Aegis Anti-DDoS

Operations Guide

Product Documentation

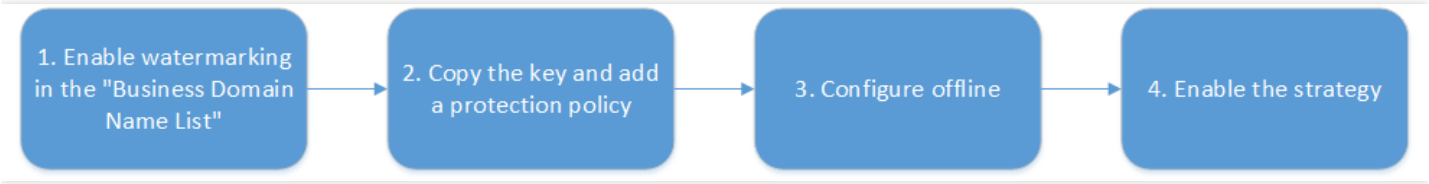
Contents

Operations Guide
Enabling Watermark Protection

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

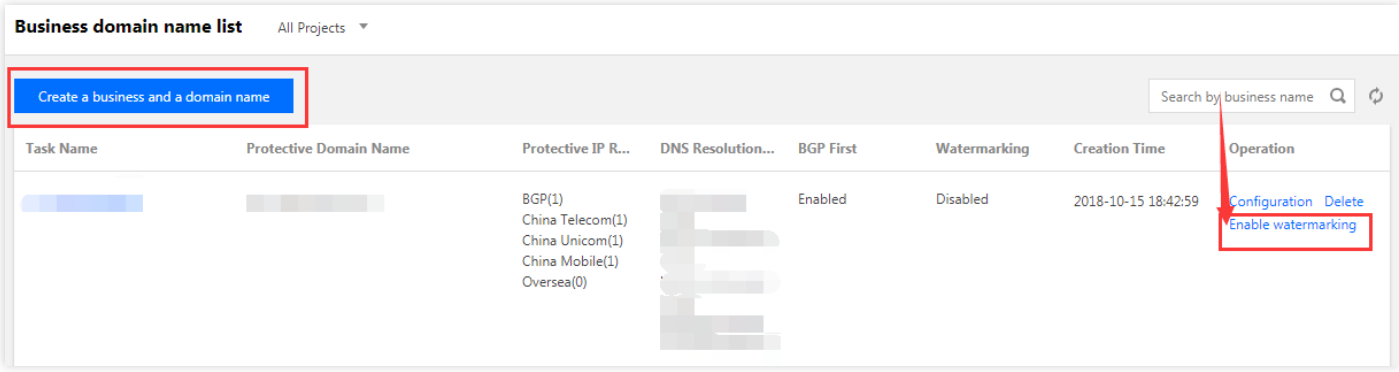
You can efficiently and comprehensively protect against layer 4 CC attacks such as masquerading and replay attacks by accessing watermark protection. By sharing the watermark algorithm and key between the business side and the Aegis protection system, watermark protection embeds a watermark in every 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



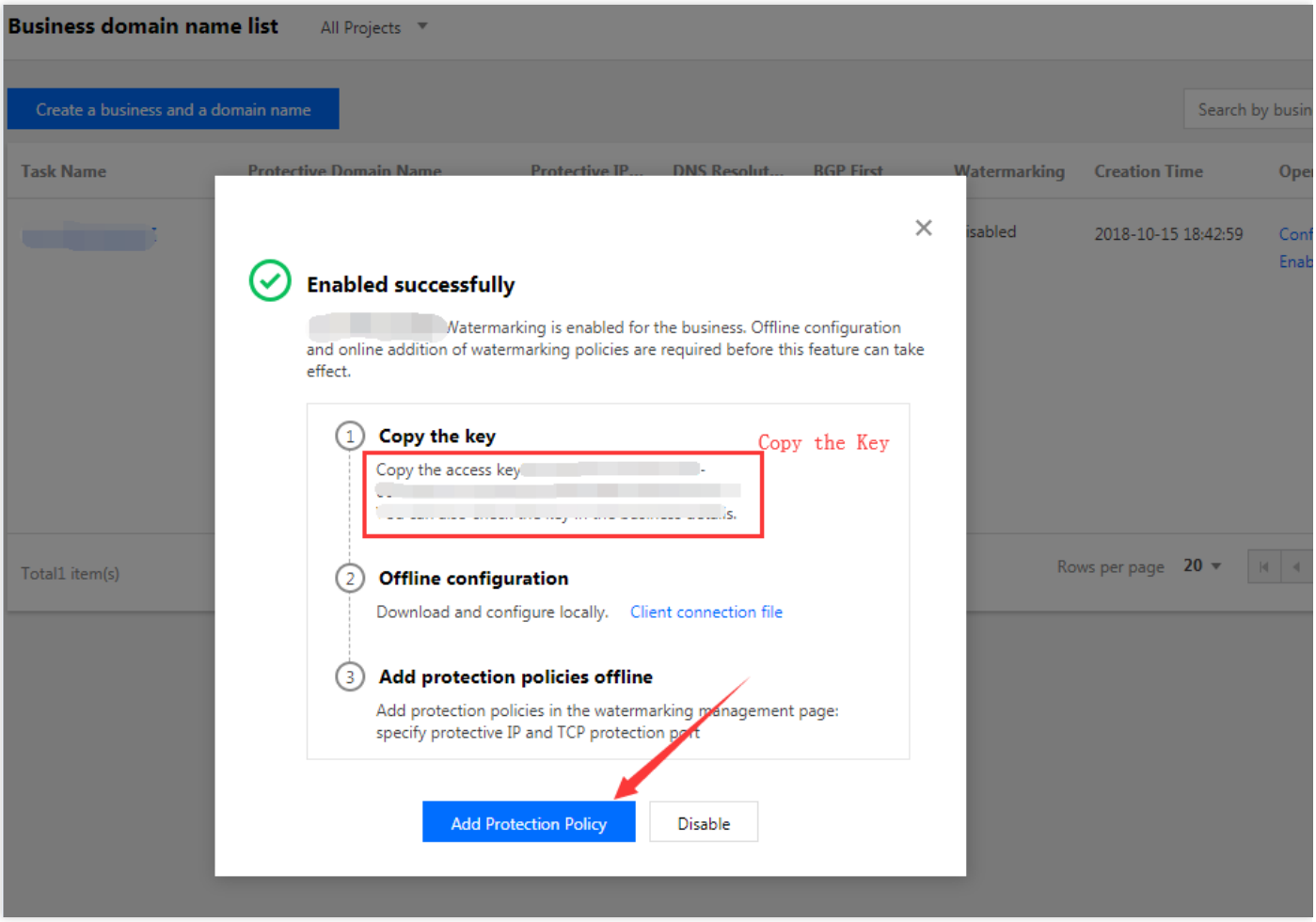
How to Enable

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**.

