Aegis Anti-DDoS

Getting Started

Product Introduction

Service Statement

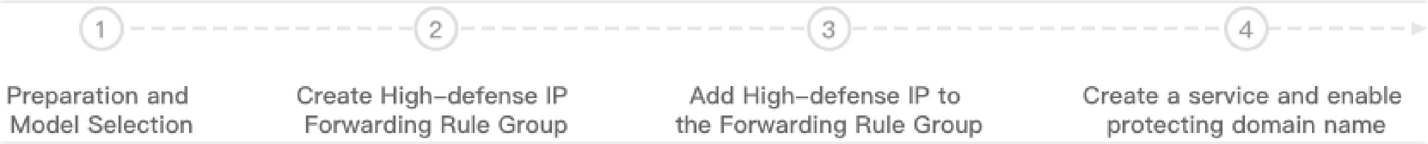
This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable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

Contents

Getting Started
DDoS High-defense IP

Last updated：2018-09-12 16:02:05

Below is the flow chart of Tencent Cloud Aegis Anti-DDoS high-defense IP protection:


1
Preparation and Model Selection
2
Create High-defense IP Forwarding Rule Group
3
Add High-defense IP to the Forwarding Rule Group
4
Create a service and enable protecting domain name

I. Preparation and Selection

1. Sign up for a Tencent Cloud account
   New user needs to **sign up** at Tencent Cloud's official website and purchase Aegis Anti-DDoS. For more information, see Signing up with Tencent Cloud and Purchase Guide for Aegis Anti-DDoS.
2. Confirm high-defense IP region and network
   - Region selection principle
     DDoS high-defense IP work in proxy forwarding mode. Therefore, please try to select a region near the physical location of your origin server. The closer the high-defense IP region is to the origin server, the lower the access latency and the higher the access speed.
   - Network selection principle
     When selecting the network, take into account the region and the needs for peak bandwidth for protection. BGP network provides a better network experience, but its highest peak bandwidth for protection is lower than that of MUT high-defense IP. The maximum peak bandwidth for protection of MUT high-defense IP decreases in sequence of China Telecom, China Unicom and China Mobile. Please select the corresponding ISP based on your end user distribution and try to avoid cross-network access.
3. Confirm the configuration plan for high-defense IP
   - Peak bandwidth for base protection
     Peak bandwidth for base protection is prepaid. It is suggested that the peak bandwidth for base protection be set to higher than the average historical attack traffic. This makes sure base protection is robust enough to prevent most attacks.
   - Peak bandwidth for elastic protection
     Peak bandwidth for elastic protection is postpaid on a daily basis. It is suggested that the peak bandwidth for elastic protection be set to higher than the highest historical attack traffic. This makes

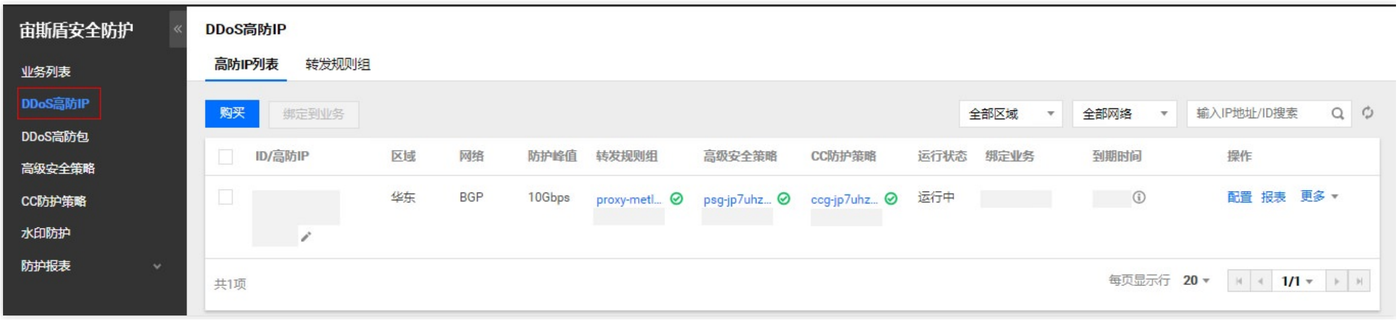
sure potential IP blocking is avoided in case of large-traffic attacks. Meanwhile, elastic protection is pay-per-use and you only pay for what you use, significantly reducing the protection costs.

- Forwarded business traffic
  This is the non-attacking traffic of normal business requests forwarded to the origin server. It can be charged by bandwidth or by traffic. It is recommended to select based on the characteristics of normal business traffic.

