Name:Erfan Ahmadbeigi

Master:Milad nourian nasab

Subject: DNS policy

DNS server policies

You can configure one DNS server policy for each Virtual Private Cloud (VPC) network. The policy can specify inbound DNS forwarding, outbound DNS forwarding, or both. In this section, inbound server policy refers to a policy that permits inbound DNS forwarding. Outbound server policy refers to one possible method for implementing outbound DNS forwarding. It is possible for a policy to be both an inbound server policy and an outbound server policy if it implements the features of both.

**Inbound server policy**

Each VPC network provides DNS name resolution services to the VMs that use it. When a VM uses its metadata server 169.254.169.254 as its name server, Google Cloud searches for DNS records according to the name resolution order.

By default, a VPC network's name resolution services—through its name resolution order—are only available to that VPC network itself. You can create an inbound server policy in your VPC network to make these name resolution services available to an on-premises network that is connected using Cloud VPN or Cloud Interconnect.

When you create an inbound server policy, Cloud DNS takes an internal IP address from the primary IP address range of each subnet that your VPC network uses. For example, if you have a VPC network that contains two subnets in the same region and a third subnet in a different region, a total of three IP addresses are reserved for inbound forwarding. Cloud DNS uses these internal IP addresses as entry points for inbound DNS requests

### Inbound server policy entry points

The regional internal IP addresses used by Cloud DNS for the inbound server policy serve as entry points into the name resolution services of the VPC network. As a best practice, routing to an inbound server policy entry point in a region should be handled by Cloud VPN tunnels or Cloud Interconnect attachments in the same region. For Cloud VPN tunnels using dynamic routing and for all Cloud Interconnect attachments, Cloud Router manages a BGP session, including advertisement of inbound entry point IP addresses. Cloud Router default route advertisements include inbound entry point IP addresses because their IP addresses come from the VPC network's subnets. For detailed information about Cloud Router advertisement options, see [Route advertisement modes](https://cloud.google.com/network-connectivity/docs/router/concepts/overview#route-advertisement) in the Cloud Router documentation.

Regardless of the entry point's region, Cloud DNS uses the region of the VPN tunnel or Cloud Interconnect attachment (VLAN) as the canonical source for the request. For more information, see [Manage DNS routing policies](https://cloud.google.com/dns/docs/zones/manage-routing-policies).

For information about how to create inbound server policies, see [Creating an inbound server policy](https://cloud.google.com/dns/docs/policies#create-in).

## Outbound server policy

You can change the name resolution order by creating an outbound server policy that specifies a list of alternative name servers. When you specify alternative name servers for a VPC network, those servers are the only name servers that Google Cloud queries when handling DNS requests from VMs in your VPC network that are configured to use their metadata servers (169.254.169.254).

**Alternative name servers and routing methods**

Cloud DNS supports three types of alternative name servers and offers standard and private routing methods for routing traffic to them.

Alternative name servers are defined in the following table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Alternative name server** | **Description** | **Standard routing supports** | **Private routing supports** | **Source of requests** |
| Type 1 | An [internal IP address](https://cloud.google.com/vpc/docs/ip-addresses) of a Google Cloud VM in *the same* VPC network where the outbound server policy is defined. | Only RFC 1918 IP addresses—traffic always routed through an authorized VPC network. | Any internal IP address, including non-RFC 1918 private IP addresses and privately re-used public IP addresses—traffic always routed through an authorized VPC network. | 35.199.192.0/19 |
| Type 2 | An IP address of an on-premises system, connected to the VPC network with the outbound server policy, using Cloud VPN or Cloud Interconnect. | Only RFC 1918 IP addresses—traffic always routed through an authorized VPC network. | Any internal IP address, including non-RFC 1918 private IP addresses and privately re-used public IP addresses—traffic always routed through an authorized VPC network. | 35.199.192.0/19 |
| Type 3 | An [external IP address](https://cloud.google.com/vpc/docs/ip-addresses) of a DNS name server accessible to the internet *or* the external IP address of a Google Cloud resource; for example, the external IP address of a VM in another VPC network. | Only internet-routable external IP addresses—traffic always routed to the internet or to the external IP address of a Google Cloud resource. | Private routing isn't supported. | [Google Public DNS source ranges](https://developers.google.com/speed/public-dns/faq#locations) |

You can choose one of the following routing methods when you specify the alternative name server of an outbound server policy:

* **Standard routing:** Routes traffic through an authorized VPC network or over the internet based on whether the alternative name server is an RFC 1918 IP address. If the alternative name server is an RFC 1918 IP address, Cloud DNS classifies the name server as either a *Type 1* or *Type 2* name server, and routes requests through an authorized VPC network. If the alternative name server is not an RFC 1918 IP address, Cloud DNS classifies the name server as *Type 3*, and expects the name server to be internet accessible.
* **Private routing:** Always routes traffic through an authorized VPC network, regardless of the alternative name server's IP address (RFC 1918 or not). Consequently, only *Type 1* and *Type 2* name servers are supported.

To access a *Type 1* or a *Type 2* alternative name server, Cloud DNS uses routes in the authorized VPC network, where the DNS client is located. These routes define a secure path to the name server:

* Cloud DNS uses automatically created [subnet routes](https://cloud.google.com/vpc/docs/routes#subnet-routes) to send traffic to *Type 1* alternative name servers. *Type 1* name servers use [a special return route for Cloud DNS responses](https://cloud.google.com/vpc/docs/routes#cloud-dns) to reply .
* Cloud DNS can use either [custom dynamic routes or custom static routes](https://cloud.google.com/vpc/docs/routes#peering-custom-routes), except for custom static routes with network tags, to send traffic to *Type 2* alternative name servers. *Type 2* name servers use routes in your on-premises network to reply.

For additional guidance about network requirements for *Type 1* and *Type 2* name servers, see [alternative name server network requirements](https://cloud.google.com/dns/docs/policies#firewall-rules).

**Alternative name server selection order**

Cloud DNS lets you configure a list of alternative name servers for an [outbound server policy](https://cloud.google.com/dns/docs/server-policies-overview#dns-server-policy-out) and a list of forwarding targets for a forwarding zone.

In case of multiple alternative name servers, Cloud DNS uses an internal algorithm to select an alternative name server. This algorithm ranks each alternative name server.

To process a request, Cloud DNS first tries a DNS query by contacting the alternative name server with the highest ranking. If that server does not respond, Cloud DNS repeats the request to the next highest ranked alternative name server. If no alternative name servers reply, Cloud DNS synthesizes a [SERVFAIL](https://cloud.google.com/dns/docs/troubleshooting#outbound-forwarded-queries-receive-servfail-errors) response.

The ranking algorithm is automatic, and the following factors increase the ranking of an alternative name server:

* The higher the number of successful DNS responses processed by the alternative name server. Successful DNS responses include NXDOMAIN responses.