

Aegis Anti-DDoS

Operations Guide

Product Documentation



Copyright Notice

©2013-2019 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



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

Operations Guide

Enabling Watermark Protection

Obtaining Client IP Address Using the TOA Scheme

Configuring an Advanced HTTP Anti-CC Defense Policy

Configuring an Advanced Anti-DDoS Policy

Binding a Protected Domain Name to a Protective IP

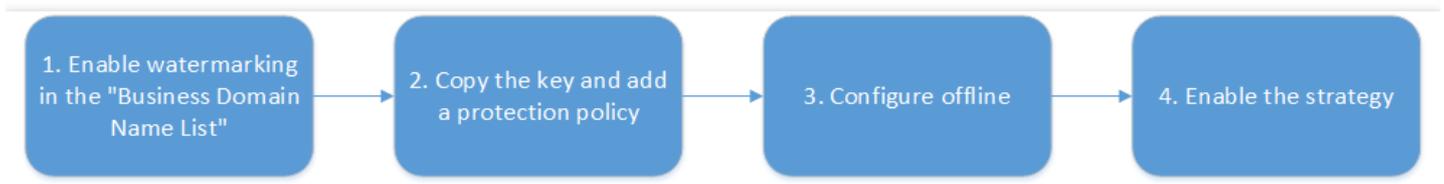
Operations Guide

Enabling Watermark Protection

Last updated : 2020-07-30 11:35:56

You can efficiently and comprehensively protect against layer 4 CC attacks such as masquerading and replay attacks by accessing watermark protection. By sharing the watermark algorithm and key between the business side and the Aegis protection system, watermark protection embeds a watermark in every message sent by the client. As the attack messages have no watermark, the protection system can easily identify and discard them. For more information on the configuration, see [Custom Advanced Security Policy](#).

Flowchart



How to Enable

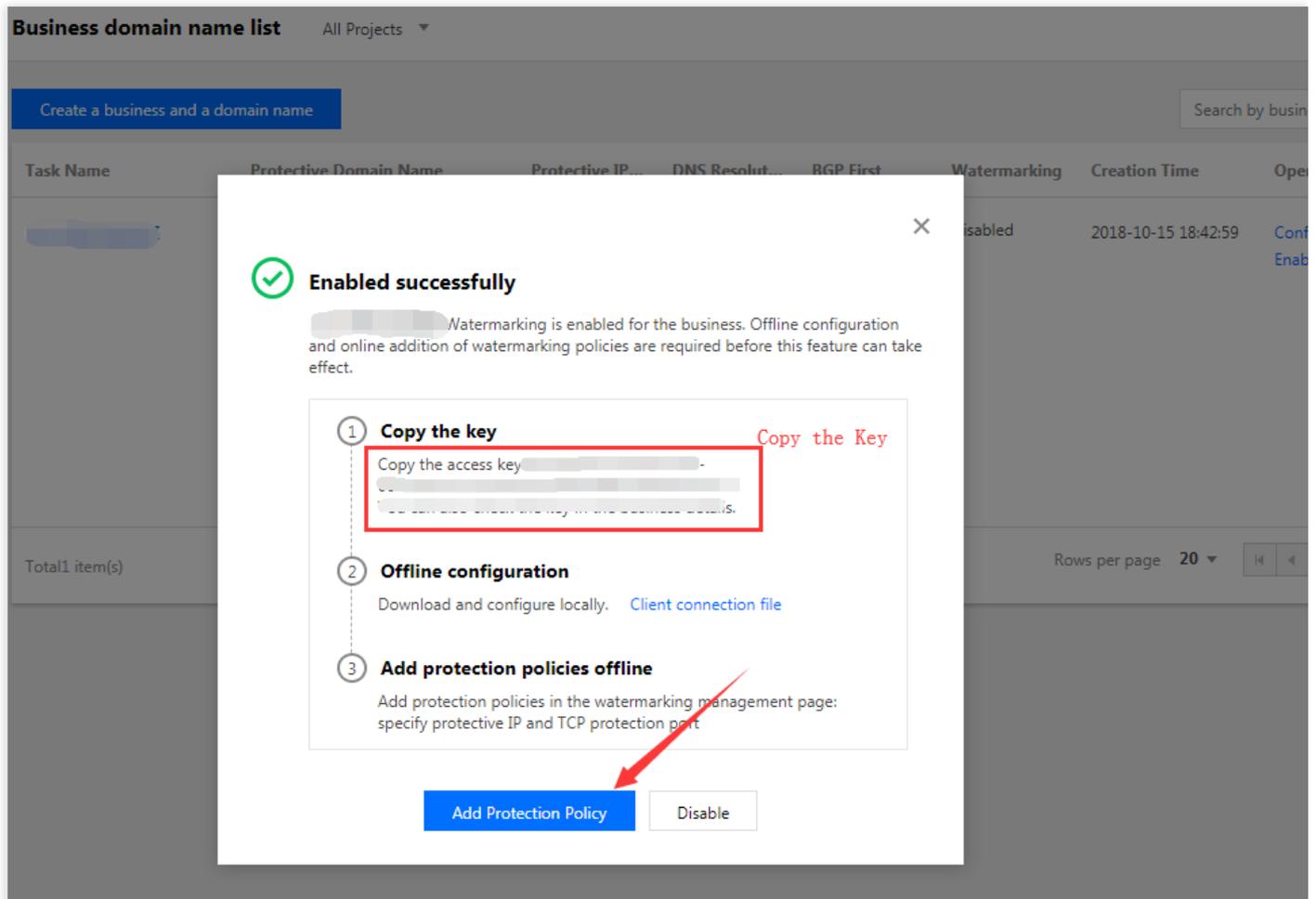
1. Enable watermarking in the "Business Domain Name List"

Go to the [Aegis Anti-DDoS Console](#), click **Business Domain Name List*** in the left pane, and click ****Enable watermark**.