II. Creating High-defense IP Forwarding Rule Group

After purchasing high-defense IP, you can view the assigned resources on the DDoS high-defense IP management page. DDoS high-defense IP provides protection service in proxy forwarding mode.
This section describes how to configure forwarding rule group and forwarding rule:

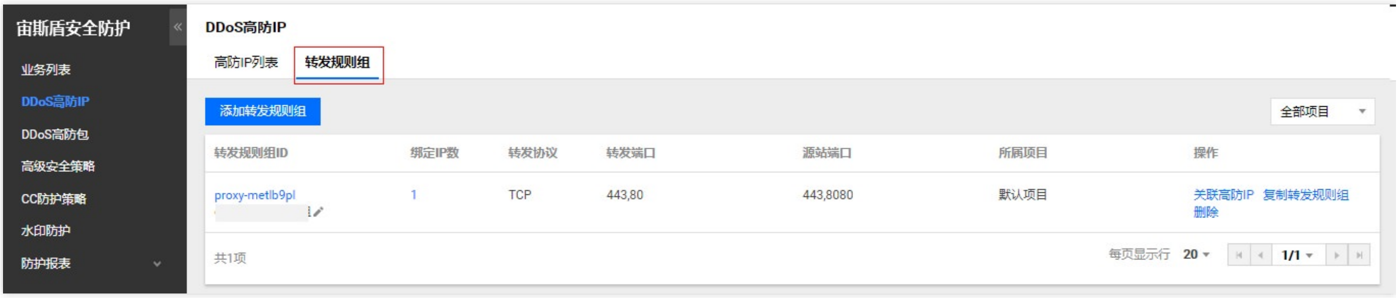
1. In Aegis Anti-DDoS Console, select **DDoS high-defense IP** to enter the DDoS high-defense IP management page;



□	ID/高防IP	区域	网络	防护峰值	转发规则组	高级安全策略	CC防护策略	运行状态	绑定业务	到期时间	操作
□		华东	BGP	10Gbps	proxy-metl... ✓	psg-jp7uhz... ✓	ccg-jp7uhz... ✓	运行中			配置 报表 更多

共1项 每页显示行 20 1/1

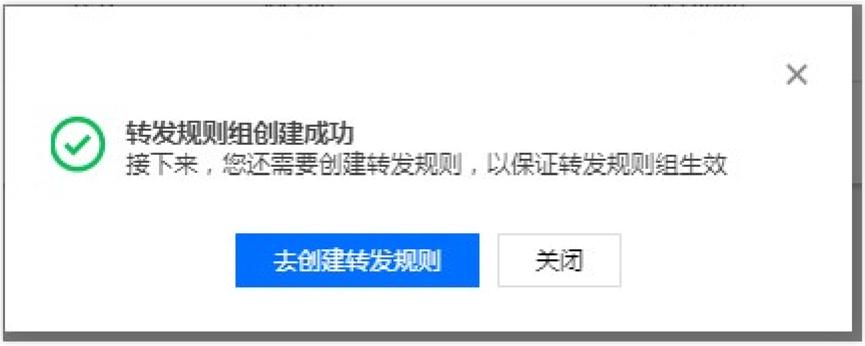
2. Click **Forwarding rule group** on the top of the page to enter the forwarding rule group management page.

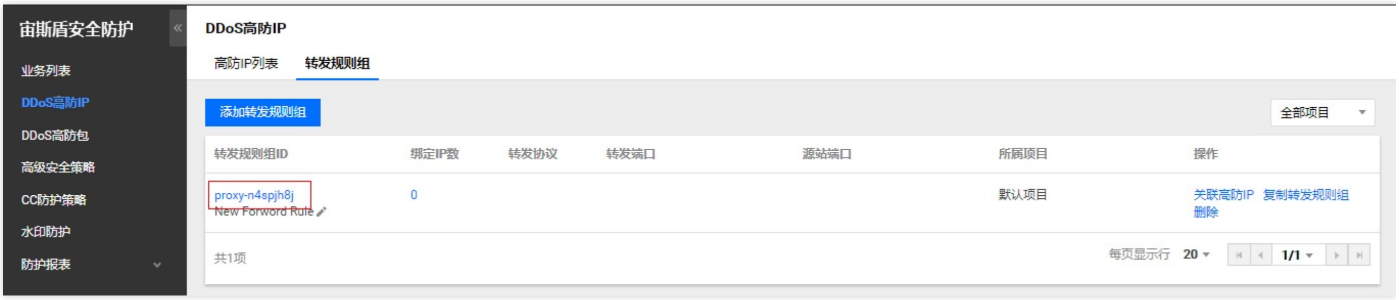


转发规则组ID	绑定IP数	转发协议	转发端口	源站端口	所属项目	操作
proxy-metlb9pl	1	TCP	443,80	443,8080	默认项目	关联高防IP 复制转发规则组 删除

共1项 每页显示行 20 1/1

3. Click **Add a forwarding rule group** on the page and enter the rule group name and linked project name. After creating the rule group, you can directly select **Create a forwarding rule** or click the forwarding rule group ID in the rule group list to enter the details page to create a forwarding rule.

