Anti-DDoS Advanced

DDoS Edge Protection

Product Documentation

Contents

DDoS Edge Protection Product Introduction Overview

Last updated : 2021-11-15 11:53:03

DDoS Edge Defender protects your business outside the Chinese mainland from different types of DDoS attacks with volumes of attack traffic. Combined with DDoS, CC and basic application layer protection capabilities, it helps keep the network layer, transport layer (L3 and L4) and application layer (L7) safe. By L4 ports or L7 domain names to access to edge protection and configure forwarding rules, attack traffic can be routed to Tencent Cloud cleansing centers for cleansing, enuring your business stable and available.

DDoS Edge Defender owns multiple Tencent Cloud entries around the world for handling bandwidth needs with all-out protection, making access to each node as smooth as possible. It provides near-source cleansing and near-source reinjection, with up to TB-level protection capability, and ensures smooth traffic and low latency by cleansing attack traffic and then forwarding normal traffic back to the real server close to the region of your instance deployed.

Note :
DDoS Edge Defender is currently available to beta users. To use it, please contact us.

Key Features

Multi-dimensional protection

Protection Types	Description
Malformed packet filtering	Filters out frag flood, smurf, stream flood, and land flood attacks as well as malformed IP, TCP, and UDP packets.
DDoS protection at the network layer	Filters out UDP Flood, SYN Flood, TCP Flood, ICMP Flood, ACK Flood, FIN Flood, RST Flood and DNS/NTP/SSDP reflection attacks and null sessions.
DDoS protection at the application layer	Filters out CC attacks and slow HTTP attacks and supports HTTP custom filtering such as host filtering, user-agent filtering, and referer filtering.

Security protection policy

DDoS Edge Defender provides basic security policies by default on the basis of protection algorithms such as IP profiling, behavior pattern analysis, and AI-based smart recognition, effectively coping with common DDoS attacks. It also offers diverse and flexible protection policies, which can be tailored to your special needs to deal with ever-changing attack tricks.

Protection statistical reports

DDoS Edge Defender provides multi-dimensional traffic reports and attack protection details to help you stay on top of the protection effects of the instances in a timely and precise manner.

> Note :
> Only DDoS, CC and basic application layer attacks can be defended against, and related reports are supported.

Strengths

Last updated : 2021-09-28 15:53:26

Wide Applicability

DDoS Edge Defender supports protecting website and non-website business and Tencent Cloud and non-Tencent Cloud business covering finance, ecommerce and gaming, satisfying your security needs for business.

Massive Protection Resources

DDoS Edge Defender, combined with multiple cleansing nodes outside the Chinese mainland, supports TB-level protection capability globally that provides security and stability for essential businesses such as promotional campaigns and launch events.

Leading Cleansing Capability

Leveraging the powerful protective clusters developed by Tencent and multi-dimensional algorithms, such as IP profiling, behavior pattern analysis, and cookie challenges, DDoS Edge Defender can accurately and promptly detect attack traffic. With the aid of a smart AI engine that continuously optimizes the algorithms, it is also flexible in coping with attack tricks.

Stable Access Experience

Tencent Cloud supports forwarding traffic to the real server with the BGP proxy, GRE tunnel, Direct Connect tunnel and internet tunnel, which can easily address access latency and ensure network quality. It also supports smart routing and automatic network scheduling, delivering a stable and smooth access experience for various user groups.

Detailed Protection Reports

DDoS Edge Defender provides multi-dimensional statistical reports to display clear and accurate protection traffic and attack details, helping you stay on top of attacks in real time.

Lower Security Protection Costs

DDoS Edge Defender charges you for the basic protection plan and the traffic you used, which helps reduce your security cost.

Use Cases

Last updated : 2021-09-28 15:53:25

DDoS Edge Defender protects your business outside the Chinese mainland including gaming, ecommerce and website business. It is important to deliver a good real-time user experience especially for real-time battle games, online finance and e-commerce while keep the network layer, transport layer (L3 and L4), and application layer (L7) safe from DDoS attacks, including their ports, domain names and IPs.

Gaming

DDoS attacks are particularly common in the gaming industry outside the Chinese mainland. DDoS Edge Defender guarantees the availability and continuity of games to deliver a smooth player experience. Meanwhile, it helps ensure that normal gaming continues throughout events, new game releases, and peak hours such as holidays.

Ecommerce

The ecommerce industry outside the Chinese mainland has been worldwide with increasing global visits and orders during festivals and promotional campaigns. DDoS Edge Defender safeguards the continuity and security for global business, especially during major ecommerce promotions.

Website

DDoS Edge Defender guarantees smooth access to websites and uninterrupted global business, maintaining a stable and safe performance for daily visits and burst visits during special festivals or events and beating DDoS extortion attacks.

Purchase Guide
Billing Overview

Last updated : 2021-09-28 15:53:25

Billing Method

DDoS Edge Defender protects Tencent Cloud and non-Tencent Cloud business outside the Chinese mainland with unlimited times of protection. DDoS Edge Defender adopts a billing combination consisting of the basic protection plan plus user traffic usage.

Billing Item	Billing Mode	Payment Mode	Payment Description
Basic protection plan	Monthly subscription	Prepaid	A total of ten instances with Anycast IP and CNAME record types can be created. Each instance is provided with 500 port forwarding rules and 500 domain name forwarding rules.
User traffic	Pay by traffic	Pay-as-you-go	You will pay for the traffic you used. See below for details

Billing Details

- Basic protection plan: 2770 USD/month for a root account
- Traffic pricing is based on a monthly cumulative tier as follows:

Traffic Tier (USD/GB)	South America (SA)	Middle East (ME)	Asia Pacific Zone 3 (AP3)	Asia Pacific Zone 2 (AP2)	Asia Pacific Zone 1 (AP1)	Europe (EU)	North America (NA)	Africa (AA)
0–2 TB	0.128	0.162	0.12	0.108	0.094	0.071	0.071	0.128
2–10 TB	0.122	0.151	0.115	0.102	0.086	0.063	0.063	0.122
10–50 TB	0.115	0.1742	0.111	0.095	0.08	0.057	0.057	0.115

Traffic Tier (USD/GB)	South America (SA)	Middle East (ME)	Asia Pacific Zone 3 (AP3)	Asia Pacific Zone 2 (AP2)	Asia Pacific Zone 1 (AP1)	Europe (EU)	North America (NA)	Africa (AA)
50–100 TB	0.109	0.132	0.105	0.086	0.074	0.051	0.051	0.109
100–500 TB	0.098	0.118	0.089	0.072	0.066	0.04	0.04	0.098
500–1000 TB	0.094	0.114	0.085	0.068	0.062	0.035	0.035	0.094
> 1 PB	0.089	0.109	0.08	0.063	0.057	0.031	0.031	0.089

Billing Sample

Assume that you have purchased DDoS Edge Defender service and consumed 4 TB of traffic (1 TB consumed in SA and 3 TB consumed in AP3) in the current month, the billing formula is as follows:

- Basic protection plan (prepaid): 2770 USD
- User traffic (pay-as-you-go):
  - Traffic consumed in SA falls into the 0–2 TB tier, resulting in a charge of 128 USD (0.128 USD/GB * 1 TB).
  - Traffic consumed in AP3 falls into the 0–2 TB and 2–10 TB tiers, resulting in a charge of 355 USD (0.12 USD/GB * 2 TB + 0.115 USD/GB * 1 TB).
- The total cost is summed by the fixed cost of basic protection plan plus the traffic usage cost, that is 3253 USD (2770 USD + 128 USD + 355 USD).

Purchase Guide

Last updated : 2021-11-15 11:50:48

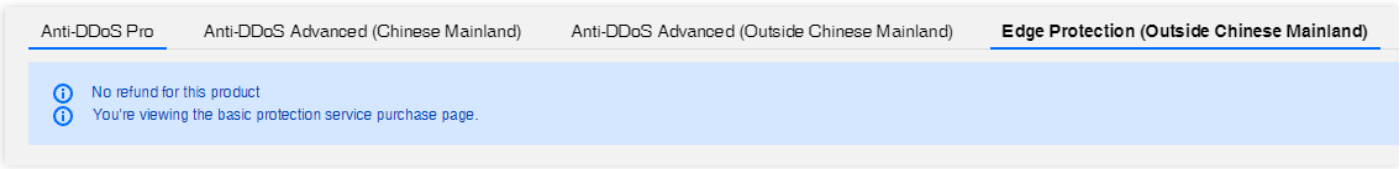
Prerequisites

Before purchasing a DDoS Edge Defender instance, you have signed up for Tencent Cloud and completed identity verification.

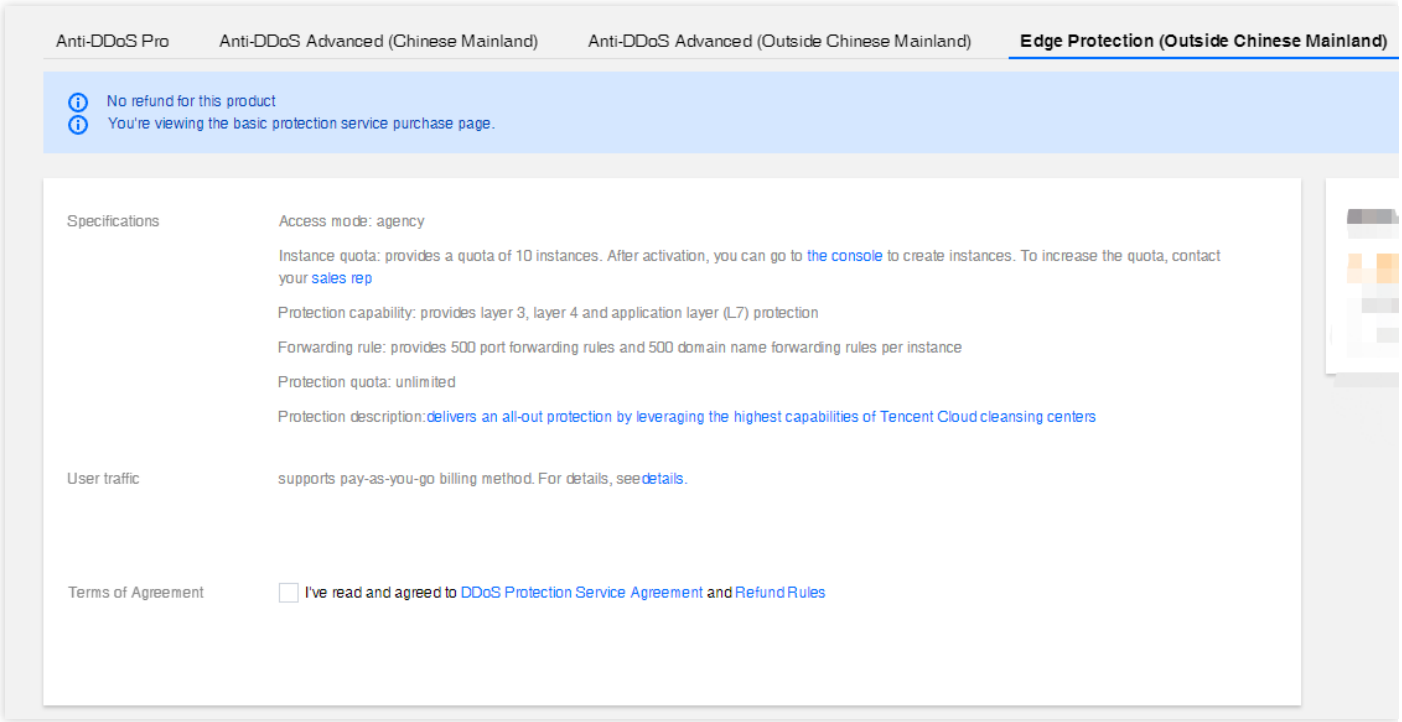
> Note :
> DDoS Edge Defender is currently available to beta users. To use it, please contact us.

Directions

1. Enter the DDoS Edge Defender (Outside Chinese Mainland) purchase page.
2. Select **Edge Defender (Outside Chinese Mainland)**.



3. Read the terms of agreement prior to checking the box.



4. Click **Pay Now** to complete your purchase.

Refund

Last updated : 2021-10-18 15:45:48

DDoS Edge Defender does not support a five-day unconditional refund. If you have bought this product, you cannot cancel and return your order.

Operation Guide
Viewing Protection Overview

Last updated : 2021-11-15 10:31:29

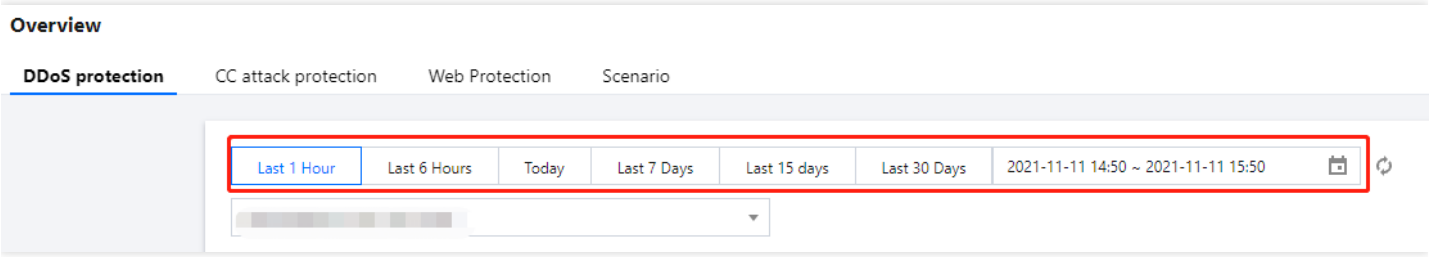
After connecting your application to and routing its traffic to the DDoS Edge Defender service, you can view the DDoS, CC, and web protection states and the application traffic state on the console.

> Note :
> DDoS Edge Defender is currently available for beta users. To use it, please contact us.

