Google Cloud alias IP ranges let you assign ranges of internal IP addresses as aliases to a virtual machine's (VM) network interfaces. This is useful if you have multiple services running on a VM and you want to assign each service a different IP address. Alias IP ranges also work with GKE Pods (/kubernetes-engine/docs/how-to/ip-aliases).

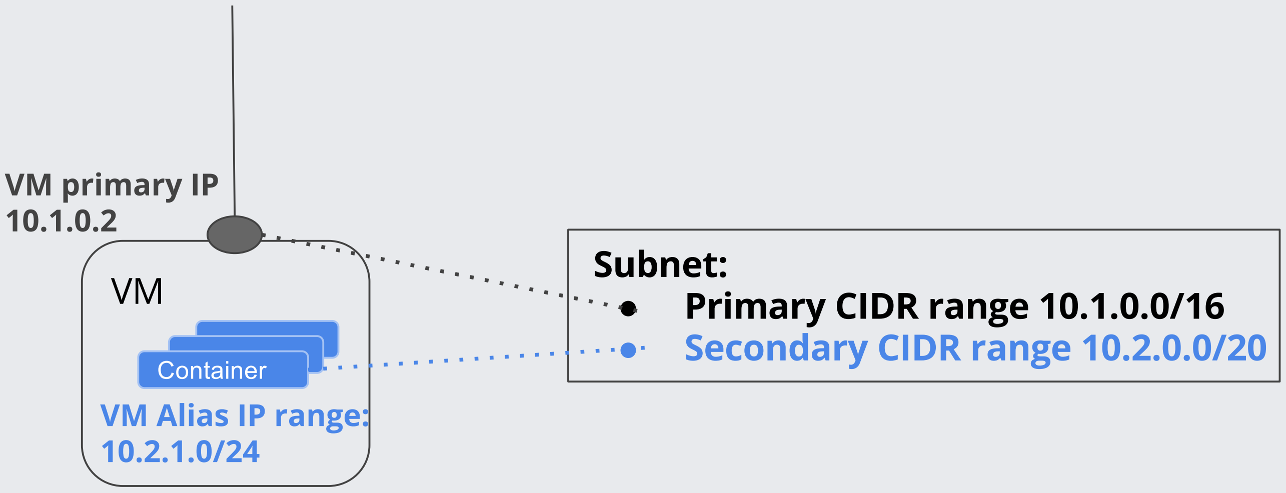
If you have only one service running on a VM, you can reference it using the interface's primary IP address. If you have multiple services running on a VM, you may want to assign each one a different internal IP address. You can do this with Alias IP ranges (https://wikipedia.org/wiki/IP_aliasing).

All subnets (/compute/docs/vpc) have a *primary CIDR range*, which is the range of internal IP addresses that define the subnet. Each VM instance gets its primary internal IP address from this range. You can also allocate alias IP ranges from that primary range, or you can add a secondary range to the subnet and allocate alias IP ranges from the secondary range. Use of alias IP ranges does not *require* secondary subnet ranges. These secondary subnet ranges merely provide an organizational tool.

Using IP aliasing, you can configure multiple internal IP addresses, representing containers or applications hosted in a VM, without having to define a separate network interface. You can assign VM alias IP ranges from either the subnet's primary or secondary ranges.

Configuring alias IP ranges (/vpc/docs/configure-alias-ip-ranges) describes commands for setting up a subnet with secondary ranges and for assigning alias IP addresses to VMs.

The following diagram provides a basic illustration of primary and secondary CIDR ranges and VM alias IP ranges on the VM's primary interface:



(/vpc/images/alias-ip/alias-ip-1.svg)

Primary and secondary CIDR ranges and VM alias IP ranges (click to enlarge)

- A primary CIDR range `10.1.0.0/16` is configured as part of a subnet.
- A secondary CIDR range `10.2.0.0/20` is configured as part of a subnet.
- The VM primary IP `10.1.0.2` is allocated from the primary CIDR range, `10.1.0.0/16`, while an alias IP range, `10.2.1.0/24`, is allocated in the VM from the secondary CIDR range, `10.2.0.0/20`.
- The addresses in the alias IP range are used as the IP addresses of the containers hosted in the VM.

