Cloud Load Balance

Backend CVMs

Product Introduction

©2013-2018 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2018 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

©2013-2018 Tencent Cloud. All rights reserved.

Backend CVMs

Access Control of Back-end CVMs

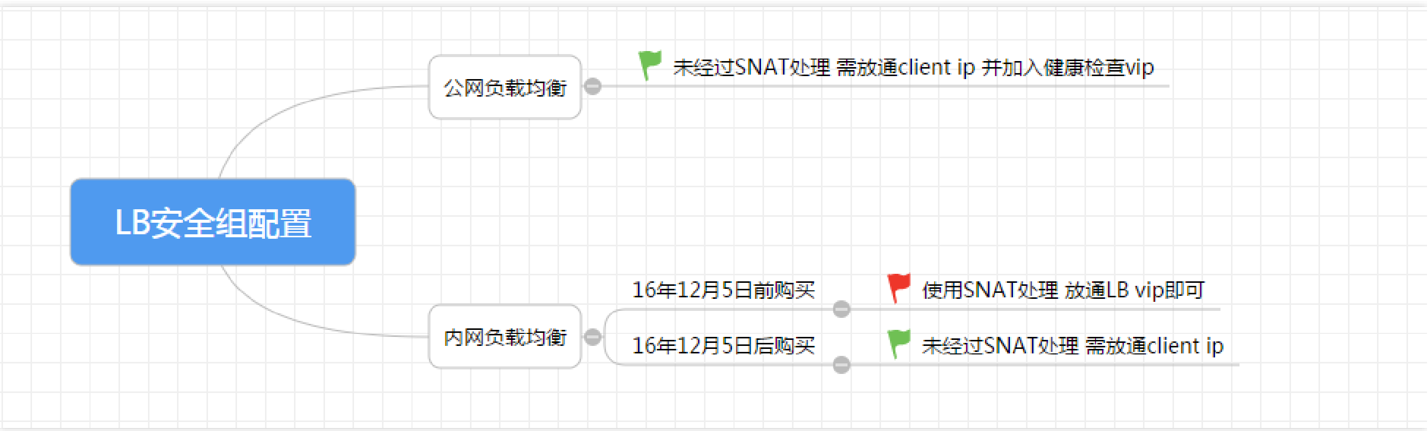
Last updated：2018-08-23 16:12:09

As with all CVMs, the access to the backend server instances of a load balancer can be controlled via a security group, which acts as a firewall. You can associate one or more security groups with a backend CVM and add one or more rules to each security group to control traffic to different servers. You can modify the rules for a security group at any time, and the new rule is automatically applied to all instances associated with that security group. For more information, please see Security Group Product Documentation. In the VPC environment, you can also use Network ACL for access control.

You can use a security group to allow the backend instances to receive traffic only from the load balancer or from other sources. Please note that, you must ensure that the security group of the instance allows the load balancer to communicate with the backend instance on the corresponding listener port and health check port. In VPC, your security groups and network ACLs must allow traffic to flow in both directions on these ports.

Recommended Rules for LB Security Group

The configuration of LB security group is as follows:


LB安全组配置
公网负载均衡
未经过SNAT处理 需放通client ip 并加入健康检查vip
内网负载均衡
16年12月5日前购买
使用SNAT处理 放通LB vip即可
16年12月5日后购买
未经过SNAT处理 需放通client ip

Type	SNAT Processing	Health Check Traffic	Recommended Security Group Configuration	Note

©2013-2018 Tencent Cloud. All rights reserved.

Type	SNAT Processing	Health Check Traffic	Recommended Security Group Configuration	Note
Public Network-based LB	No	Initiated via LB vip	If you want to specify a static access IP, both client IP and LB vip need to be open to internet. If not, it is recommended that all IPs of the backend server port are open to internet, i.e. 0.0.0.0/0.	Applicable to both basic network and VPC
Private Network-based LB (purchased prior to December 5, 2016)	Yes	Health check IP is open to internet by default.	Since the client IP is processed via SNAT, LB vip needs to be open to internet.	Applicable to both basic network and VPC
Private Network-based LB (purchased prior to December 5, 2016)	No	Health check IP is open to internet by default.	The LB can be accessed once the health check IP is open to internet.	Applicable to both basic network and VPC

Application scenario 1:

If the public network-based load balancer listener is configured with TCP: port 80 and backend server port: 8080, and only client IPs (clientA IP and clientB IP) are allowed to access the load balancer, configure the security group rules of the backend server as follows:

```
clientA ip+8080 allow
clientB ip+8080 allow
LB vip +8080 allow
0.0.0.0/0 +8080 drop
```

Application scenario 2:

If the public network-based LB listener is configured with HTTP: port 80 and backend server port: 8080, and all client IPs are allowed to access the LB, configure the security group rules of the backend server as follows:

```
0.0.0.0/0 +8080 allow
```

©2013-2018 Tencent Cloud. All rights reserved.

Application scenario 3:

The private network-based LB (purchased after December 5, 2016) is configured with TCP: port 80 and backend server port: 8080 in the VPC. Only client IPs (clientA IP and clientB IP) are allowed to access the LB vip. Client IPs are only allowed to access the backend CVMs bound to the LB.

a. Configure the security group of the backend server as follows:

```
clientA ip+8080 allow
clientB ip+8080 allow
0.0.0.0/0 +8080 drop
```

b. Configure the security group of the client server as follows:

```
LB vip+8080 allow
0.0.0.0/0 + 8080 drop
```

Application scenario 4: Blacklist

If you need to set a blacklist for some client IPs to deny their accesses, you can configure the security group associated with the cloud services. Configure the security group rules as follows:

- Add the client IPs from which access needs to be rejected plus ports to the security group, and choose **Reject the access from the IPs** in the Policy section.
- When the setting is made, add another security group rule that allows all accesses to the port from all IPs by default.

  When the configuration is completed, the security group rules are as follows:

  ```
  clientA ip+port drop
  clientB ip+port drop
  0.0.0.0/0+port accept
  ```

  Notes:

  The above configuration steps should be performed ***in a correct order***, otherwise the blacklist configuration cannot take effect.

  Security groups are stateful. Therefore, the above configurations are used for ***inbound rules***, and outbound rules do not need special configuration.

Manage Backend Server Security Groups via Console

1) Log in to CLB Console and click the load balancer instance ID to go to the load balancer details page.

2) In the **Backend Server** tab, click the corresponding backend server ID to go to the CVM details page.

©2013-2018 Tencent Cloud. All rights reserved.

3) Click the **Security Group** tab, and click the **Edit** button under **Security Groups Joined** to edit the associated security group. Click **Configure Security Group** to add a new security group for association.

Managing Backend Server Security Groups via API

Please see ModifySecurityGroupsOfInstance API and ModifySecurityGroupPolicy API.

©2013-2018 Tencent Cloud. All rights reserved.