Aegis Anti-DDoS

Getting Started

Product Documentation

Contents

Getting Started
Product Configuration Instructions

Last updated : 2018-12-21 12:01:56

Before purchasing a DDoS protective IP or protection pack, you need to confirm the following points:

Preparations and Selection

- DDoS protective IP
  DDoS protective IP uses proxy forwarding mode in which business traffic is pointed to the protective IP and then forwarded to the real server after being cleansed, achieving protection against DDoS attacks. Currently, DDoS protective IP can provide stable and secure protection against heavy-traffic DDoS attacks for Internet servers (including non-Tencent Cloud servers).
- DDoS protection pack
  DDoS protection pack is a security product that directly provides protection capabilities for a range of cloud products such as CVM. Unlike DDoS protective IP, it directly binds cloud protection services to cloud products, so you don't need to have a forwarding IP or configure port-to-port forwarding rules.

DDoS Protective IP

Confirm the protective IP region and network

- Region selection principle
  DDoS protective IP work in proxy forwarding mode. Therefore, please try to select a region near the physical location of your real server. The closer the protective IP region is to the real 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 protection bandwidth. BGP network provides a better network experience, but its protection bandwidth is lower than that of non-BGP protective IPs. The protection bandwidth of non-BGP IPs 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-ISP access.

Confirm the configuration scheme for protective IP

- Base protection bandwidth
  Prepaid. It is suggested that the base protection bandwidth be set to higher than the average historical attack traffic. This makes sure base protection is robust enough to prevent most attacks.
- Elastic protection bandwidth
  Pay-per-use on a daily basis. It is suggested that the elastic protection bandwidth 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 billed on a monthly basis and you only pay for what you use, significantly reducing the costs.
- Forwarded business traffic
  This is the non-attacking traffic of normal business requests forwarded to the real server. It can be charged by bandwidth or by traffic. It is recommended to select based on the characteristics of normal business traffic.

DDoS Protection Pack

Principle for Protection Pack Region Selection

- Region selection principle
  DDoS protection pack can only provide protection for Tencent Cloud public IPs in the same region where it is available. Therefore, please be sure to select the pack available in the region where your Tencent Cloud real server is located.

Confirm the configuration scheme for protection pack

- Protection scope
  You can choose single-IP or multi-IP mode. In single-IP mode, the protection pack can be bound to one Tencent Cloud public IP which utilizes the protection bandwidth exclusively. In multi-IP mode, the protection pack can be bound to multiple Tencent Cloud public IPs which share the resources. When multiple IPs are under DDoS attacks, if the bandwidth of the combined attack traffic is higher than the protection bandwidth, blocking will start from the IP address suffering the largest attack traffic.
- Base protection bandwidth
  Prepaid. It is suggested that the base protection bandwidth be set to higher than the average historical attack traffic. This makes sure base protection is robust enough to prevent most attacks.
- Elastic protection bandwidth
  Pay-per-use on a daily basis. It is suggested that the elastic protection bandwidth 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 billed on a monthly basis and you only pay for what you use, significantly reducing the costs.

- Elastic billing method
  Elastic protection supports two billing methods: elastic traffic pack and elastic bandwidth. An elastic traffic pack needs to be purchased in advance. If the attack exceeds the base protection bandwidth and elastic protection traffic is consumed, the usage amount will be deducted from the pack accordingly. Compared with the elastic bandwidth method, elastic protection packs can significantly reduce your costs of elastic protection in scenarios with low-frequency, high-bandwidth short attacks If your business is attacked frequently and the attack lasts for a prolonged time, you can choose to be billed by the elastic bandwidth which is pay-per-use on a daily basis.
- Elastic traffic pack
  If "elastic traffic pack" is selected as the billing method for elastic protection and elastic protection is triggered, the incurred elastic traffic will be deducted from a purchased elastic traffic pack in the same region. If no pack has been purchased or the purchased pack is used up, the elastic protection capability will be suspended.
- Elastic protection bandwidth
  If "elastic protection bandwidth" is selected as the billing method for elastic protection and elastic protection is triggered, you will be billed by the elastic protection bandwidth on a daily basis.

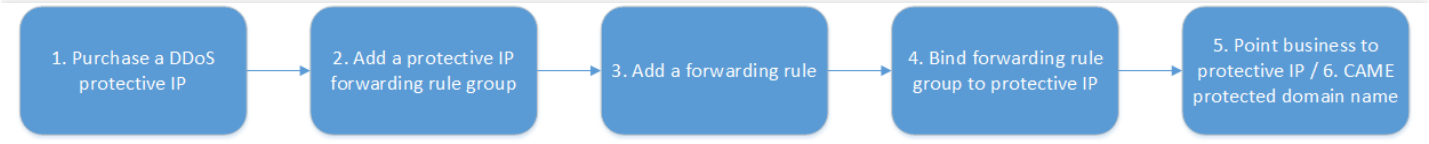
Configuring DDoS Protective IP

Last updated : 2020-01-14 11:10:30

The DDoS Protective IP product provides protection and traffic cleansing services against high-traffic DDoS attacks for Internet business servers through proxy forwarding. With simple configuration, you can point business traffic and attack traffic to a DDoS protective IP, so when the attack traffic passes through the protective IP, it will be detected and cleansed by the protection system, and then the clean business traffic will be forwarded to the business server, ensuring business availability in scenarios under DDoS attacks.

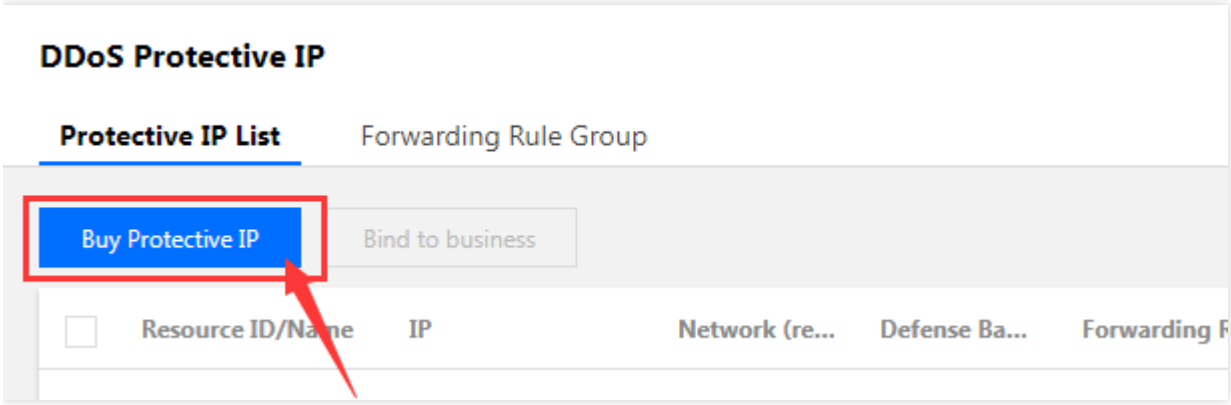
This document details the steps for configuring and launching a DDoS protective IP. For details on how to purchase a configuration, see Product Configuration Instructions.