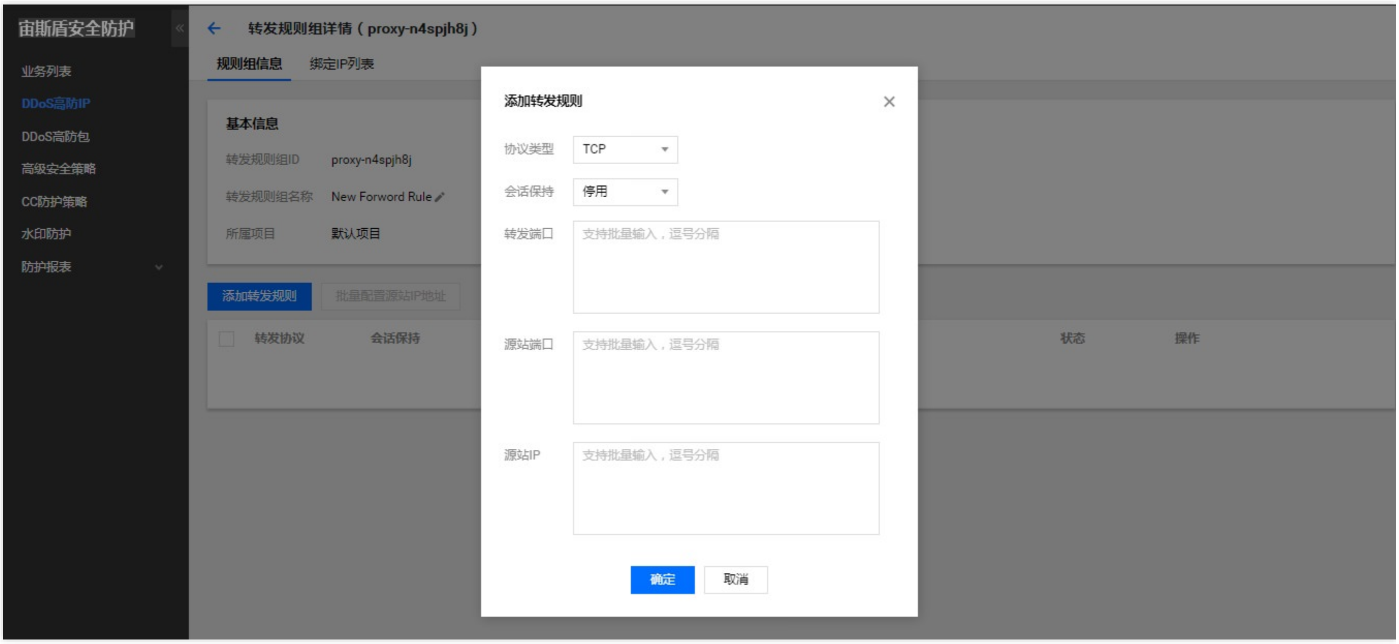

转发规则组创建成功
接下来，您还需要创建转发规则，以保证转发规则组生效



转发规则组ID	绑定IP数	转发协议	转发端口	源站端口	所属项目	操作
proxy-n4spjh8j New Forword Rule	0				默认项目	关联高防IP 复制转发规则组 删除

共1项 每页显示行 20 1/1

4. On the rule group details page, click **Add a forwarding rule**, choose the protocol type and session hold, enter the forwarding port, origin server port and origin server IP address, and then click **OK** to complete forwarding rule creation.
Forwarding ports and origin server ports can be entered in batch where these ports correspond one-to-one in sequence, so you can batch create multiple rules.