When alias IP ranges are configured, Google Cloud automatically installs Virtual Private Cloud (VPC) network routes for primary and alias IP ranges for the subnet of the primary network interface. Your container orchestrator does not need to specify VPC network connectivity for these routes. This simplifies routing traffic and managing your containers. You do need to perform in-guest configuration as described in Alias IP ranges key properties (#alias_ip_ranges_key_properties).

When container IP addresses are allocated by Google Cloud, validation processes in Google Cloud ensure that container pod IP addresses do not conflict with VM IP addresses.

When alias IP addresses are configured, anti-spoofing checks are performed against traffic, ensuring that traffic exiting VMs uses VM IP addresses and pod IP addresses as source addresses. The anti-spoofing checks verify that VMs do not send traffic with arbitrary source IP addresses. Use of static routes for container networking would be a less secure approach compared to IP aliasing because it would require anti-spoofing checks to be disabled on container host VMs (anti-spoofing checks are disabled when IP forwarding is enabled).

Alias IP ranges are routable within the Google Cloud virtual network without requiring additional routes. You do not have to add a route for every IP alias and you do not have to take route quotas into account.

Alias IP addresses can be announced by Cloud Router (/sdk/gcloud/reference/compute/routers/create) to an on-premises network connected via VPN or Interconnect.

There are advantages to allocating alias IP ranges from a secondary CIDR range. By allocating from a range separate from the range used for primary IP addresses, you can separate infrastructure (VMs) from services (containers). When you configure separate address spaces for infrastructure and services, you can set up firewall controls for VM alias IP addresses separately from the firewall controls for a VM’s primary IP addresses. For example, you can allow certain traffic for container pods and deny similar traffic for the VM's primary IP address.

Consider a scenario in which you want to configure containerized services on top of Google Cloud. You need to create the VMs that will host the services, and, additionally, the containers.

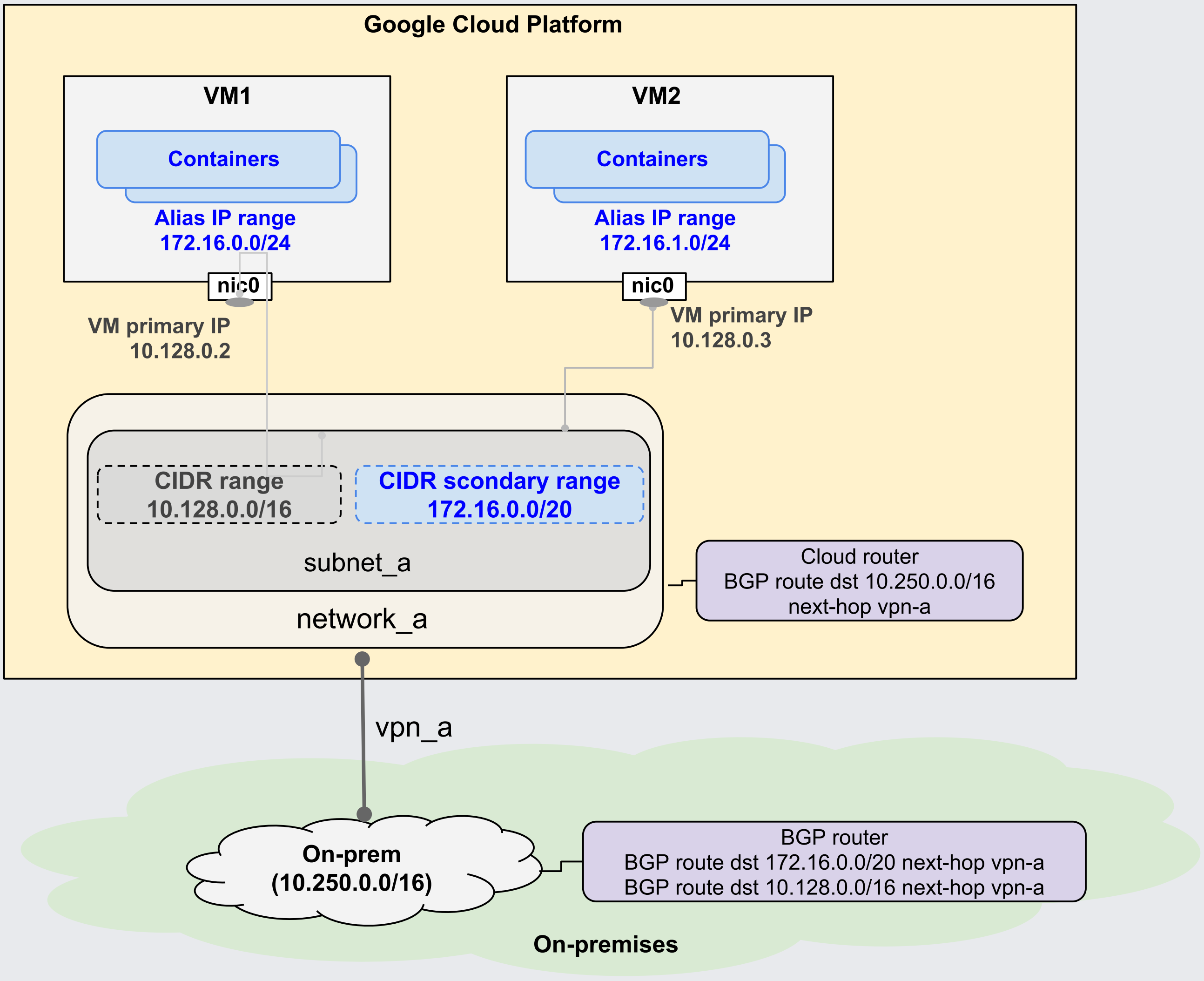
In this scenario, you want to route traffic from and to the containers to and from on-premises locations that are connected through a VPN. However, you don't want the primary VM IP addresses to be reachable through the VPN. To create this configuration, the container IP range need to be routable through the VPN, but not the VM primary IP range. At VM creation time, you also want to automatically assign a pool of IP addresses that are used for the container.