Flowchart

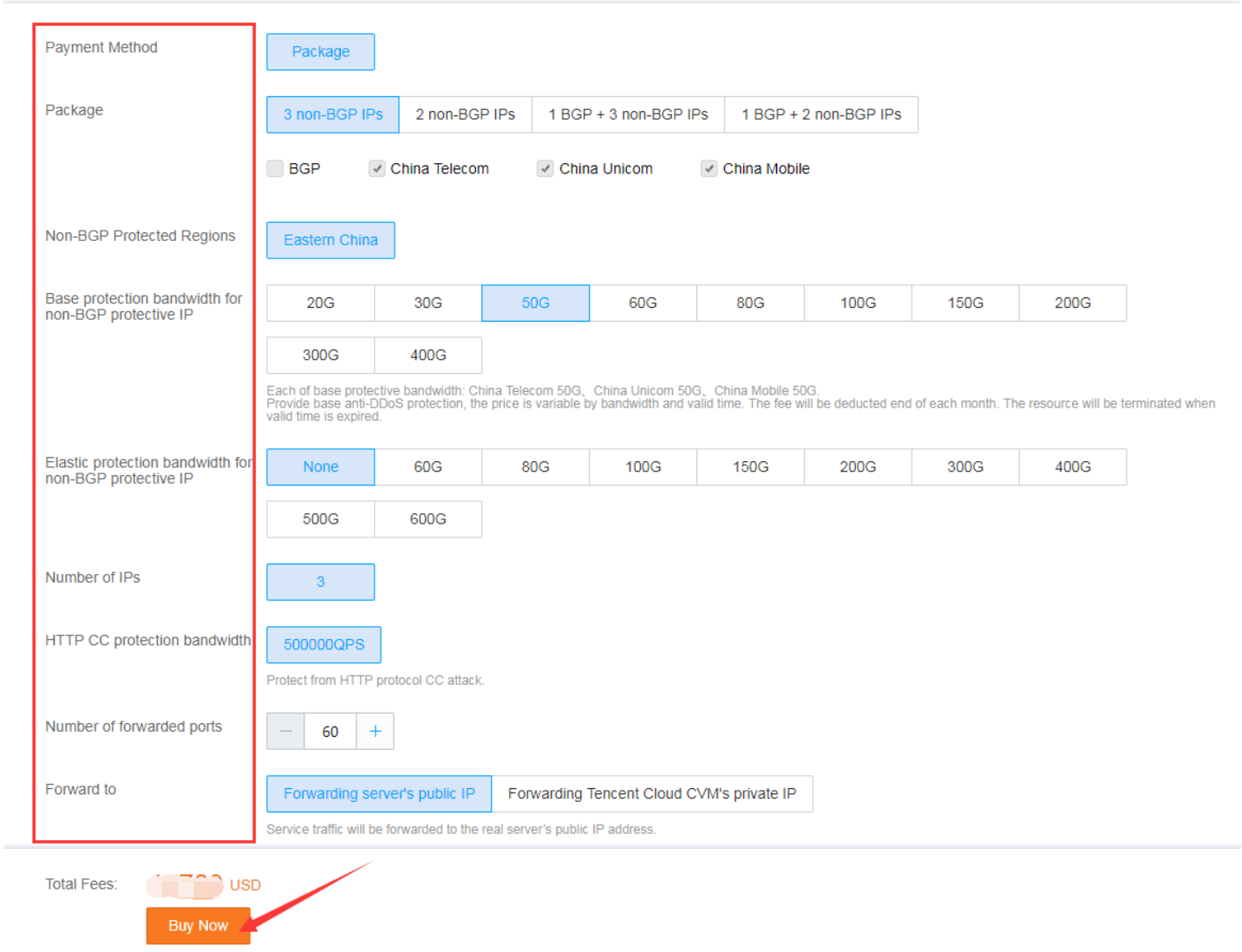


Access Steps

1. **Purchase a DDoS protective IP**
   a. Go to the Aegis Anti-DDoS Console, click **DDoS Protective IP* in the left pane, and click **Purchase Protective IP** under "Protective IP List".



b. Select the required configuration according to the business needs, confirm the configuration and click **Purchase Now**.

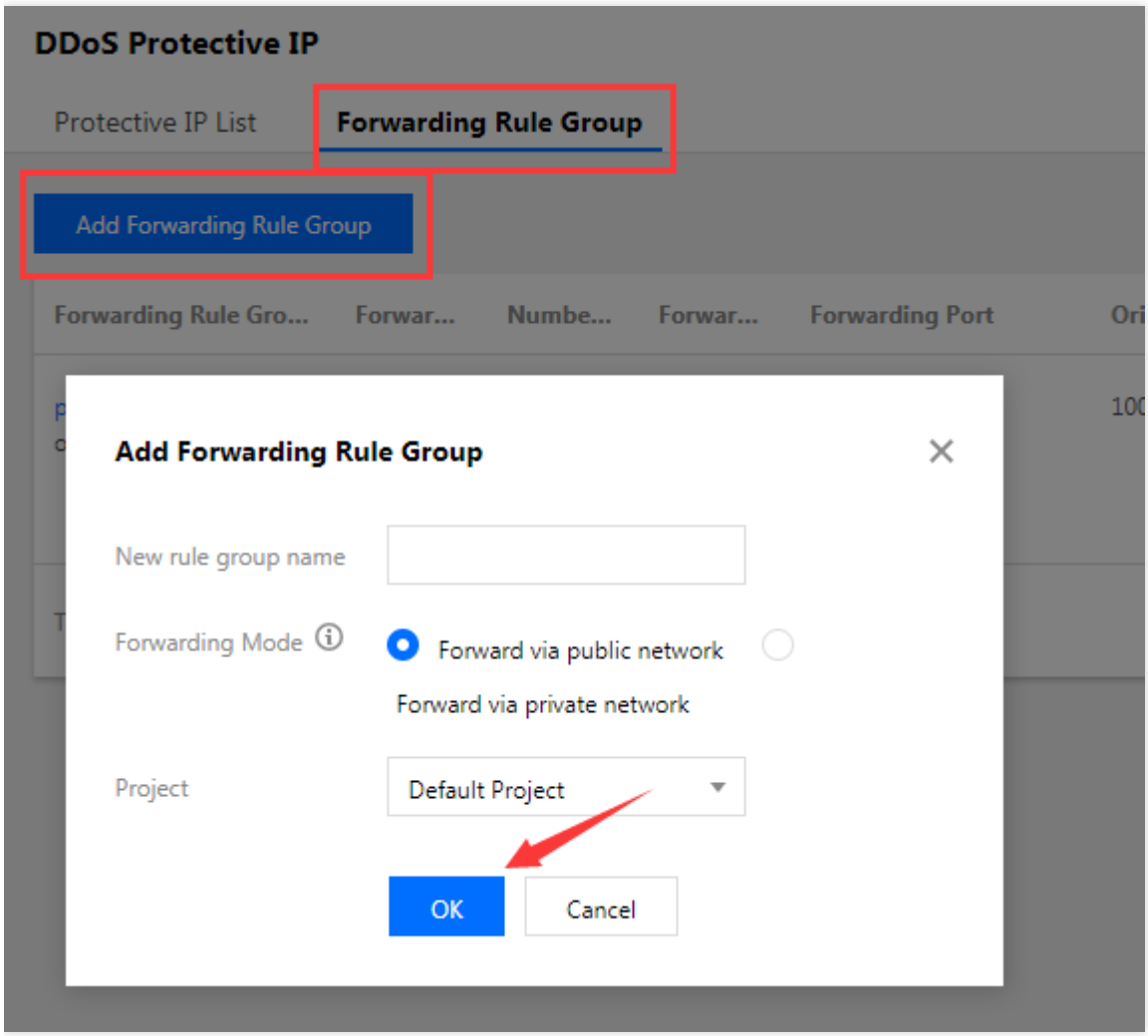


2. **Add a protective IP forwarding rule group**

a. On the "DDoS Protective IP" page, click **Forwarding rule group** and click **Add forwarding rule**

group.