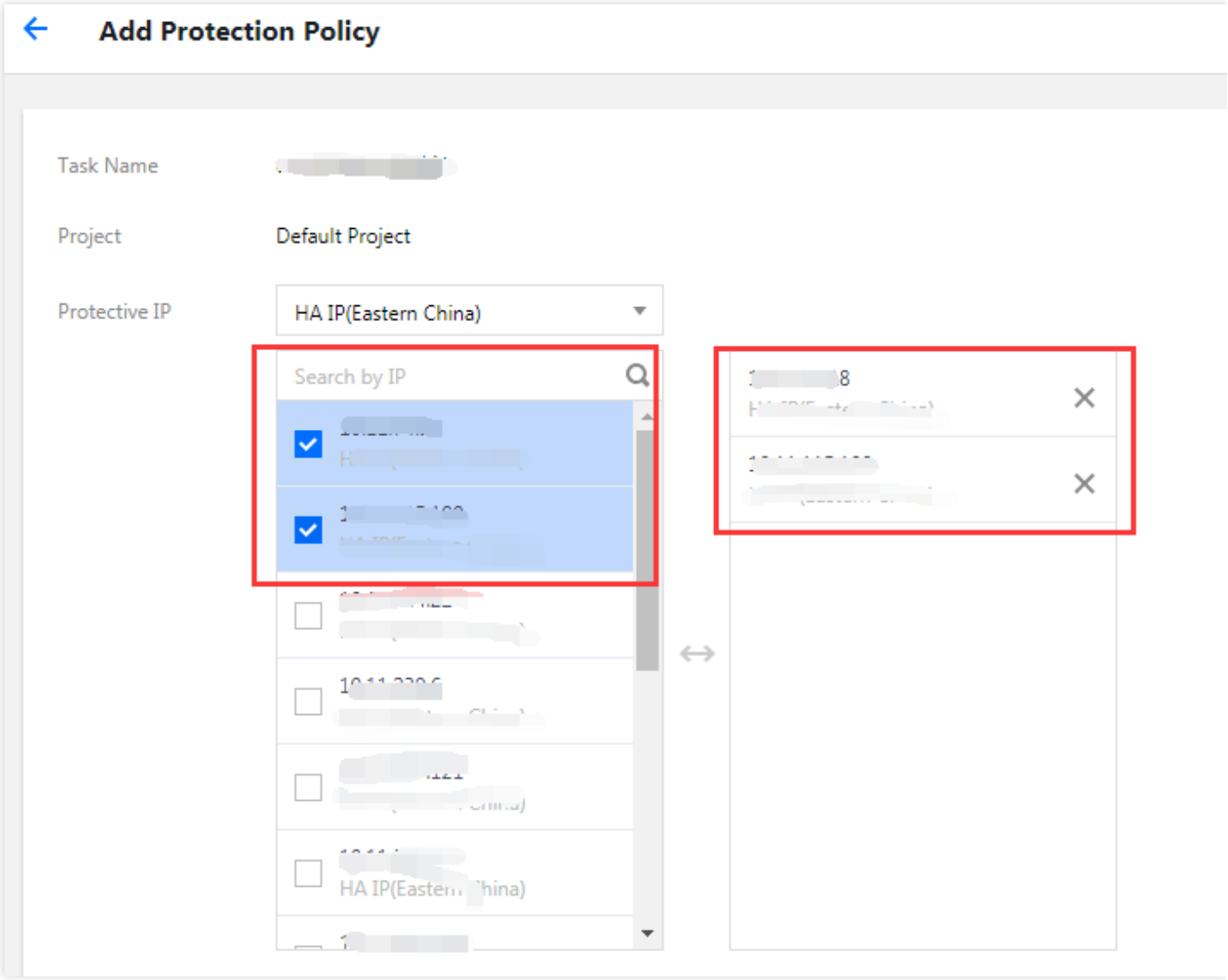


2. **Copy the key**

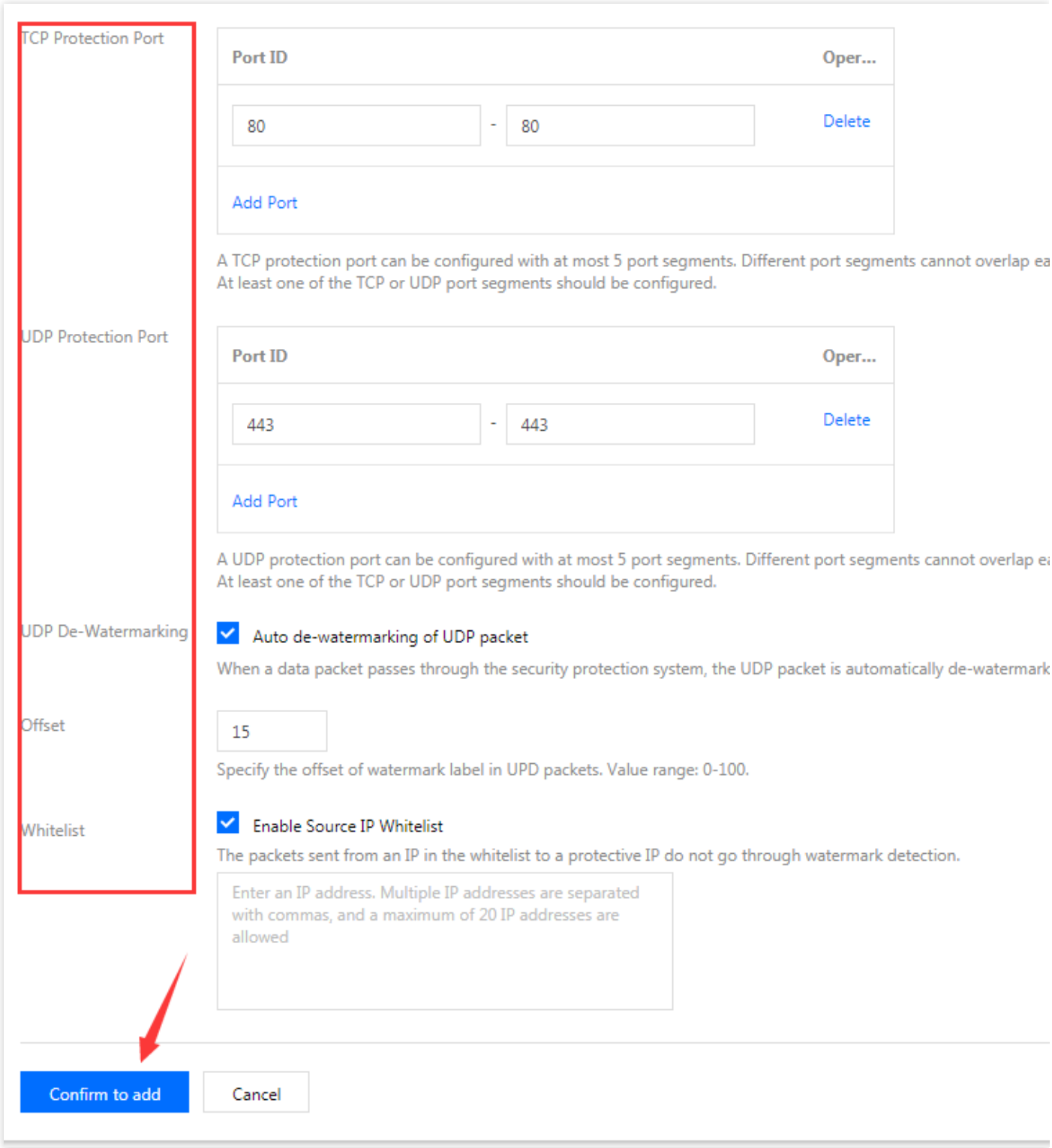
a. After watermarking is successfully enabled, select "Copy the key" in the "Enabled successfully" pop-up and click **Add Protection Policy**.



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**.

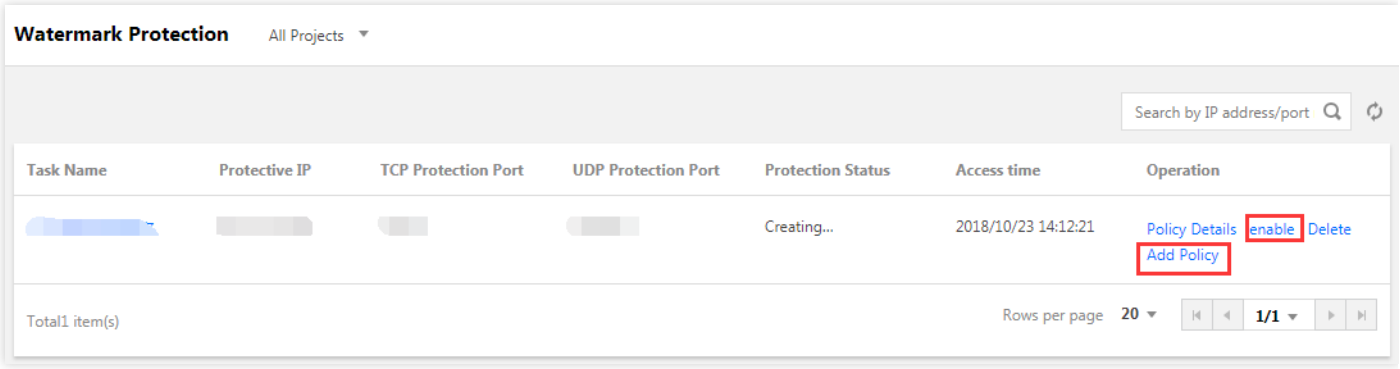


3. **Offline configuration**

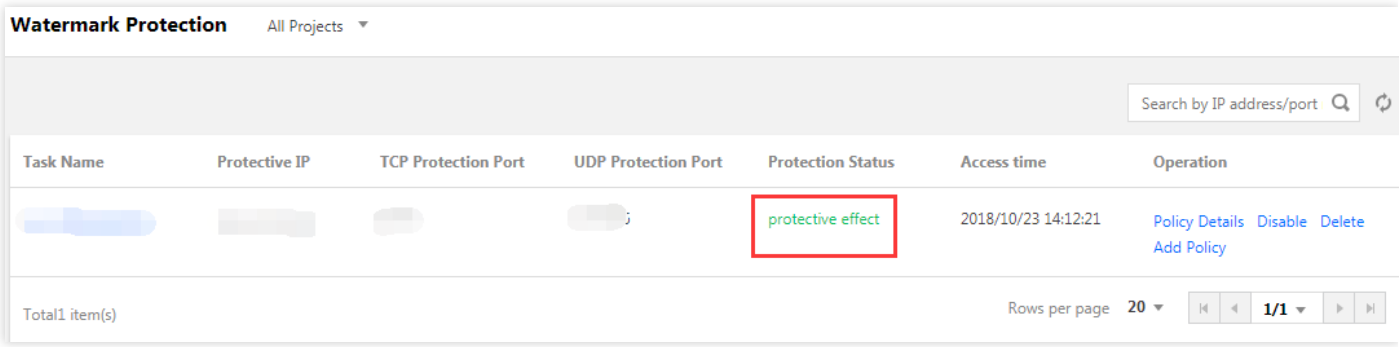
   In the "Enabled successfully" pop-up, click **Client connection file** to download the file for connecting the client and the server.