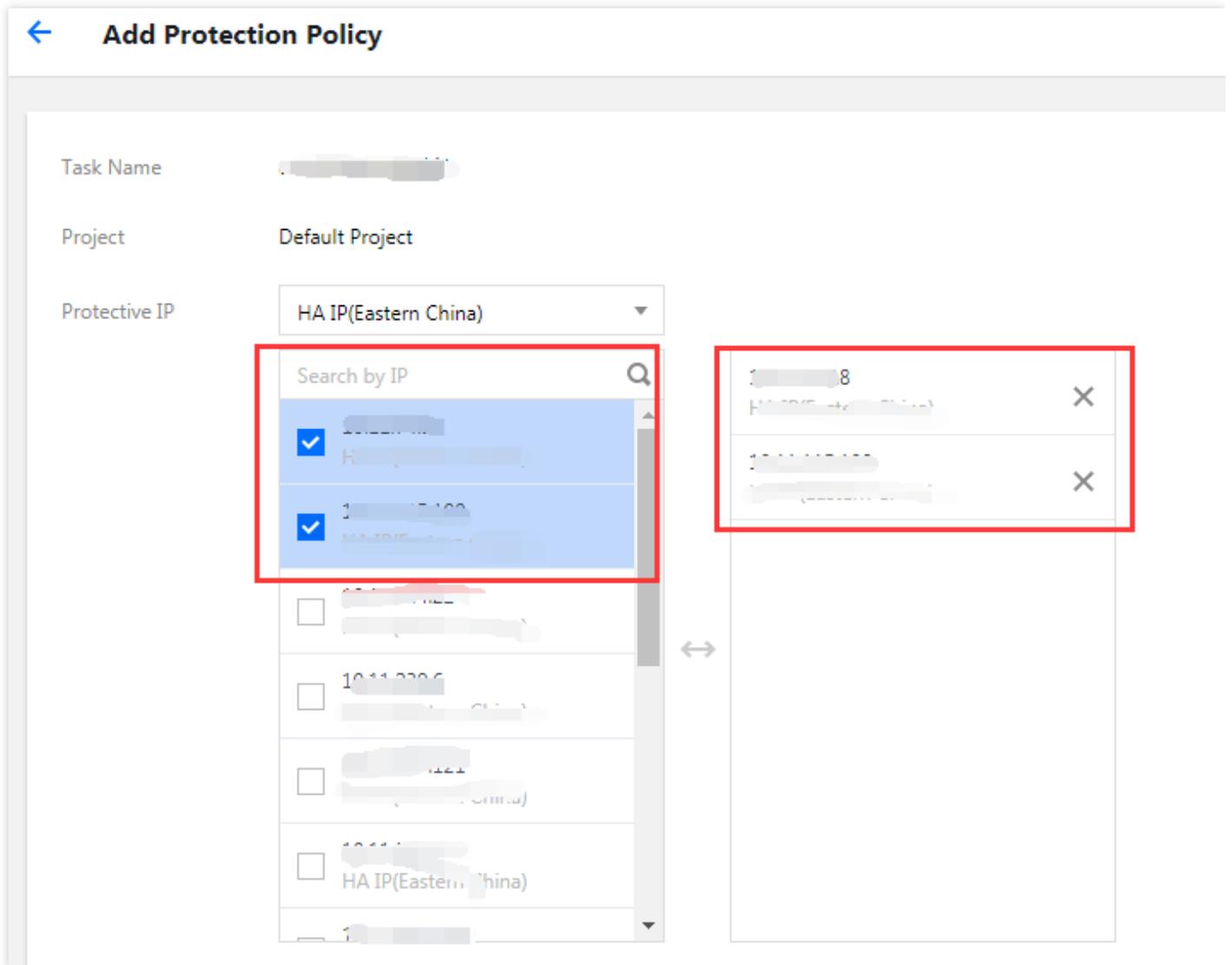
Task Name	Protective Domain Name	Protective IP R...	DNS Resolution...	BGP First	Watermarking	Creation Time	Operation
		BGP(1) China Telecom(1) China Unicom(1) China Mobile(1) Oversea(0)		Enabled	Disabled	2018-10-15 18:42:59	Configuration Delete Enable watermarking

2. Copy the key

a. After watermarking is successfully enabled, select "Copy the key" in the "Enabled successfully" pop-up and click **Add Protection Policy**.



b. Go to the "Add Protection Policy" page and select "Protected IP".



c. Add the TCP protection port, UDP protection port and allowlist and then click **Confirm to add**.

TCP Protection Port

Port ID		Oper...
80 - 80	-	Delete
Add Port		

A TCP protection port can be configured with at most 5 port segments. Different port segments cannot overlap each other. At least one of the TCP or UDP port segments should be configured.

UDP Protection Port

Port ID		Oper...
443 - 443	-	Delete
Add Port		

A UDP protection port can be configured with at most 5 port segments. Different port segments cannot overlap each other. At least one of the TCP or UDP port segments should be configured.

UDP De-Watermarking

Auto de-watermarking of UDP packet

When a data packet passes through the security protection system, the UDP packet is automatically de-watermarked.

Offset

Specify the offset of watermark label in UDP packets. Value range: 0-100.

Whitelist

Enable Source IP Whitelist

The packets sent from an IP in the whitelist to a protective IP do not go through watermark detection.

Enter an IP address. Multiple IP addresses are separated with commas, and a maximum of 20 IP addresses are allowed.

[Confirm to add](#)

3. Offline configuration

In the "Enabled successfully" pop-up, click **Client connection file** to download the file for connecting the client and the server.

4. Enable the policy

a. After the policy is created successfully, under **Watermark Protection**, click **Add Policy** to modify it and then click **Enable policy**.

Watermark Protection All Projects ▾

Search by IP address/port 🔍 ↻

Task Name	Protective IP	TCP Protection Port	UDP Protection Port	Protection Status	Access time	Operation
				Creating...	2018/10/23 14:12:21	Policy Details enable Delete Add Policy

Total 1 item(s) Rows per page 20 ▾ 1/1

b. Wait a few seconds before the protection status is changed to "protective effect", and watermarking is successfully enabled.

Watermark Protection All Projects ▾

Search by IP address/port 🔍 ↻

Task Name	Protective IP	TCP Protection Port	UDP Protection Port	Protection Status	Access time	Operation
				protective effect	2018/10/23 14:12:21	Policy Details Disable Delete Add Policy

Total 1 item(s) Rows per page 20 ▾ 1/1

Obtaining Client IP Address Using the TOA Scheme

Last updated : 2018-12-21 12:02:19

After the business request is forwarded through layer 4 of the protective IP, the source IP address that the business server sees after receiving the message is the egress IP address of the protective IP. In order to enable the server to obtain the actual IP address of the client, you can use the following TOA scheme. On the Linux server of the business service, install the corresponding TOA kernel package and reboot the server. Then the service side can obtain the actual IP address of the client.

How TOA Works

After forwarded, the data packet will undergo SNAT and DNAT at the same time, and its source and destination addresses will be modified.

In the TCP protocol, in order to pass the client IP to the server, the client's IP and port are placed in the custom tcp option field when forwarding.

```
#define TCPOPT_ADDR 200
#define TCPOLEN_ADDR 8 /* |opcode|size|ip+port| = 1 + 1 + 6 */

/*
 *insert client ip in tcp option, now only support IPV4,
 *must be 4 bytes alignment.
 */
struct ip_vs_tcpo_addr {
    __u8 opcode;
    __u8 opsize;
    __u16 port;
    __u32 addr;
};
```

The Linux kernel's state transits from `SYN_RECV` to `TCP_ESTABLISHED` after the listening socket receives the ACK packet of three-way handshake. At this point, the kernel will call the `tcp_v4_syn_recv_sock` function. The Hook function `tcp_v4_syn_recv_sock_toa` first calls the original `tcp_v4_syn_recv_sock` function, then calls the `get_toa_data` function to extract the TOA OPTION from the TCP OPTION and stores it in the `sk_user_data` field.