基本信息

转发规则组ID proxy-n4spjh8j

转发规则组名称 New Forword Rule

所屬项目 默认项目

添加转发规则

协议类型 TCP

会话保持 停用

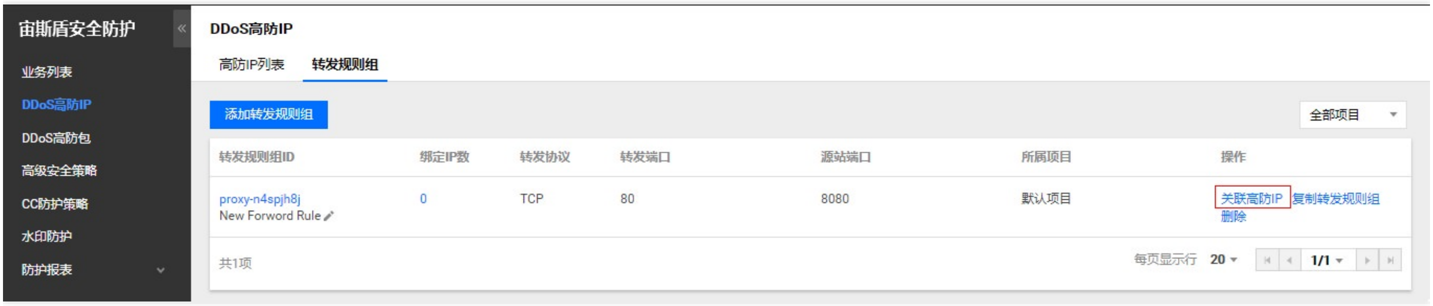
转发端口 支持批量输入，逗号分隔

源站端口 支持批量输入，逗号分隔

源站IP 支持批量输入，逗号分隔

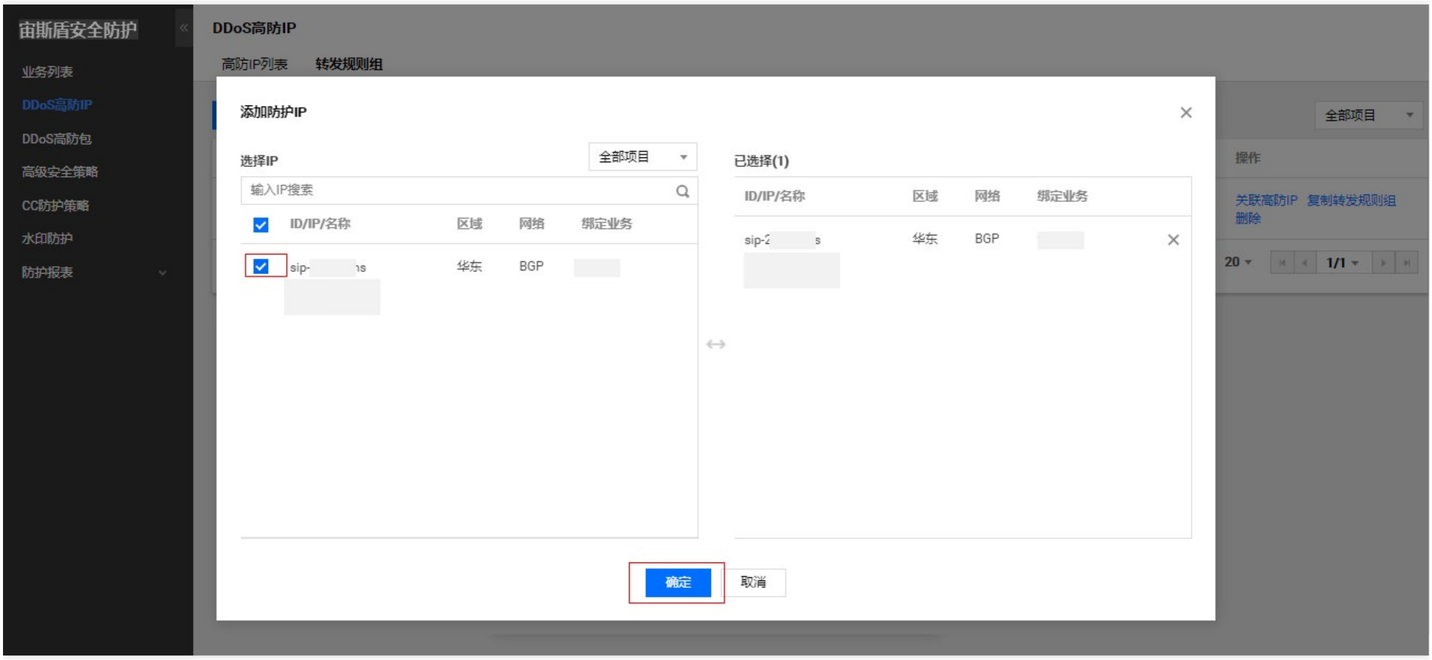
III. Binding Forwarding Rule Group to High-defense IP

After the forwarding rule group and forwarding rule are created, you need to bind them to high-defense IP in the Action column.
Click **Bind to high-defense IP** in the column to enter the protected IP interface, select the high-defense IP to bind and click **OK** to complete binding.



转发规则组ID	绑定IP数	转发协议	转发端口	源站端口	所属项目	操作
proxy-n4spjh8j New Forword Rule	0	TCP	80	8080	默认项目	关联高防IP 复制转发规则组 删除

共1项　每页显示行 20　1/1



添加防护IP

选择IP　全部项目

输入IP搜索

☑	ID/IP/名称	区域	网络	绑定业务
☑	sip-[redacted]s [redacted]	华东	BGP	[redacted]

已选择(1)

ID/IP/名称	区域	网络	绑定业务
sip-[redacted]s [redacted]	华东	BGP	[redacted]

确定　取消

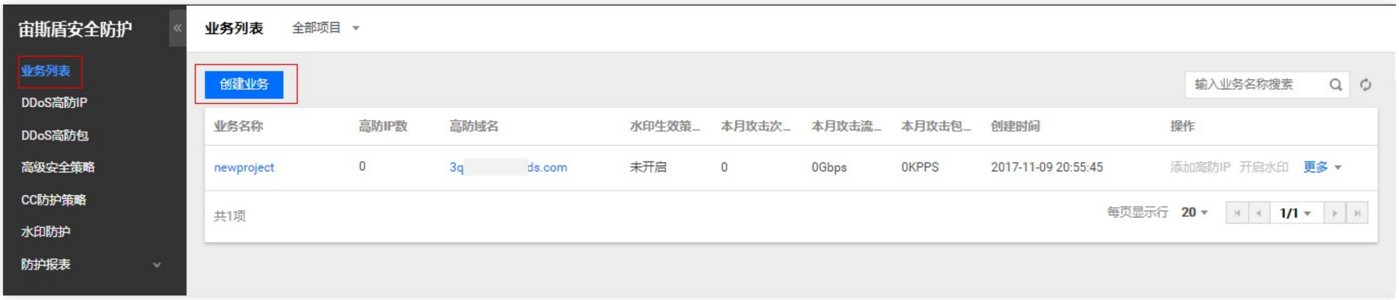
After completing the configuration described above, your origin server is protected by high-defense IP. Verify end-to-end connectivity and then point the business requests to the high-defense IP to get protection from Aegis Anti-DDoS.

IV. Creating Business and Enabling Protective Domain Name (Optional)

If your business supports access via domain name, you can also configure the CNAME set at your primary domain name's DNS provider to the free protective domain name, add high-defense IP to the business, and then enable domain name resolution to intelligently resolve end user's source IP to the high-defense IP.

