

Product or feature is in a pre-release state and might change or have limited support. For more information, see the [product launch stages](#) (/products/#product-launch-stages).

Use Packet Mirroring to mirror traffic to and from particular VM instances. You can use the collected traffic to help you detect security threats and monitor application performance. For details about Packet Mirroring, see the [Packet Mirroring overview](#) (/vpc/docs/packet-mirroring).

The following sections describe how to create and manage packet mirroring policies.

Before you create a packet mirroring policy, you must have the appropriate permissions. You must also create an internal load balancer, which is the collector destination, in the same region as the instances to mirror.

To create and manage packet mirroring policies, Google Cloud provides two roles that are related to Packet Mirroring:

- [compute.packetMirroringUser](#) (/compute/docs/access/iam#compute.packetMirroringUser) grants users permission to create, update, and delete packet mirroring policies. To use Packet Mirroring, users must have this role in projects where they create packet mirroring policies.
- [compute.packetMirroringAdmin](#) (/compute/docs/access/iam#compute.packetMirroringAdmin) grants users permission to mirror particular resources. Even if users have permission to create a packet mirroring policy, they still require permission to mirror related sources. Use this role in projects where the owner of a policy might not have any other permissions, for example, in Shared VPC scenarios.

For more information about using Cloud IAM roles, see [Granting, changing, and revoking access to resources](#) (/iam/docs/granting-changing-revoking-access) in the Cloud IAM documentation.

You must have an [internal TCP/UDP load balancer](/load-balancing/docs/internal/) that is configured for packet mirroring, and it must be located in the same region as the instances that you're mirroring. All traffic from mirrored sources is sent to the collector instances that are behind the load balancer.

To configure the internal load balancer for Packet Mirroring, the forwarding rule must be configured as a packet mirroring collector. Non-mirrored traffic that is sent to the load balancer is dropped. Also, if a packet mirroring policy might apply to the collector instances, Packet Mirroring ignores them and doesn't mirror their traffic.

For details about configuring internal load balancers, see [configuring load balancer components](/load-balancing/docs/internal/setting-up-internal#configure_the_load_balancer).