Then, `inet_getname_toa` hook `inet_getname` is used. When getting the source IP address and port, the original `inet_getname` function is called first, and then it is judged whether `sk_user_data` is empty. If data is present there, the real IP and port are extracted from it to replace the return of `inet_getname`.

The client program calls `getpeername` in user mode, and the returned IP and port are the client's original IP.

Kernel Package Installation Steps

CentOS 6.x/7.x

Installation steps

1. Download the installation package;

- (1) [Download CentOS 6.x](#)
- (2) [Download CentOS 7.x](#)

2. Install the package file;

```
rpm -hiv kernel-2.6.32-220.23.1.el6.toa.x86_64.rpm --force
```

3. Reboot the server after the installation is completed;

```
reboot
```

4. Execute the following command to check whether the TOA module is successfully loaded;

```
lsmod | grep toa
```

5. If not, manually start it;

```
modprobe toa
```

6. Use the following command to enable automatic loading of the TOA module.

```
echo "modprobe toa" >> /etc/rc.d/rc.local
```

Ubuntu 16.04

Download the installation package:

- (1) [Download kernel package](#)
- (2) [Download kernel header package](#)

Installation steps:

```
dpkg -i linux-image-4.4.87-toa_1.0_amd64.deb
```

The header package is optional. If needed for related development, install it.

After the installation is completed, reboot the server, then execute the `lsmod | grep toa` command to check whether the TOA module is loaded, and if not, start it by executing the `modprobe toa` command.

Use the following command to enable loading of the TOA module.

```
echo "modprobe toa" >> /etc/rc.d/rc.local
```

Debian 8

- (1) [Download kernel package](#)
- (2) [Download kernel header package](#)

The installation method is the same as Ubuntu.

Please download the appropriate kernel package according to the type and version of the Linux operating system of your business server and follow the steps below. If there is no kernel package for your operating system, you can install the TOA source code by following the instructions below.

TOA Source Code Installation Guide

Source Code Installation

1. Download the source code package containing the [TOA patch](#) and click the TOA patch to download the installation package;
2. Decompress it;
3. Edit `.config` by changing `CONFIG_IPV6=M` to `CONFIG_IPV6=y` ;
4. If you need to add some custom descriptions, you can edit `Makefile`;
5. Execute `make -jn` (n is the number of threads);
6. Execute `make modules_install` ;
7. Execute `make install` ;

8. Modify `/boot/grub/menu.lst` by changing default to the newly installed kernel (the title order starts at 0);
9. Reboot and the kernel has TOA;
0. Execute `lsmod | grep toa` to check whether the TOA module is loaded, and if not, start it by executing `modprobe toa`.

Making a Kernel Package

You can make your own rpm package or use the one provided by us.

1. Install `kernel-2.6.32-220.23.1.el6.src.rpm`;

```
rpm -hiv kernel-2.6.32-220.23.1.el6.src.rpm
```

2. Generate the kernel source code directory;

```
rpmbuild -bp ~/rpmbuild/SPECS/kernel.spec
```

3. Copy the source code directory;

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/ cp -a linux-2.6.32-220.23.1.el6.x86_64/ linux-2.6.32-220.23.1.el6.x86_64_new
```

4. Apply the TOA patch to the copied source directory;

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/linux-2.6.32-220.23.1.el6.x86_64_new/  
patch -p1 < /usr/local/src/linux-2.6.32-220.23.1.el6.x86_64.rs/toa-2.6.32-220.23.1.el6.patch
```

5. Edit `.config` and copy it to the SOURCE directory;

```
sed -i 's/CONFIG_IPV6=m/CONFIG_IPV6=y/g' .config  
echo -e '\n# toa\nCONFIG_TOA=m' >> .config  
cp .config ~/rpmbuild/SOURCES/config-x86_64-generic
```

6. Delete `.config` from the original source code;

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/linux-2.6.32-220.23.1.el6.x86_64  
rm -rf .config
```

7. Generate the final patch;

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/  
diff -uNr linux-2.6.32-220.23.1.el6.x86_64 linux-2.6.32-220.23.1.el6.x86_64_new/ >  
~/rpmbuild/SOURCES/toa.patch
```

8. Edit kernel.spec;

```
vim ~/rpmbuild/SPECS/kernel.spec
```

Add the following two lines under ApplyOptionPath (you can also modify custom kernel package names such as buildid)

```
Patch999999: toa.patch
```

```
ApplyOptionalPatch toa.patch
```

9. Make an rpm package;

```
rpmbuild -bb --with baseonly --without kabichk --with firmware --without debuginfo --target=x86_64 ~/rpmbuild/SPECS/kernel.spec
```

0. Install the kernel rpm package;

```
rpm -hiv kernel-xxxx.rpm --force
```

Reboot to load the TOA module

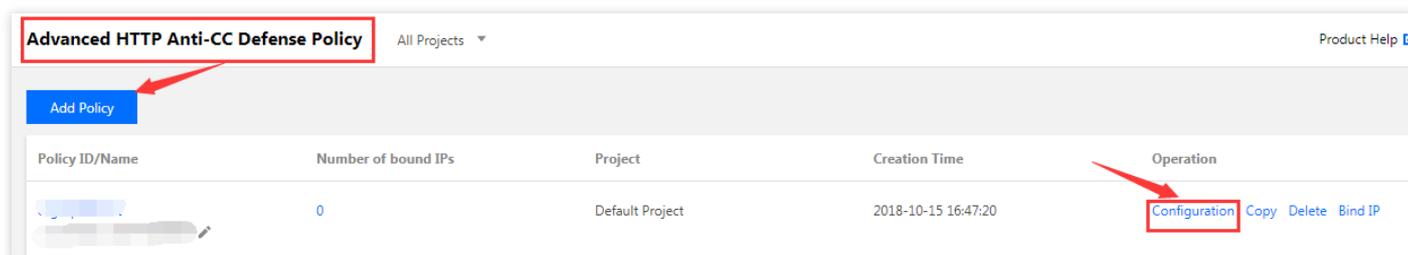
Configuring an Advanced HTTP Anti-CC Defense Policy

Last updated : 2020-07-30 11:37:44

Aegis Anti-DDoS provides advanced protection policies against HTTP CC attacks. The anti-CC defense policy triggers CC protection when the number of HTTP requests exceeds the set QPS value. For more information on the configuration, see [Custom Advanced Security Policy](#).

Adding a CC Protection Policy

1. Go to the [Aegis Anti-DDoS Console](#), click **Advanced HTTP Anti-CC Defense Policy*** in the left pane, and click ****Add Policy**. After successful addition, click **Configuration** in the "Operation" column to enter the policy configuration page.