Viewing DDoS Protection Details

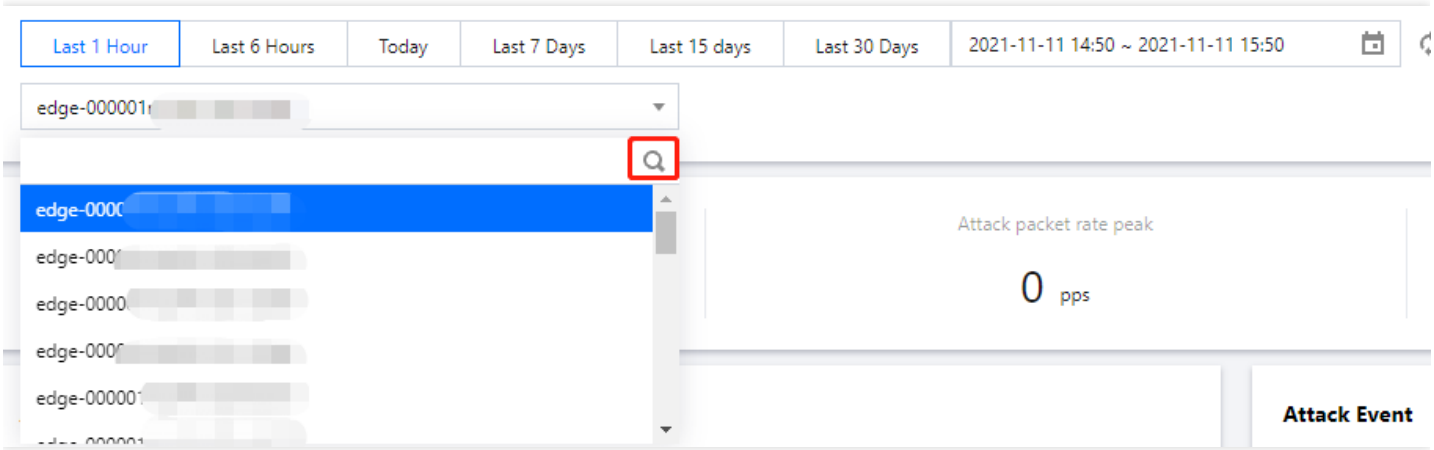
1. Log in to the DDoS Edge Defender Console, click **Overview** on the left sidebar, and then select **DDoS Protection**.
2. On the **DDoS Protection** page, select a query period.

> Note :
> You can query attack traffic and DDoS attack events in the past 180 days.

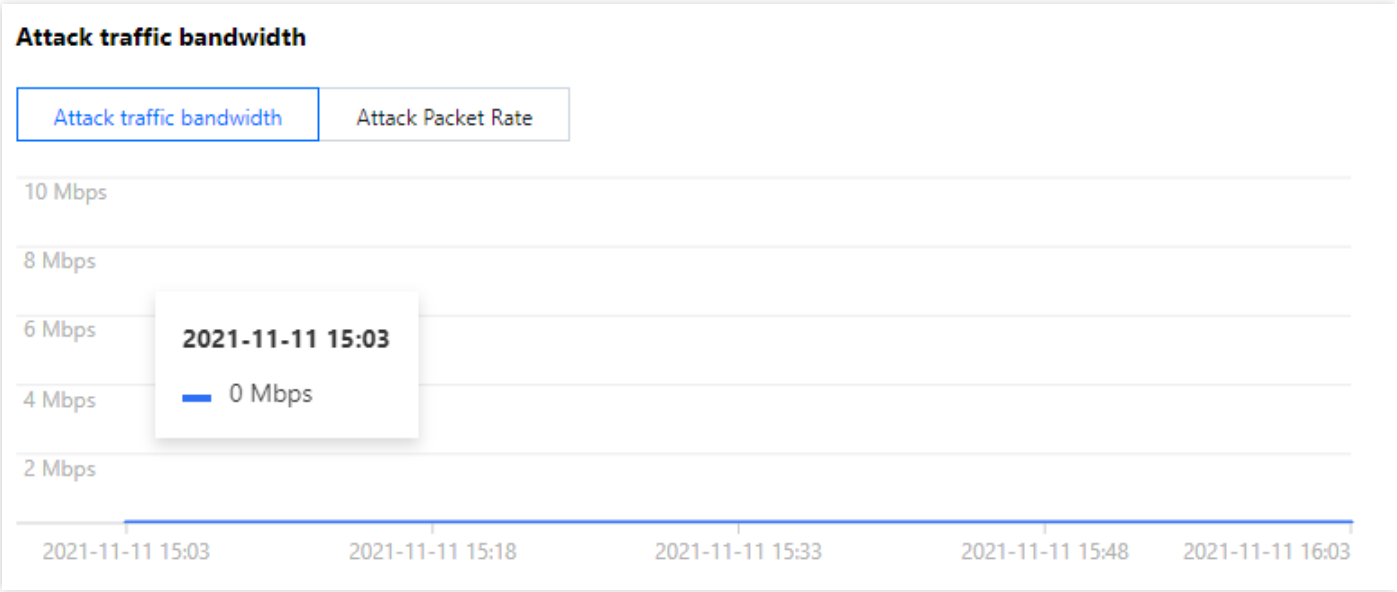


3. Click to search the protected instance in the drop-down list and view whether it is hit by DDoS

attacks.



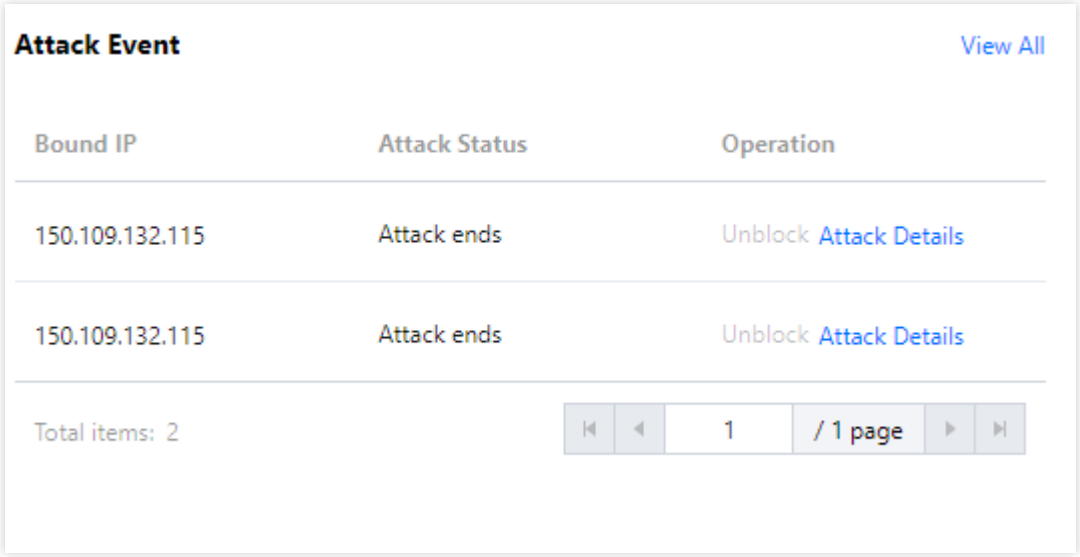
- **Attack Traffic Bandwidth**
  Displays the changes of the attack traffic bandwidth/attack packet rate within the selected time period. As shown below, you can spot a spike in the bandwidth trend graph when the instance is attacked.



- **Attack Event**
  Displays the start time, duration, type and status of an attack event.

> Note :
>
> - Only the details of a single attacker IP can be queried.

- Attacker IP information is randomly collected for statistics. The data will appear around 5 minutes after an attack ends.



- **Attack Statistics**
  Displays the total number of attacks, attack traffic and packets, giving you an overall picture of attacks within the selected time period.

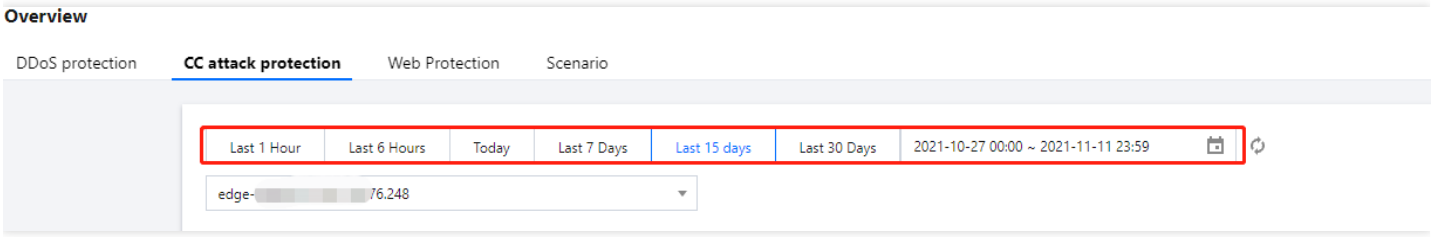
  Note :

  - Total attack traffic: presents how the attack traffic distributes over different protocols within the selected time period.
  - Attack packets: presents how the attack packets distribute over different protocols within the selected time period.
  - Total attacks: presents how the attacks distribute over different attack types within the selected time period.

Viewing CC Protection Details

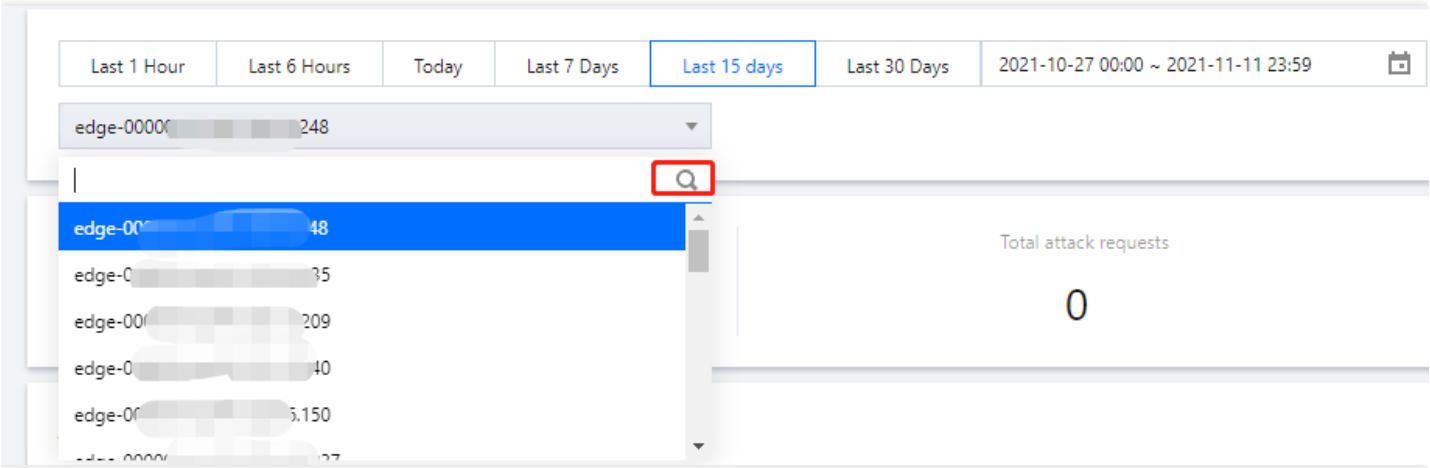
1. Log in to the DDoS Edge Defender Console, click **Overview** on the left sidebar, and then select **CC Protection**.
2. On the **CC Protection** page, select a query period.

> Note :
> You can query the number of attack requests and CC attack events in the last 180 days.



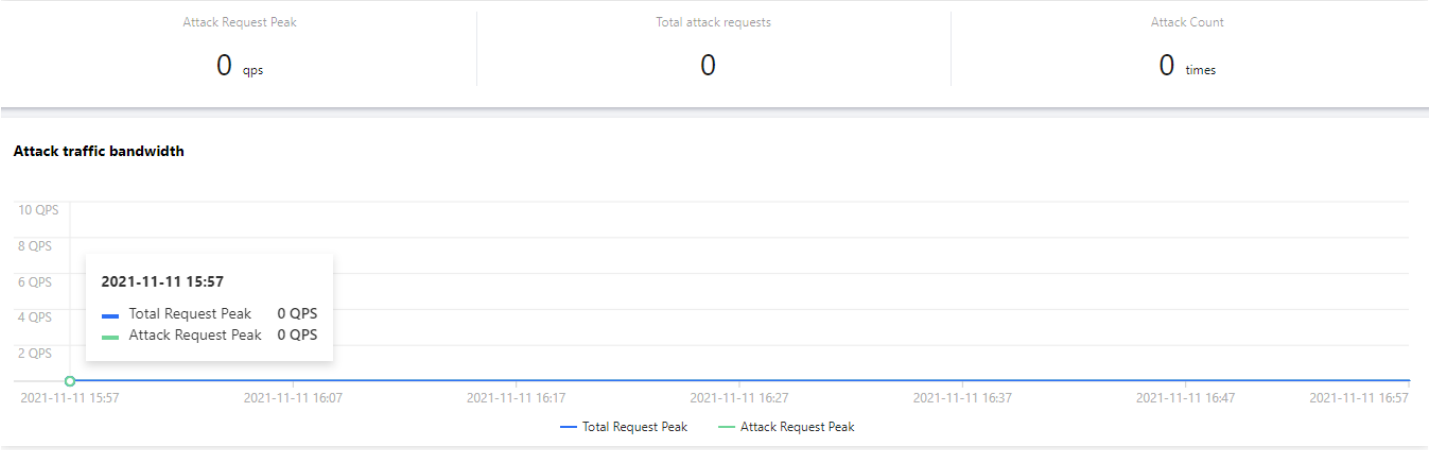
3. Click to search the protected instance in the drop-down list and view whether it is hit by CC

attacks.



- **Attack Traffic Bandwidth**
  - You can select **Today** to view the trend in the number of attack requests. You can check whether the total number of requests is far higher than the normal QPS, whether the attack QPS has a value, and whether the value is extremely high.

> Note :
>
> - Total request peak: the peak number of total attack requests received by the protected IP.
> - Attack request peak: the peak number of attack requests blocked by the Edge Defender system.

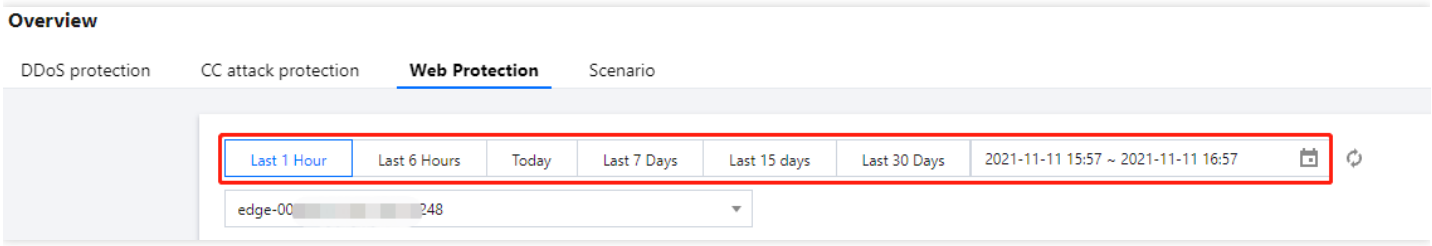


- **CC Attack Records**
  If the protected instance is subject to CC attacks, the system will record the attack start time and end time, attacked domain names, attacked URLs, total request peak, attack request peak, and attacker IP.