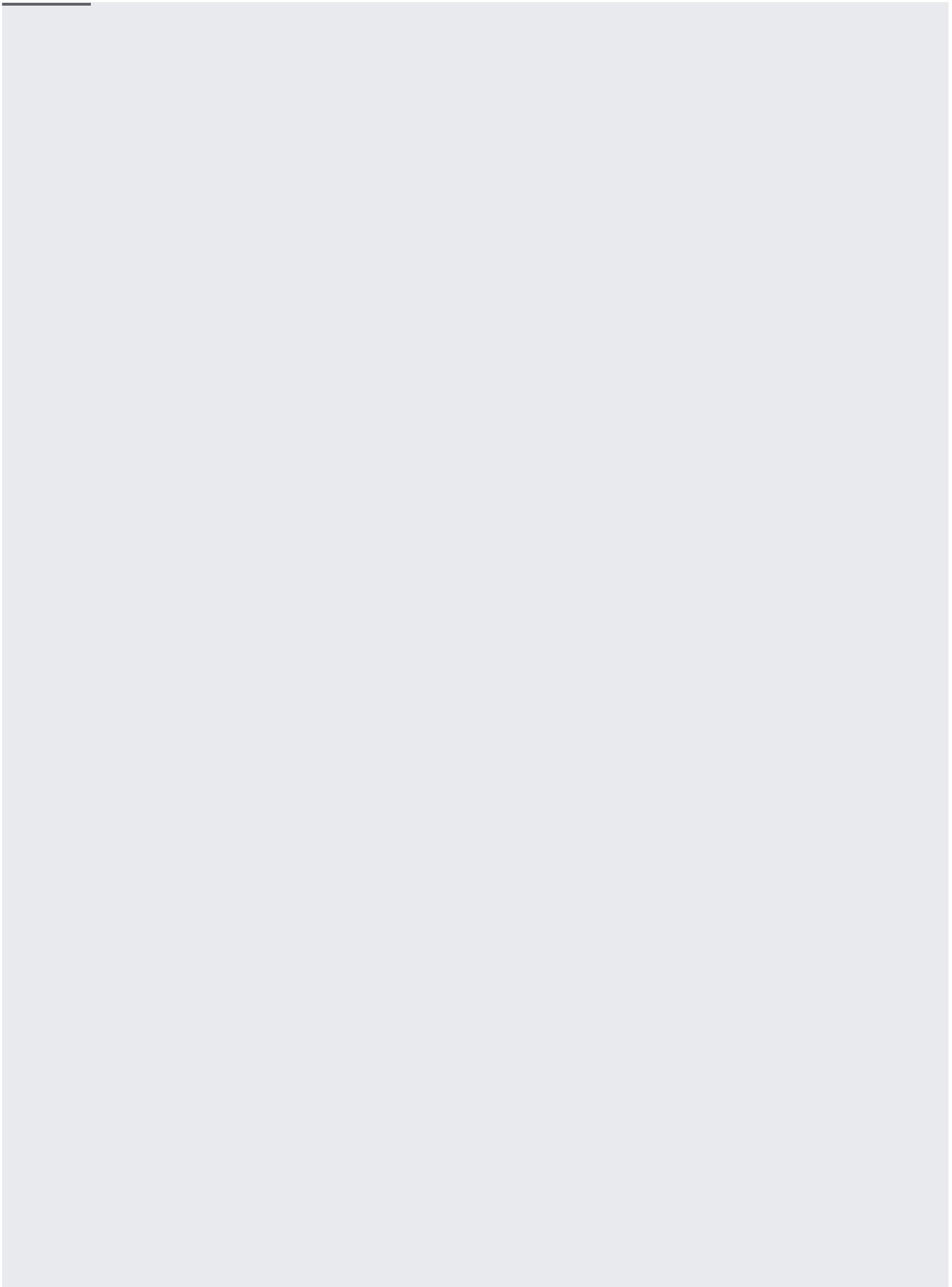
Due to the [packet collection behavior](/vpc/docs/packet-mirroring#collection), use an unmanaged instance group with an instance.