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**.



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



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_REVC` 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 `lsmode | 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=x8
6_64 ~/rpmbuild/SPECS/kernel.spec
```

0. Install the kernel rpm package;

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

Reboot to load the TOA module

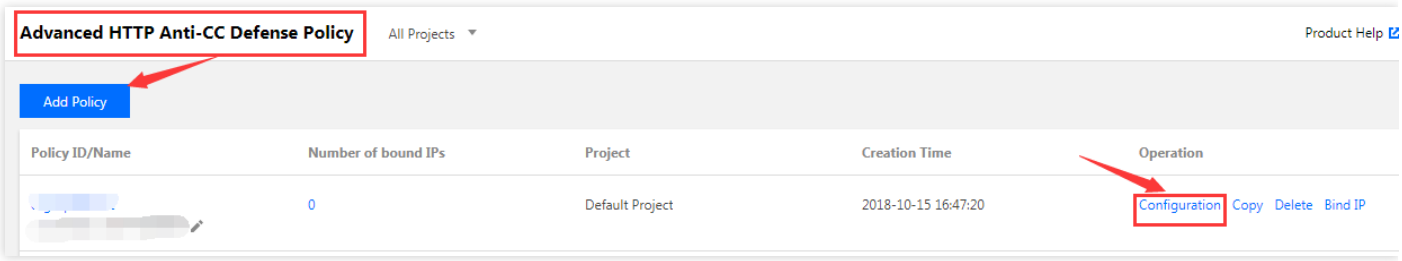
Configuring an Advanced HTTP Anti-CC Defense Policy

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**.

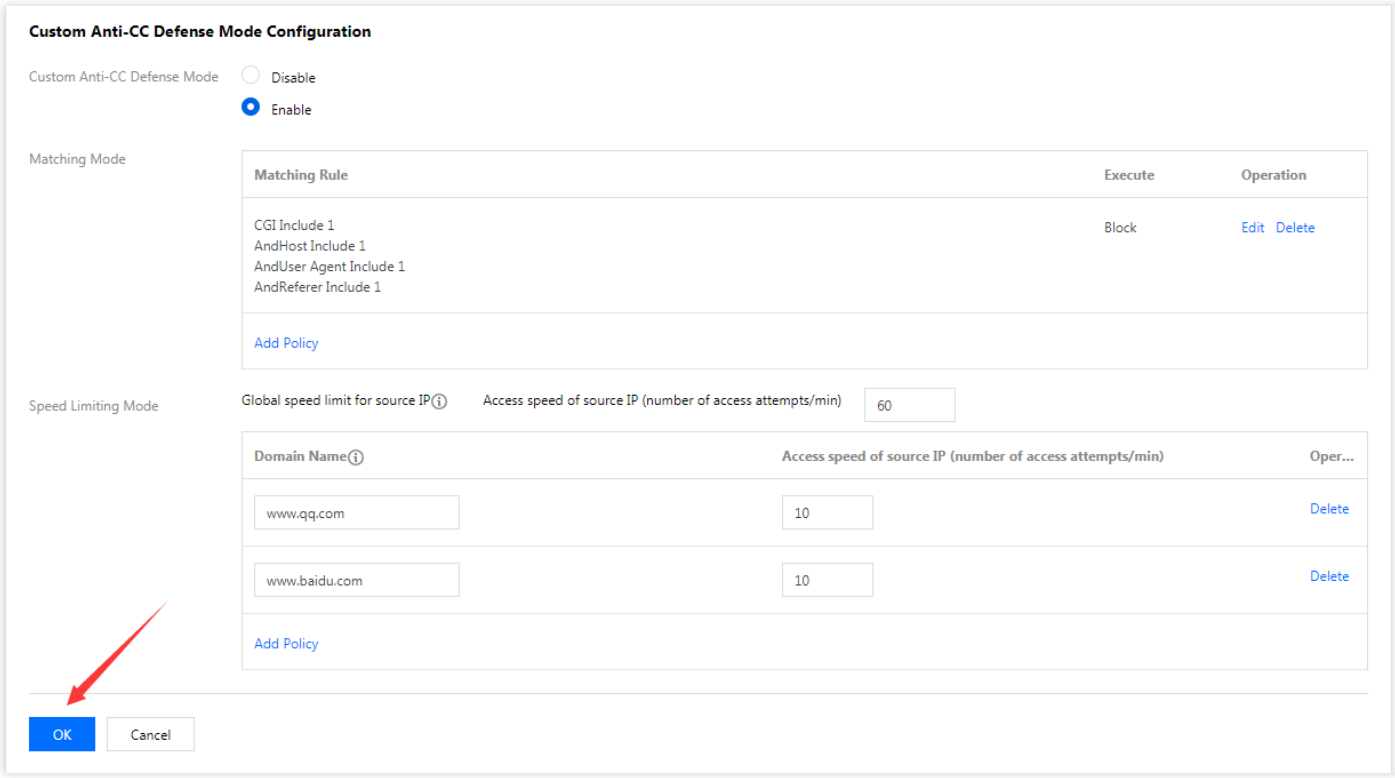
Adding a CC Protection Policy

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.



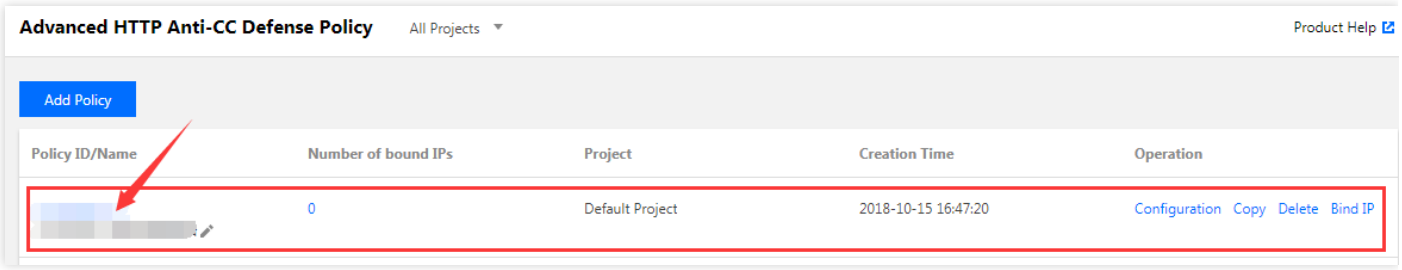