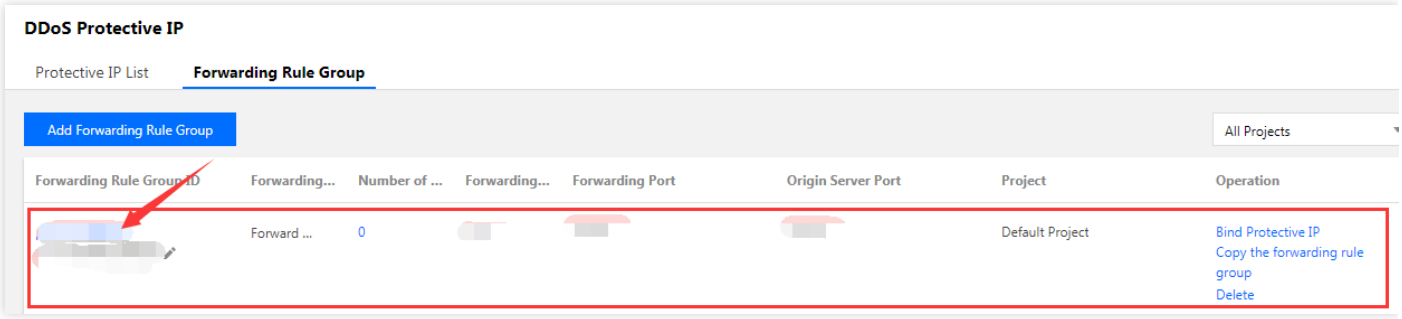
b. Enter "New rule group name", select the "Forwarding mode" and "Project" and click **OK**.



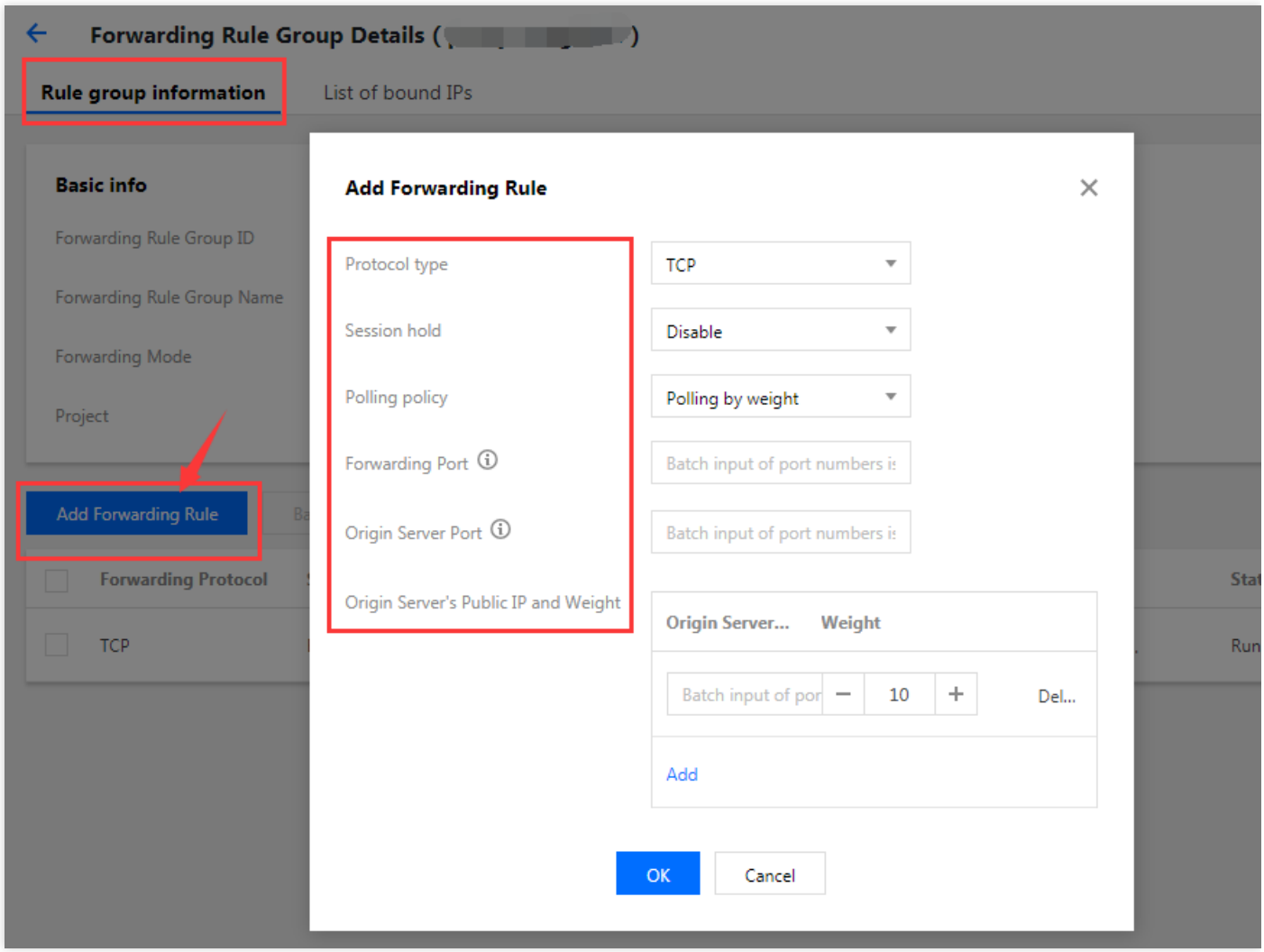
Note:
60 forwarding rules are provided free of charge by default for each forwarding rule group.

3. **Add a forwarding rule***

   a. After creating a forwarding rule group, click a **Forwarding rule group ID to enter the forwarding rule group details page.



b. Under **Rule group information**, click **Add Forwarding Rule** to add a rule based on layer 4 port forwarding. Based on the business protocol requirements, select the "Protocol type", configure "Session hold", select the appropriate "Polling policy", and enter the "Forwarding port" number, "Real server port" number and "Real server's public IP and weight" and click **OK**. Forwarding rules can be created and added in batches.

