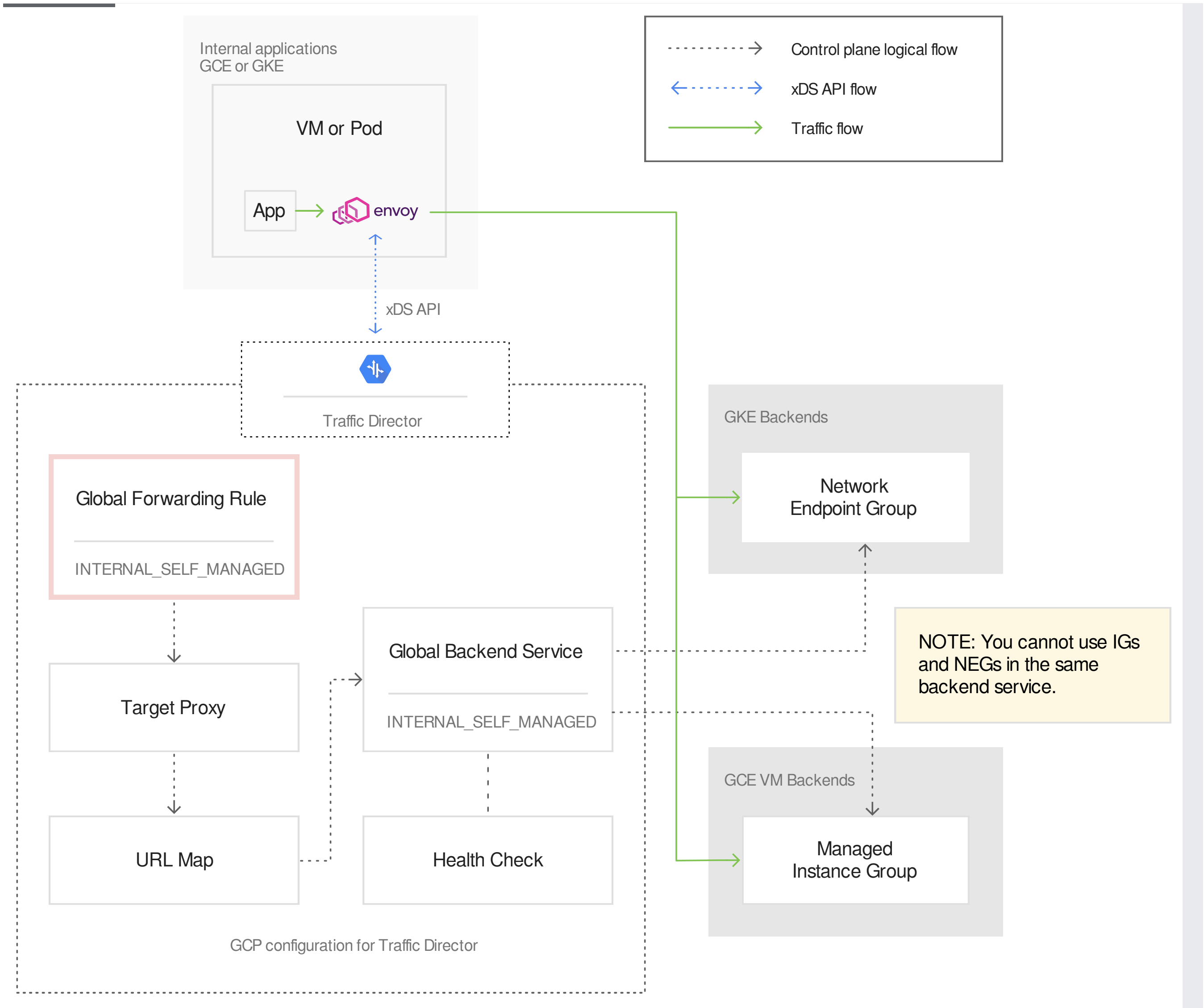
For Traffic Director, forwarding rules are internal, self-managed, and global (/compute/docs/reference/rest/v1/globalAddresses/insert). Each Traffic Director forwarding rule provides a single global IPv4 address for a service. You can use that address to create internal DNS records for your service (for example, using a Cloud DNS managed private zone (/dns/zones/#creating_private_zones)). Metadata filters in the forwarding rule specify the criteria for which an xDS-compliant sidecar proxy receives the configuration.