2. Configure options such as HTTP QPS request threshold, URL allowlist, IP blocklist and allowlist and custom anti-CC defense mode based on business characteristics and protection requirements.

Click OK to finish adding the policy.

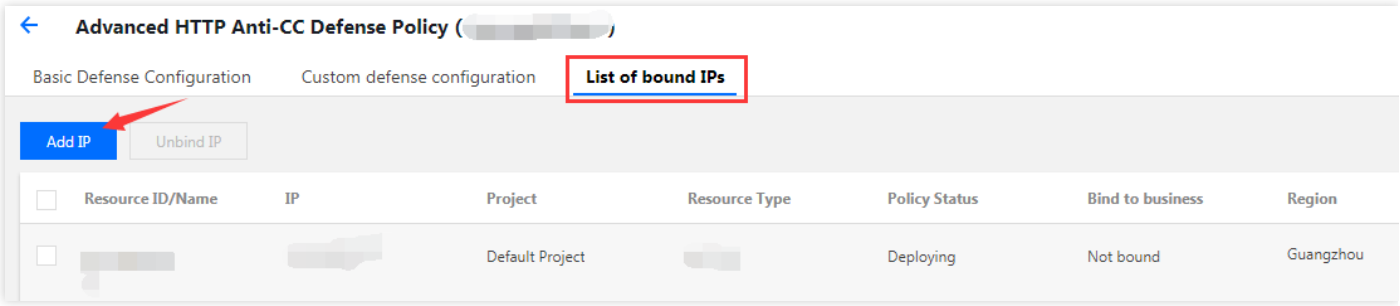


Binding an Anti-CC Defense Policy Directly to a Protected IP

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

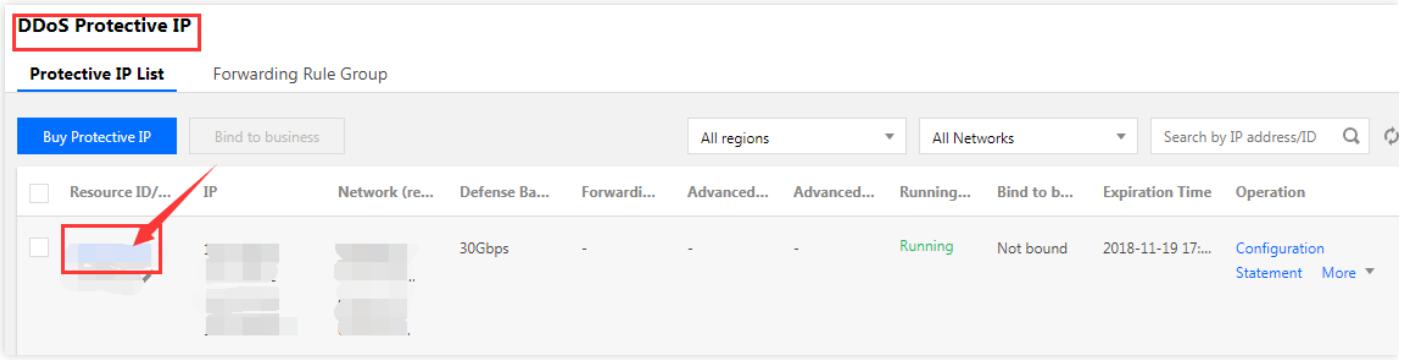


2. Click **List of bound IPs** and click **Add IP**.

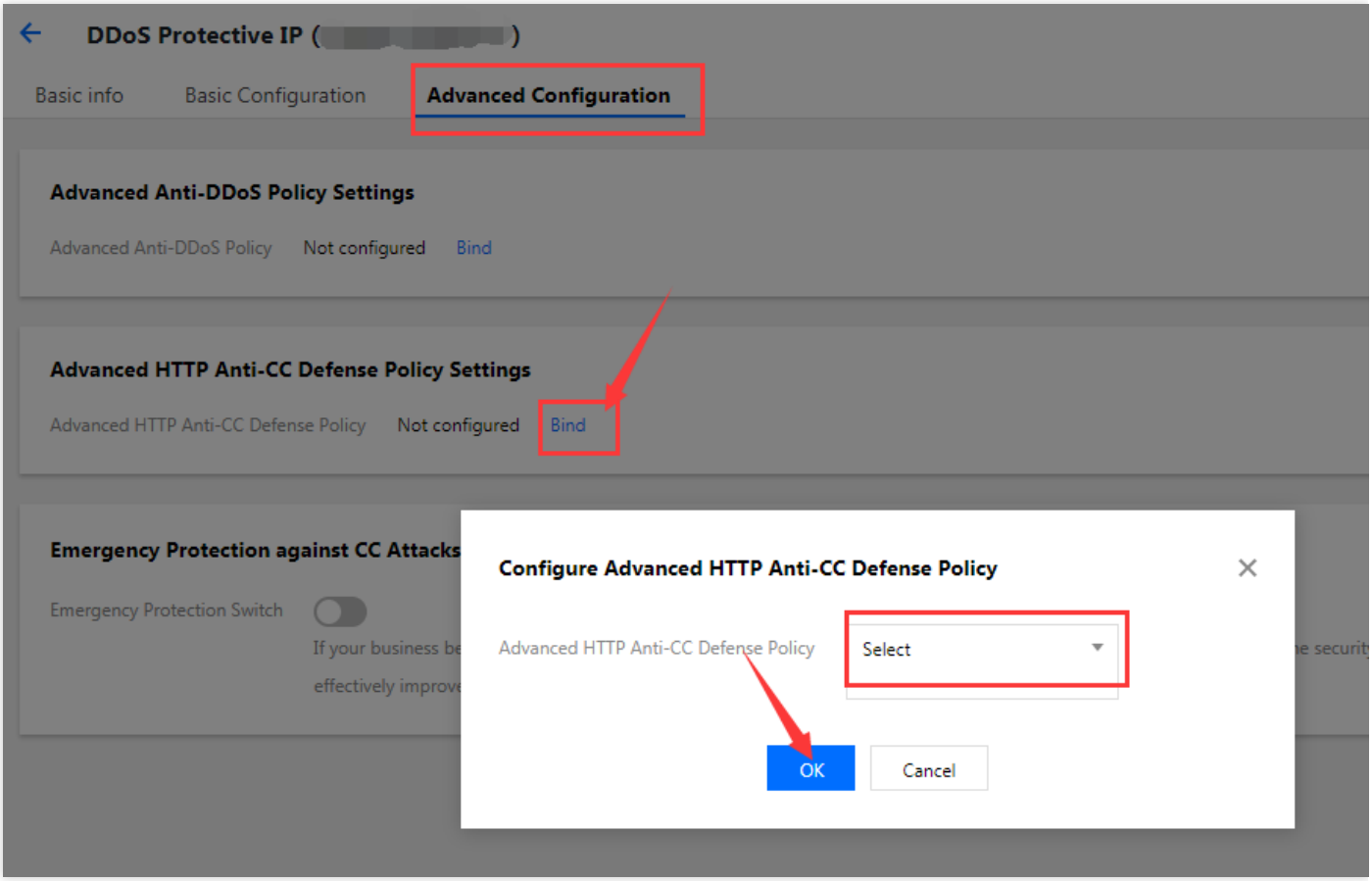


Binding a DDoS Protective IP with an Anti-CC Defense Policy

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

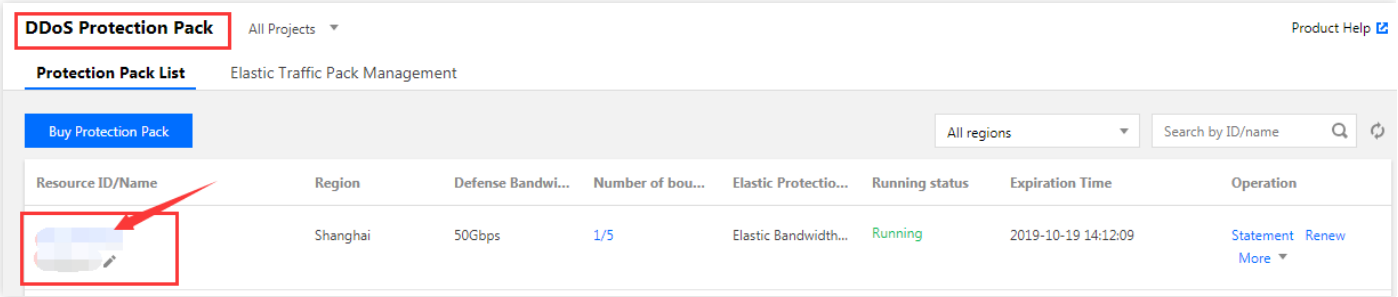


2. Click "Advanced Configuration". Click **Bind**, select an anti-CC defense policy and click **OK**.