Relevant configurations are described below:

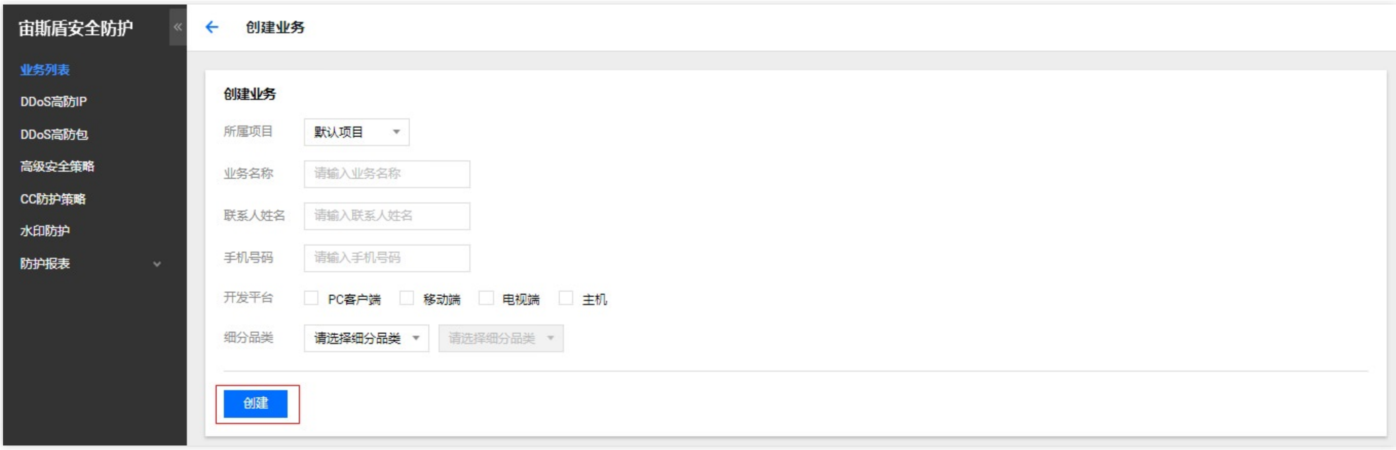
1. In Aegis Anti-DDoS Console, select **Business list** on the left to enter the business management page and click **Create a business**;



业务名称	高防IP数	高防域名	水印生效策_	本月攻击次_	本月攻击流_	本月攻击包_	创建时间	操作
newproject	0	3q ds.com	未开启	0	0Gbps	0KPPS	2017-11-09 20:55:45	添加高防IP 开启水印 更多

共1项 每页显示行 20 1/1

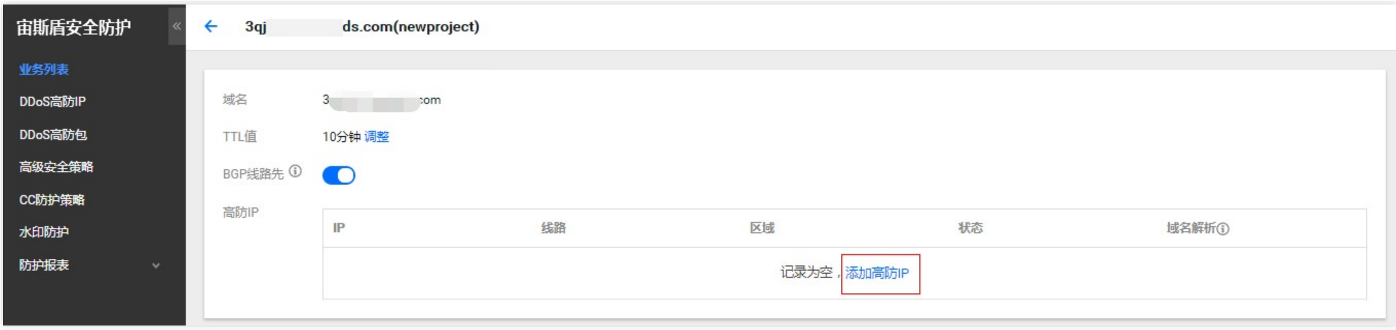
2. Choose the linked project, enter the business name, contact and mobile number, and choose the development platform and business category. Click **Create** to complete;



创建业务

所属项目	默认项目
业务名称	请输入业务名称
联系人姓名	请输入联系人姓名
手机号码	请输入手机号码
开发平台	□ PC客户端 □ 移动端 □ 电视端 □ 主机
细分品类	请选择细分品类 请选择细分品类

3. After creating the business, click Protective domain name in the business list to enter the domain name management page and click **Add a high-defense IP**;

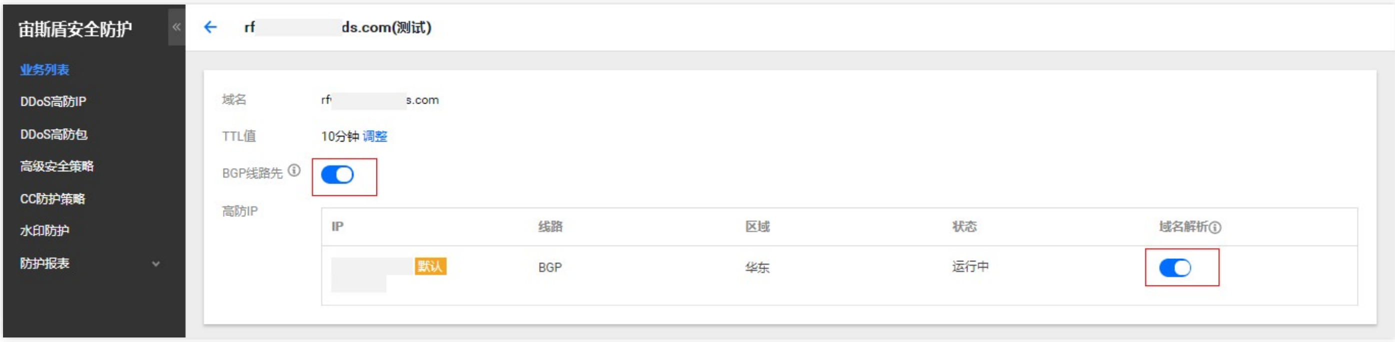


3qj ds.com(newproject)