To create this configuration, do the following:

- When you create the subnet, you configure
  - One primary CIDR range, for example, `10.128.0.0/16`
  - One secondary CIDR range, for example, `172.16.0.0/16`
- Use an instance template to create VMs and automatically assign each the following:
  - A primary IP from the `10.128.0.0/16` range
  - An Alias range `/24` from the secondary CIDR `172.16.0.0/16` space, so that you can assign each container on a VM an IP from the `/24` secondary CIDR range

- Create two firewall rules (/vpc/docs/firewalls).
  - One rule that denies traffic traveling across the VPN from on-premises from reaching the subnet primary CIDR range.
  - One rule that allows traffic traveling across the VPN from on-premises to reach the subnet secondary CIDR range.

Using alias IP ranges, container IP addresses can be allocated from a secondary CIDR range and configured as alias IP addresses in the VM that is hosting the container.



(/vpc/images/alias-ip/alias-ip-2.svg)

Configuring containers with alias IP addresses (click to enlarge)

To create the configuration illustrated above:

1. Create a subnet (/vpc/docs/vpc) with a CIDR range 10.128.0.0/16, from which VM IP addresses are allocated from, and a secondary CIDR range 172.16.0.0/20 for the containers' exclusive use, which will be configured as alias IP ranges in the VM that is hosting them:

2. Create VMs with a primary IP from range 10.128.0.0/16 and an alias IP range 172.16.0.0/24 from the secondary CIDR range 172.16.0.0/20 for the containers in that VM to use:

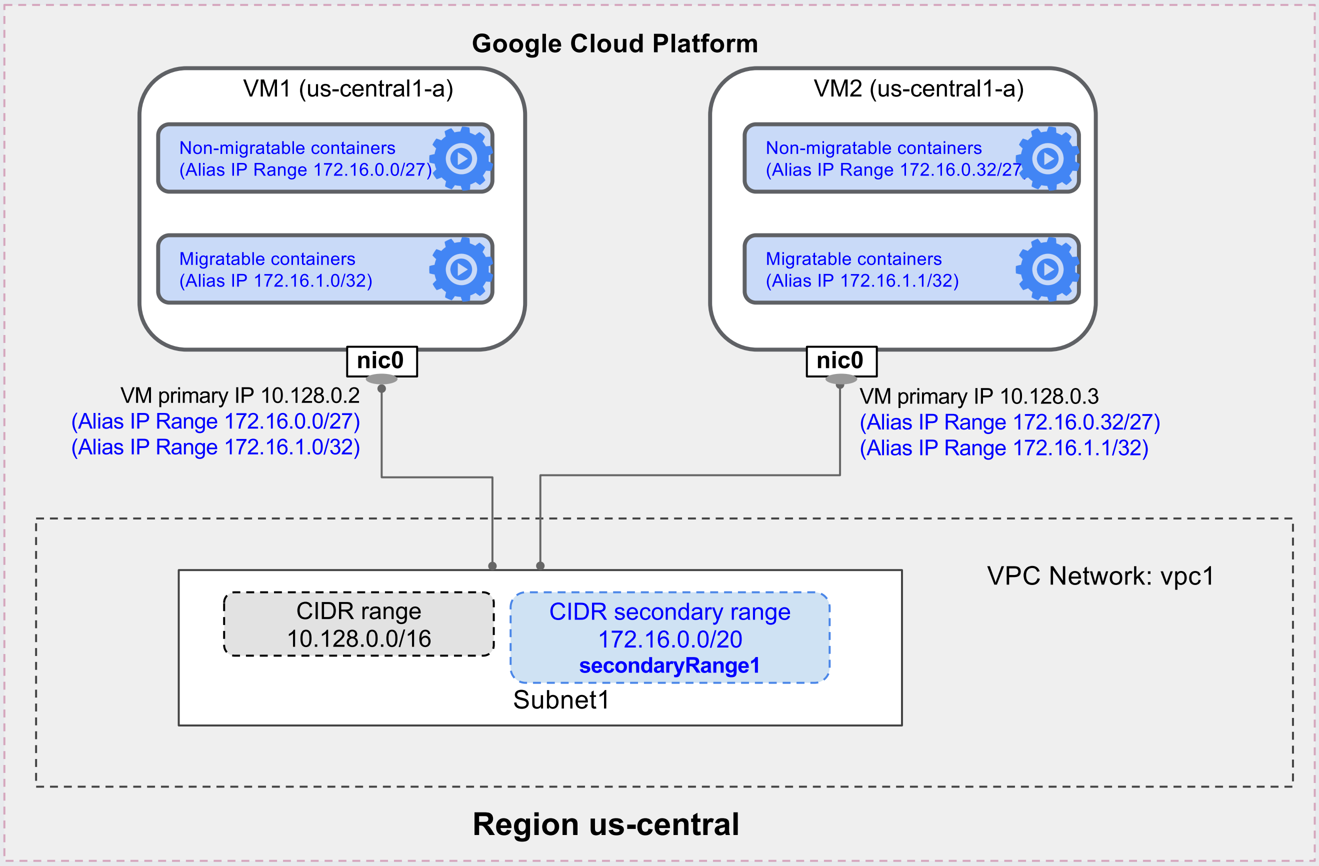
3. Container IP addresses are configured in Google Cloud as alias IP addresses. In this setup, both primary and alias IPs will be reachable through the VPN tunnel. If Cloud Router is configured, it will automatically advertise the secondary subnet range 172.16.0.0/20. For more information on using VPN with Cloud Router, see Creating a VPN tunnel using dynamic routing (/vpn/docs/how-to/creating-vpn-dynamic-routes).

Refer to Configuring alias IP addresses and ranges (/compute/docs/alias-ip/configure-alias-ip-ranges) for more information on the commands used to create this configuration.

Alias IP ranges allow you to manage IP allocation for applications running within VMs, including with containers.

You may have a deployment in which some containers are migratable across VMs and some are not. The migratable containers can be configured using /32 ranges, making it easy to migrate them individually. The non-migratable containers can be configured using a larger range, since they will stay together.

In these type of deployments, you might require more than one alias IP range per VM instance, for example a /27 for non-migratable containers and several /32s for migratable containers.