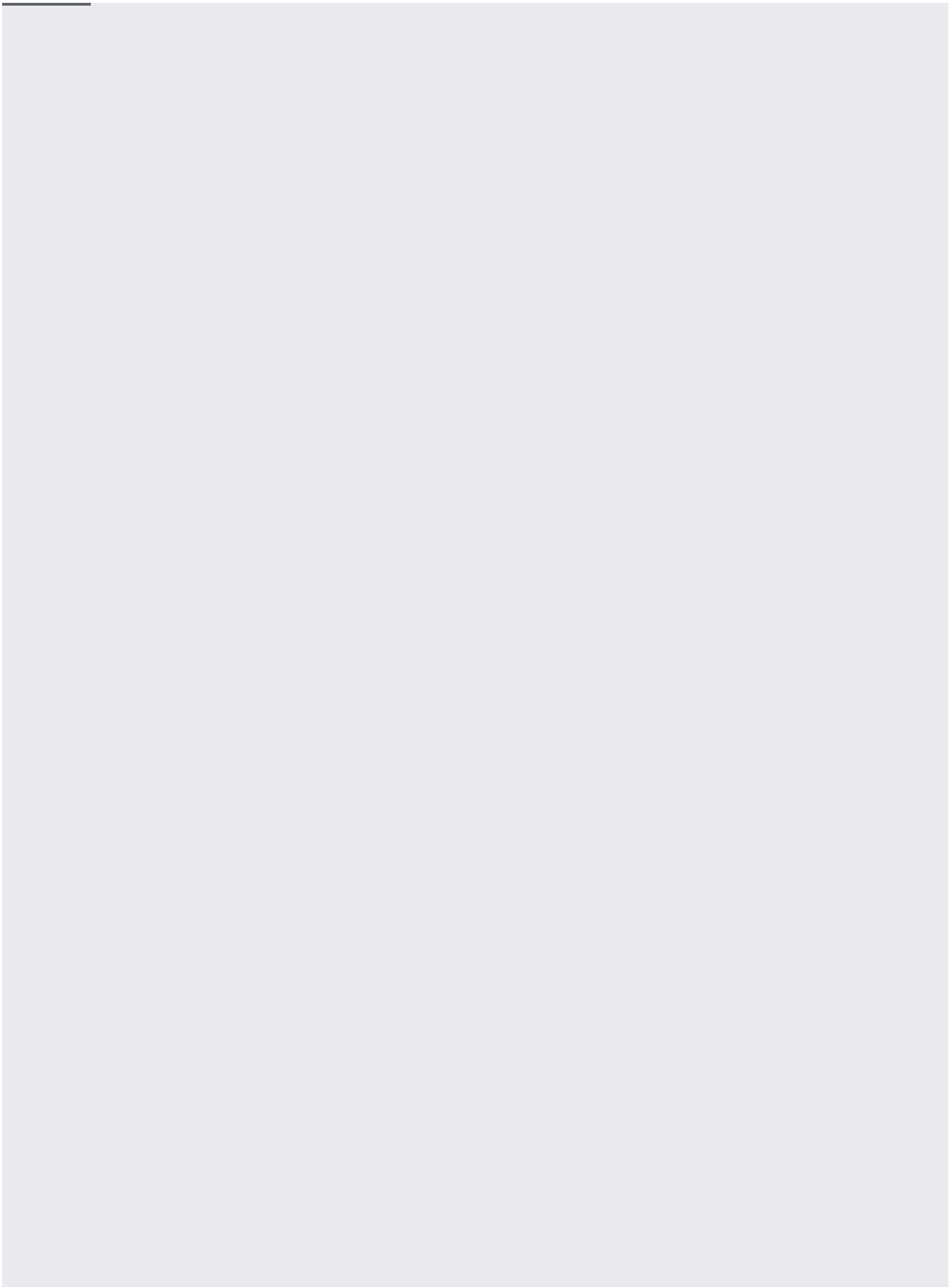
Mirrored traffic must be allowed to go from source instances to the destination instances that are part of the internal load balancer. You might already have existing rules that allow this traffic.