2. Configure options such as HTTP QPS request threshold, URL allowlist, IP blocklist and allowlist and custom anti-CC defense mode based on business characteristics and protection requirements.

Click OK to finish adding the policy.

Custom Anti-CC Defense Mode Configuration

Custom Anti-CC Defense Mode Disable Enable

Matching Mode

Matching Rule	Execute	Operation
CGI Include 1 AndHost Include 1 AndUser Agent Include 1 AndReferer Include 1	Block	Edit Delete

[Add Policy](#)

Speed Limiting Mode

Global speed limit for source IP Access speed of source IP (number of access attempts/min)

Domain Name <input type="text"/>	Access speed of source IP (number of access attempts/min)	Oper...
<input type="text" value="www.qq.com"/>	<input type="text" value="10"/>	Delete
<input type="text" value="www.baidu.com"/>	<input type="text" value="10"/>	Delete

[Add Policy](#)

[OK](#) [Cancel](#)

Binding an Anti-CC Defense Policy Directly to a Protected IP

1. Click **Advanced HTTP Anti-CC Defense Policy*** in the left pane, and click a ****Policy ID**.

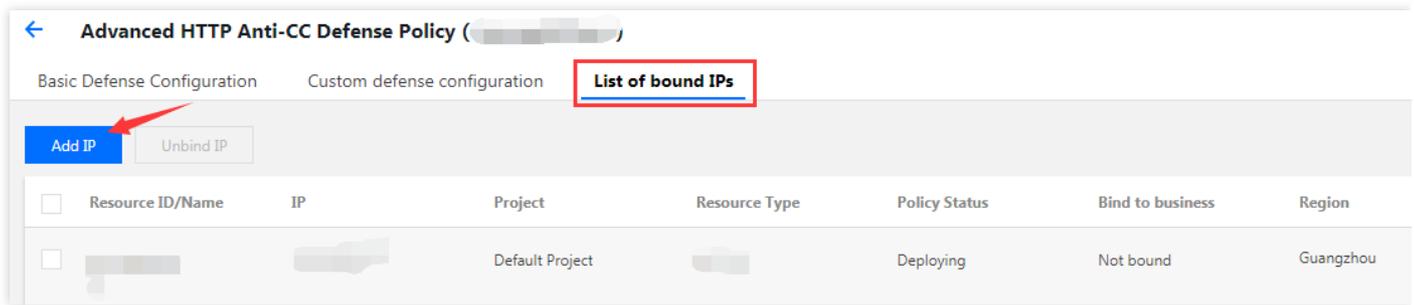
Advanced HTTP Anti-CC Defense Policy

All Projects Product Help [?](#)

[Add Policy](#)

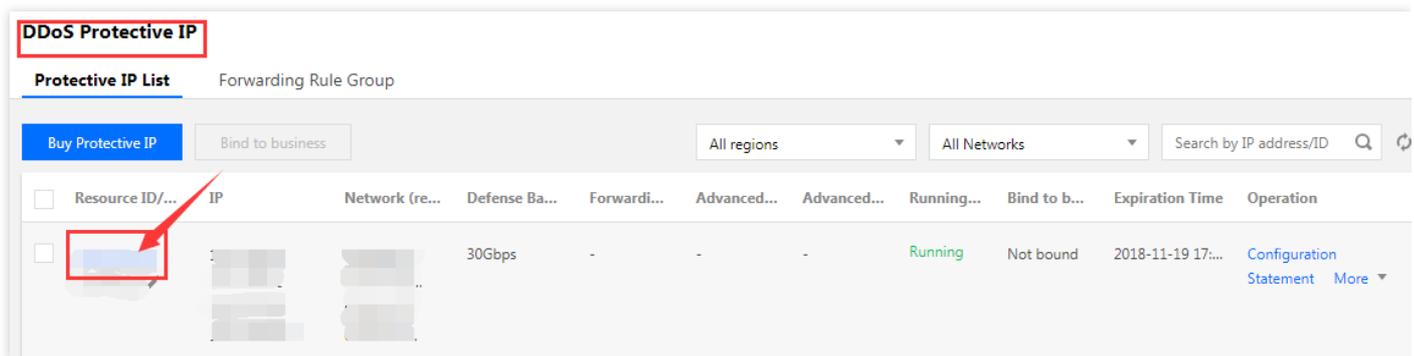
Policy ID/Name	Number of bound IPs	Project	Creation Time	Operation
 <input type="text"/>	0	Default Project	2018-10-15 16:47:20	Configuration Copy Delete Bind IP