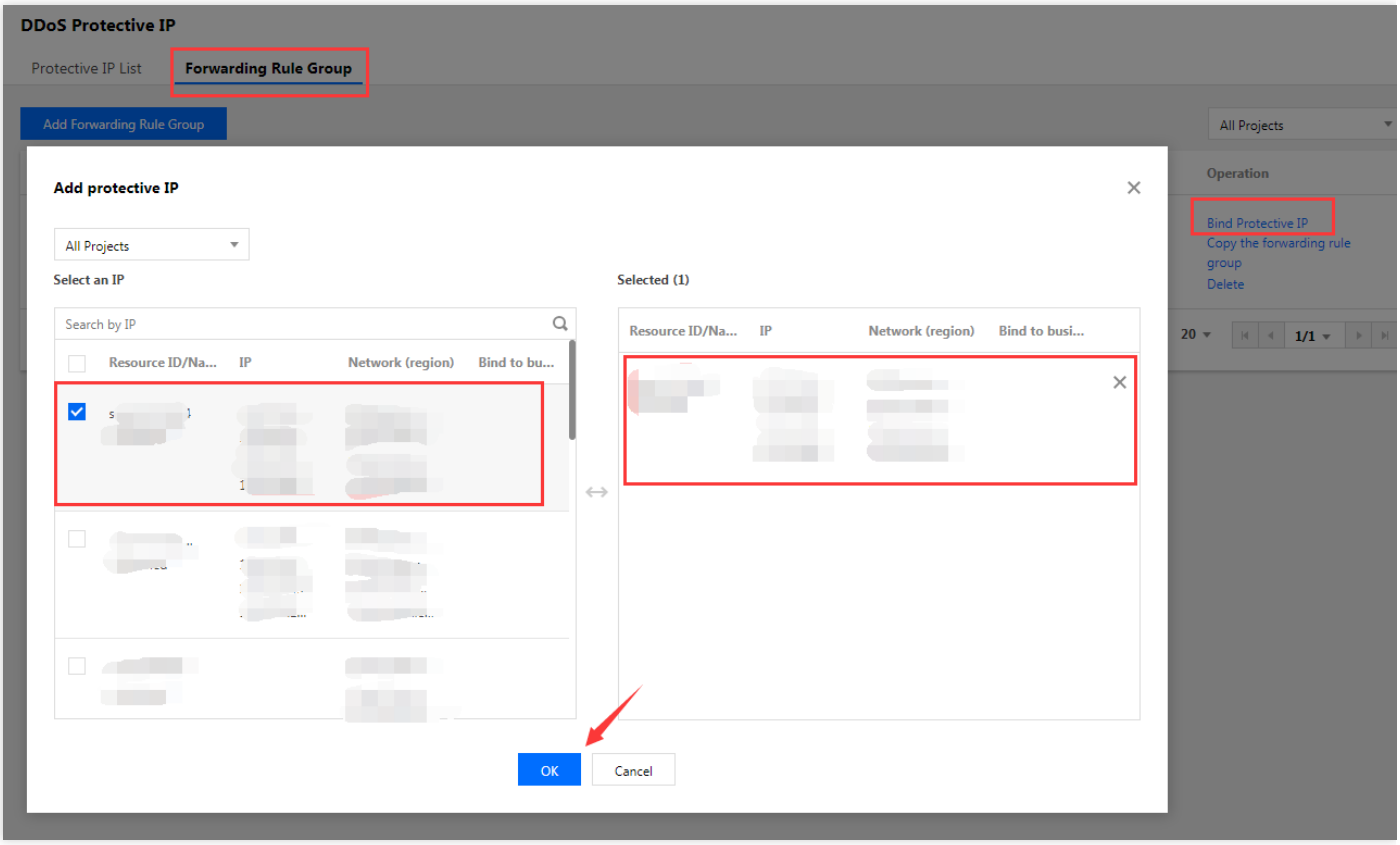


> **Note:**
> Each forwarding rule can be configured with 40 public IPs of the real server.

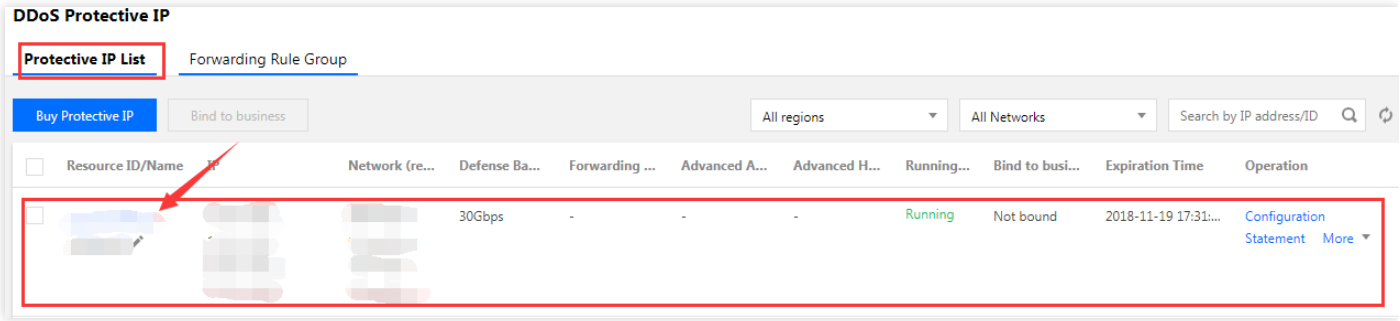
Protocol type: Select the protocol type (TCP or UDP) of the port of the service.
Session hold: Enabling session hold ensures that a series of related access requests are allocated to the same server. When there are multiple real server IPs under the same forwarding rule, if you want the same client's requests to be processed by the same server, you need to enable session hold.
Polling policy: When there are multiple real server IPs under the same forwarding rule, you can select polling by weight or polling by minimum number of connections to allocate the proportion of a backend real server for processing business requests. Polling by weight is to allocate based on the real server's IP weight; while polling by minimum number of connections is to allocate based on the minimum number of public IP connections.
Forwarding port: This refers to the port number that needs to provide services on the protective IP. The client's or user's business requests directly access the port of the protective IP.
Real server port: In contrast with the forwarding port, this refers to the port number that provides services on the real server. The protective IP forwards the user's business requests on the forwarding port to the real server port defined by the real server IP.
Real server's public IP and weight: This refers to the IP address of the backend real server that provides services. When there are multiple public IPs of the real server, the protective IP will poll the business request to each real server IP. The set weight represents the proportion of the requests processed by a real server IP. The bigger the weight, the more requests received.