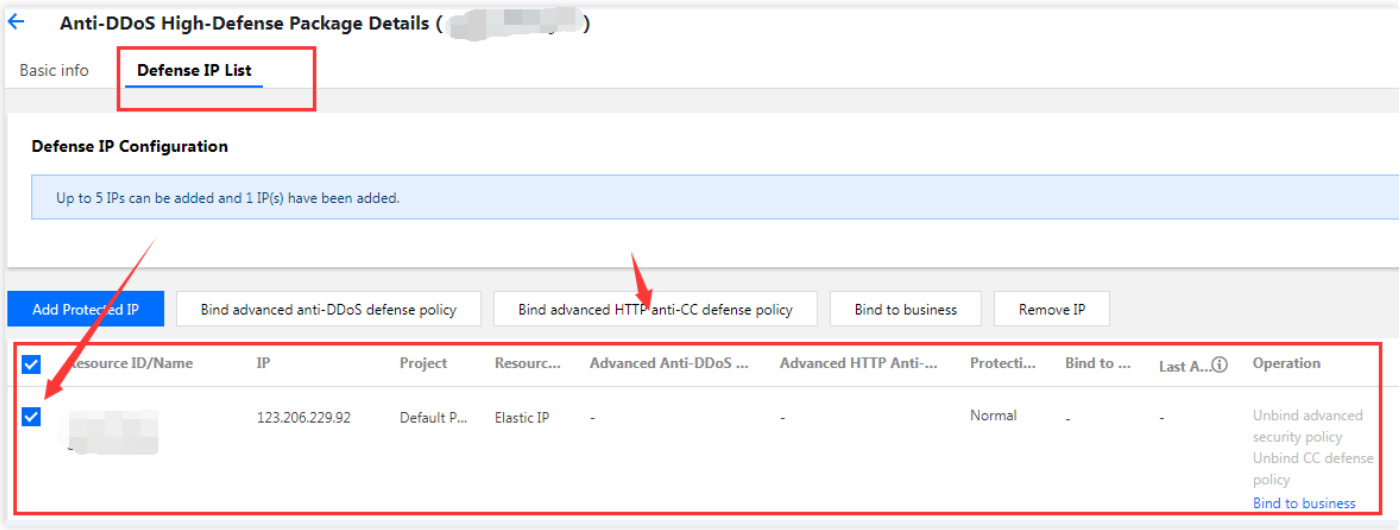


Configuring an Anti-CC Defense Policy for a Protected IP Under a DDoS Protection Pack

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



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



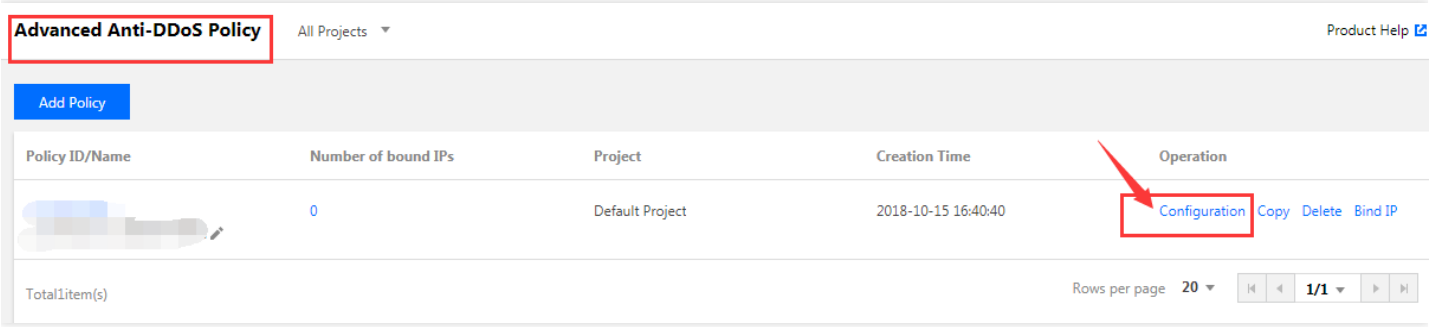
Configuring an Advanced Anti-DDoS Policy

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

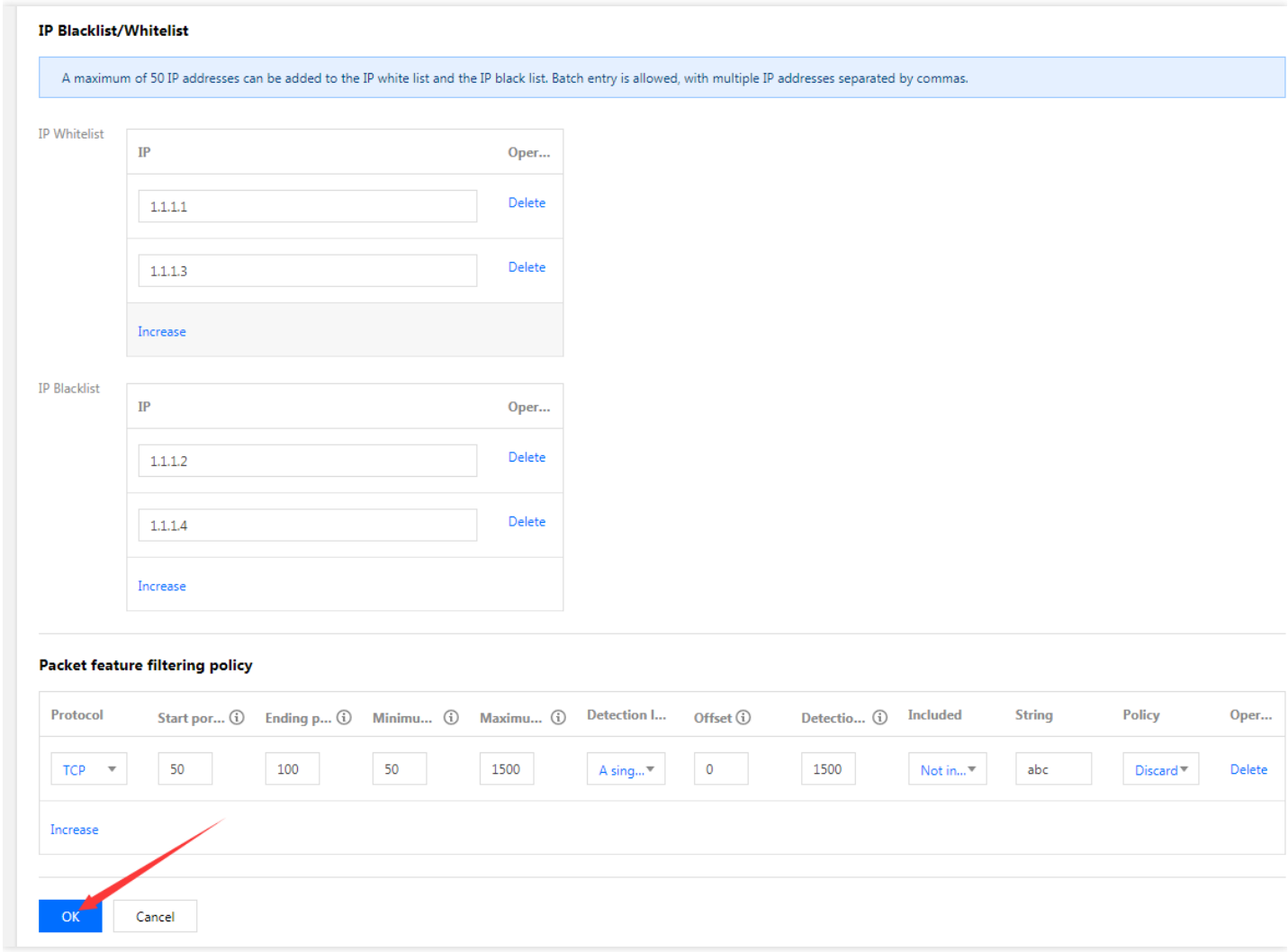
Aegis Anti-DDoS provides advanced security protection policies against DDoS attacks. You can bind the policies to protective IPs or IPs protected by protection packs based on the needs of your business platform, and then use features such as protocol disabling, port disabling, IP blocklist/allowlist, 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.