2. Click **List of bound IPs** and click **Add IP**.

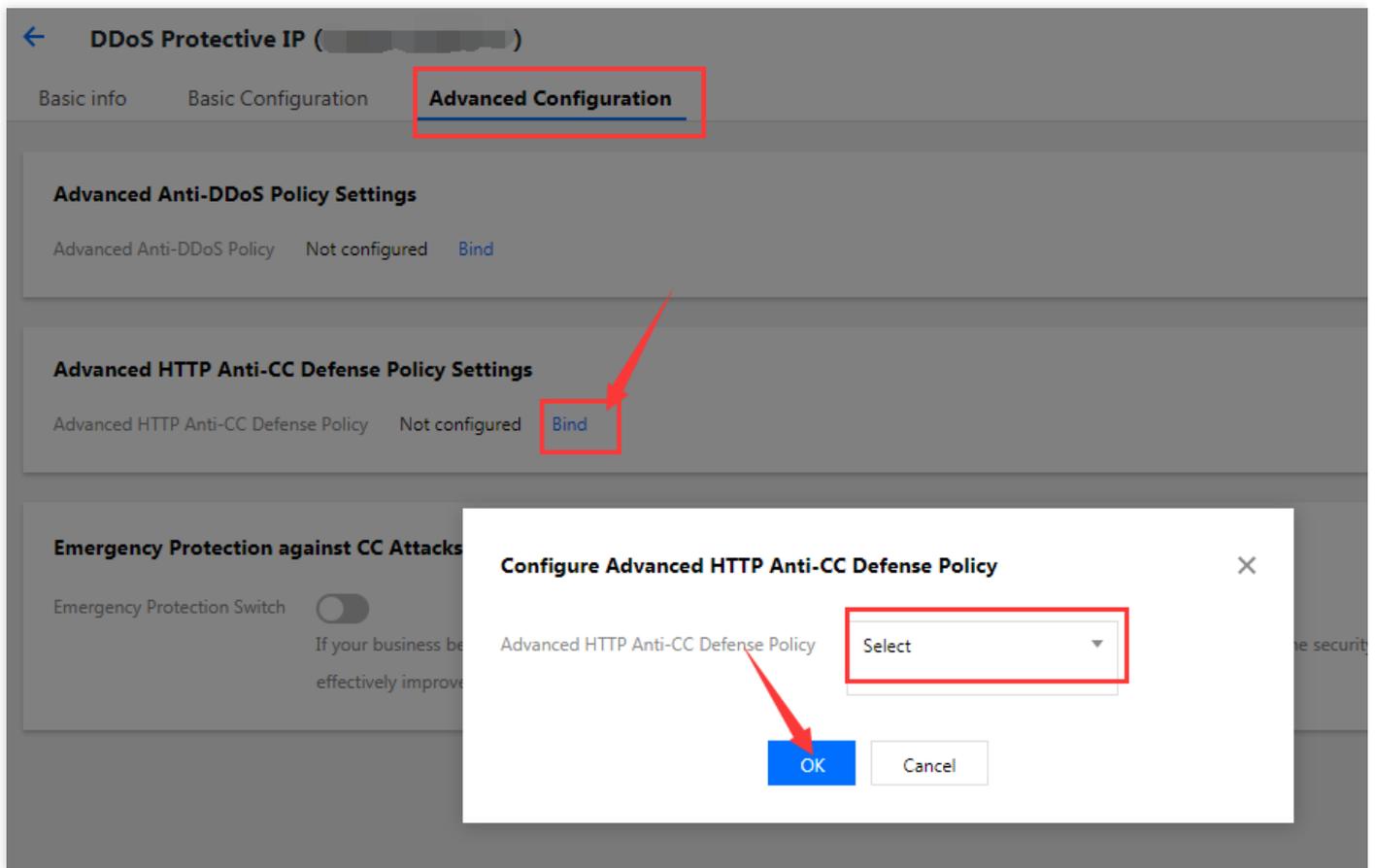


Binding a DDoS Protective IP with an Anti-CC Defense Policy

1. Click **DDoS Protective IP** and select a protective IP to enter the DDoS protective IP details page.

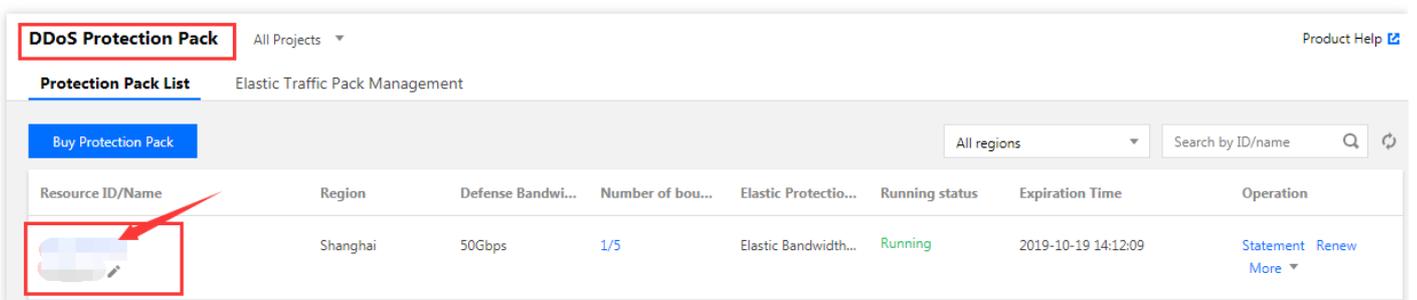


- Click "Advanced Configuration". Click **Bind**, select an anti-CC defense policy and click **OK**.



Configuring an Anti-CC Defense Policy for a Protected IP Under a DDoS Protection Pack

- Click **DDoS Protection Pack** and select a protection Pack ID to enter the DDoS protection pack details page.



- Click **Protected IP List**, select the IP to be configured and click "Configure HTTP anti-CC defense policy".

← Anti-DDoS High-Defense Package Details ([redacted])

Basic info **Defense IP List**

Defense IP Configuration

Up to 5 IPs can be added and 1 IP(s) have been added.

[Add Protected IP](#) [Bind advanced anti-DDoS defense policy](#) [Bind advanced HTTP anti-CC defense policy](#) [Bind to business](#) [Remove IP](#)

<input checked="" type="checkbox"/>	Resource ID/Name	IP	Project	Resourc...	Advanced Anti-DDoS ...	Advanced HTTP Anti-...	Protecti...	Bind to ...	Last A... [ⓘ]	Operation
<input checked="" type="checkbox"/>	[redacted]	123.206.229.92	Default P...	Elastic IP	-	-	Normal	-	-	Unbind advanced security policy Unbind CC defense policy Bind to business

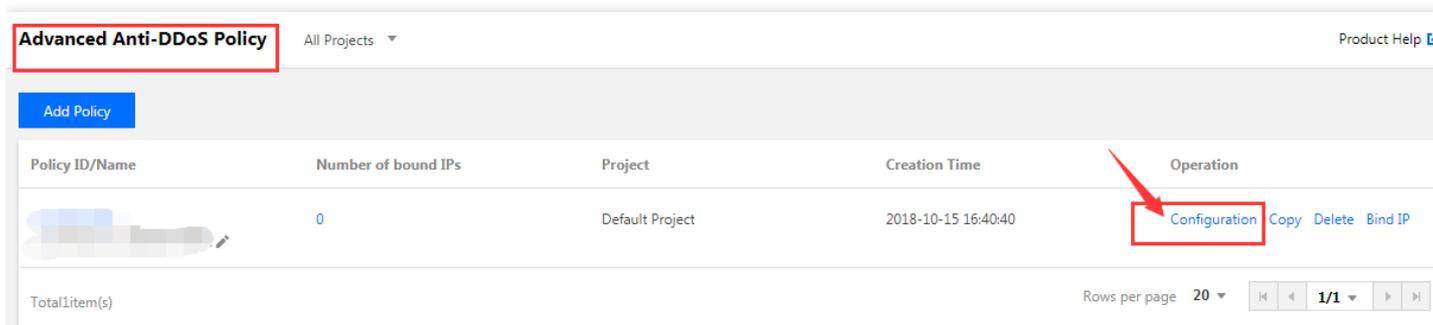
Configuring an Advanced Anti-DDoS Policy

Last updated : 2020-07-30 11:38:32

Aegis Anti-DDoS provides advanced security protection policies against DDoS attacks. You can bind the policies to protective IPs or IPs protected by protection packs based on the needs of your business platform, and then use features such as protocol disabling, port disabling, IP blocklist/allowlist, message characteristic filtering policies and null session prevention to achieve targeted protection capabilities for the platform. For more information on the configuration, see [Custom Advanced Security Policy](#).

Adding an Advanced Security Policy

1. Go to the [Aegis Anti-DDoS Console](#), click **Advanced Anti-DDoS Policy*** in the left pane, and click ****Add Policy**. After successful addition, click **Configuration** in the "Operation" column to enter the policy configuration page.