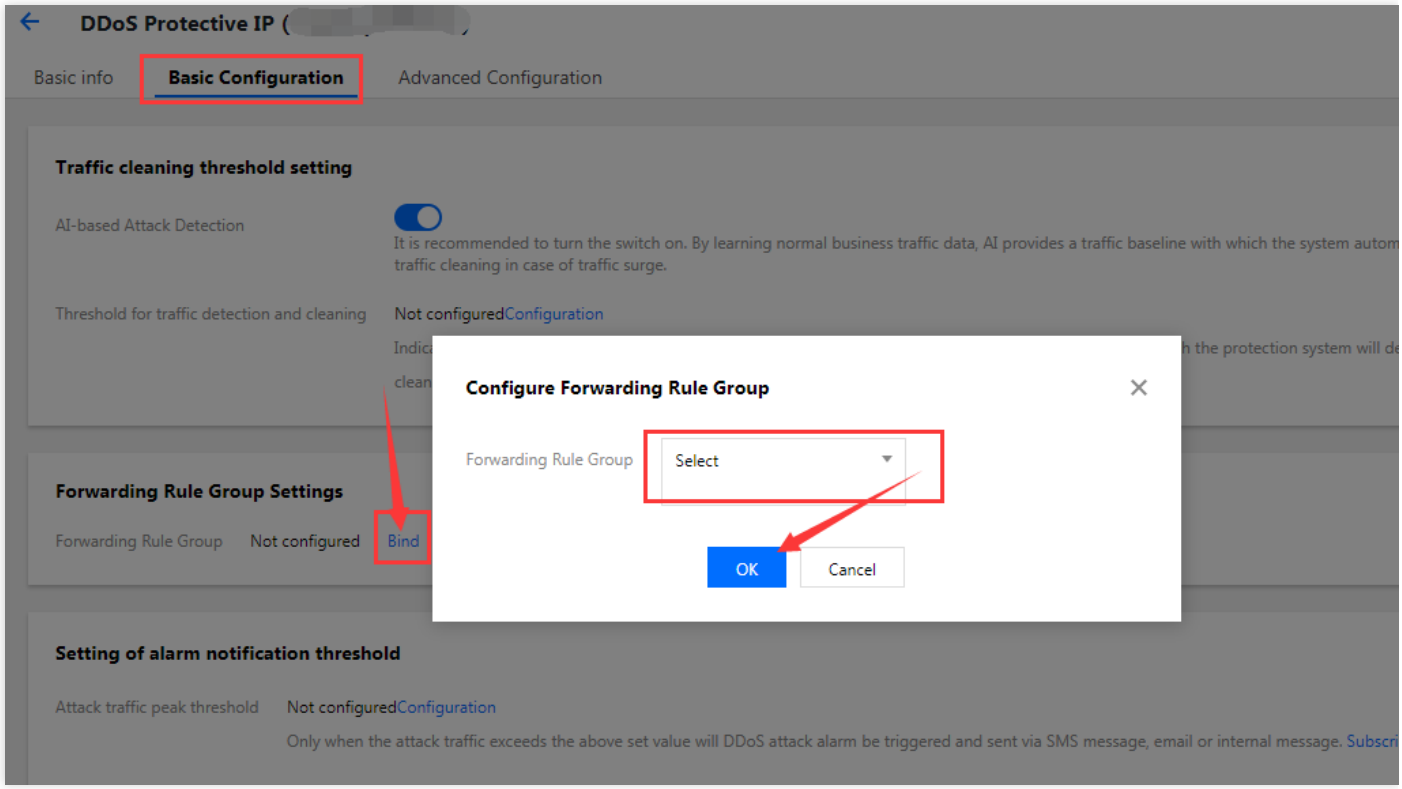
> **Note:**
> - If there are multiple forwarding rules, they can be created in batches. Enter multiple port numbers in the forwarding port and real server port boxes and separate them with commas. Forwarding rules will created one by one in port order.
> - The following port numbers are reserved for the forwarding cluster and cannot be added as forwarding ports: 843, 3306, 1433, 1434, 36000, 56000 and 3389.

4. **Binding Forwarding Rule Group to Protective IP**
   After creating a forwarding rule group, under "DDoS Protective IP", click **Forwarding Rule Group**. In the "Operation" column, click **Bind Protective IP** to bind the forwarding rule group to a protective IP.



You can also click **DDoS Protective IP** and select a protective IP to enter the DDoS protective IP details page. Then, click **Basic Configuration**, click **Bind** under "Forwarding Rule Group Settings" and click **Bind** to bind the forwarding rule group to the protective IP.





5. **Pointing Business to Protective IP**

   After binding a forwarding rule group to the protective IP, you can verify the connectivity from the protective IP's forwarding port to the real server's real server port. Point the business to the protective IP to complete the protective IP accessing configuration. If your business uses DNS service, you can change the DNS in your business' DNS service provider and replace the original IP address with the bound protective IP address.

   After completing the configuration, your real server is protected by protective IP.

6. **CNAME Protected Domain Name**

   You can also create a free protected domain name and resolve to it for access by adding a CNAME

record at your business' DNS service provider. For configuration details, see **Binding a Protected Domain Name to a Protective IP**.

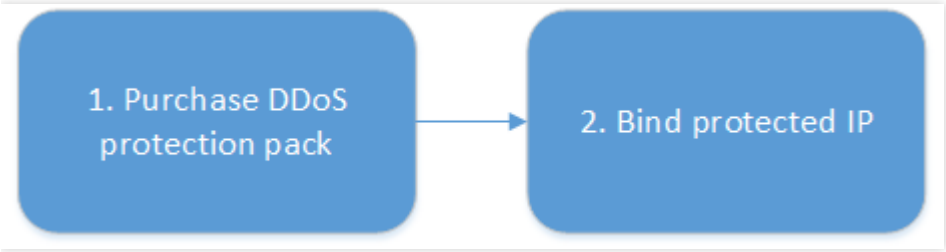
Configuring DDoS Protection Pack

Last updated : 2020-01-14 11:11:37

Aegis DDoS protection pack provides protection capabilities for Tencent Cloud's public IP addresses, including CVM, CLB, CPM, BM CLB, NAT IP, EIP and GAAP IP. It enables convenient and quick protection configuration for scenarios where the business IP address cannot be changed or there are a large number of IPs to be protected. Currently, it works in both single-IP mode and multi-IP mode.

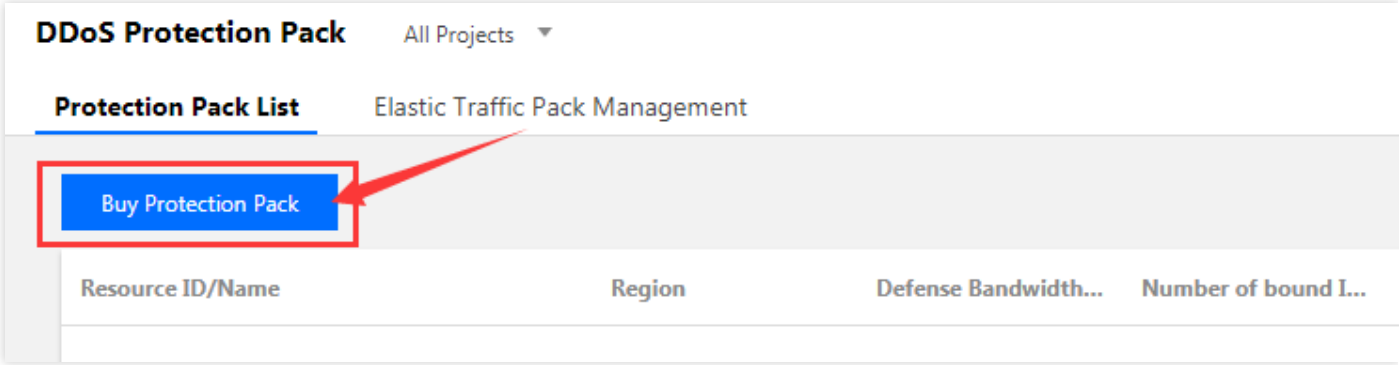
This document details the steps for configuring and accessing a DDoS protection pack. For details on how to purchase a configuration, see Product Configuration Instructions.