(/vpc/images/alias-ip/alias-ip-multiple.svg)

Configuring VMs with multiple alias IP ranges (click to enlarge)

In order to configure this example, use the following `gcloud` commands:

In auto mode VPC networks, a subnet exists in each region. These automatically created subnets each have a primary CIDR range, but no secondary range. To use alias IP with an auto mode VPC network, you can allocate alias IP ranges from the automatically created subnet's primary CIDR range or add a secondary range (/vpc/docs/configure-alias-ip-ranges#adding_secondary_cidr_ranges_to_an_existing_subnet) to the automatically created subnet and allocate alias IP ranges from the new secondary range.

Alternatively, you can create a new subnet (/vpc/docs/configure-alias-ip-ranges#creating_a_subnet_with_one_or_more_secondary_cidr_ranges) with secondary ranges in the auto mode VPC network as long as none of its ranges overlap with `10.128.0.0/9`. You can then create VM instances in the new subnet and allocate alias IP ranges from any range on that subnet.

See Adding secondary CIDR ranges to an existing subnet (/vpc/docs/configure-alias-ip-ranges#adding_secondary_cidr_ranges_to_an_existing_subnet) if you want to add secondary ranges to your subnet.

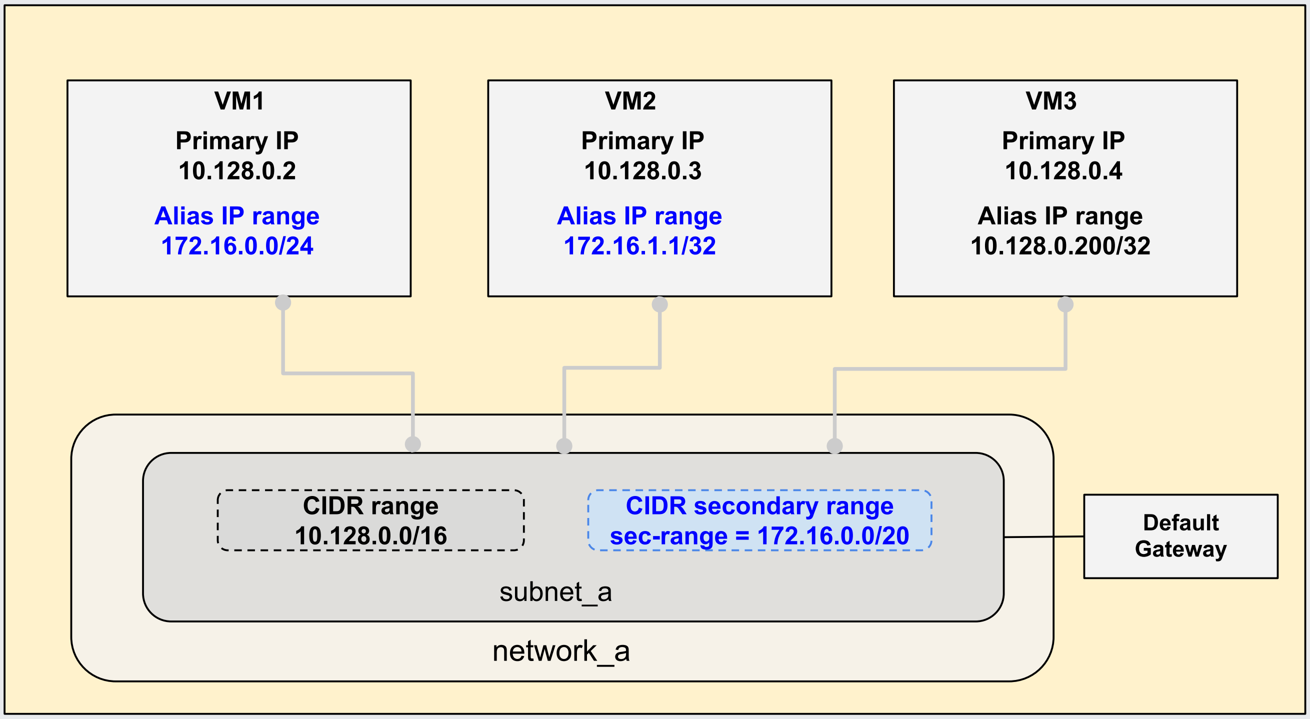
In custom-mode networks:

- All of the subnets are created manually
- One primary CIDR range is mandatory.
- You can optionally create secondary CIDR ranges.

