Step 4 Click **Next**.

Step 5 Enter the following information:

- **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.
- **Gateway Tpe** - Select either Ingress or Egress.

Note Select **Egress** if you have an east-west network flow.

- **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) **NTP Profile** - Network Time Protocol (NTP) for time synchonization.

Step 6 Click **Next**.

Step 7 Provide the following parameters:

- **Security** - Select either Egress or Ingress.

  Note Select **Egress** if you have an east-west network flow.

- **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.
- **Resource Groups** - Select the resource group to associate the gateway with.
- **SSHPublic Key** - Paste the SSH public key. This public key is used by the controller to access the CLI of the deployed gateway instances for debug and monitoring.
- **VNet ID** - Select the VNet to associate with the gateway.
- **User Assigned Identity ID** - Enter the cloud service provider identity to associate with this gateway.
- **Mgmt. Security Group** - Select the security group to associate with the management interface.
- **Datapath Security Group** - Select the security group to associate with the datapath interface.
- **Disk Encryption** - Select the appropriate option from the drop-down menu. For customer managed encryption key, the user will need to input the resource ID of the encryption key.

Step 8 Select the **Availability Zone**, the **Mgmt Subnet** and the **Datapath Subnet**. The available subnets will be based on the VPC or 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.

Note Some cloud service provider regions do not support multiple availability zones. In such regions the gateway instances are deployed in only a single zone.

Step 9 (Azure only, optional) If you are deploying in distributed model with Multicloud Defense Gateway in the same VNet as application, ensure you complete the following:

- Add a route table in the Azure portal and associate the route table with all the subnets.

- Add a default route for 0.0.0.0/0 with **next-hop** as the IP address of the Gateway Network Load Balancer.

Step 10 Click **Next** to view the Advanced Settings.

Step 11 By default, the Multicloud Defense Gateway enables the use of the public IP of the router available. If you do not want this enabled, check the **Disable Public IP** box.

Step 12 Click **Save**. Multicloud Defense deploys the gateway.

What to do next

You **must** attach at least one ruleset to the gateway before you secure a spoke VPC/VNet. See Rule Sets and Rule Set Groups for more information.

Secure Spoke VPC/VNet from Service Menu

Use the following procedure to add a spoke VPC or spoke VNet from the service menu to a gateway:

Before you begin

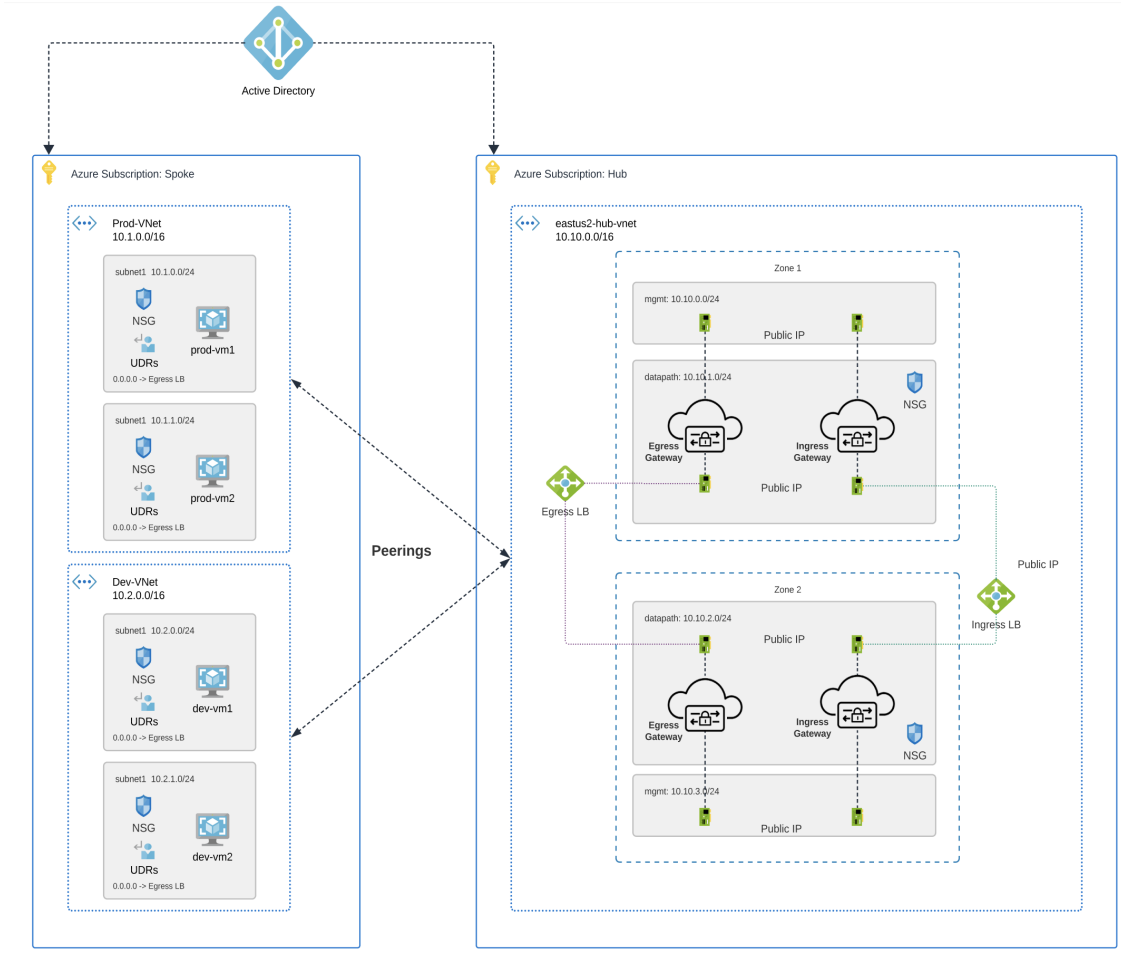
The following must be done prior to creating and assigning a spoke VPC or VNet:

- In AWS and GCP accounts, you must secure remote accounts before you add a gateway.
- Azure environments require a route table attached **prior** to securing spoke VPC/VNet. See the "Associate a route table to a subnet" chapter in the Azure user guide for more.

Note that when you protect an AWS spoke with VPCs in centralized model, Multicloud Defense attach VPCs to the Transit Gateway that is associated to the Service VPC. When attaching VPCs to the Transit Gateway, users can choose which subnet in each availability zone to place the ENIs. By default, Multicloud Defense will randomly select a subnet in each availability zone for Transit Gateway attachment.

VNet pairing is supported across accounts within the same CSP type. You can add spoke VPC/VNets within an account and across accounts. In Azure, for spoke VPCs peering across subscriptions, the CSP accounts should be onboarded using the same app registrations, and subscriptions should be within the same Active Directory.

Figure 4: Azure Combined Hub - Multisubscriptions



Step 1 From the Multicloud Defense Controller dashboard, navigate to **Manage** > **Service VPCs/VNets**.

Step 2 Select Service VPC or Service VNet and navigate to **Actions** > **Manage Spoke VPC/VNet**.

Step 3 Add all spoke VPC or VNets to protect the spoke table.

You can select spoke VPC or VNets from **Spoke VNets for Current Account**. If you want to add spoke VPC or VNets from another account, select from **Spoke VNets for Other Accounts**.

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

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

Step 6 Click **Update routes**.

Step 7 Click **Save**.

Manage Your Gateway

View your Multicloud Defense Gateways and statistic in **Manager** > **Gateways**. From this page you can search and filter your gateways, view the cloud service providers assocaited with each gateway, current instance count and type, and more.

For more information on the supported use cases for specific gateway environments, see Supported Gateway Use Cases, on page 1.

Edit a Multicloud Defense Gateway

You can edit a gateway in any state, whether it is enabled or disabled. Use the following procedure to edit an existing Multicloud Defense Gateway:

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

Step 2 Select the Multicloud Defense Gateway you want to edit in the table so it is highlighted.

Step 3 Expand the **Actions** drop-down menu and click **Edit**.

Step 4 Modify the gateway configuration as needed.

Step 5 Click **Save** to confirm the changes. Alternatively, click **Cancel** to exit the changes.

Upgrade the Multicloud Defense Gateway

Multicloud Defense Gateways serve as an autoscaling self-healing Platform-as-a-Service (Paas), functioning as inline network-based security enforcement nodes. Unlike traditional firewalls, Multicloud Defense eliminates the need for customers to construct virtual firewalls, configure high-availability setups, or manage software installations.

Multicloud Defense Gateway instances operate on highly optimized software, incorporating a single pass datapath pipeline for efficient traffic processing and advanced security enforcement. Each gateway instance comprises three core processes: a "worker" process responsible for policy enforcement, a "distributor" process for traffic distribution and session management, and an "agent" process communicating with the controller. Gateway instances can seamlessly transition "in service" for a "datapath restart," enabling smooth upgrades without disrupting traffic flow.