Flowchart

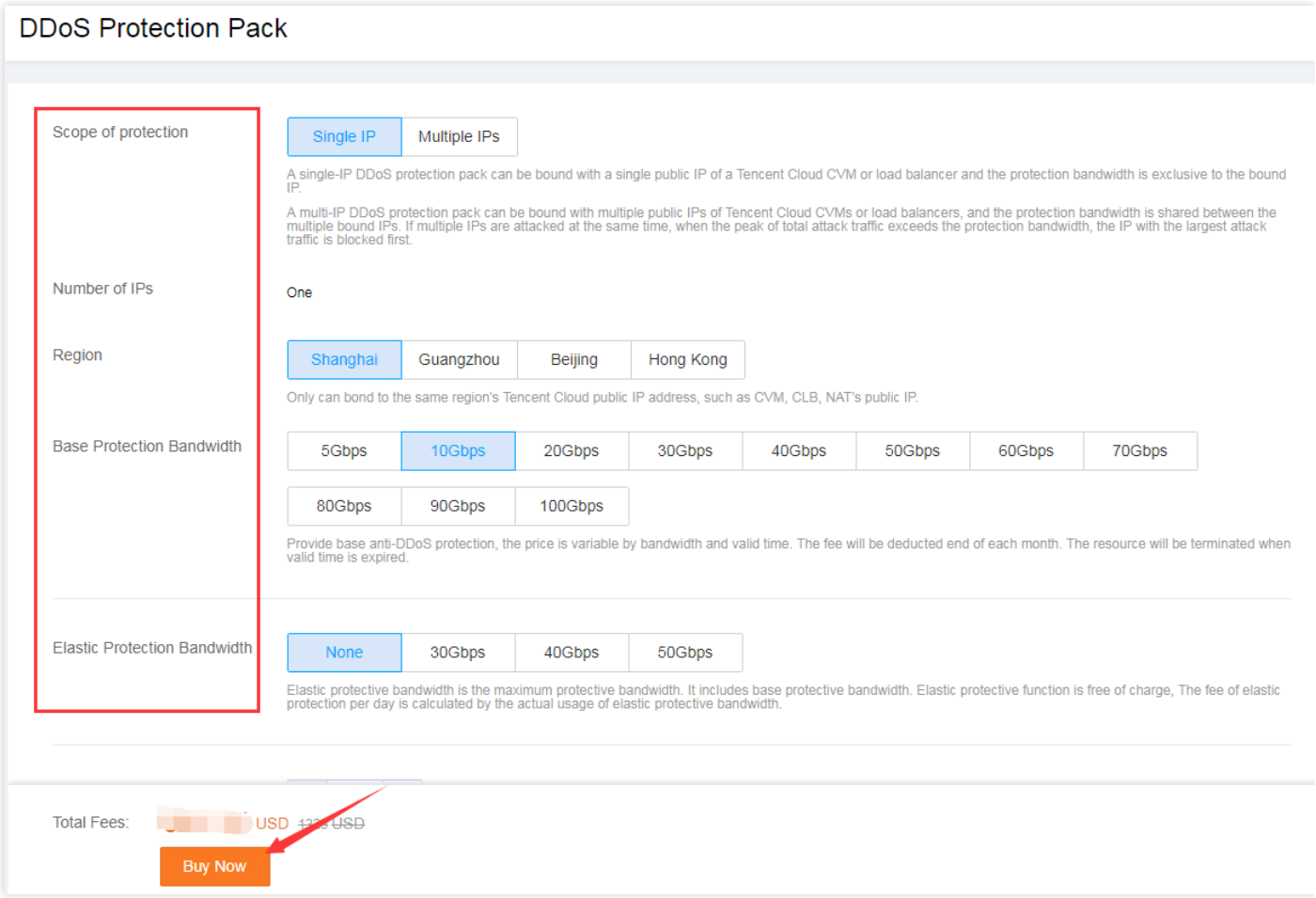


Access Steps

1. **Purchase a DDoS protection pack**
   a. Go to the Aegis Anti-DDoS Console, click **DDoS Protection Pack* in the left pane, and click **Purchase Protection Pack** under "Protection Pack List".



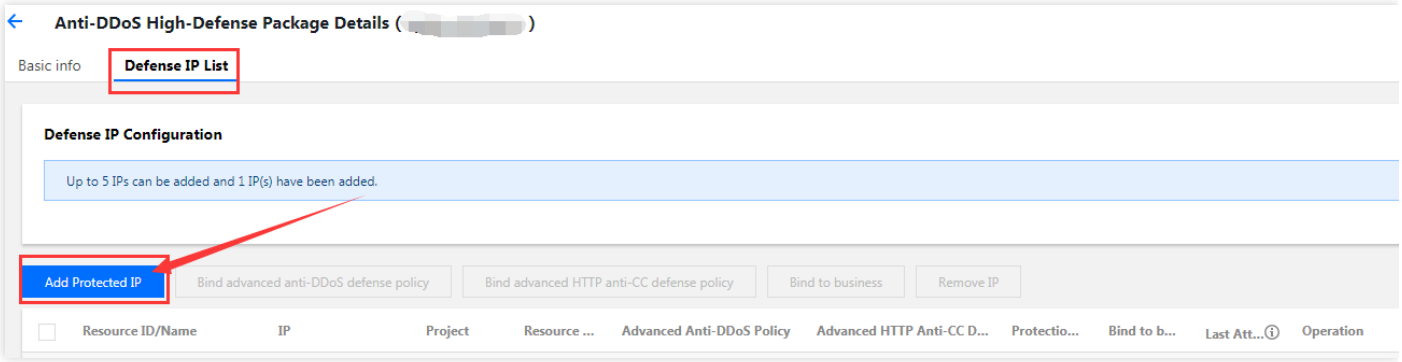
b. Select the configuration and click **Purchase Now**.