域名	3 com
TTL值	10分钟 调整
BGP线路先 ⓘ	●
高防IP	

IP	线路	区域	状态	域名解析ⓘ
记录为空，添加高防IP				

4. Choose the high-defense IP to be used for the business and enable Name resolution.



rf ds.com(测试)

域名 rf s.com

TTL值 10分钟 调整

BGP线路先 ⓘ ●

高防IP

IP	线路	区域	状态	域名解析ⓘ
默认	BGP	华东	运行中	●

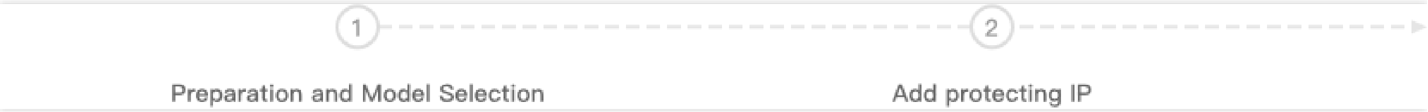
After the aforementioned configurations are completed, domain name resolution takes effect. Then, configure the CNAME resolution to the protective domain name at the primary domain name service provider to enable domain name access.

DDoS High-defense Packet

Last updated：2018-09-12 16:03:28

Getting Started with DDoS High-defense Packet

Below is the flow chart of Tencent Cloud Aegis Anti-DDoS high-defense packet:



I. Preparation and Selection

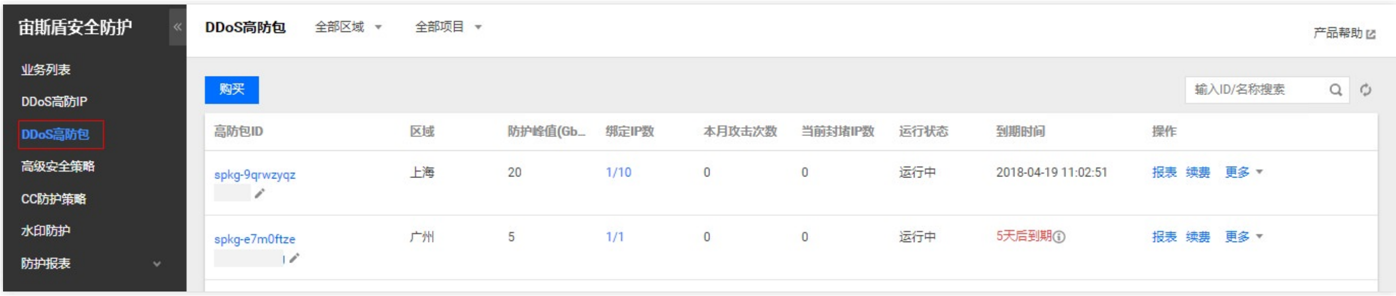
1. Sign up for a Tencent Cloud account
   New user needs to **sign up** at Tencent Cloud's official website and purchase Aegis Anti-DDoS. For more information, see Signing up with Tencent Cloud and Purchase Guide for Aegis Anti-DDoS.
2. Confirm the region for high-defense packet
   - Region selection principle
     DDoS high-defense packet can only provide high-defense protection for Tencent Cloud public IPs in the same region where it is available. Therefore, please be sure to select the packet available in the region where your Tencent Cloud origin server is located.
3. Confirm the configuration plan for high-defense IP
   - Protection scope
     You can choose single-IP or multi-IP mode. In single-IP mode, high-defense packet can be bound to one Tencent Cloud public IP which utilizes the peak bandwidth for protection exclusively. In multi-IP mode, high-defense packet can be bound to multiple Tencent Cloud public IPs which share the resources. When multiple IPs are under DDoS attacks, if the peak bandwidth of the combined attack traffic is higher than the peak bandwidth for protection, blocking will start from the IP address suffering the largest attack traffic.
   - Peak bandwidth for base protection
     Peak bandwidth for base protection is prepaid. It is suggested that the peak bandwidth for base protection be set to higher than the average historical attack traffic. This makes sure base protection is robust enough to prevent most attacks.

- Peak bandwidth for elastic protection
  Peak bandwidth for elastic protection is postpaid on a daily basis. It is suggested that the peak bandwidth for elastic protection be set to higher than the highest historical attack traffic. This makes sure potential IP blocking is avoided in case of large-traffic attacks. Meanwhile, elastic protection is pay-per-use and you only pay for what you use, significantly reducing the protection costs.