New instances are spun up with new image. Once the instances are fully up, they are placed in the loadbalancer's (layer 4 sprayer of flows to gateway instances) target pool. The old instances are put in flow draining mode or flow timeout mode for the existing flows going through them. New flows will hit the new instances. Once the timeout (Azure) or the flows are drained (AWS), the old instances are reaped by the controller.

Use the following procedure to

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

Step 2 Select the checkbox for the gateway you want to upgrade. You can make only one selection at this time.

Step 3 Select **Actions** > **Upgrade**.

Step 4 From the **Gateway Image** list, select the desired image.

Step 5 Click **Save**.

Step 6 Confirm the cloud service provider resource allocation necessary for the upgrade.

Step 7 Click **Yes** if the resource allocation is sufficient. Click **No** if the resource allocation is insufficient, increase the resource allocation in the cloud service provider, and return to continue the upgrade.

Note You can view the upgrade progress and new gateway instances being created from theinstances info for the gateway. Select the gateway and view the **Instances** in the Details pane.

Abort a Multicloud Defense Gateway

You can only abort a Multicloud Defense Gateway that is currently going through an in-progress gateway update.

Use the following procedure to abort an existing Multicloud Defense Gateway:

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

Step 2 Select the Multicloud Defense Gateway you want to abort in the table so it is highlighted.

Step 3 Expand the **Actions** drop-down menu and click **Abort**.

Step 4 Confirm you want to abort the gateway and click **Yes**. To back out of the action, click **No**.

Enable a Multicloud Defense Gateway

You can only enable gateways that have been disabled. Use the following procedure to enable a

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

Step 2 Select the Multicloud Defense Gateway you want to enable in the table so it is highlighted.

Step 3 Expand the **Actions** drop-down menu and click **Enable**.

Step 4 Multicloud Defense validates the gateway configuration. If the validation is successful, a table of current and required resources for an upgrade generate for review. If you approve of the gateway resource allocation, click **Yes** to confirm the action.

What to do next

Wait a few minutes for the Multicloud Defense Gateway to successfully enable.

If you've disabled a Multicloud Defense Gateway and deleted the site-to-site VPN tunnels affiliated with it, you **must** create a new site-to-site VPN tunnel connection, or recreate the previous VPN tunnel connection and then add it to the gateway. When a gateway is disabled, Multicloud Defense forgets the public IP address associated with the VPN tunnel. You must create a new tunnel connection to establish a new IP for the gateway instance.

Disable a Multicloud Defense Gateway

You can only disable a Multicloud Defense Gateway if it is currently enabled. You cannot disable gateways that are already disabled.

Use the following procedure to disable a Multicloud Defense Gateway:

Step 1 Navigate to **Manage** > **Gateways**.
Step 2 Select the Multicloud Defense Gateway you want to disable in the table so it is highlighted.
Step 3 Expand the **Actions** drop-down menu and click **Disable**.
Step 4 Confirm you want to disable the gateway and click **Yes**. To cancel this action, click **No**.

What to do next

Wait a few minutes for the gateway to succesfully disable.

To completely disable the gateway, you **must** delete any site-to-site VPN tunnels affiliated with the gateway.

Export a Multicloud Defense Gateway

Use the following procedure to export the configuration of a Multicloud Defense Gateway:

Step 1 Navigate to **Manage** > **Gateways**.
Step 2 Select the Multicloud Defense Gateway you want to export in the table so it is highlighted.
Step 3 Expand the **Actions** drop-down menu and click **Export**.
Step 4 Multicloud Defense generates an export wizard.
Step 5 Either click **Download** to download the terraform locally or scroll down and click **Copy Code** to copy the JSON resource.
Step 6 Manually paste into the terraform script.
Step 7 Within the terraform prompt, execute the command provided in the lower half of the window: `terraform import "ciscomcd_gateway"."object-name" <object name>`.
Step 8 Follow the prompts within the terraform prompt to complete the task. **Close** the export window in Multicloud Defense. There are no more steps in the dashboard.

Delete a Multicloud Defense Gateway

Use the following procedure to delete a Multicloud Defense Gateway. Note that this action is different from disabling the gateway.

Step 1 Navigate to **Manage** > **Gateways**.
Step 2 Select the Multicloud Defense Gateway you want to delete in the table so it is highlighted.
Step 3 Expand the **Actions** drop-down menu and click **Delete**.

Step 4 Confirm the action and click **Yes**. To cancel the deletion action, click **Cancel**.

What to do next

We strongly recommend deleting any site-to-site VPN tunnel connections associated with this gateway after it is successfully deleted from the gateway table.