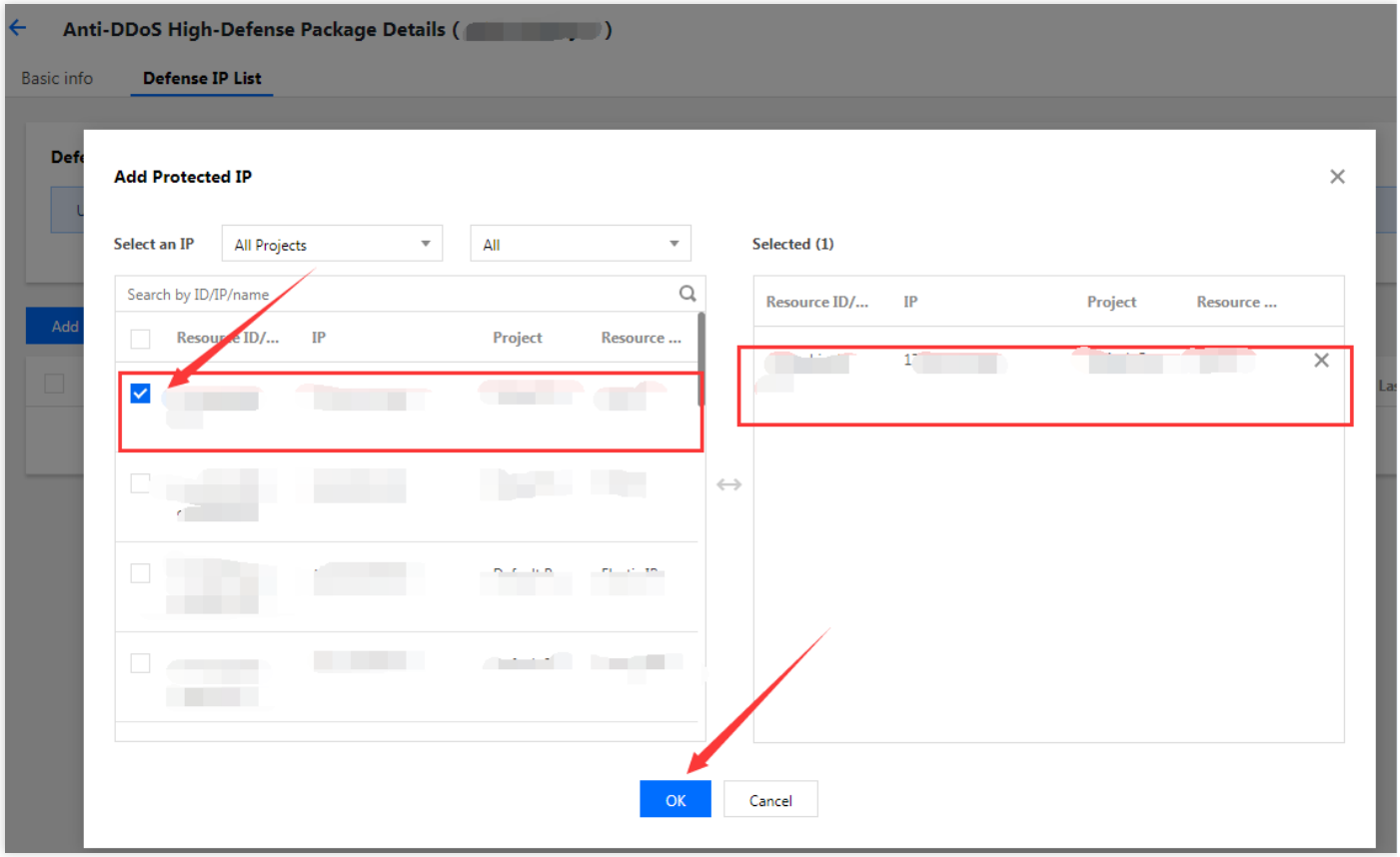
2. **Bind a protected IP**

a. On the "DDoS Protection Pack" page, click a protection pack ID under the "Protection Pack List" to enter the basic information page.

b. On the DDoS protection pack details page, click **Protected IP List** and click **Add Protected IP**.

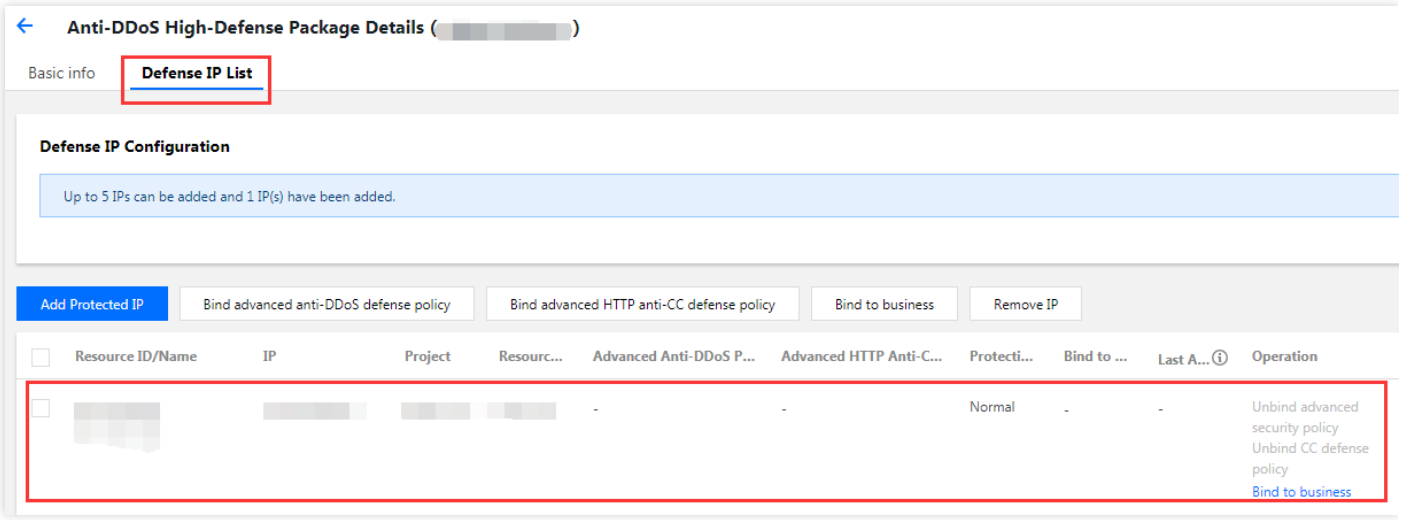


c. In the "Add Protected IP" pop-up, select the IP address of the CVM instance and click **OK**.



d. After successful addition, you can see that the IP address is protected by the DDoS protection

pack under the **Protected IP List**.



Customizable Advanced Security Policies

Last updated : 2020-07-30 11:36:59

Aegis Anti-DDoS provides a basic security policy by default, which can effectively cope with common DDoS attacks based on algorithms such as AI engine, IP profiling and behavior pattern analysis. It also provides advanced policies that can be customized based on business characteristics or attacking behaviors in case of certain special or masquerading attacks, which can achieve more targeted protection against specific attacks.

Advanced policies can be bound to protective IPs and IPs protected by protection packs. Based on your own needs, you can configure Advanced security policies, HTTP anti-CC defense policies and watermark protection. When an attacking behavior contained in the current business request is detected, the attack traffic will be cleansed according to the configuration of the advanced policy.

Custom Advanced Security Policy

Advanced security policy	Anti-CC defense policy
Protocol disabling	HTTP QPS request threshold
Port disabling	Blocklist/allowlist configuration (URL, IP)
IP blocklist/allowlist	Custom anti-CC defense
Message characteristic filtering	Match mode: blocking, human-machine verification
Overseas traffic disabling	Speed limit mode: source IP access speed
Null session protection	-