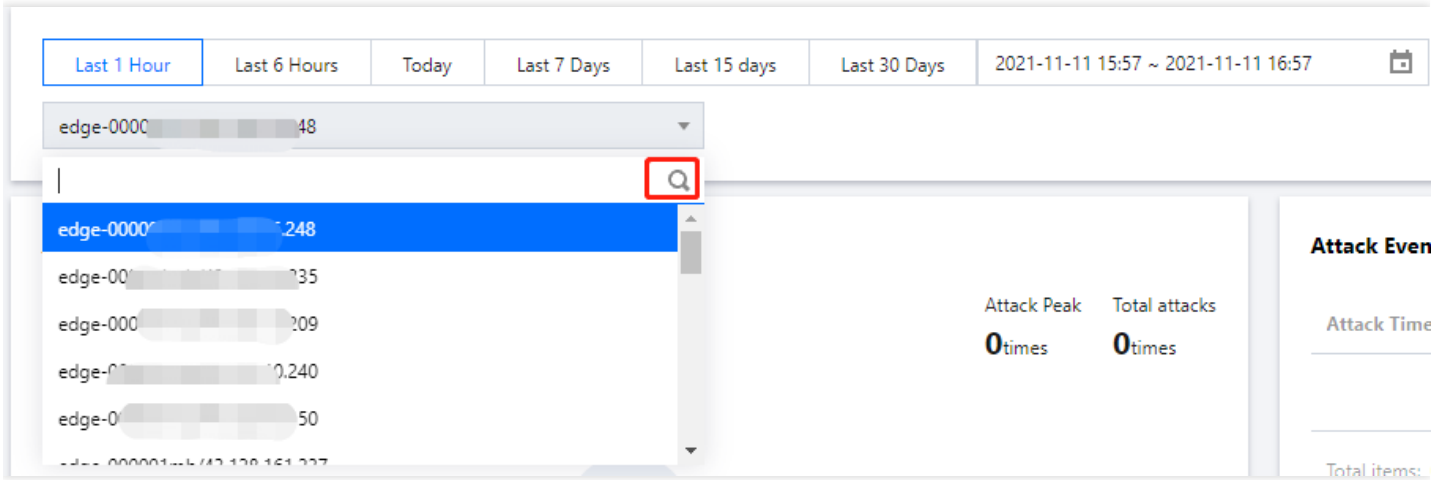
Viewing Web Protection Details

1. Log in to the DDoS Edge Defender Console, click **Overview** on the left sidebar, and then select **Web Protection**.
2. On the **Web Protection** page, select a query period.

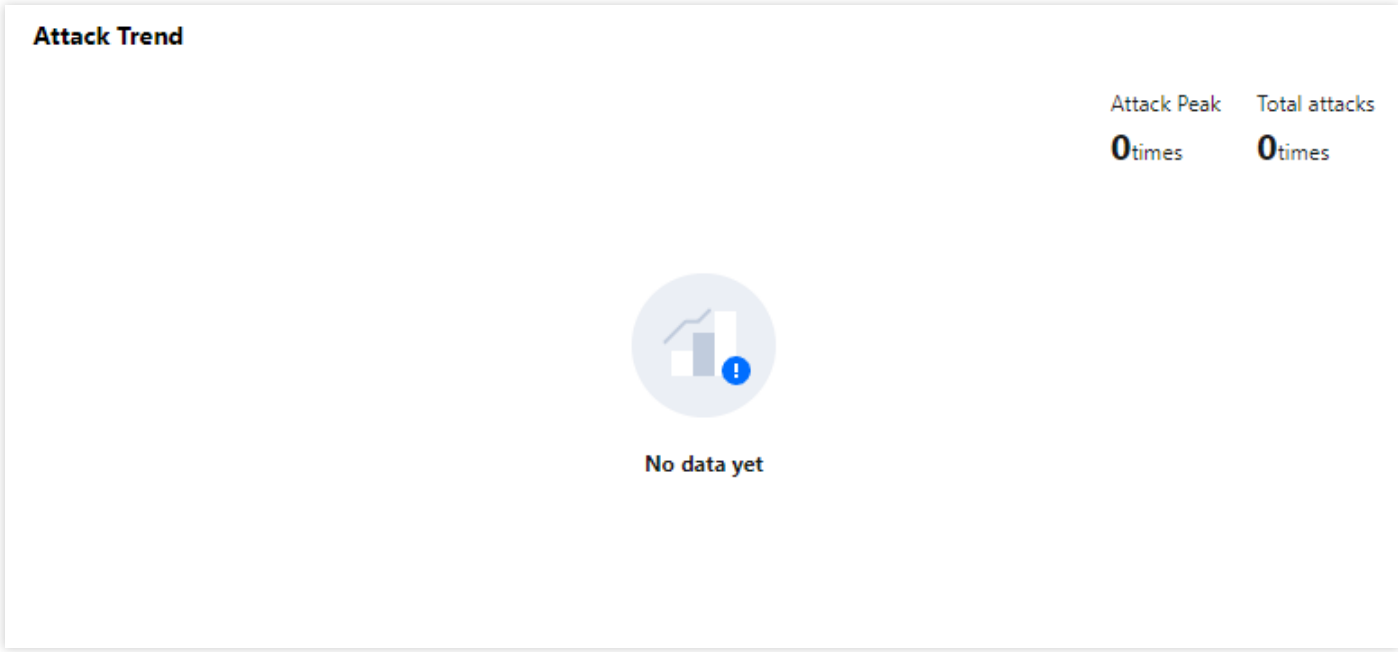
> Note :
> You can query attack traffic and web attack events in the past 180 days.



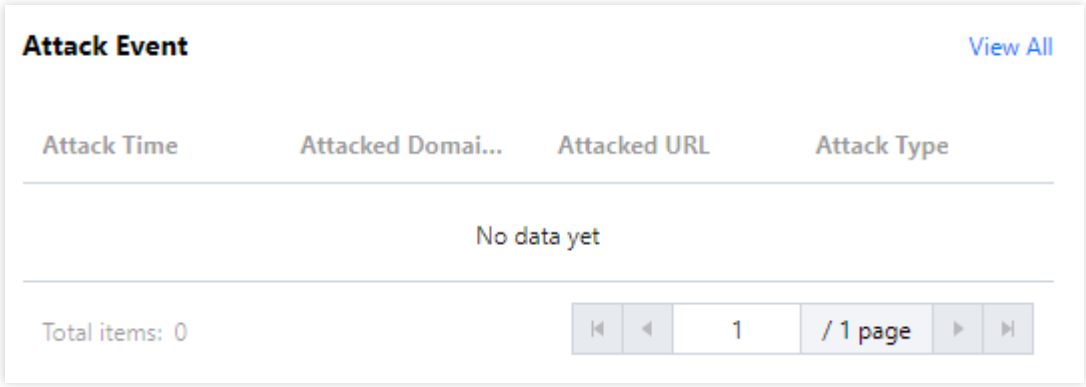
3. Click to search the protected instance in the drop-down list and view whether it is hit by web attacks.



- **Attack Trend**
  Displays the attack trend within the selected time period in terms of the attack peak and total number of attacks.



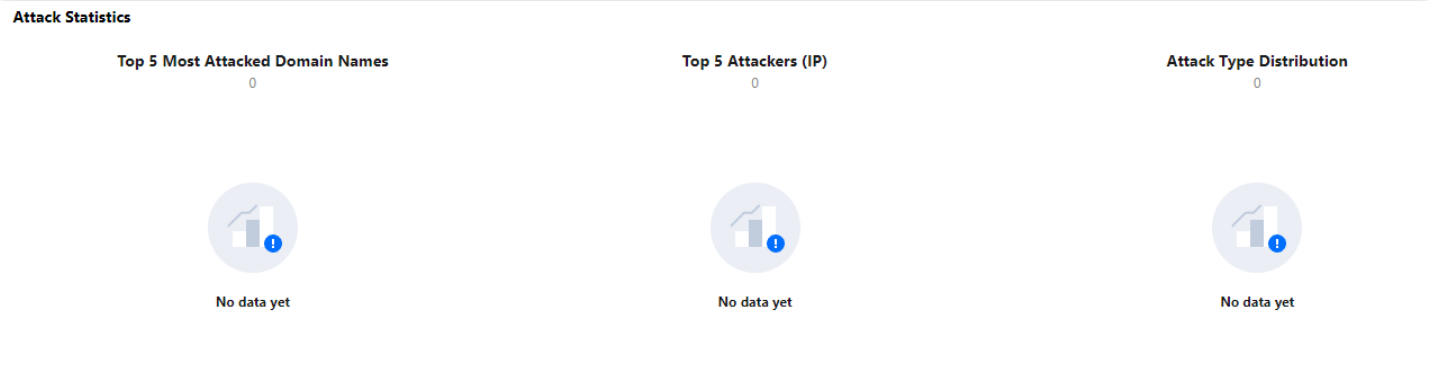
- **Attack Event**
  Displays the start time, attacked domain names, attacked URLs and type of an attack event.



- **Attack Statistics**
  Displays the total number of attacks, attack traffic and packets, giving you an overall picture of attacks within the selected time period.

> Note :
>
> - Top 5 most attacked domain names: presents the top five domain names that are bound to the protected instance subject to most attacks within the selected time period.

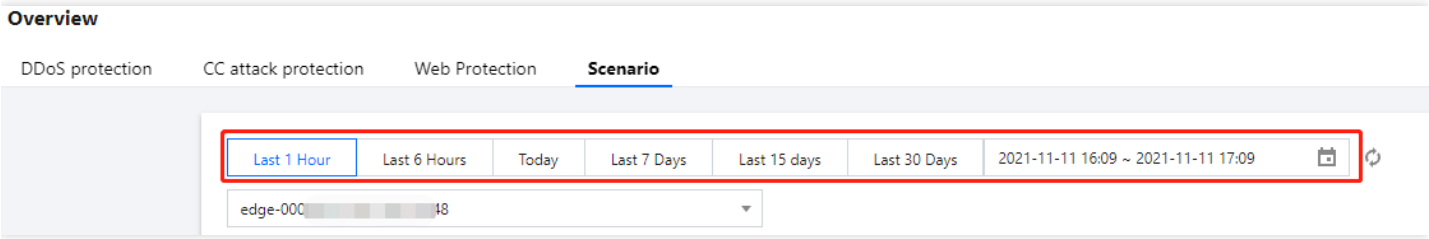
- Top 5 attackers (IP): presents the top five attacker IPs that launch most attacks to the protected instance within the selected time period.
- Attack type distribution: presents the attack type distribution within the selected time period.



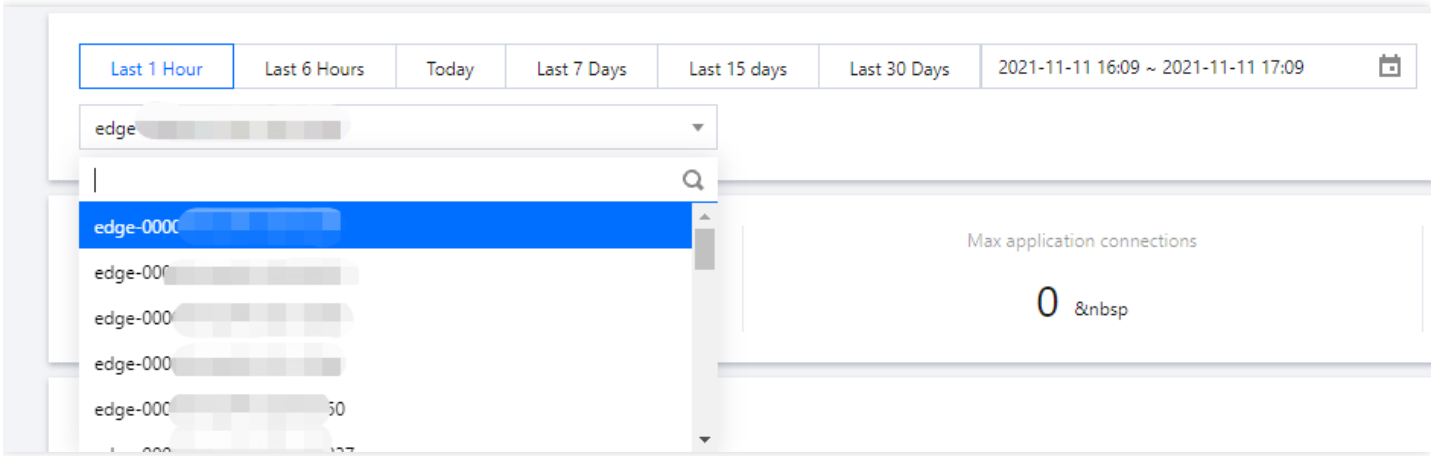
Viewing User Traffic Details

1. Log in to the DDoS Edge Defender Console, click **Overview** on the left sidebar, and then select **Scenario**.
2. On the **Scenario** page, select a query period.

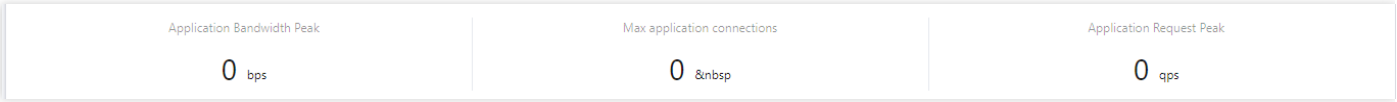
Note :
You can query scenario details in the past 180 days.



3. Click to search the protected instance in the drop-down list.



- You can view the application bandwidth peak, maximum application connections, and application request peak.

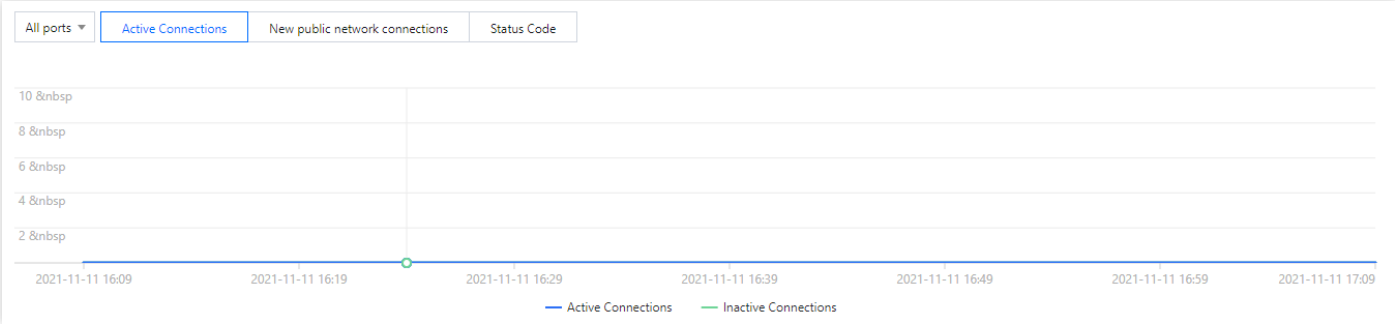


- You can view the trends for inbound/outbound application traffic bandwidth, inbound/outbound application packet rate, and the number of active connections and new connections within the selected time period.

- You can view the trends for the number of active connections and new connections, and the status code within the selected time period.

> Note :

- Active connections: the number of TCP connections that are already established and currently active.
- New connections: the number of TCP connections that are newly established per second for communication between the client and Edge Defender system.



Protection Configuration
DDoS Protection
Protection Level and Cleansing Threshold

Last updated : 2021-11-15 14:42:00

This guide describes protection levels that DDoS Edge Defender provides in different scenarios and how to set them in the console.