The following properties apply to alias IP ranges configured in VMs:

- From the VM OS perspective, the primary IP address and the default gateway are typically allocated using DHCP. Alias IP addresses can be configured in the VM OS, which is typically Linux or Windows, manually or by using scripts.
- The primary IP address and the alias IP range of the interface must be allocated from CIDR ranges configured as part of the same subnet. Note the following requirements:

- The primary IP address must be allocated from the CIDR primary range.
- The alias IP range can be allocated either from the primary CIDR range or from a secondary CIDR range of that same subnet.
- For a VM network interface, the alias IP must be from the same subnet resource that provides the IP address for the primary network interface. You can't select a primary or secondary CIDR range from another subnet resource.
- The primary IP address can be user-configured with a static private IP address or system auto-allocated with an ephemeral static IP address.
- Alias IP ranges are optional and they are not automatically added. An alias IP range can be configured during instance creation or modification.
- An alias IP range can be configured as an explicit CIDR range (for example, `10.128.1.0/24`), a single IP address (for example, `10.128.7.29`), or as a netmask (`/24`). An alias IP range can be fully specified or auto-allocated by specifying the netmask.
- Because all subnets (/vpc/docs/vpc) in a VPC network share a single default gateway, all alias IP addresses within an interface share the same default gateway as the primary IP address.



(/vpc/images/alias-ip/alias-ip-4.svg)

Alias IPs within an interface share the same default gateway as the primary IP address (click to enlarge)

Google Cloud automatically configures internal DNS for the primary IP of the primary interface of every VM instance. This associates the instance host name with the primary interface primary IP address. However, the DNS lookup on that host name only works in the network that contains the primary interface.

Google Cloud does not automatically associate any other IP addresses with the host name. Google Cloud does not associate alias IP addresses on the primary interface with the host name, and it does not associate any IP addresses of secondary interfaces with the host name.

You can manually configure DNS to associate other IP addresses.

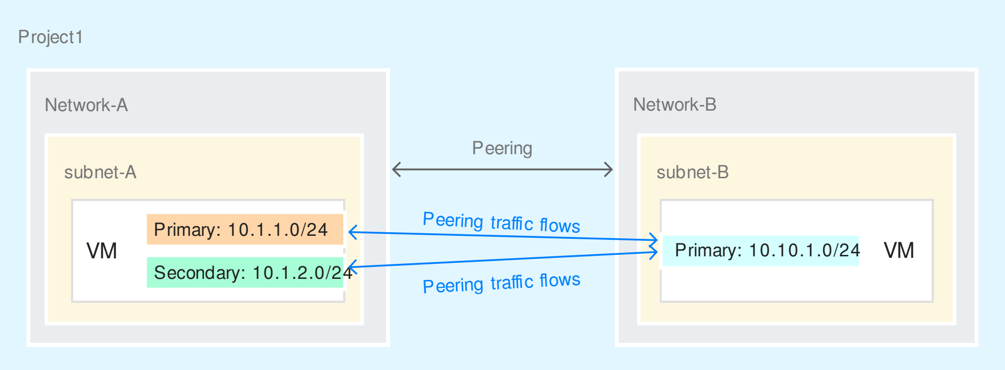
Firewall source tags are not supported for alias IP addresses. When you configure source tags in firewall rules, the source tag matches the VM primary IP address, but not the alias IP addresses. Use source ranges to allow or deny ingress traffic from IP Alias addresses.

In a static route, the next-hop IP address must be the primary IP address of the virtual machine instance. An alias IP address is not supported as the next-hop IP address.

VPC Network Peering (/vpc/docs/vpc-peering) allows you to peer two VPC networks so that the VMs in the two networks can communicate via internal, private IP addresses.

Both primary and secondary IP ranges of a subnet are reachable by VM instances in a peered network.

Subnet overlap checks across peered networks ensure that primary and secondary ranges do not overlap with any peered ranges.



(/vpc/images/peering/network-peering-09.svg)
IP aliasing with network peering (click to enlarge)

- Learn how to configure alias IP addresses and alias IP ranges (/vpc/docs/configure-alias-ip-ranges).