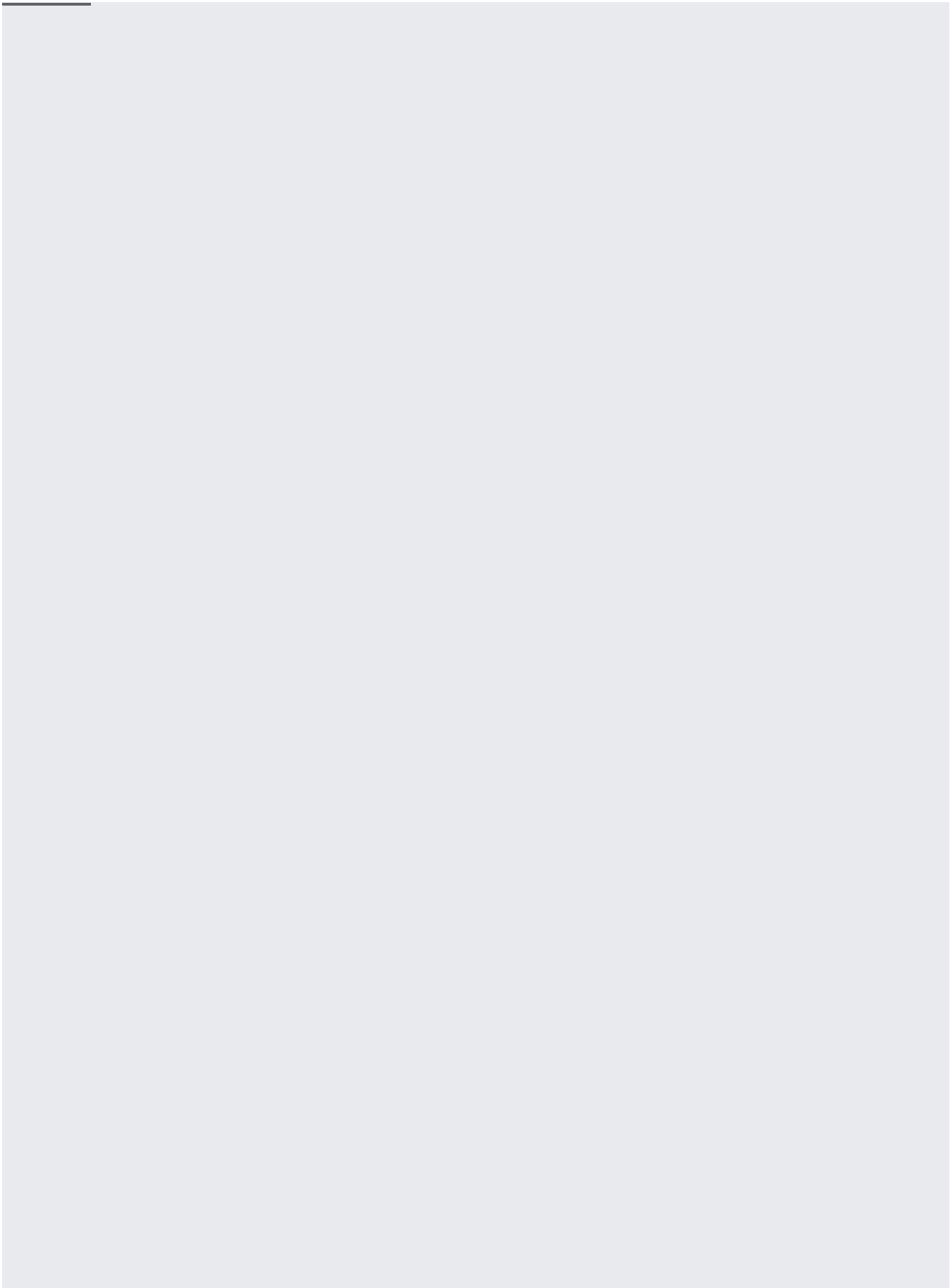
- Check that mirrored instances have an egress rule that allows them to send traffic to the forwarding rule of the internal load balancer.
- Check that collector instances in the load balancer's instance group have an ingress rule that allows them to receive traffic from mirrored instances or from the IP address range of mirrored instances. For example, you can specify a source range `0.0.0.0/0` to collect all incoming traffic from mirrored instances. To prevent internet traffic from reaching the collector instances, assign only internal IP addresses to them.

If you don't have existing rules that allow this traffic, see [Using firewall rules](/vpc/docs/using-firewalls) to create them.

Create a packet mirroring policy to start mirroring traffic to and from particular instances.