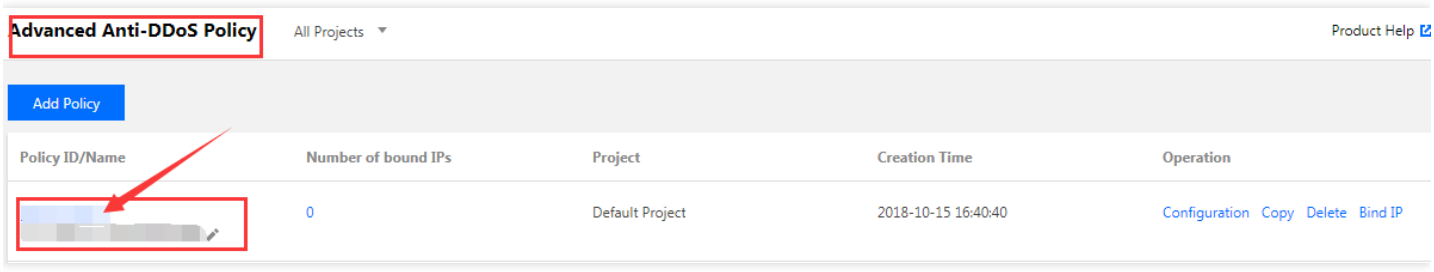


2. Select the disabled protocol and port to be configured, set the IP blocklist/allowlist, and filter the message characteristics. You can optionally enable the prevention against traffic from outside China and null sessions. Click OK to finish adding the policy.

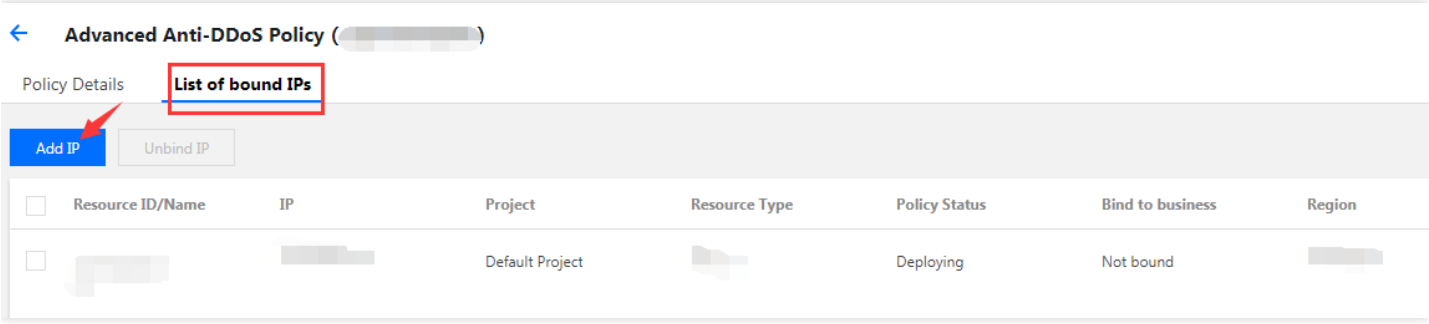


Binding an Advanced Security Policy Directly to a Protected IP

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

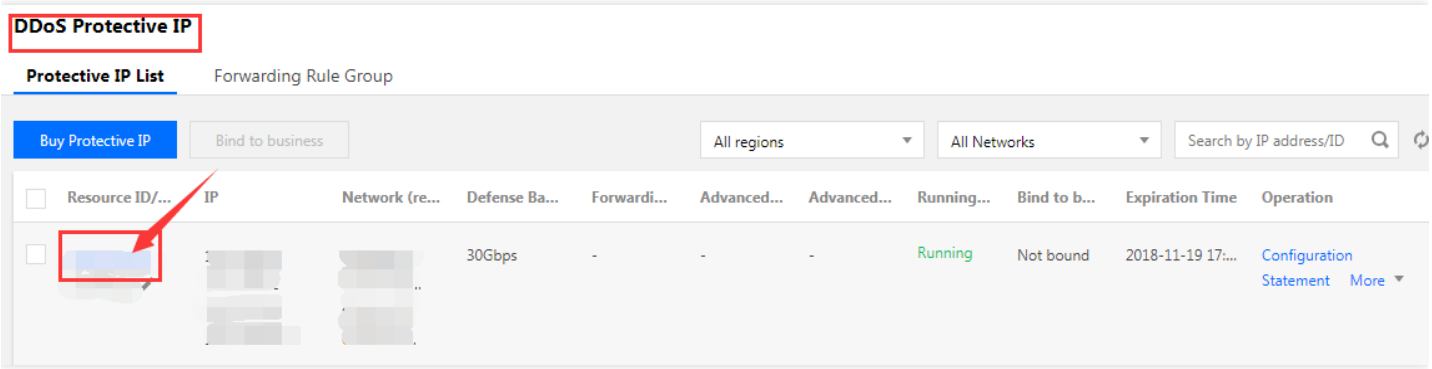


2. Click **List of bound IPs** and click **Add IP**.

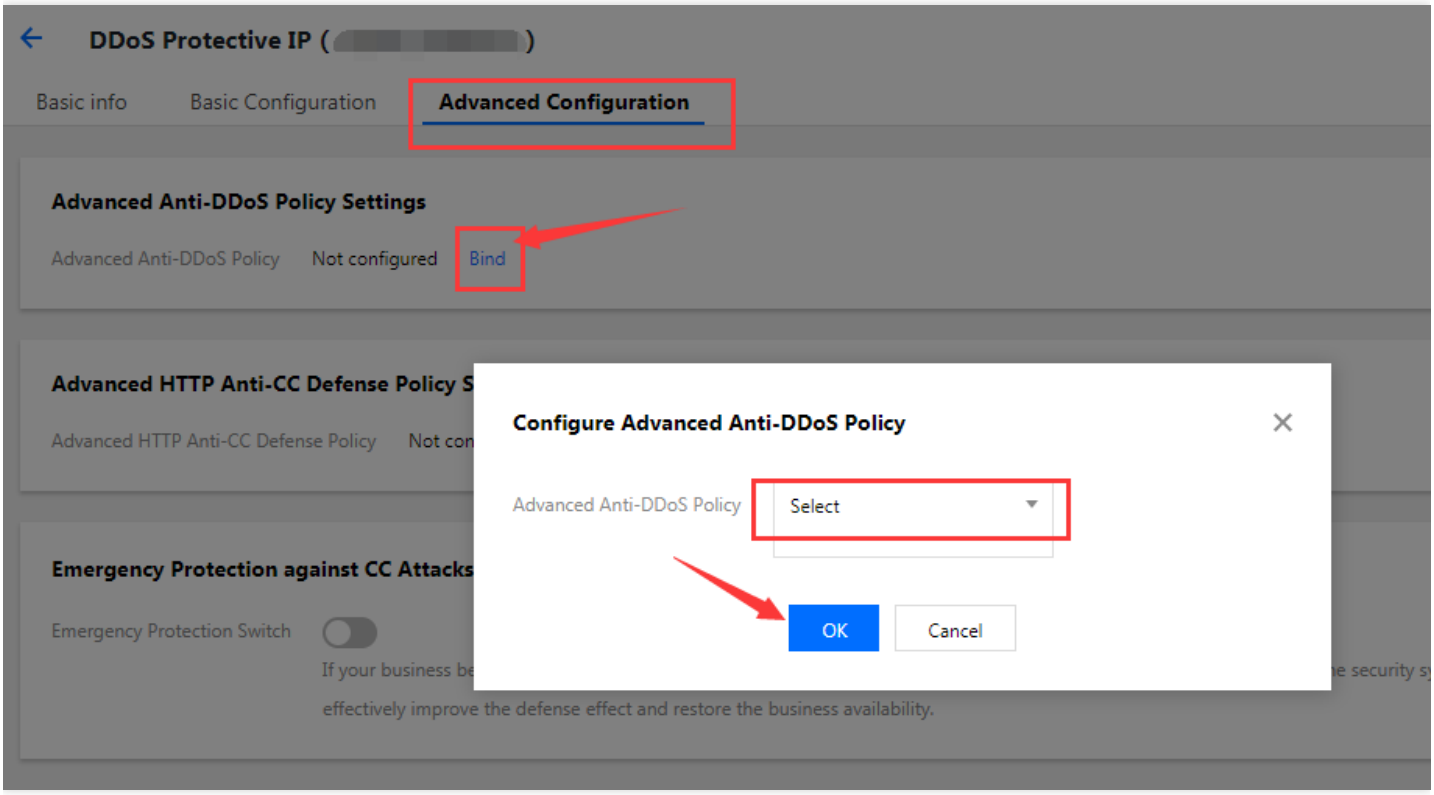


Binding a DDoS Protective IP with an Advanced Security Policy