II. Adding Protected IP

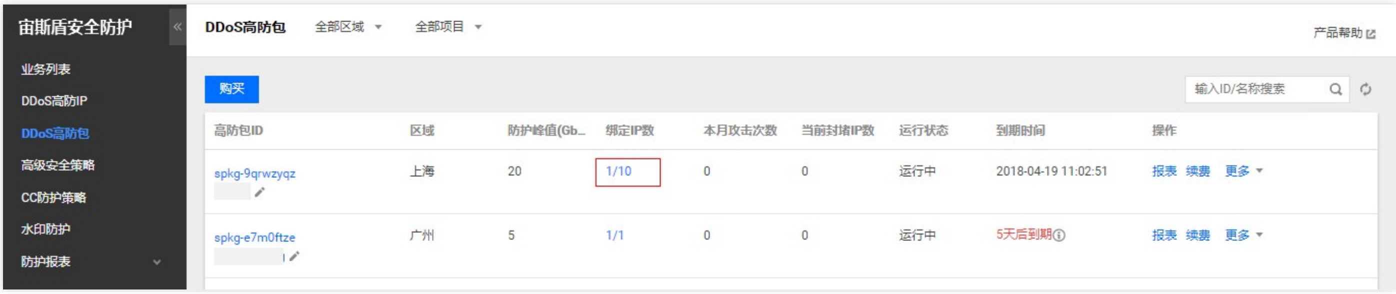
After purchasing high-defense packet, you can view the assigned resources on the DDoS high-defense packet management page. DDoS high-defense packet provides direct DDoS protection capabilities to Tencent Cloud public IP addresses.
This section describes how to add IPs.

1. In Aegis Anti-DDoS Console, select **DDoS high-defense packet** on the left to enter the DDoS high-defense packet management page;



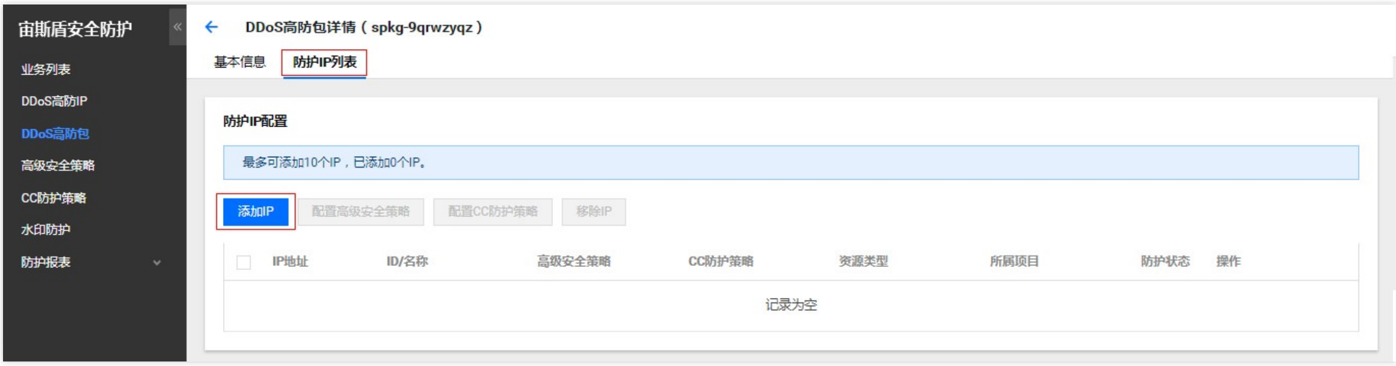
高防包ID	区域	防护峰值(Gb...	绑定IP数	本月攻击次数	当前封堵IP数	运行状态	到期时间	操作
spkg-9qrwzyqz	上海	20	1/10	0	0	运行中	2018-04-19 11:02:51	报表 续费 更多
spkg-e7m0ftze	广州	5	1/1	0	0	运行中	5天后到期	报表 续费 更多

2. In the high-defense packet list, click the number of IPs in the **Number of bound IPs** column to enter the protected IP list;



高防包ID	区域	防护峰值(Gb...	绑定IP数	本月攻击次数	当前封堵IP数	运行状态	到期时间	操作
spkg-9qrwzyqz	上海	20	1/10	0	0	运行中	2018-04-19 11:02:51	报表 续费 更多
spkg-e7m0ftze	广州	5	1/1	0	0	运行中	5天后到期	报表 续费 更多

3. In the protected IP list, click **Add an IP** and choose the IP address to be added to the high-defense packet for protection;