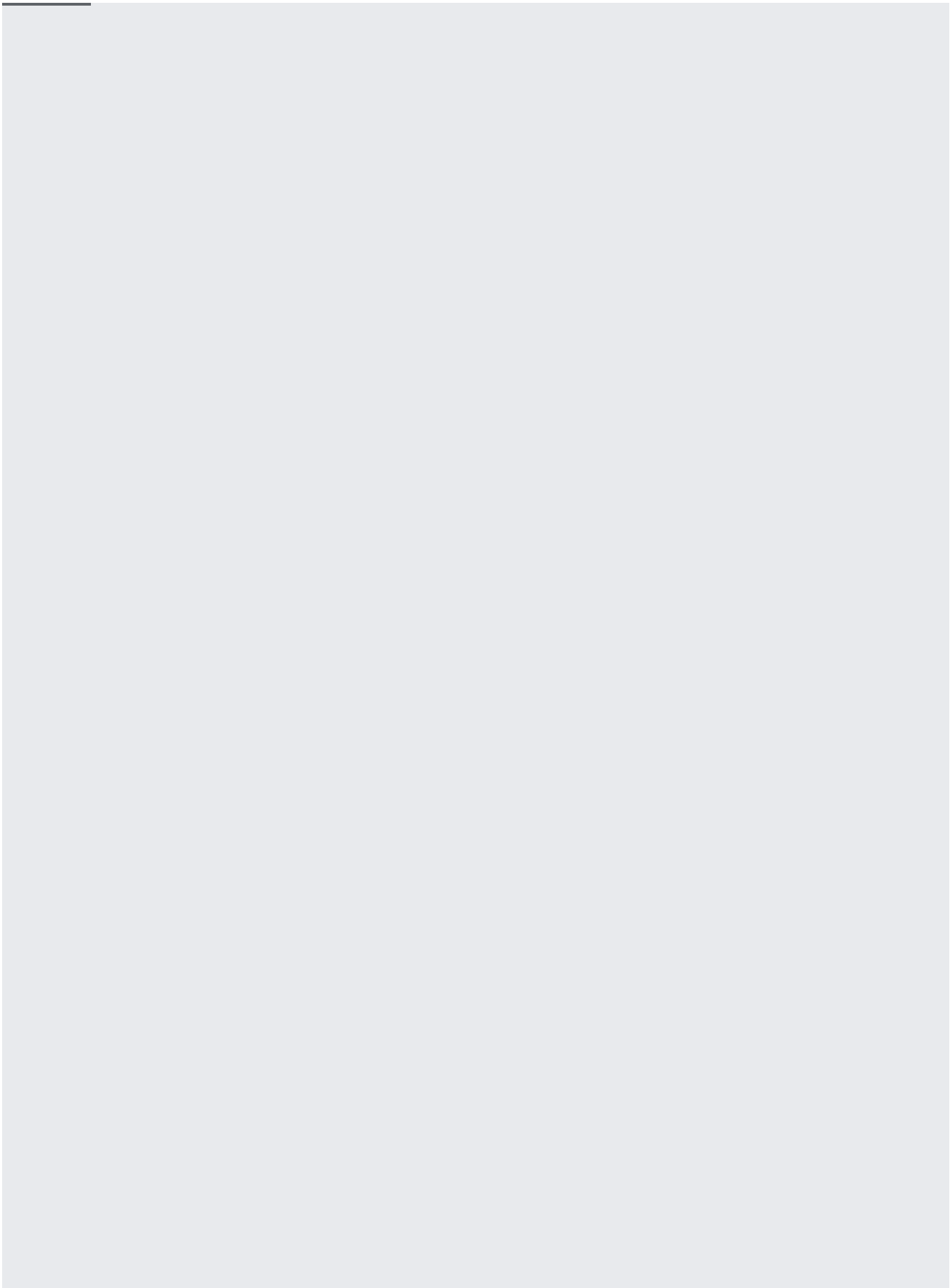






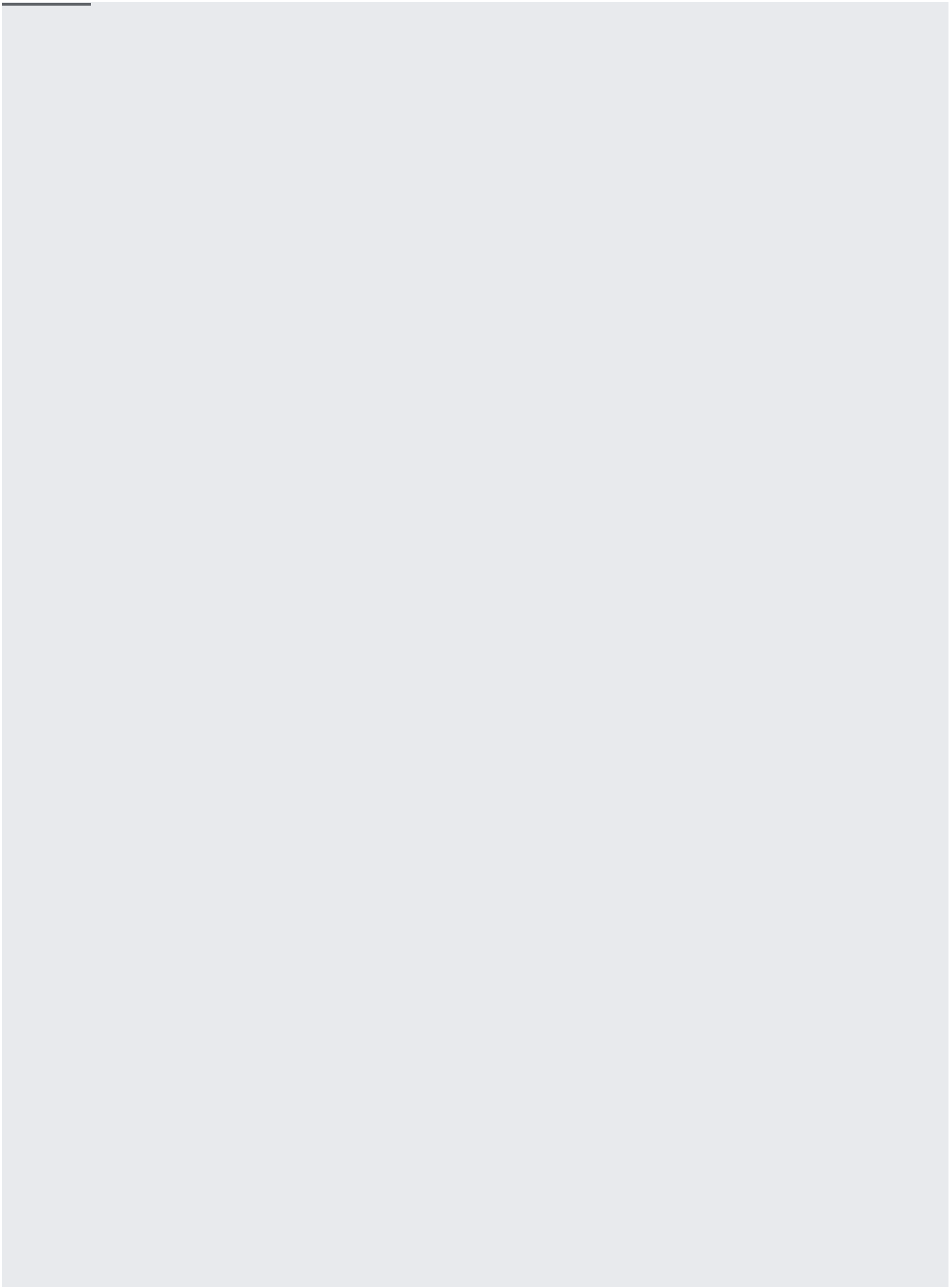
To verify that your packet mirroring policy is in effect, see [Monitoring packet mirroring policies \(/vpc/docs/monitoring-packet-mirroring\)](/vpc/docs/monitoring-packet-mirroring).

Update an existing policy to change its priority, mirrored sources, or collector destination.

