



NAT-aware Public-Private GSLB Configuration

Avi Technical Reference (v20.1)

Copyright © 2021

NAT-aware Public-Private GSLB Configuration

[view online](#)

An Avi GSLB configuration can serve clients from a mixture of public and private networks.

Introduction

Typically, the VIP configured in a local virtual service (configured as a GSLB pool member) is a private IP address. But this IP address may not always be reachable by the client. For example, a user on a laptop could come in via the corporate intranet or VPN, but also directly from the public Internet. In the former case, the source IP address would be an intranet private IP address. In the latter case, it would be a public IP address. Note that, with resolvers (LDNS) in the middle and no support for extension mechanism for DNS (EDNS), this may not be as simple.

Note ? If EDNS processing is enabled, the client's IP address is found within the ECS option. For more information, refer to the [Extension Mechanisms for DNS Client Subnet Option Insertion](#) article.

The source being a certain set of resolver IP addresses could indicate that the client is coming in from a private network, and another set of IP addresses could indicate that the client is coming in from a public network.

How It Works

Client DNS requests coming in from within the intranet have the private IP served in the A record, and requests from outside are served the public IP address. Please note that datapath health monitoring is performed only against the private IP address.

UI Configuration

In the GSLB global configuration (navigating to Infrastructure -> GSLB -> Edit), the user can specify a list of IP addresses (specific addresses, ranges or prefixes), and categorize them as either private or public. Refer to the below screenshot. If a private list is specified, all other addresses are deemed public, and vice versa.

Edit GSLB Configuration ✕

GSLB Subdomain ⓘ
 🗑️

GSLB Subdomain ⓘ
 🗑️

[+ Add GSLB Subdomain](#)

Client Group IP Address Type
 ▾

🗑️

🗑️

🗑️

[+ Add Group IP Address](#)

In the GSLB pool member configuration, an optional public IP address can be specified. This field is used to host the public IP address for the VIP, which gets NAT'ed to the private IP by a firewall. Refer to the below screenshot.

← Edit GSLB Pool
✕

SI

Priority* ?

LB Algorithm* ?

Pool Member

IP Address
 Virtual Service

IP Address or FQDN* ?

Third-party Site Cluster Controller ?

Public IP Address ?

Ratio* ?

Enabled ?

Add GSLB Pool Member

CLI Configuration

In the below CLI sequence, private and public address ranges are defined.

```
{% cli %}: > configure gslb glb-1
gslb> client_ip_addr_group
gslb:client_ip_addr_group>
gslb:client_ip_addr_group> type gslb_ip_p gslb_ip_private Private IP Address. gslb_ip_public Public IP Address.
gslb:client_ip_addr_group> type gslb_ip_public
gslb:client_ip_addr_group> prefixes 1.1.1.0/24
gslb:client_ip_addr_group> addrs 2.1.1.1
gslb:client_ip_addr_group> ranges begin 3.3.3.0 end 3.3.3.42 New object being created
gslb:client_ip_addr_group:ranges> save
gslb:client_ip_addr_group> save
gslb> save ... client_ip_addr_group type GSLB_IP_PUBLIC addrs[1] 2.1.1.1 ranges[1] begin 3.3.3.0 end 3.3.3.42 prefixes
[1] 1.1.1.0/24 tenant_ref admin -----+{% endcli %}
```

In the below CLI sequence, a public IP address is added to an existing pool member.

```
{% cli %}: > configure gslbservice gs-1 Updating an existing object. Currently, the object is: : gslbservice> groups index 1 :  
gslbservice:groups> members index 1 : gslbservice:groups:members> public_ip ip 2.2.2.2 : gslbservice:groups:members:  
public_ip> save : gslbservice:groups:members> save : gslbservice:groups> save : gslbservice> save ... members[1] ip 10.10.10.1  
ratio 1 enabled True public_ip ip 2.2.2.2{% endcli %}
```

Recommended Reading

- [Extension Mechanisms for DNS Client Subnet Option Insertion](#)