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

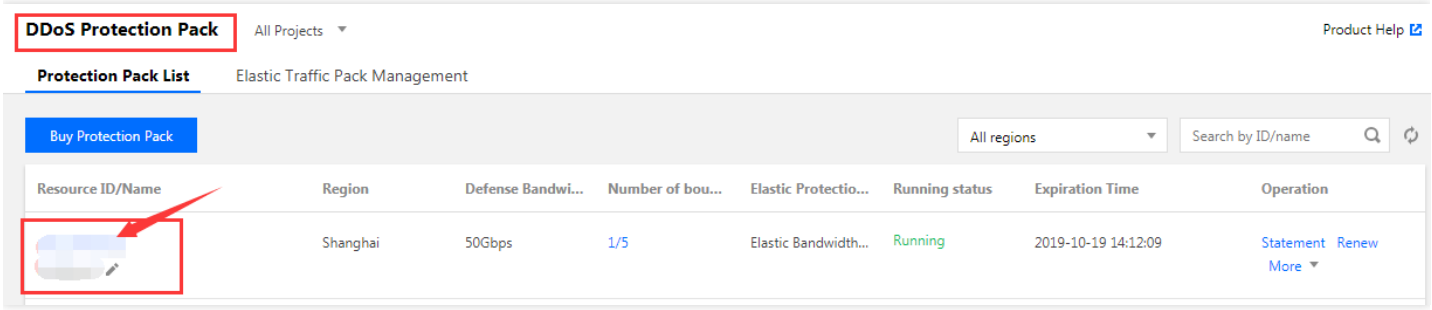


2. Click **Advanced configuration** on the **DDoS Protective IP** page. Click **Bind**, select an advanced anti-DDoS policy in the "Configure Advanced Anti-DDoS Policy" pop-up and click **OK**.

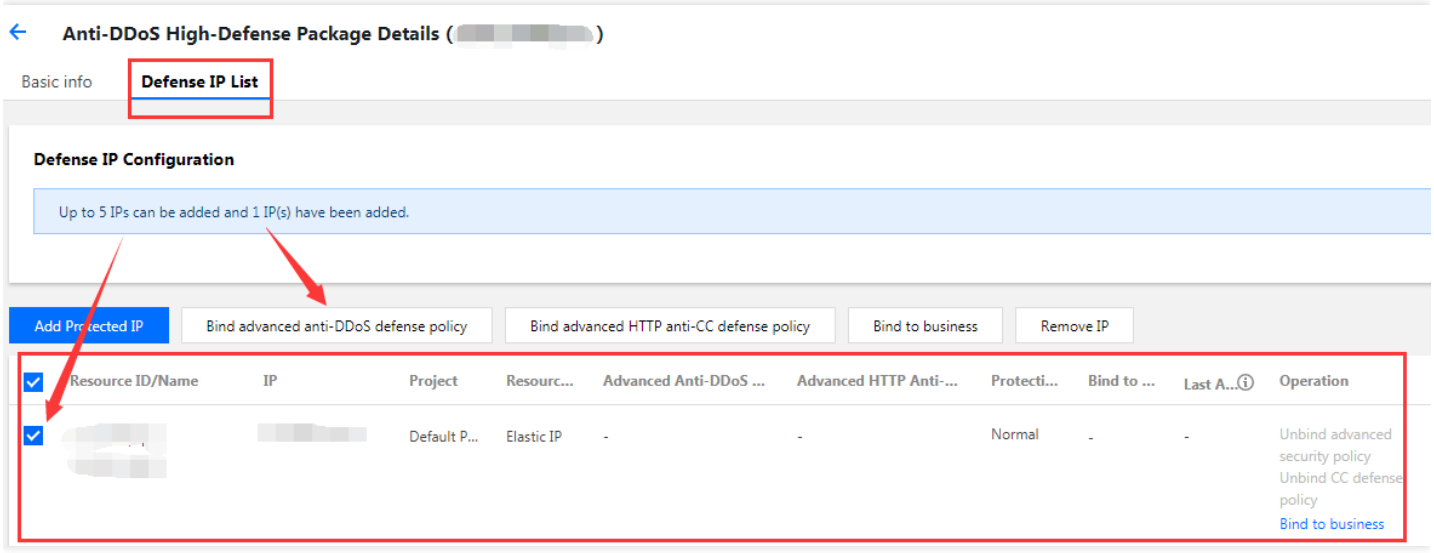


Configuring an Advanced Security Policy for a Protected IP Under a DDoS Protection Pack

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".

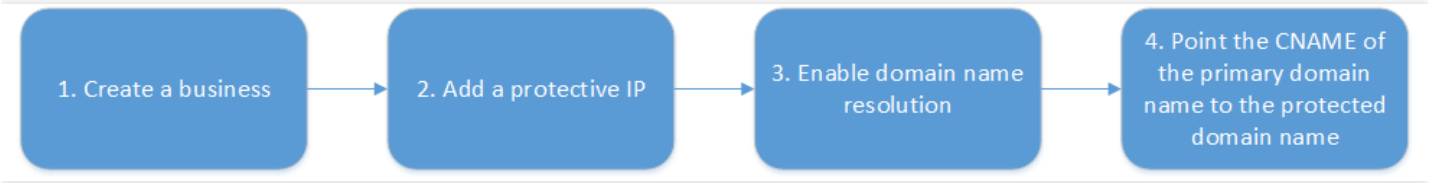


Binding a Protected Domain Name to a Protective IP

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



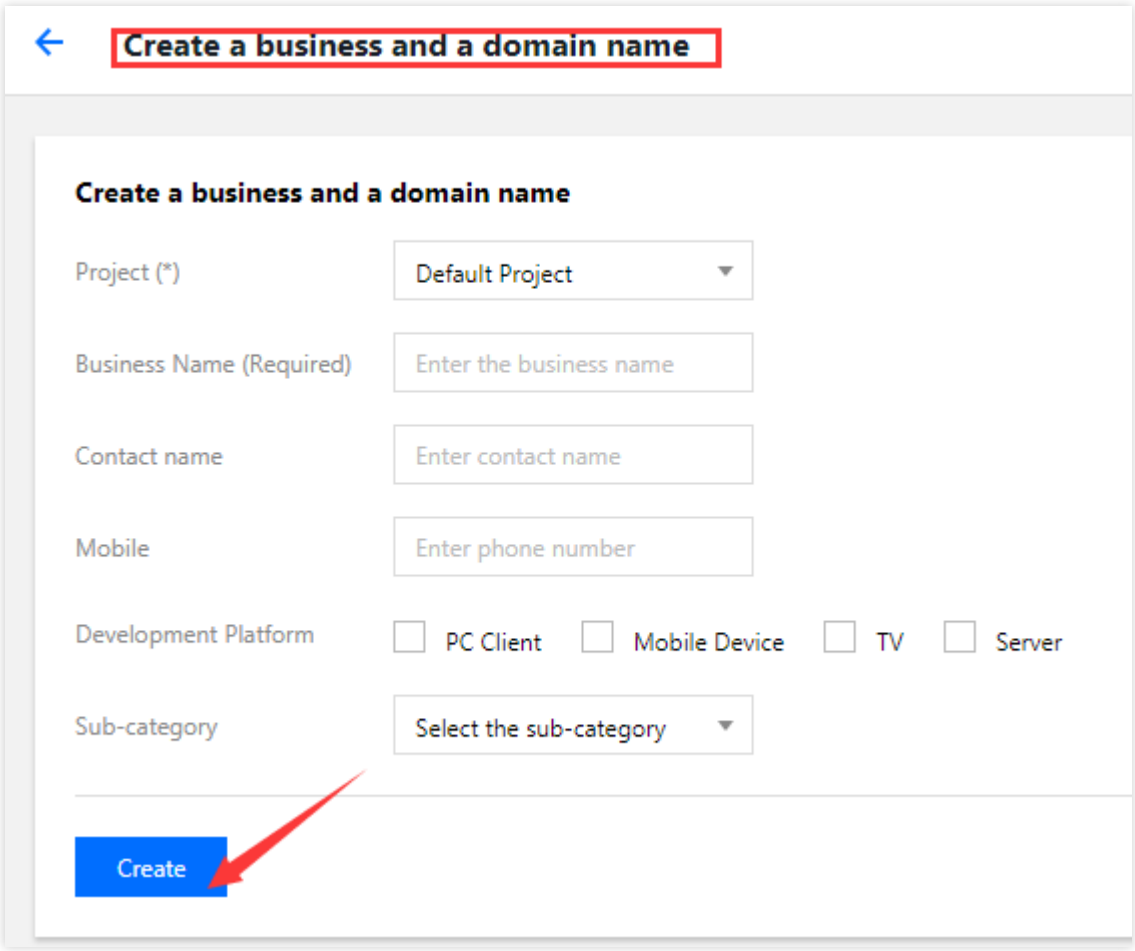
Process for Binding a Protected Domain Name to a Protective IP

1. **Create a business**