Advanced Security Policy

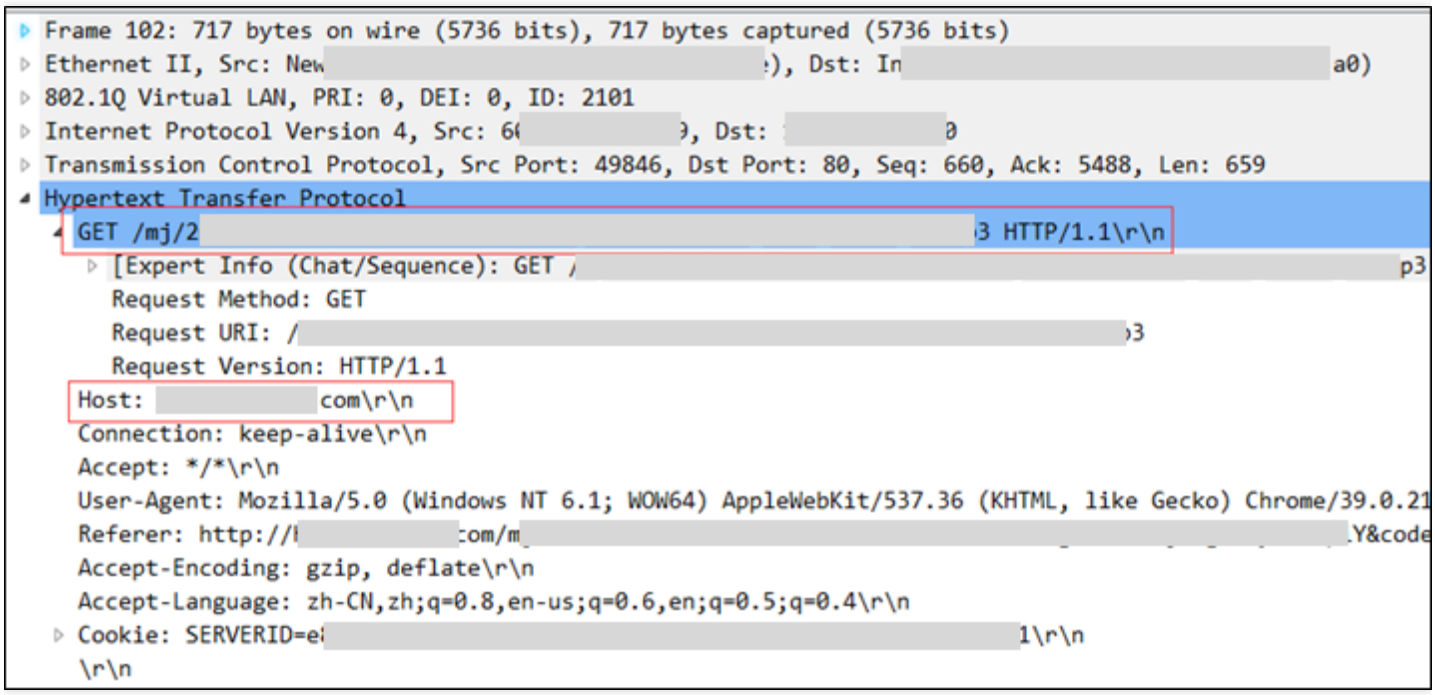
- Protocol or port disabling
  You can disable protocols or ports that are not used by the business. When an attack is detected, the protection system will cleanse the traffic of the disabled protocols or ports.
- IP blocklist/allowlist configuring
  Business traffic from IPs in the allowlist will not be detected for attacks or cleansed by the

protection system, while traffic from IPs in the blocklist will be cleansed. Up to 50 IP addresses can be added to the IP blocklist/allowlist.

- Message characteristic filtering
  You can configure a policy with message length or message length + payload as conditions for characteristics of business or attack messages. When the system detects that a message matches the policy condition, it can perform operations such as discarding, blocking the source IP or disconnecting.
- Null session protection
  This addresses null session attacks. If null session protection is required for the IPs protected by protection packs, it can be enabled accordingly.
- Rejecting traffic from outside China
  TCP traffic requests from outside China (Mainland China, Hong Kong (China), Macau (China) and Taiwan (China)) can be rejected.

Case description:

The following is a normal business message.



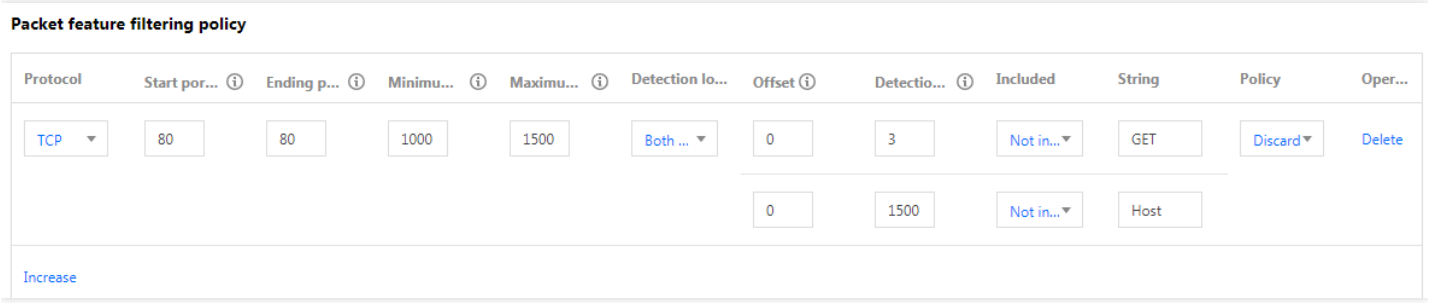
After analysis, its characteristics are as follows:

- The destination port is 80.
- The packet length is 1000 bytes or below.
- The payload starts with "GET" and carries a "Host" field.

You can configure a message characteristic filtering policy to block messages that don't meet the normal business characteristics.
Messages that meet the following conditions:

- The destination port is 80.
- The packet length is 1000 bytes or above.
- The payload doesn't start with "GET" and doesn't carry a "Host" field.

Executed operation:
If a message meets all the conditions above at the same time, it will be blocked.



CC Protection Policy

- HTTP request threshold
  CC protection is triggered when the number of HTTP requests exceeds the set QPS value.
- URL allowlist
  The protection system doesn't perform CC attack detection and protection on allowed URLs.
- IP blocklist/allowlist
  HTTP access requests from IPs in the allowlist will not be detected for CC attacks or prevented by the protection system, while those from IPs in the blocklist will be rejected. Up to 50 IP addresses can be added to the IP blocklist/allowlist.
- Custom anti-CC defense
  This mainly blocks or requires human-machine verification for HTTP requests that have specific fields in the header.
  - Match mode: If an HTTP request with the specified field header is detected, it will be blocked or processed for human-machine verification.
  - Speed limit mode: The speed of access requests from the source IP will be limited. It supports configuring speed limit globally or for source IPs of specified URLs. After configured, when all the source IPs access the protective IP (or IP of a protection pack) bound to this policy, the access frequency will be controlled for speed limit by the configured value. If configured as 0, it

is not enabled. A policy for speed limit for specified URLs has a higher priority than a global speed limit policy.

Watermark Protection

- Protected IP
  The business traffic accessing this IP and the specified port is detected for watermark, and the attack messages are discarded.
- TCP protection port and UDP protection port
  A TCP/UDP protection port can be configured with up to five port ranges. Different port ranges cannot overlap one another. If the starting and ending port numbers are the same, a range will be considered as one port. You need to configure at least one of the TCP or UDP port ranges.
- UDP watermark stripping
  Select "Automatically strip watermark from UDP message". After the data message passes through the security protection system, the watermark in a UDP message is automatically stripped and then transferred to the real server. You can also configure the offset (0-100) of the specified watermark tag in the UDP message. Note: If the protection system is not required to strip the UDP watermark, the server side needs to be modified for watermark stripping.
- Allowlist
  Select "Enable source IP allowlist" to add an IP. Watermark detection is not performed for messages from the IPs in the allowlist.

You can efficiently and comprehensively protect against layer 4 CC attacks such as masquerading and replay attacks by accessing watermark protection.

- The watermark algorithm and key are shared between the business side and the Aegis protection system.
- A watermark is embedded in every message sent by the client, while the attack messages have no watermark.
- The protection system can easily identify and discard the attack messages.