Note :
DDoS Edge Defender is currently available to beta users. To use it, please contact us.

Use Cases

DDoS Edge Defender provides three available protection levels for you to adjust protection policies against different DDoS attacks. The details are as follows:

- Loose
- Medium
- Strict

Protection Level	Protection Action	Description
Loose	• Filters SYN and ACK data packets with explicit attack attributes. • Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specifications. • Filters UDP data packets with explicit attack attributes.	• This cleansing policy is loose and only defends against explicit attack packets. • We recommend choosing this protection level when normal requests are blocked. Complex attack packets may pass through the security system.

Note：

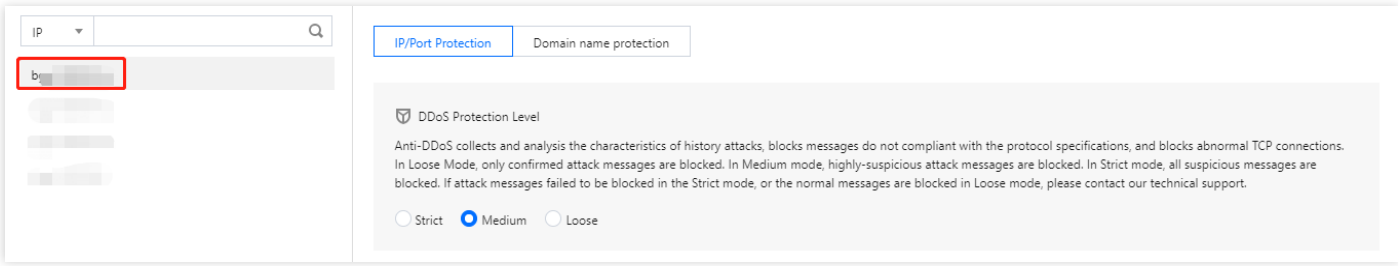
- If you need to use UDP in your business, please contact Tencent Cloud Technical Support to customize an ideal policy for not letting the level Strict affect normal business process.
- The level Medium is chosen by default for your DDoS Edge Defender instance. You can set the DDoS protection level for your business needs and also the cleansing threshold. Attack traffic will be cleansed when it is detected higher than the threshold you set.

Prerequisites

You have successfully purchased a DDoS Edge Defender instance and set the object to protect.

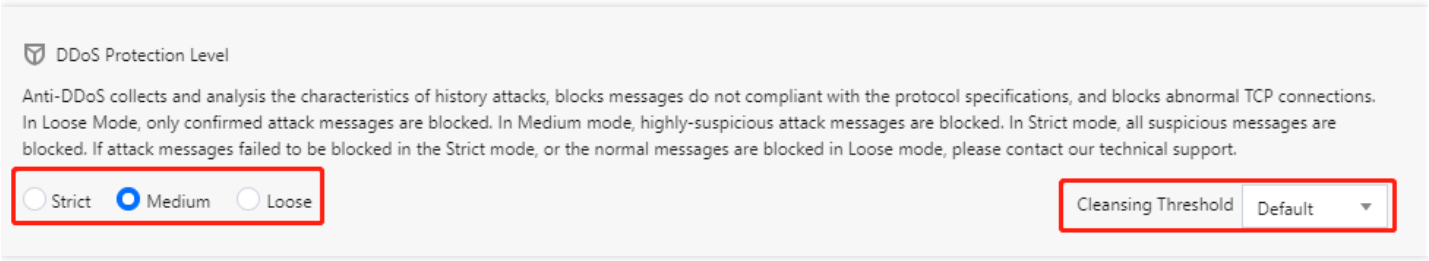
Directions

1. Log in to the DDoS Edge Defender Console, click **Protection Policy** on the left sidebar, and then select the tab **DDoS Protection**.
2. Select an Edge Defender instance ID, such as "edge-xxxxxxx".



3. Set the protection level and cleansing threshold in the **DDoS Protection** section on the right.

Note：
If you have a clear concept about the threshold, set it as required. Otherwise leave it to the default value. The DDoS protection system will automatically learn through AI algorithms and calculate the default threshold for you.



Parameter Description:

- **Level**
  If the protection is enabled, the level Medium is chosen by default for your DDoS Edge Defender instance. You can adjust the DDoS protection level for your business needs.
- **Cleansing Threshold**
  - This indicates a value to trigger cleansing. Cleansing will not be triggered by the traffic below the threshold you set even though it is found malicious.
  - If the protection is enabled, your DDoS Edge Defender instance will use the default cleansing threshold after your business is connected, and the system will generate a baseline based on historical patterns of your business traffic. You can also set the cleansing threshold for your business needs.

IP Blocklist/Allowlist

Last updated : 2021-11-15 14:26:59

DDoS Edge Defender supports configuring IP blocklist and allowlist to block or allow source IPs accessing the DDoS Edge Defender service, restricting the users accessing your business resources. If the accessing traffic exceeds the cleansing threshold, the allowed IPs will be allowed to access resources without being filtered by any protection policy; while the access requests from the blocked IPs will be directly denied.

Prerequisites

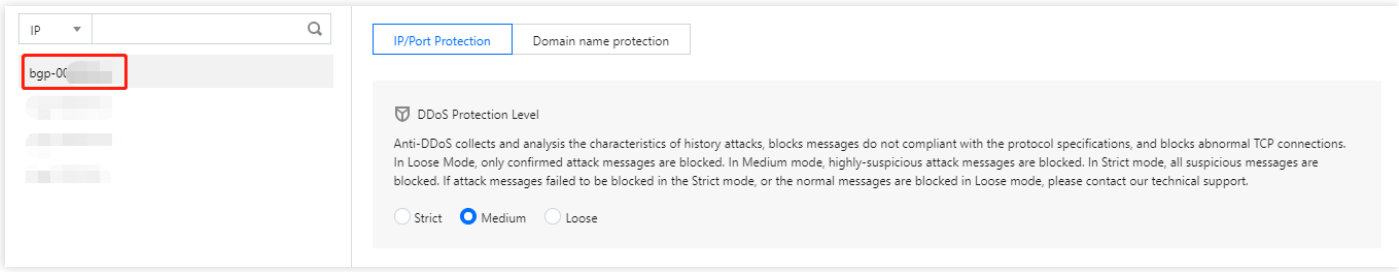
You have successfully purchased a DDoS Edge Defender instance and set the object to protect.

Note :

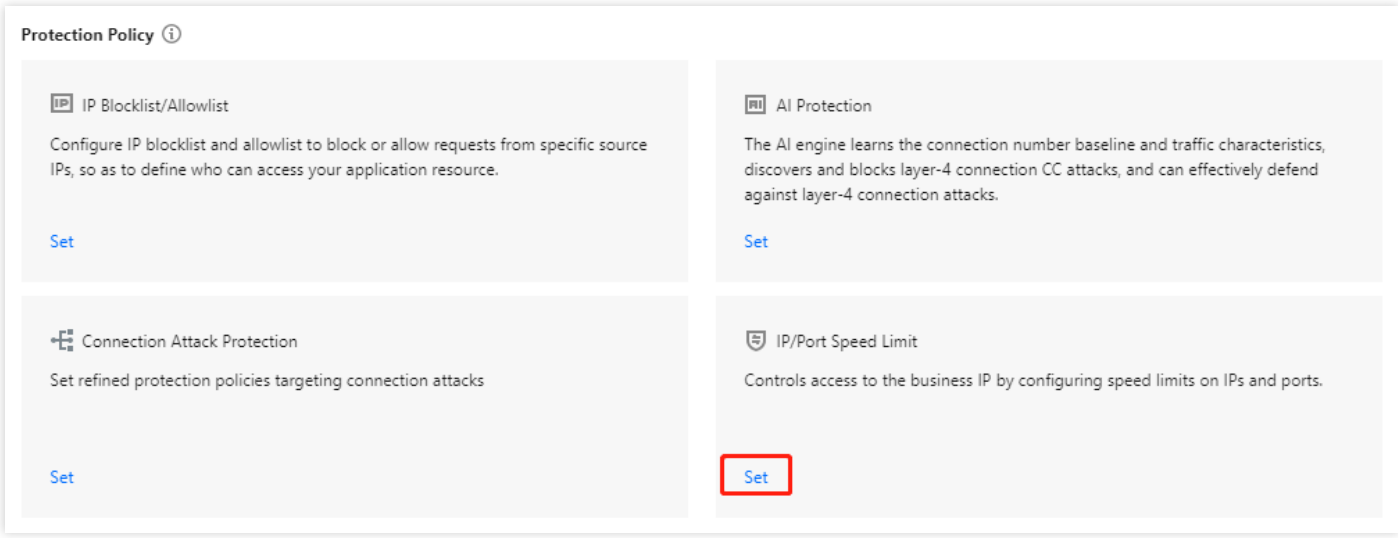
- The IP blocklist and allowlist filtering take effect only when your business is under DDoS attacks.
  - The allowed IPs will be allowed to access resources without being filtered by any protection policy.
  - The access requests from the blocked IPs will be directly denied.
- DDoS Edge Defender is currently available to beta users. To use it, please contact us.

Directions

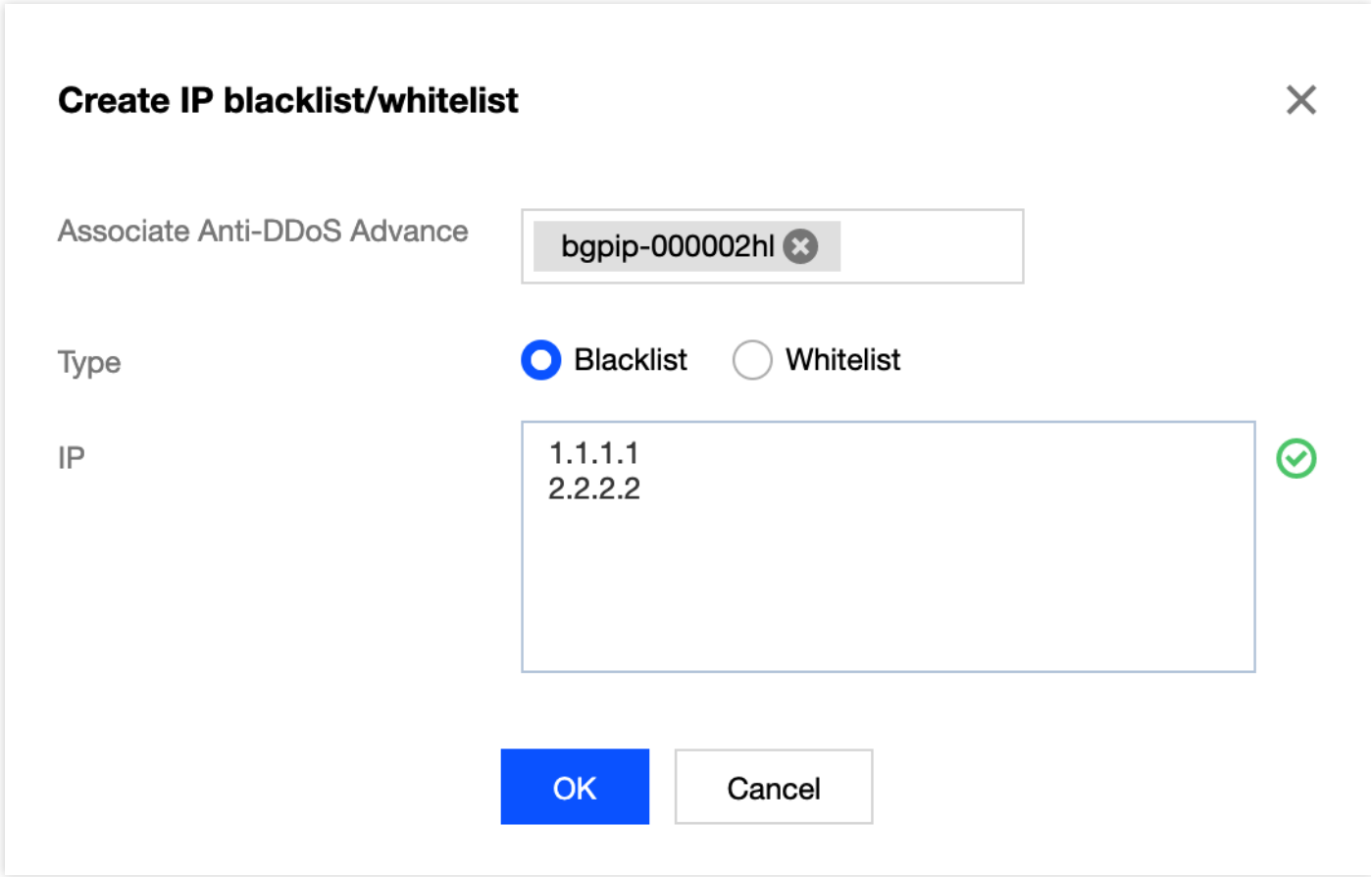
1. Log in to the DDoS Edge Defender Console, click **Protection Policy** on the left sidebar, and then select **DDoS Protection**.
2. Select an Edge Defender instance ID in the list on the left, such as "edge-xxxxxxx".



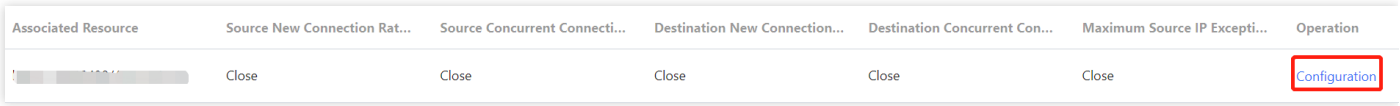
3. Click **Set** in the **IP Blocklist/Allowlist** section to enter the IP blocklist/allowlist.



4. Click **Create**.
5. In the pop-up window, select the rule type to create a rule, and click **OK**.



6. Now the new rule is added to the list. You can click **Delete** on the right of the rule to delete it.



Feature Filtering

Last updated : 2021-11-15 14:29:37

DDoS Edge Defender supports configuring custom blocking policies against specific IP, TCP, UDP message header and payload. After enabling feature filtering, you can combine the matching conditions of the source port, destination port, message length, IP message header and payload, and set the protection action to continue protection, allow/block/discard matched requests, block the IP for 15 minutes, or discard the request and then block the IP for 15 minutes, etc. With feature filtering, you can configure accurate protection policies against business message features or attack message features.