Policy ID/Name	Number of bound IPs	Project	Creation Time	Operation
	0	Default Project	2018-10-15 16:40:40	Configuration Copy Delete Bind IP

2. Select the disabled protocol and port to be configured, set the IP blocklist/allowlist, and filter the message characteristics. You can optionally enable the prevention against traffic from outside China and null sessions. Click OK to finish adding the policy.

IP Blacklist/Whitelist

A maximum of 50 IP addresses can be added to the IP white list and the IP black list. Batch entry is allowed, with multiple IP addresses separated by commas.

IP Whitelist

IP	Oper...
1.1.1.1	Delete
1.1.1.3	Delete
Increase	

IP Blacklist

IP	Oper...
1.1.1.2	Delete
1.1.1.4	Delete
Increase	

Packet feature filtering policy

Protocol	Start por...	Ending p...	Minimu...	Maximu...	Detection l...	Offset	Detectio...	Included	String	Policy	Oper...
TCP	50	100	50	1500	A sing...	0	1500	Not in...	abc	Discard	Delete
Increase											

OK Cancel

Binding an Advanced Security Policy Directly to a Protected IP

1. Click **Advanced Anti-DDoS Policy*** in the left pane, and click a ****Policy ID**.

Advanced Anti-DDoS Policy All Projects Product Help

Add Policy

Policy ID/Name	Number of bound IPs	Project	Creation Time	Operation
	0	Default Project	2018-10-15 16:40:40	Configuration Copy Delete Bind IP

2. Click **List of bound IPs** and click **Add IP**.

← Advanced Anti-DDoS Policy ([redacted])

Policy Details **List of bound IPs**

Add IP Unbind IP

<input type="checkbox"/>	Resource ID/Name	IP	Project	Resource Type	Policy Status	Bind to business	Region
<input type="checkbox"/>	[redacted]	[redacted]	Default Project	[redacted]	Deploying	Not bound	[redacted]

Binding a DDoS Protective IP with an Advanced Security Policy

1. Click **DDoS Protective IP** and click "Protective IP".

DDoS Protective IP

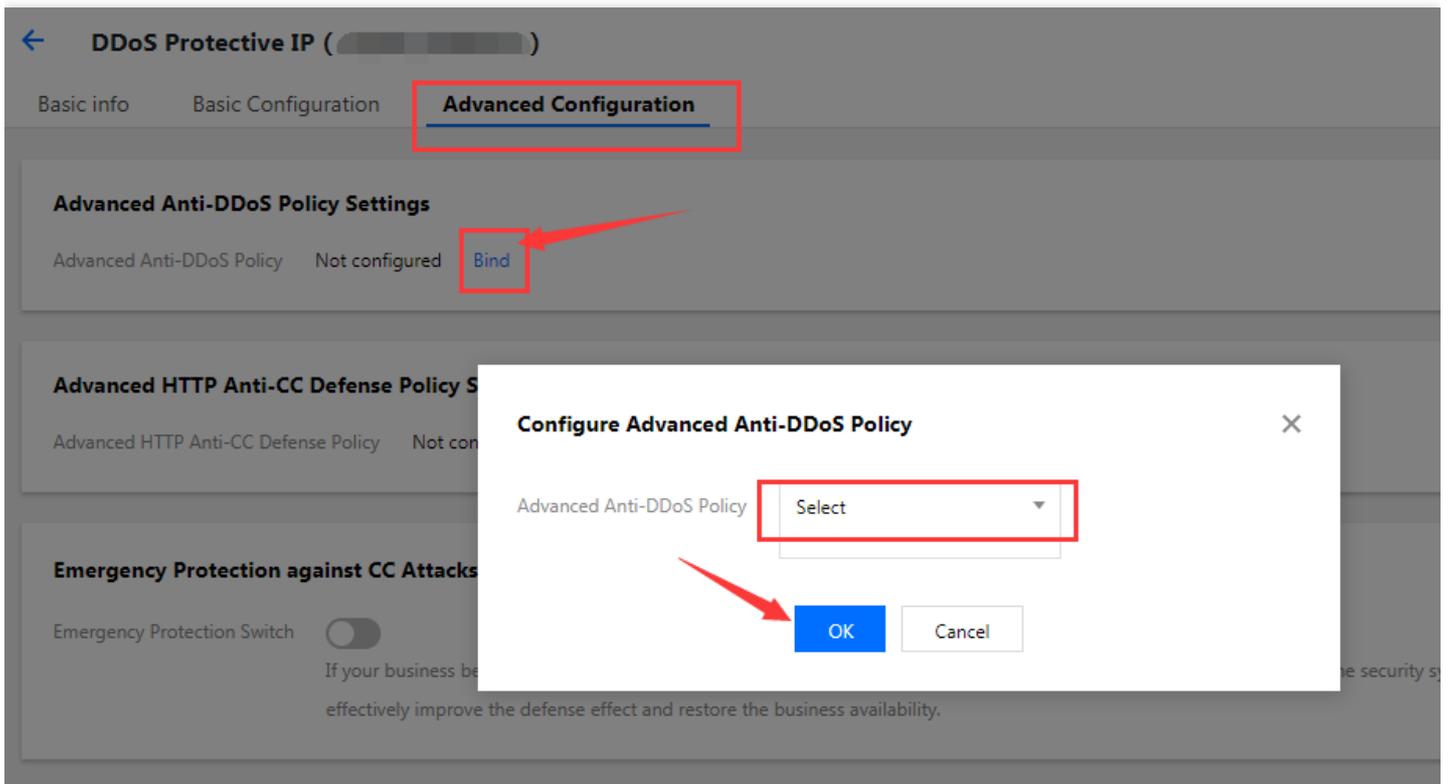
Protective IP List Forwarding Rule Group

Buy Protective IP Bind to business

All regions All Networks Search by IP address/ID

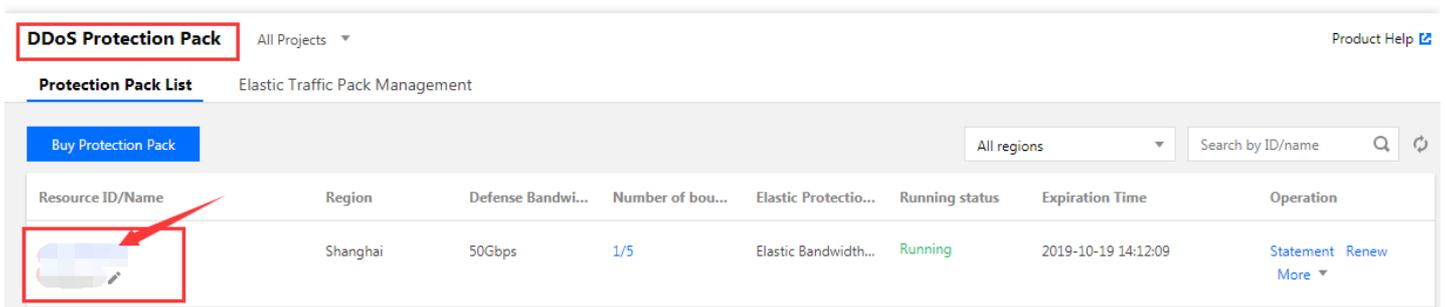
<input type="checkbox"/>	Resource ID/...	IP	Network (re...	Defense Ba...	Forwardi...	Advanced...	Advanced...	Running...	Bind to b...	Expiration Time	Operation
<input type="checkbox"/>	[redacted]	[redacted]	[redacted]	30Gbps	-	-	-	Running	Not bound	2018-11-19 17:...	Configuration Statement More

2. Click **Advanced configuration** on the **DDoS Protective IP** page. Click **Bind**, select an advanced anti-DDoS policy in the "Configure Advanced Anti-DDoS Policy" pop-up and click **OK**.