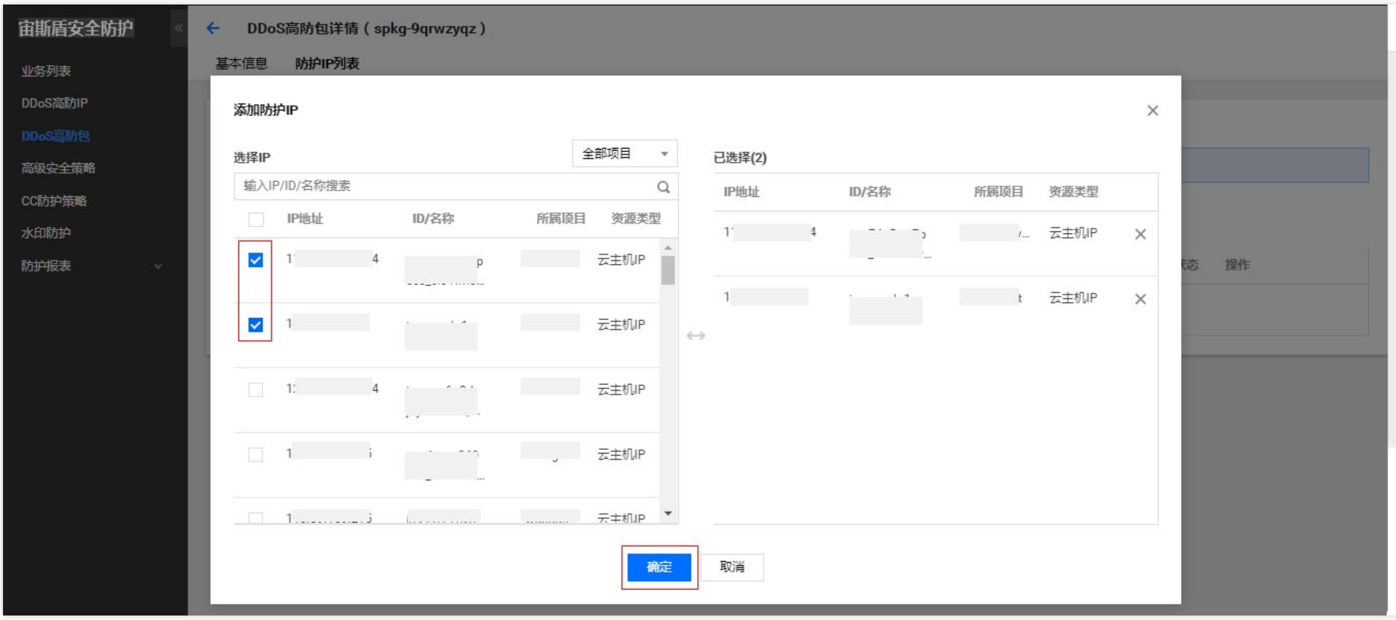


DDoS高防包详情（spkg-9qrwzyqz）

防护IP配置

最多可添加10个IP，已添加0个IP。

□	IP地址	ID/名称	高级安全策略	CC防护策略	资源类型	所属项目	防护状态	操作
记录为空								



DDoS高防包详情（spkg-9qrwzyqz）

添加防护IP

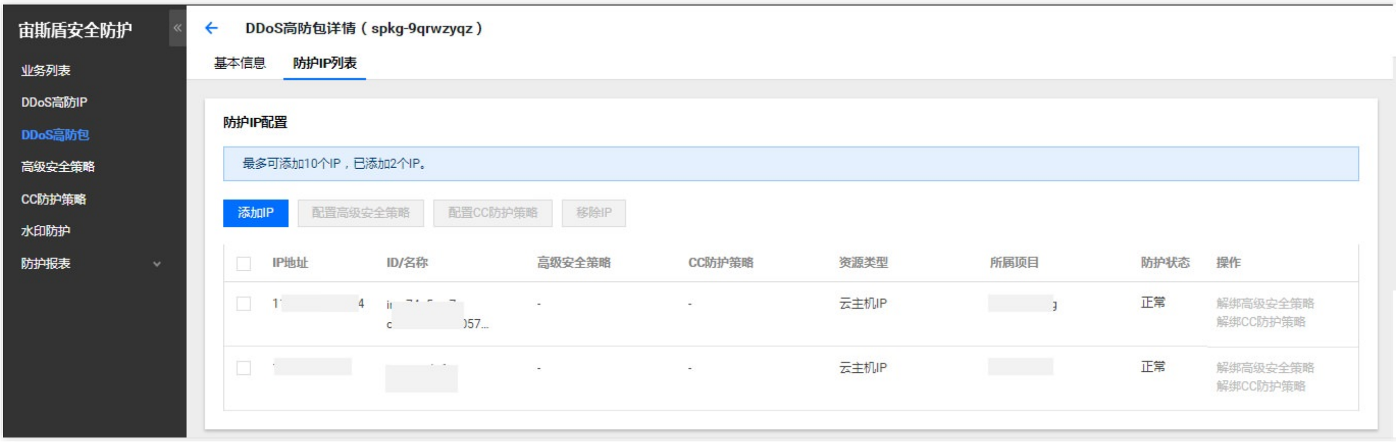
选择IP

□	IP地址	ID/名称	所属项目	资源类型
☑	[redacted]	[redacted]	[redacted]	云主机IP
☑	[redacted]	[redacted]	[redacted]	云主机IP
□	[redacted]	[redacted]	[redacted]	云主机IP
□	[redacted]	[redacted]	[redacted]	云主机IP
□	[redacted]	[redacted]	[redacted]	云主机IP

已选择(2)

IP地址	ID/名称	所属项目	资源类型	
[redacted]	[redacted]	[redacted]	云主机IP	×
[redacted]	[redacted]	[redacted]	云主机IP	×

4. After added, the IP address will be protected by Aegis Anti-DDoS.



DDoS高防包详情（spkg-9qrwzyqz）

防护IP配置

最多可添加10个IP，已添加2个IP。

□	IP地址	ID/名称	高级安全策略	CC防护策略	资源类型	所属项目	防护状态	操作
□	[redacted]	[redacted]	-	-	云主机IP	[redacted]	正常	解绑高级安全策略 解绑CC防护策略
□	[redacted]	[redacted]	-	-	云主机IP	[redacted]	正常	解绑高级安全策略 解绑CC防护策略