Prerequisites

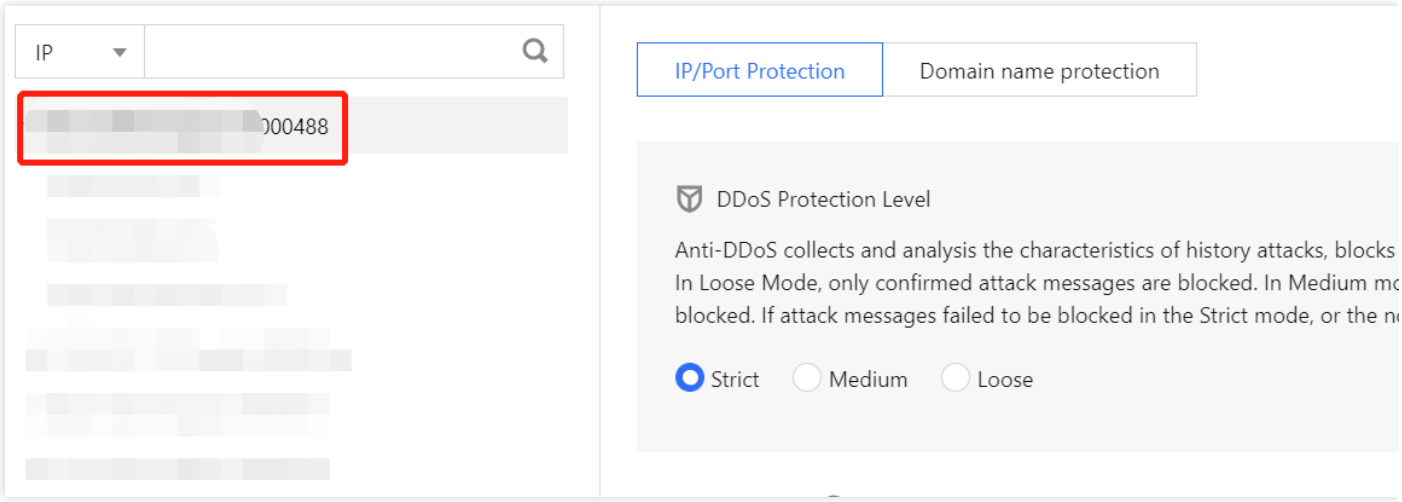
You have successfully purchased a DDoS Edge Defender instance and set the object to protect.

> Note :
> DDoS Edge Defender is currently available to beta users. To use it, please contact us.

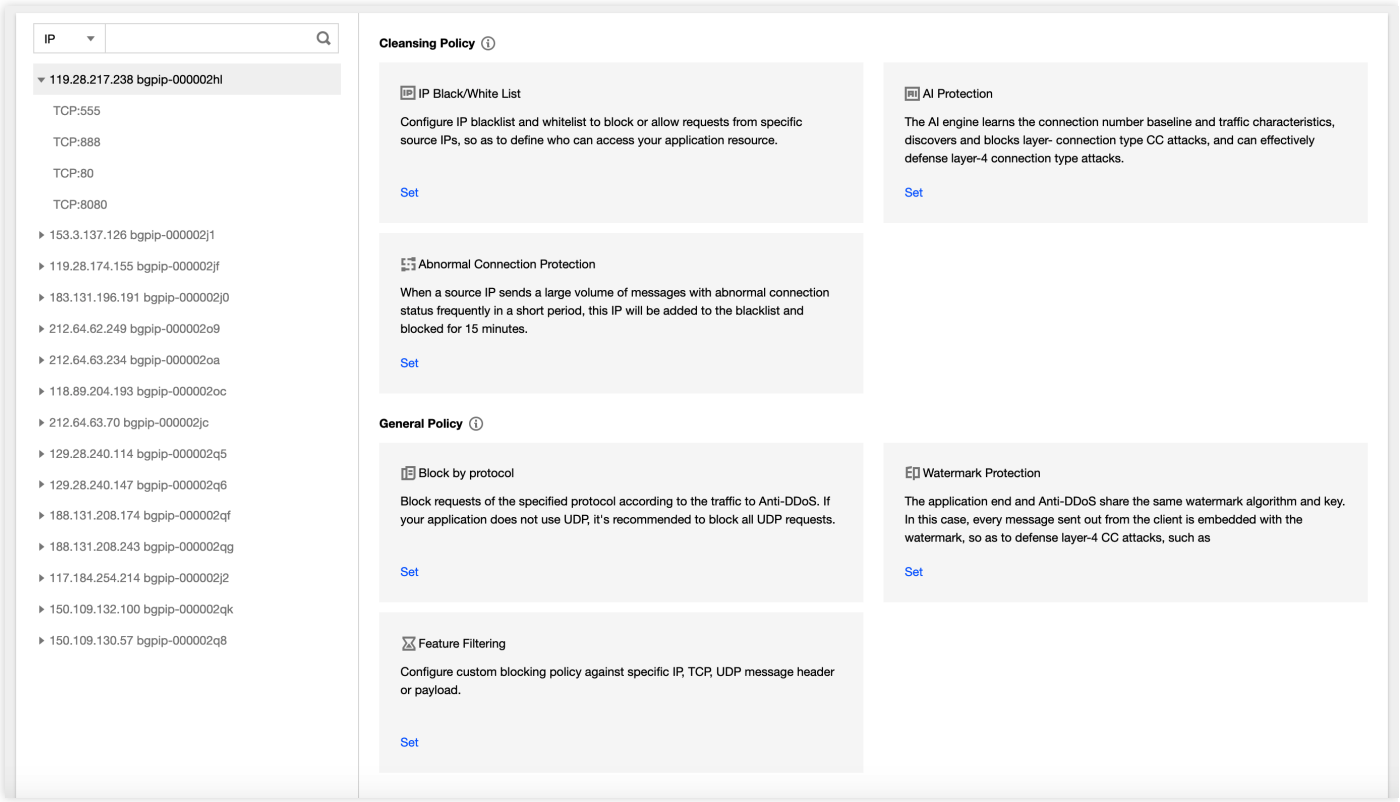
Directions

1. Log in to the DDoS Edge Defender Console, click **Protection Policy** on the left sidebar, and then select the tab **DDoS Protection**.

2. Select an Edge Defender instance ID, such as "edge-xxxxxxx".

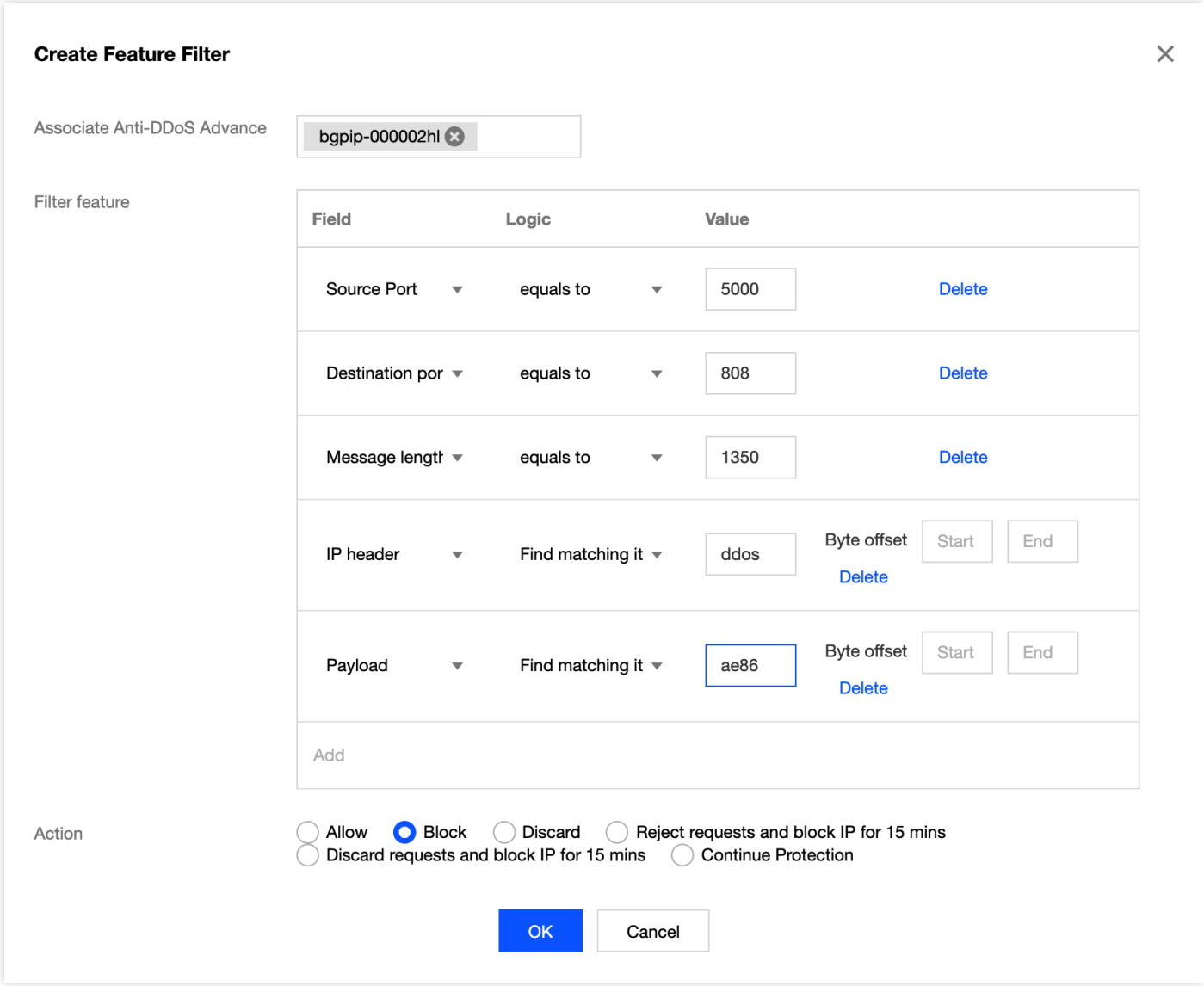


3. Click **Set** in the **Feature Filtering** section on the right.

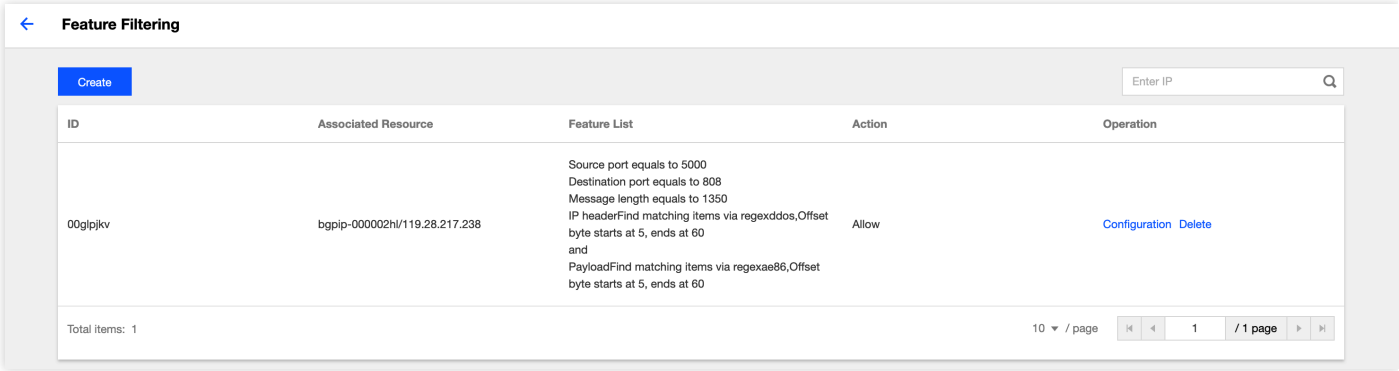


4. Click **Create**.

5. In the pop-up window, fill in the configuration fields, and click **OK**.



6. Now the new rule is added to the list. You can click **Configuration** on the right of the rule to modify it.



Port Filtering

Last updated : 2021-11-15 14:31:44

DDoS Edge Defender enables you to block or allow inbound traffic by ports. With port filtering enabled, you can customize port settings against inbound traffic, including the protocol type, source port and destination port ranges and set the protection action (allow/block/discard) for the matched rule.

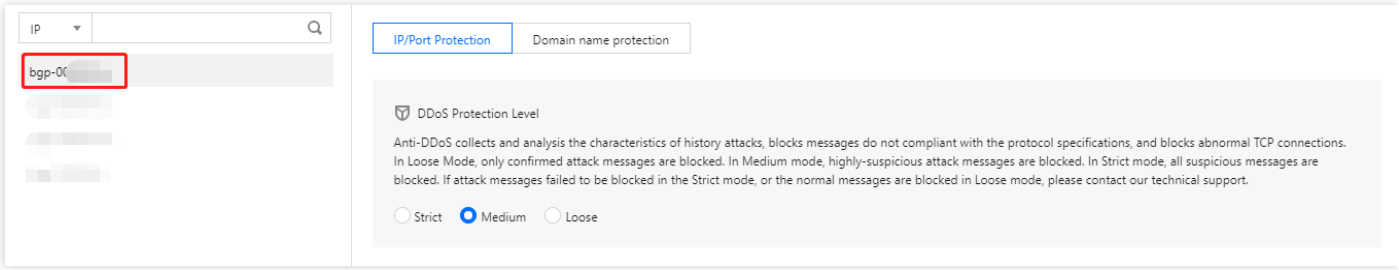
Prerequisites

You have successfully purchased a DDoS Edge Defender instance and set the object to protect.

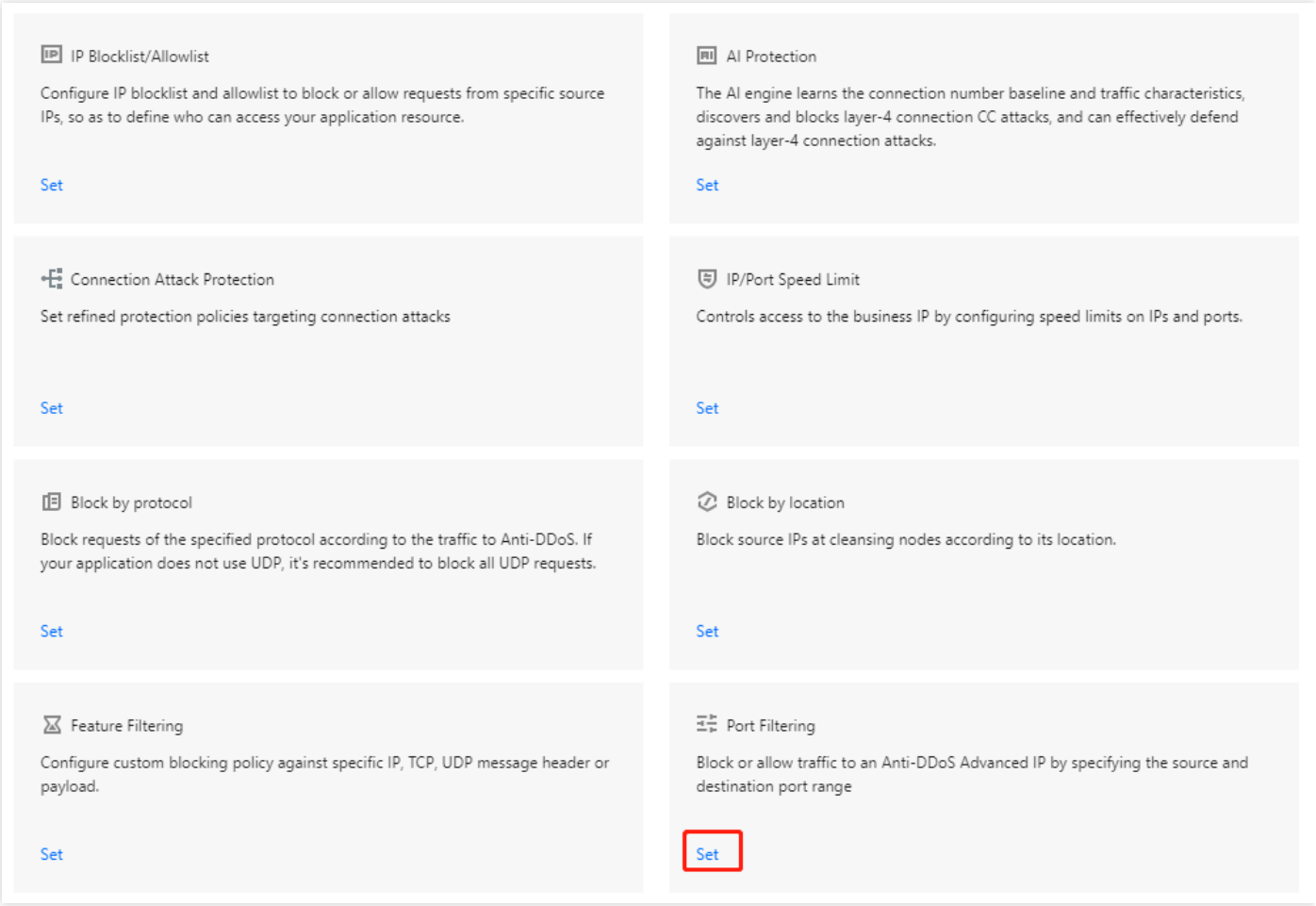
> Note :
> DDoS Edge Defender is currently available to beta users. To use it, please contact us.