Configuring an Advanced Security Policy for a Protected IP Under a DDoS Protection Pack

1. Click **DDoS Protection Pack** and click a protection pack ID.



2. On the DDoS protection pack details page, click **Protected IP List**, select the IP to be configured and click "Configure advanced security policy".

← Anti-DDoS High-Defense Package Details ([redacted])

Basic info

Defense IP List

Defense IP Configuration

Up to 5 IPs can be added and 1 IP(s) have been added.

Add Protected IP

Bind advanced anti-DDoS defense policy

Bind advanced HTTP anti-CC defense policy

Bind to business

Remove IP

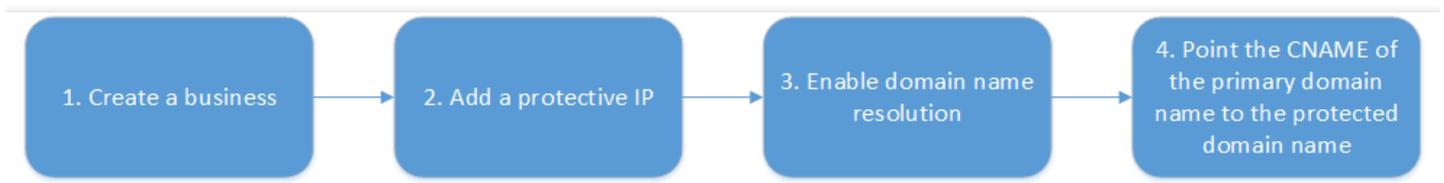
<input checked="" type="checkbox"/>	Resource ID/Name	IP	Project	Resourc...	Advanced Anti-DDoS ...	Advanced HTTP Anti-...	Protecti...	Bind to ...	Last A...①	Operation
<input checked="" type="checkbox"/>	[redacted]	[redacted]	Default P...	Elastic IP	-	-	Normal	-	-	Unbind advanced security policy Unbind CC defense policy Bind to business

Binding a Protected Domain Name to a Protective IP

Last updated : 2020-01-14 11:13:44

In the [Aegis Anti-DDoS Console](#), select "Business Domain Name List" in the left pane, and click "Create a business and a domain name" in the right to automatically generate a protected domain name. You can access the protection service by pointing the CNAME of your business domain name to a protected domain name.

Flowchart



Process for Binding a Protected Domain Name to a Protective IP

1. Create a business

- Click **Business Domain Name List** and then click **Create a business and a domain name**.



- Enter the relevant information and click **Create**. After successful creation, the business and the

free protected domain name are generated in "Business Domain Name List".

← **Create a business and a domain name**

Create a business and a domain name

Project (*)

Business Name (Required)

Contact name

Mobile

Development Platform PC Client Mobile Device TV Server

Sub-category

[Create](#)

2. Add a protective IP

a. In the business domain name list management page, click "Add IP" to go to the business details page.

Business domain name list All Projects ▾

[Create a business and a domain name](#)

Task Name	Protective Domain Name	Protective IP R...	DNS Resolutio...	BGP First	Watermarking	Creation Time	Operation
		Add IP	-	Enabled	Disabled	2018-10-23 11:21:18	Configuration Delete Enable watermarking

b. Click "Add IP" under "Settings of IP resources and resolution" in the "Business Details" page.

← Business Details ([redacted])

Basic info

Task Name [redacted]

Project Default Project

Contact Person [redacted]

Development Platform Mobile Device

Protective Domain Name Resolution Settings

Domain Name [redacted]

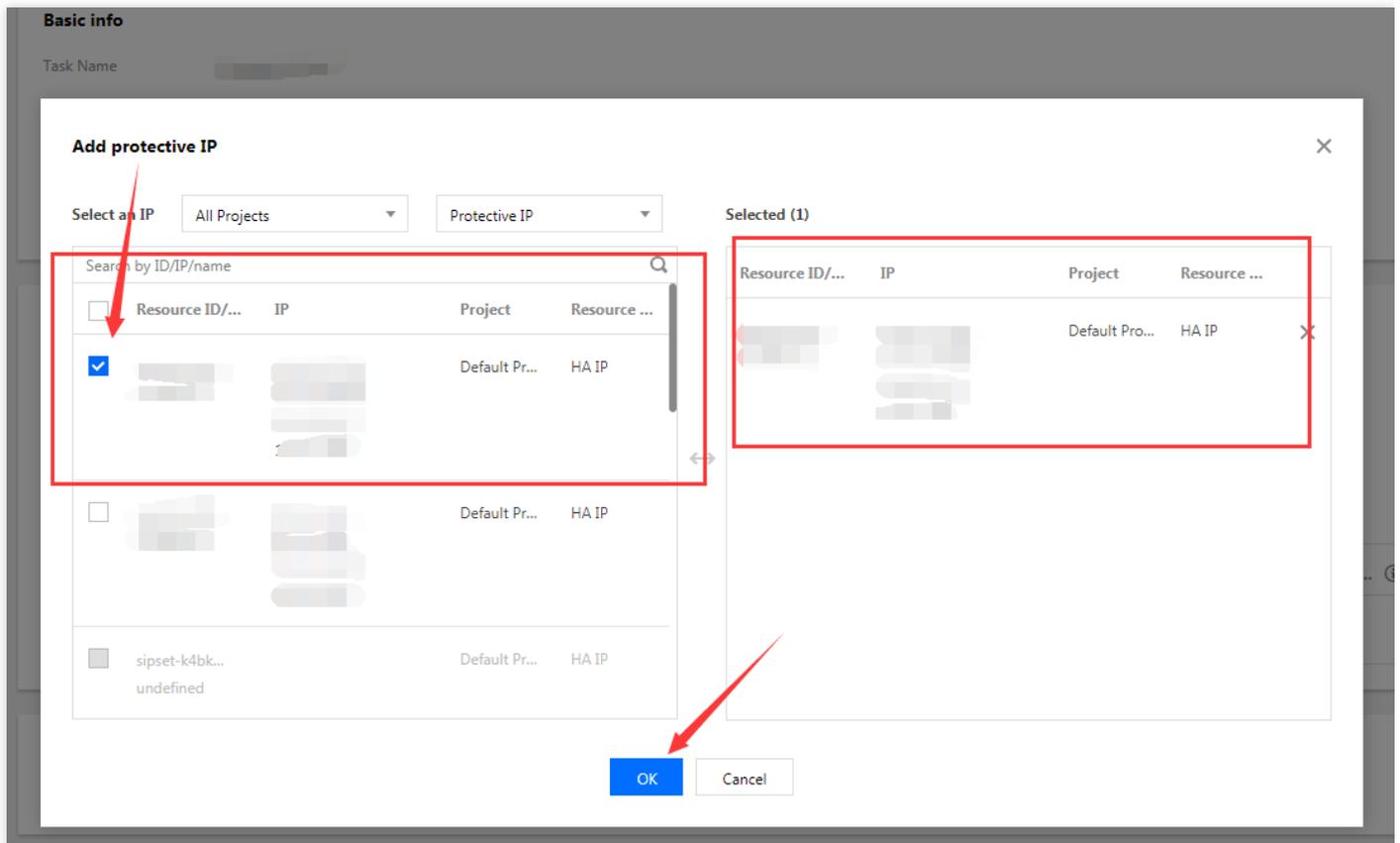
TTL Value 1 minute [Adjust](#)