Forwarding rules are also used for protocol forwarding (/compute/docs/protocol-forwarding), for Classic VPN gate
/docs/concepts/overview#classic-vpn), and for Google Cloud load balancers
-balancing/docs/using-forwarding-rules) to provide forwarding information in the control plane. Refer to Forwardin
pts (/load-balancing/docs/forwarding-rule-concepts) for a more comprehensive overview of forwarding rules. This p
scusses forwarding rules in the context of Traffic Director.

For the Traffic Director control plane, the internal, self-managed, and global forwarding rule routes traffic by IP address, port, and protocol to a target proxy, which points to a URL map containing rules that determine the destination of the traffic. The URL map specifies the appropriate backend service, which performs a health check and then determines the appropriate backend, such as an instance group containing your virtual machine instances or a network endpoint group (/kubernetes-engine/docs/how-to/container-native-load-balancing) containing GKE backend pods.



(/traffic-director/images/td-forwarding-rule.svg)

Traffic Director forwarding rule highlighted (click to enlarge)

The diagram shows how a forwarding rule fits into the Traffic Director architecture.

A forwarding rule resource contains the following properties that apply to Traffic Director. Traffic that matches the destination IP address, protocol, and port number is handled by the forwarding rule.

`name`

> *[Required]* The name of the forwarding rule. The name must be unique in this project, from 1-63 characters long and match the regular expression: `[a-z]([-a-z0-9]*[a-z0-9])?` which means the first character

must be a lowercase letter, and all following characters must be a dash, lowercase letter, or digit, except the last character, which cannot be a dash.

`IPAddress`

[Required] Must be one of the following: `0.0.0.0`, `127.0.0.1`, or any RFC 1918 address. IP addresses for Traffic Director forwarding rules do not need to correspond to IP address ranges of subnets in the VPC network. For a given VPC network, IP address, and port, you can have only one internal, self-managed forwarding rule. For example, in the same VPC network, you cannot create two forwarding rules that use the `0.0.0.0` IP address and port `80`.

`target`

[Required] The target proxy that this forwarding rule directs traffic to. Traffic Director only supports `target-http-proxy`. When you use the GCP Console to configure the forwarding rule, the target proxy is configured automatically. When you use `gcloud` or the API, the target proxy must exist before you create your forwarding rule. You can use more than one forwarding rule with a given proxy.

`IPProtocol`

[Required] The type of protocol that this forwarding rule matches. The only supported value is `TCP`.

`loadBalancingScheme`

[Required] Specifies how the forwarding rule is used. The valid value for Traffic Director is `INTERNAL_SELF_MANAGED`.

`portRange`

[Required] A port or a port range joined by a dash. Packets of the specified protocol sent to these ports are forwarded to the appropriate backend. You can specify a single number of a range. For example, `80` or `80-8080`. For a given VPC network, IP address, and port, you can have only one internal, self-managed forwarding rule. For example, in the same VPC network, you cannot create two forwarding rules that use the `0.0.0.0` IP address and port `80`.

`network`

[Required] Specifies the VPC where the Google Cloud VMs running Envoy proxies are located. The Envoy proxies read the Traffic Director configuration that you define for the same network where the proxies are deployed. You can use the VPC network named `default` or a custom network.

Traffic Director supports load balancing for clients only within the Google Cloud network, and you specify the network name in the forwarding rule. VPC Peering isn't supported.

To learn how to configure a forwarding rule within the overall Traffic Director setup, see:

- Setting Up Traffic Director for Compute Engine with VMs (/traffic-director/docs/set-up-gce-vms).
- Setting Up Traffic Director for Google Kubernetes Engine with pods (/traffic-director/docs/set-up-gke-pods)

- For overview information about Traffic Director, see Traffic Director concepts (/traffic-director/docs/traffic-director-concepts).
- For information about using metadata filters to control which sidecar proxies receive the configuration attached to the forwarding rule, see Configuring advanced traffic management (/traffic-director/docs/configure-advanced-traffic-management#config-filtering-metadata).