Directions

1. Log in to the DDoS Edge Defender Console, click **Protection Policy** on the left sidebar, and then select the tab **DDoS Protection**.
2. Select an Edge Defender instance ID, such as "edge-xxxxxxx".

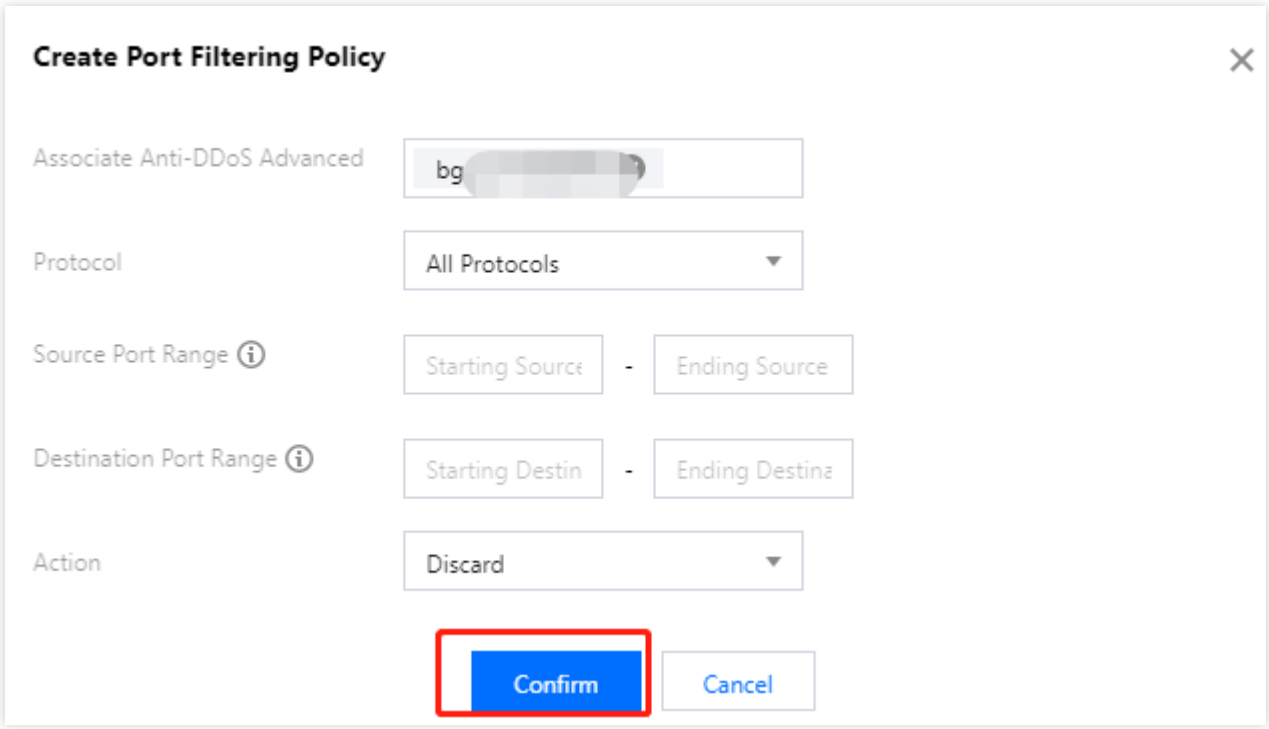


3. Click **Set** in the **Port Filtering** section to enter the attribute filtering page.

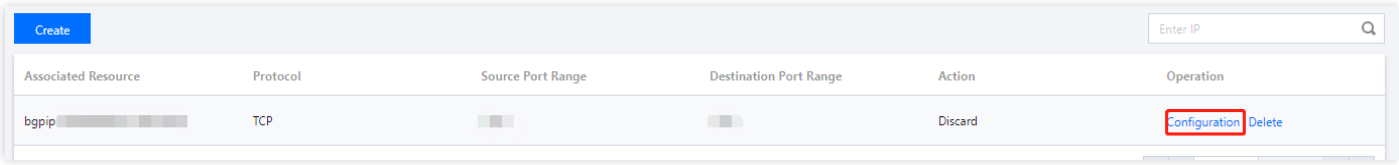


4. Click **Create**.

5. In the pop-up window, fill in the configuration fields, and click **OK**.



6. Now the new rule is added to the list. You can click **Configuration** on the right of the rule to modify it.



Protocol Blocking

Last updated : 2021-11-15 14:33:12

DDoS Edge Defender supports blocking inbound traffic by blocking protocols such as ICMP, TCP and UDP. When you complete the configuration, the access requests will be blocked directly. Of these protocols, UDP as a connectionless protocol dose not provide a three-way handshake process like TCP, and thus has security vulnerabilities. We recommend blocking UDP if it is not used for your application.

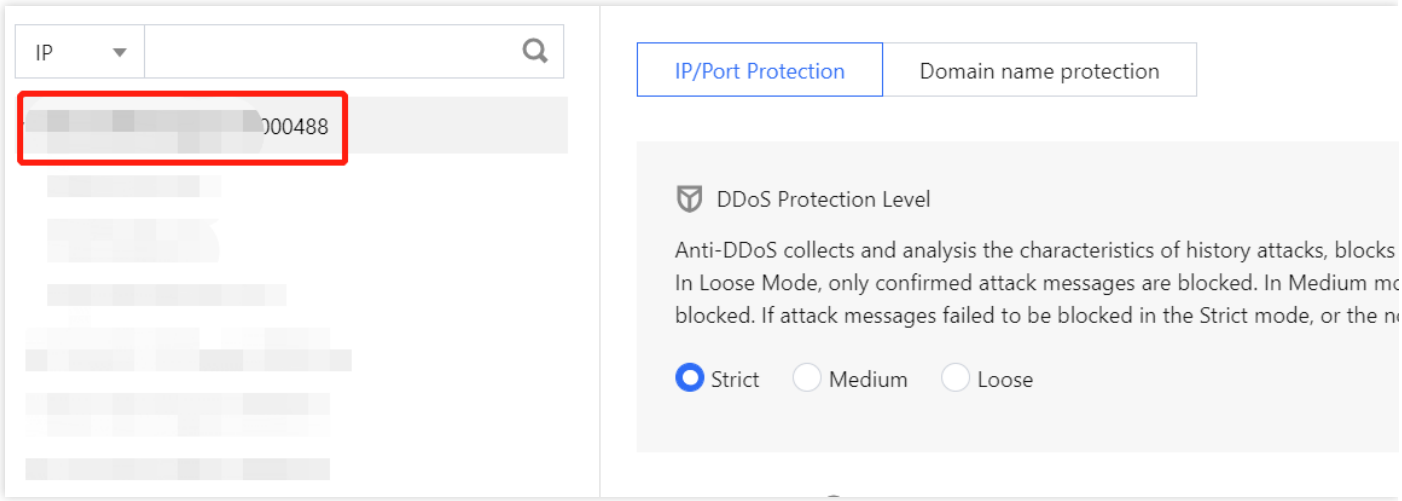
Prerequisites

You have successfully purchased a DDoS Edge Defender instance and set the object to protect.

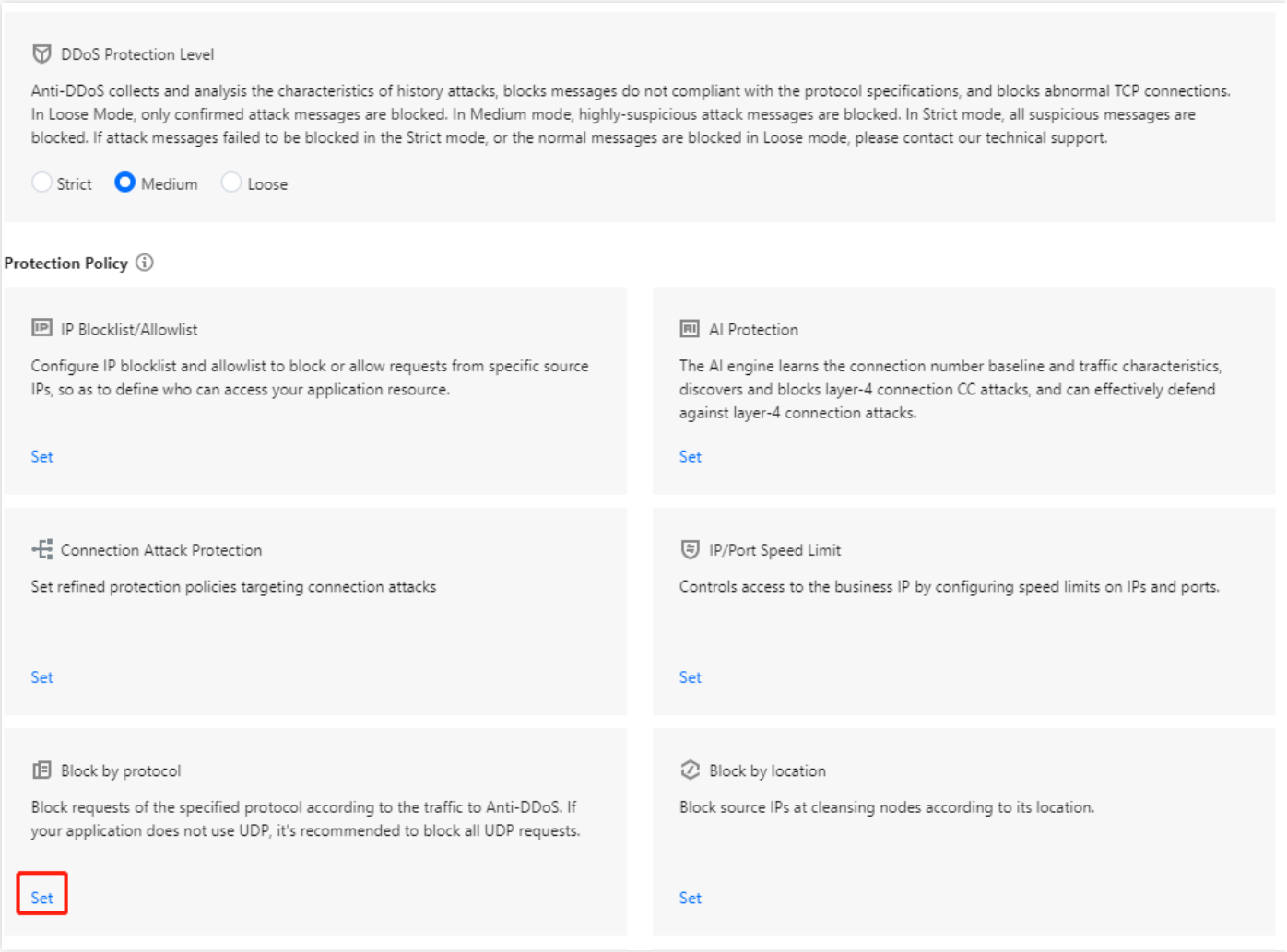
> Note :
> DDoS Edge Defender is currently available to beta users. To use it, please contact us.

Directions

1. Log in to the DDoS Edge Defender Console, click **Protection Policy** on the left sidebar, and then select the tab **DDoS Protection**.
2. Select an Edge Defender instance ID, such as "edge-xxxxxxx".