BGP Line First ⓘ

Setting of IP resource and resolution [Add IP](#)

Resource ID	IP	Line	Region
Record is empty			

c. Select a protective IP and click **OK**.

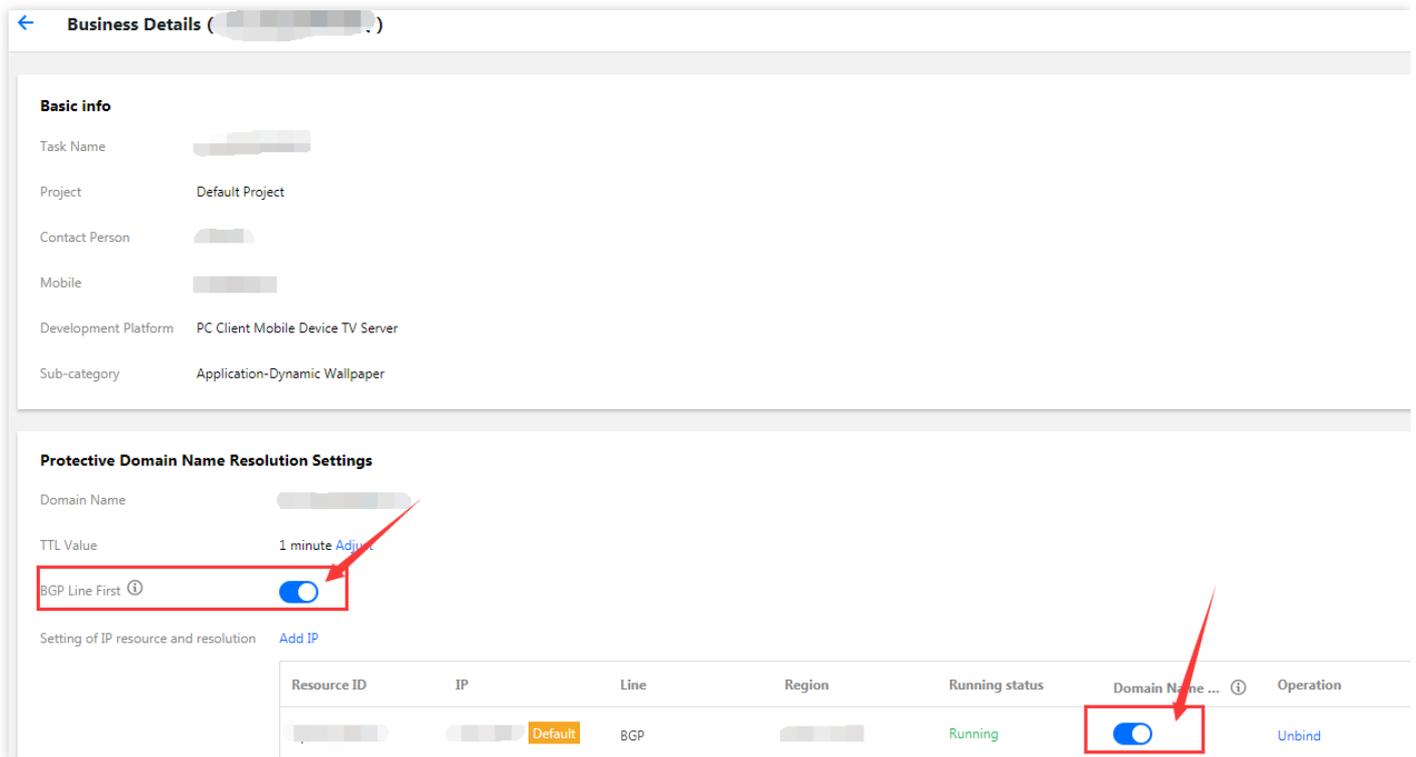


3. Enable domain name resolution

After adding a protective IP, enable "Domain Name Resolution". The protected domain name provides intelligent resolution, i.e. the source IP of the end user is resolved to the IP of the corresponding line. For example, China Telecom users will be resolved to the protective IP for China Telecom, while China Unicom users will be resolved to the protective IP for China Unicom. If the protective IP of a line is blocked due to excessive attacks, it will be automatically resolved to another available protective IP.

If "BGP Line First" is enabled, and a BGP line IP is bound, the protected domain name will preferentially schedule all business requests to be resolved to the BGP IP address. (Other non-BGP IPs with resolution enabled are in stand by.) If the BGP protective IP is jammed due to heavy-traffic attacks, the system will intelligently schedule business requests to non-BGP protective IPs with resolution enabled to provide high-bandwidth protection. After the BGP protective IP is unblocked,

the system will schedule all business requests to it.



Business Details ([redacted])

Basic info

Task Name [redacted]

Project Default Project

Contact Person [redacted]

Mobile [redacted]

Development Platform PC Client Mobile Device TV Server

Sub-category Application-Dynamic Wallpaper

Protective Domain Name Resolution Settings

Domain Name [redacted]

TTL Value 1 minute [Adjust](#)

BGP Line First

Setting of IP resource and resolution [Add IP](#)

Resource ID	IP	Line	Region	Running status	Domain Name ... ?	Operation
[redacted]	[redacted]	Default	BGP	Running	<input checked="" type="checkbox"/>	Unbind

4. Point the CNAME of the primary domain name to the protected domain name

After line resolution is enabled, the business' primary domain name can be intelligently resolved to the protective IP by pointing the CNAME to the protected domain name.

You can verify whether the domain name can be resolved to the protective IP using ping or nslookup locally.