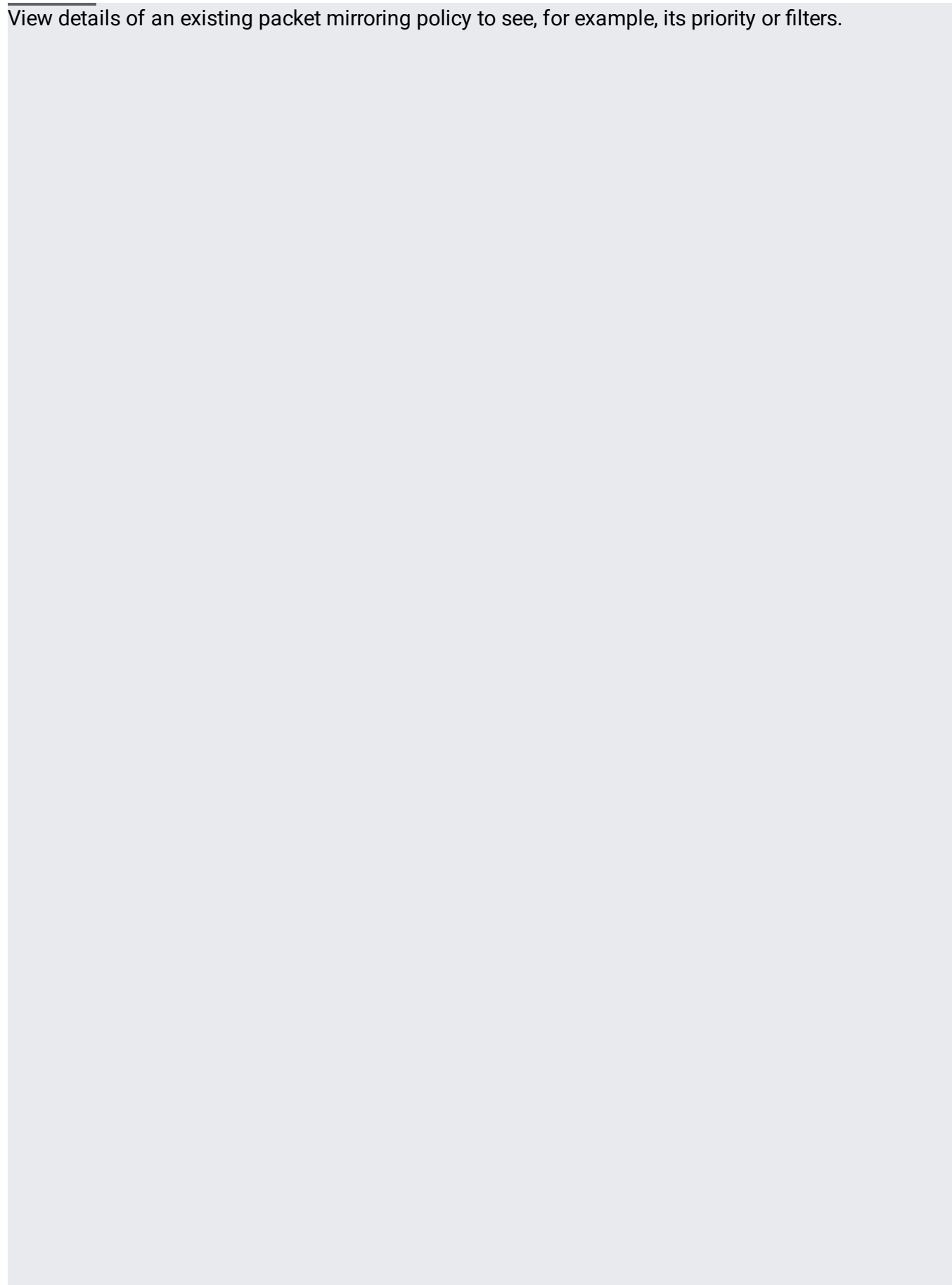


List packet mirroring policies to view existing policies.





View details of an existing packet mirroring policy to see, for example, its priority or filters.



Disable or enable a packet mirroring policy to stop or start collecting mirrored traffic.

Delete a packet mirroring policy to remove it from your project. After you delete a policy, Google Cloud stops mirroring all traffic that is related to the policy.

If your packet mirroring policy isn't collecting the intended mirrored traffic, check the following configurations:

- Check that you have firewall rules that allow traffic from mirrored instances to the collector instances.
- Check that your mirrored sources include or exclude the instances to mirror. For example, if you specify a subnet as a mirrored source, all existing and future instances in the subnet are

mirrored. If you specify tags, only instances that have matching tags are mirrored.

- Check that the packet mirroring filters aren't too broad or too narrow. You might have unintentionally configured filters to include or exclude certain traffic.