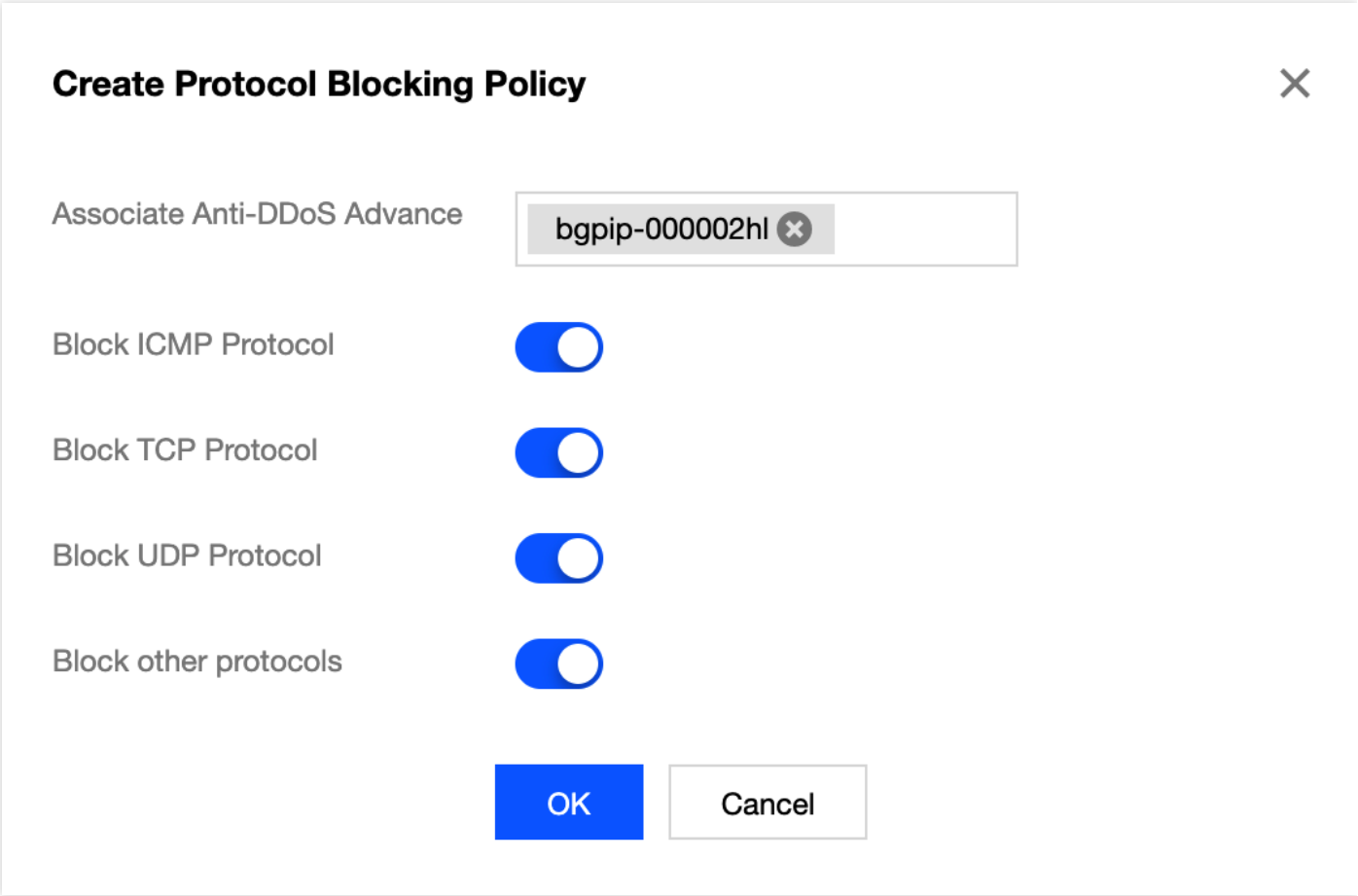


3. Click **Set** in the **Block by Protocol** section on the right.

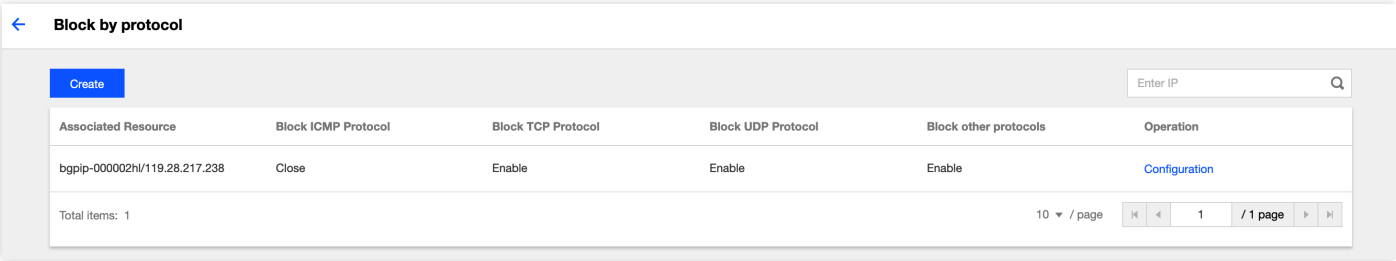


4. Click **Create**.

5. In the pop-up window, fill in the configuration fields and click **OK**.



6. Now the new is added to the list. You can click **Configuration** on the right of the rule to modify it.



CC Protection
Protection Level and Cleansing Threshold

Last updated : 2021-11-15 14:34:59

Protection Description

DDoS Edge Defender provides three protection levels against CC attacks for stronger protection and less false blocking. The default level is Medium.

- Loose
- Medium
- Strict

This level applies to a protected website without obviously exceptional traffic. It will run checks on all visitor requests by using human verification algorithm. Only the visitors who successfully authenticate are allowed to access the website. As this CC protection policy is loose, a small number of exceptional requests may pass through the security system.

Note :

- The protection algorithms for the above three CC protection levels are only applicable to webpages and HMTL5 pages.
- False blocking is highly likely to occur in a visited website for API or native app businesses, as requests to the website cannot pass the verification.
- To protect your API or native app business from CC attacks, please contact us to customize protection policies.

Prerequisites

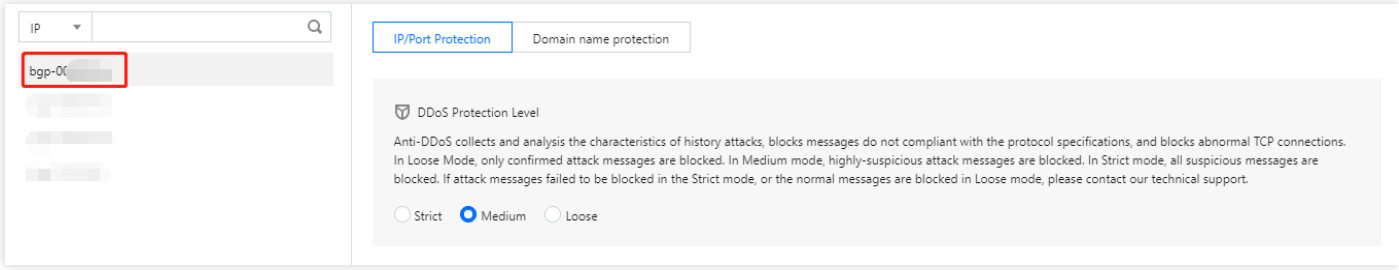
You have successfully purchased a DDoS Edge Defender instance and set the object to protect.

Note :

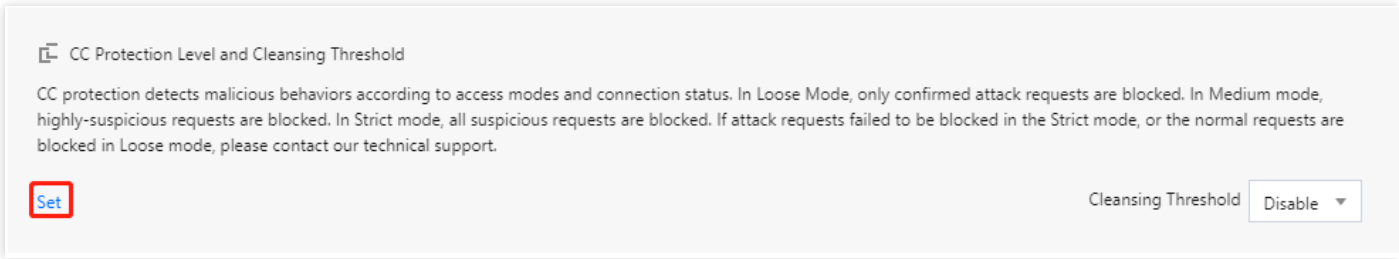
DDoS Edge Defender is currently available to beta users. To use it, please contact us.

Directions

1. Log in to the DDoS Edge Defender Console, click **Protection Policy** on the left sidebar, and then select the tab **CC Protection**.
2. Select an Edge Defender instance ID, such as "edge-xxxxxxx".



3. Click **Set** in the **CC Protection Level and Cleansing Threshold** section on the right.

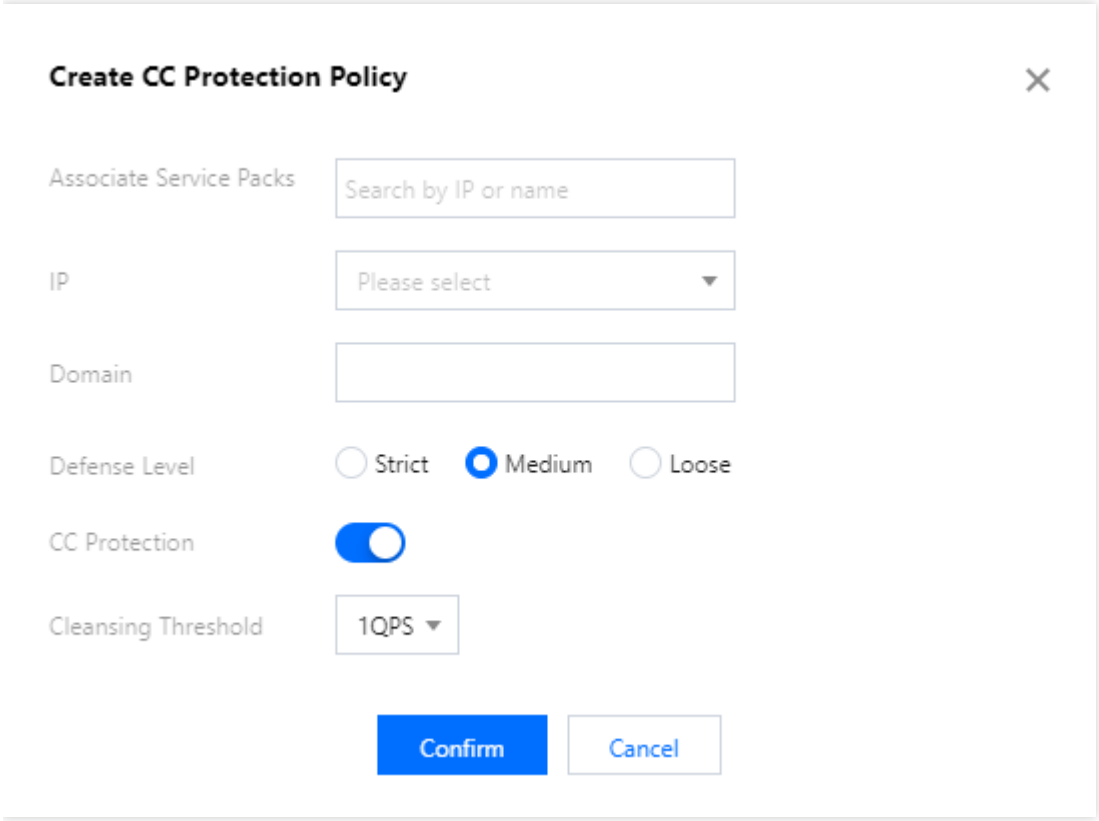


4. Click **Create**.
5. In the pop-up window, fill in the configuration fields, set the protection level and click **OK**.

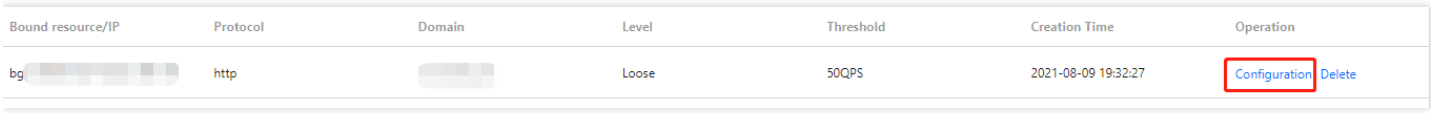
Note :

- The cleansing threshold is the threshold for Anti-DDoS services to start cleansing traffic. If the number of HTTP requests sent to the specified domain name exceeds the threshold, CC protection will be triggered.
- If the protection is enabled, your instance will use the default cleansing threshold after your business is connected, and the system will generate a baseline based on historical patterns of your business traffic. You can also set the cleansing threshold for your business needs.
- If you have a clear concept about the threshold, set it as required. Otherwise leave it to the default value. Anti-DDoS will automatically learn through AI algorithms and calculate

the default threshold for you.



6. Now a CC domain name protection rule is added to the CC protection level and cleansing threshold list. You can click **Configuration** on the right of the rule to modify the CC protection level and cleansing threshold.



Precise Protection

Last updated : 2021-11-15 14:37:16

DDoS Edge Defender supports precise protection for connected web applications. With the precise protection, you can configure protection policies combining multiple conditions of common HTTP fields, such as URI, UA, Cookie, Referer, and Accept to screen access requests. For the requests matched the conditions, you can configure CAPTCHA to verify the requesters or a policy to automatically drop the packets. Precise protection is available for policy customization in various use cases to precisely defend against CC attacks.

The match conditions define the request characteristics to be checked, i.e., the attribute characteristics of the HTTP field in a request. Precise protection supports checking the HTTP fields below:

Field	Description	Logic
URI	URL address of the access request	Equal to; Include; Exclude
UA	Information including identifier of the client browser that initiates the access request	Equal to; Include; Exclude
Cookie	Cookie information in the access request	Equal to; Include; Exclude
Referer	Source website of the access request, from which the access request is redirected	Equal to; Include; Exclude
Accept	Data type to be received by the client that initiates the access request	Equal to; Include; Exclude

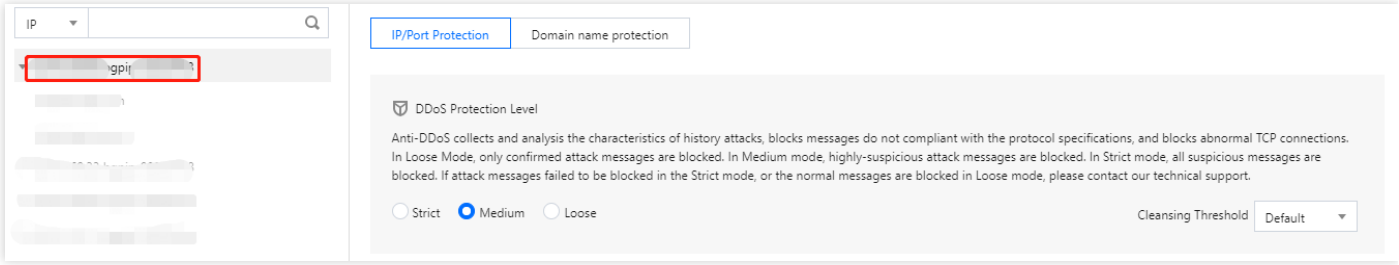
Prerequisites

You have successfully purchased a DDoS Edge Defender instance and set the object to protect.