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

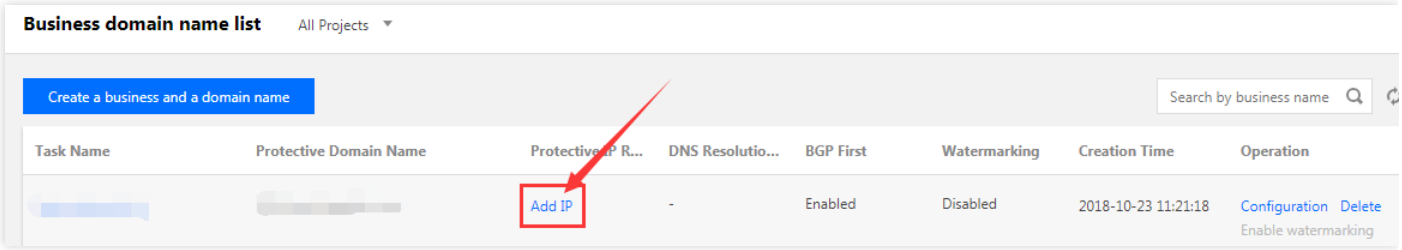
   b. Enter the relevant information and click **Create**. After successful creation, the business and the

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

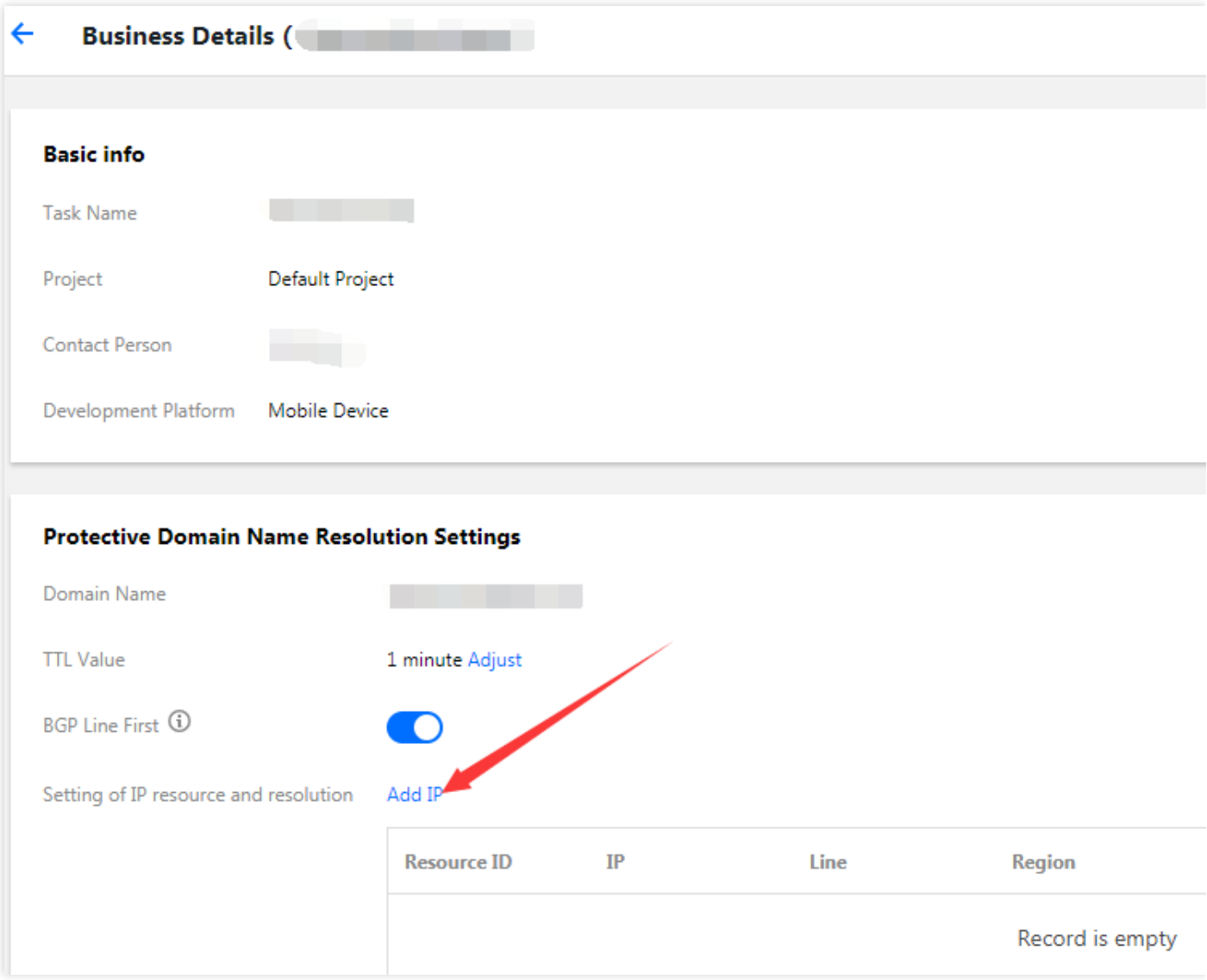


2. **Add a protective IP**

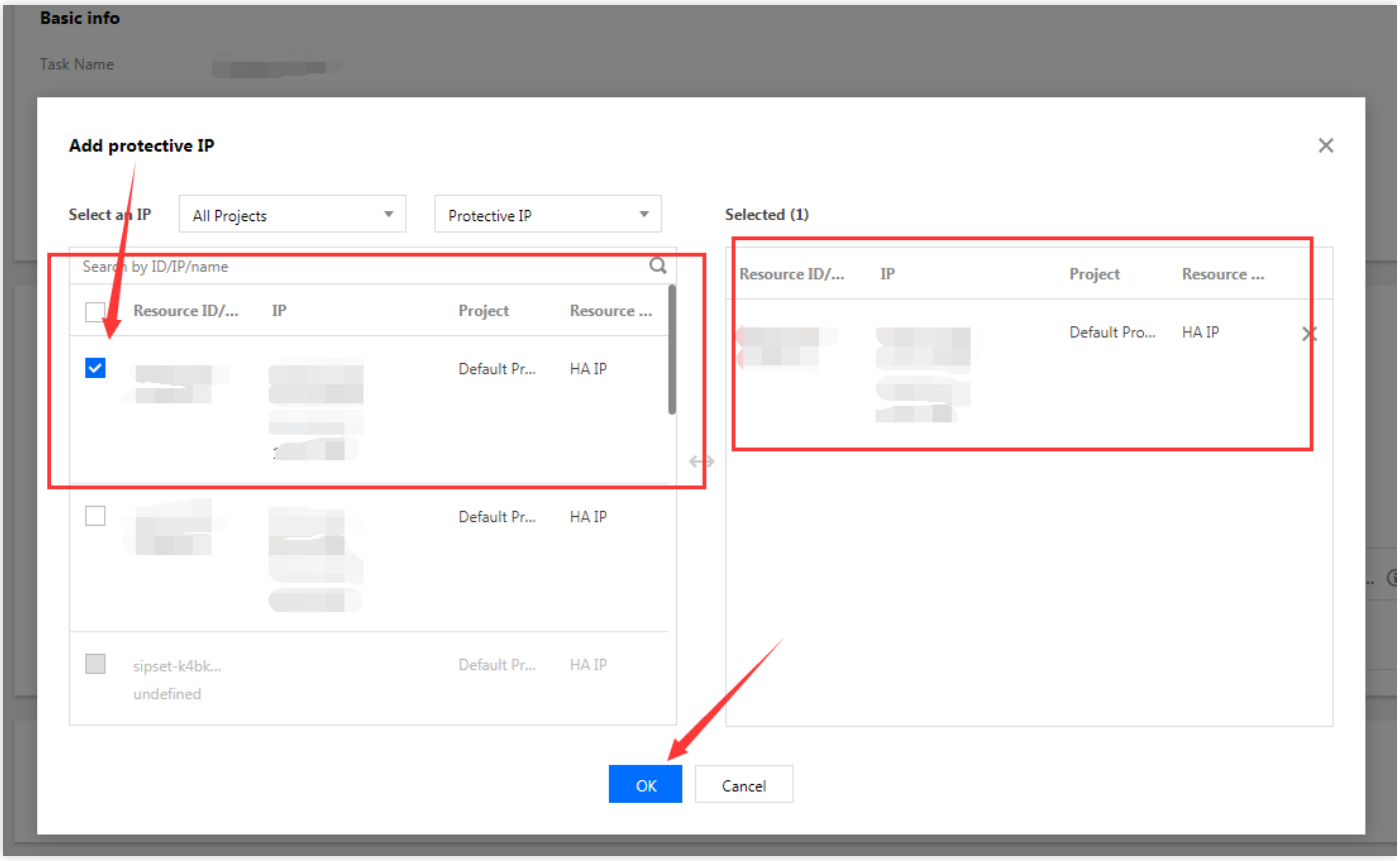
a. In the business domain name list management page, click "Add IP" to go to the business details page.



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



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

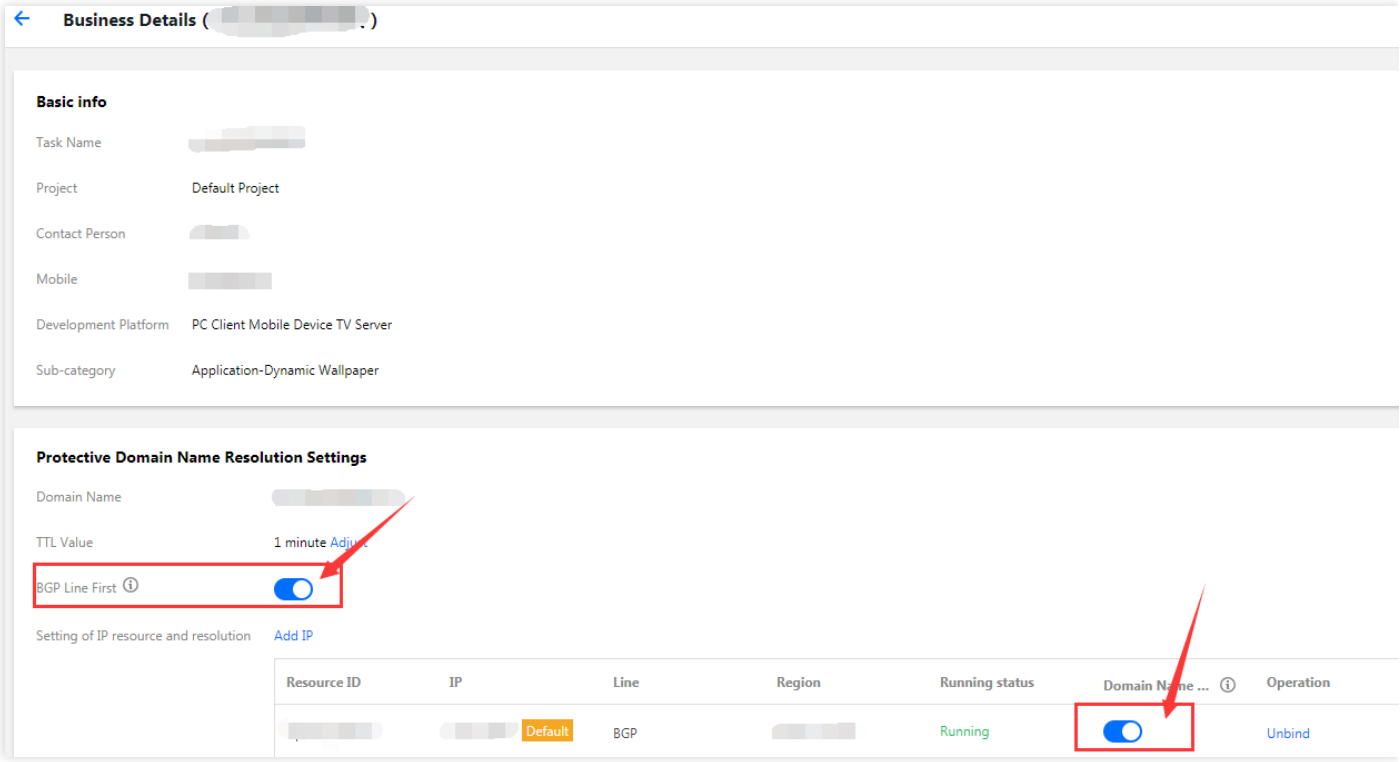


3. **Enable domain name resolution**

   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.



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.