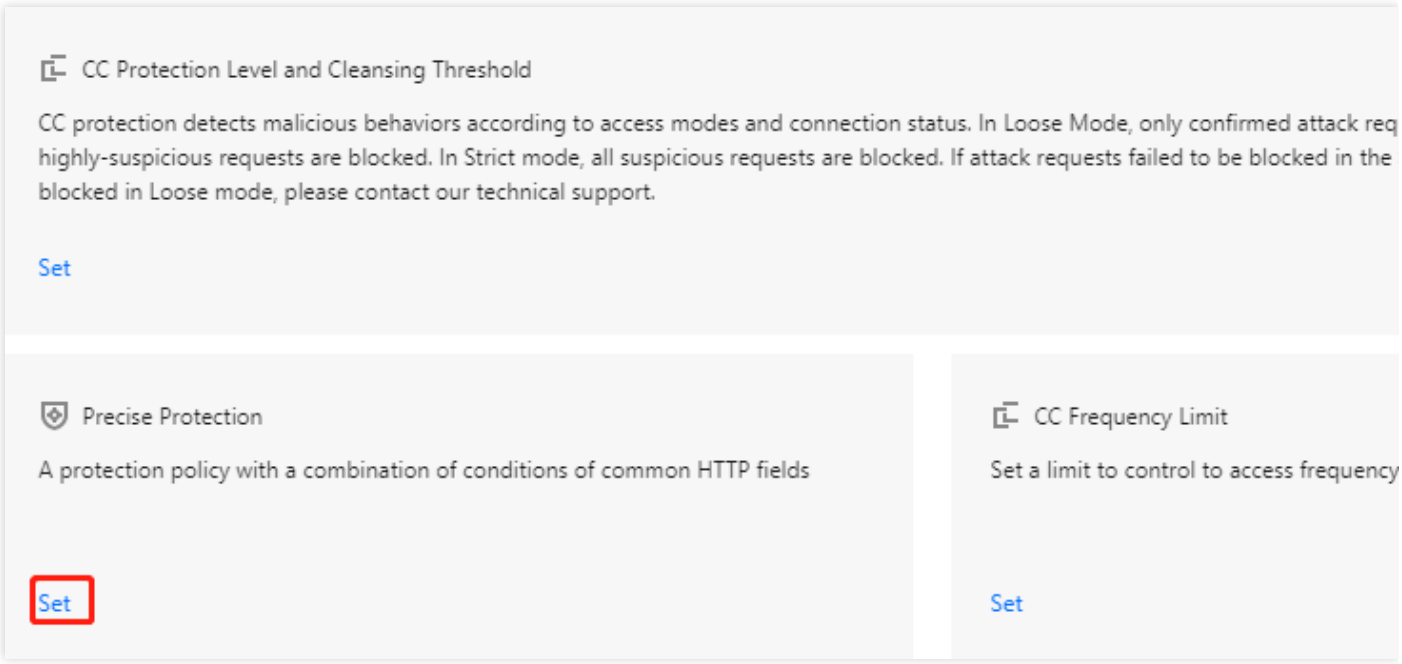
Note :
DDoS Edge Defender is currently available to beta users. To use it, please contact us.

Directions

1. Log in to the DDoS Edge Defender Console, click **Protection Policy** on the left sidebar, and then select the tab **CC Protection**.
2. Select an Edge Defender instance ID, such as "edge-xxxxxxx".

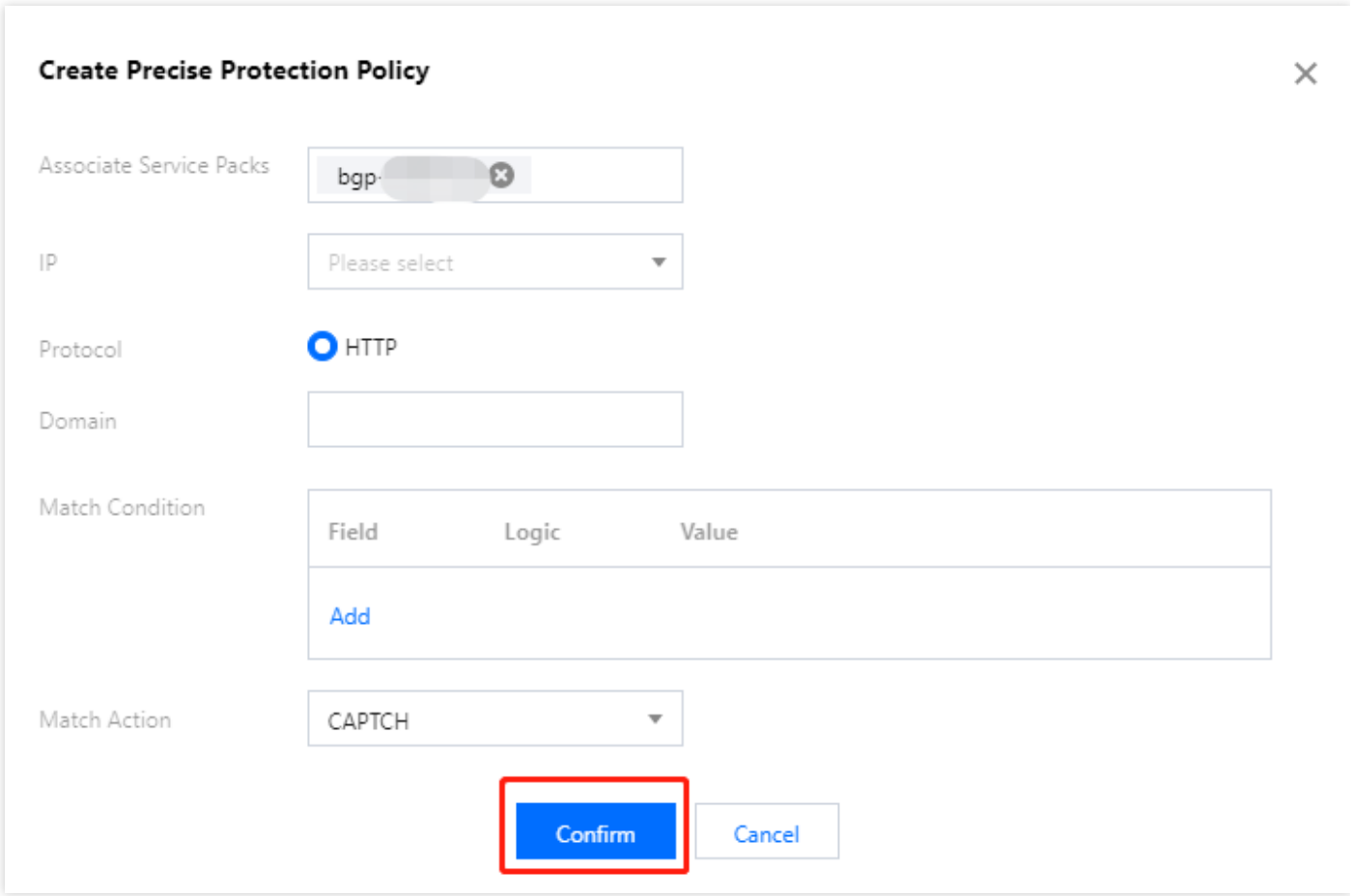


3. Click **Set** in the **Precise Protection** section on the right.

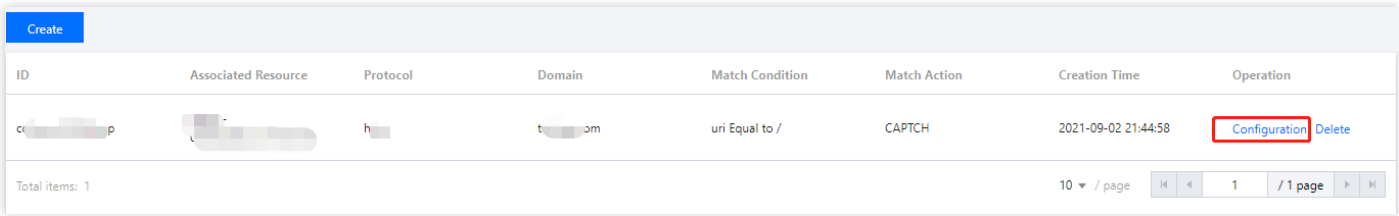


4. Click **Create**.

5. In the pop-up window, fill in the configuration fields, and click **OK** to create a rule.



6. Now the new rule is added to the rule list, you can click **Configuration** on the right of the rule to modify it.



CC Frequency Control

Last updated : 2021-11-15 14:38:34

DDoS Edge Defender supports configuring CC frequency policy for connected web businesses to restrict the access frequency of source IPs. You can customize a frequency policy to apply CAPTCHA and discard on source IPs if any IP accesses a certain page too frequently in a short time.

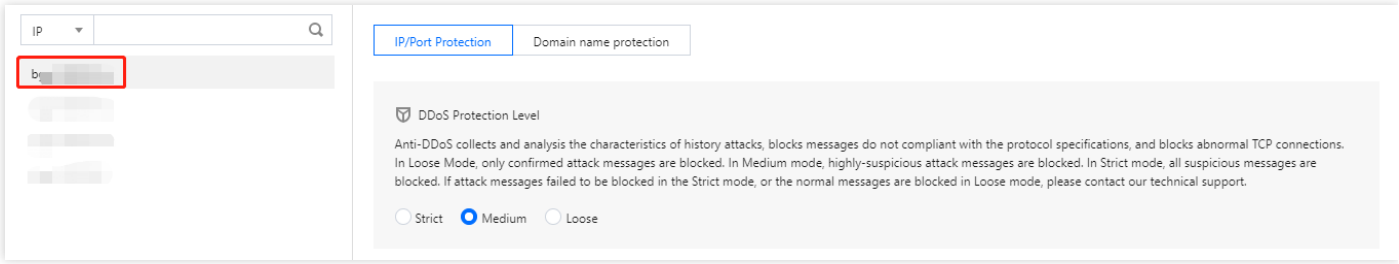
Prerequisites

You have successfully purchased a DDoS Edge Defender instance and set the object to protect.

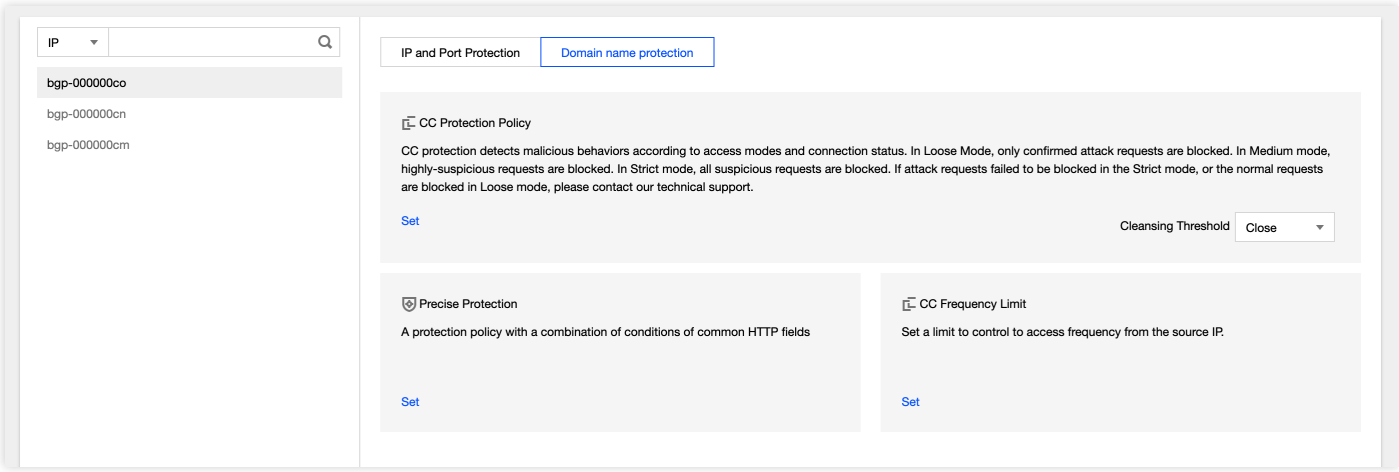
> Note :
> DDoS Edge Defender is currently available to beta users. To use it, please contact us.

Directions

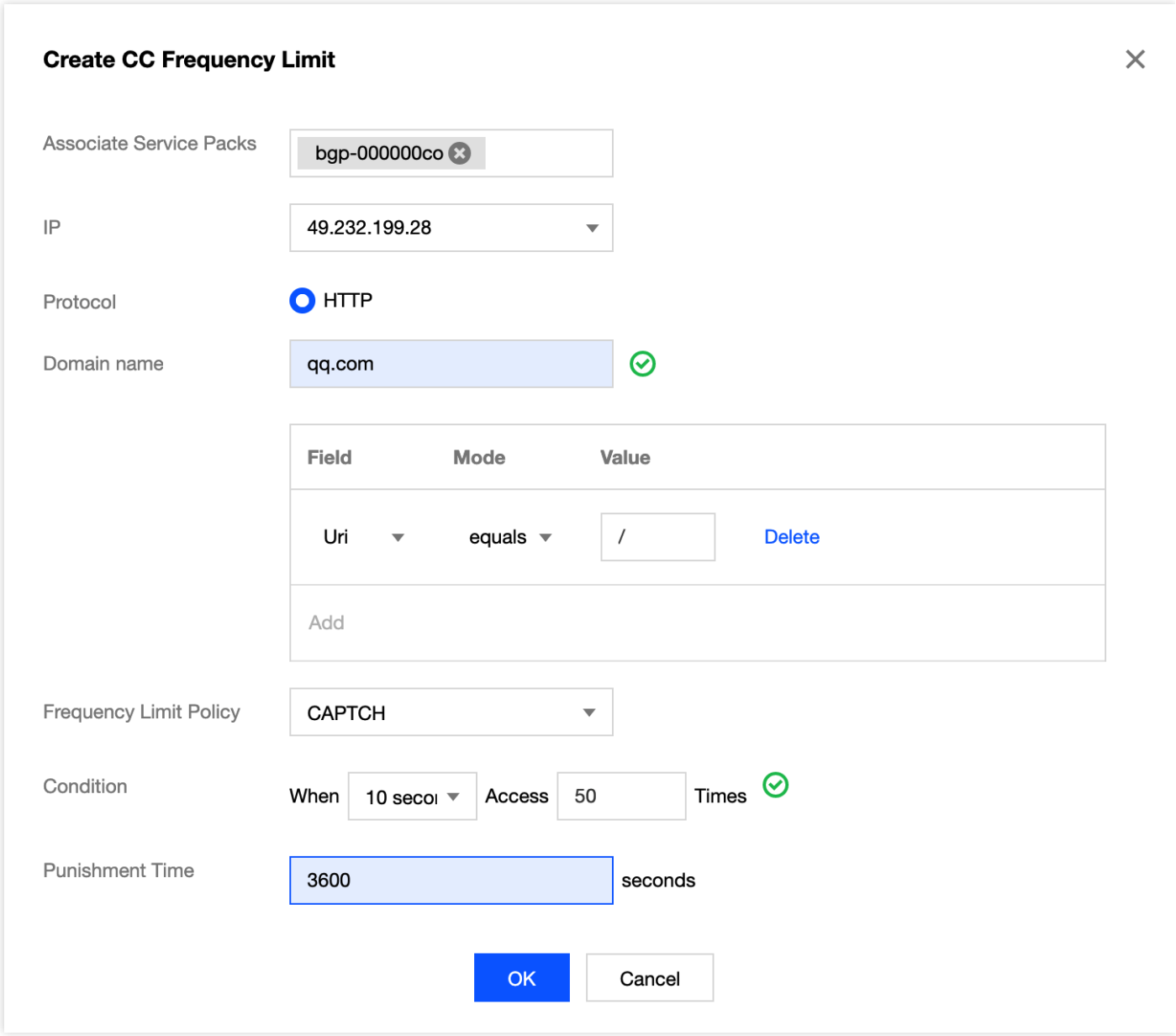
1. Log in to the DDoS Edge Defender Console, click **Protection Policy** on the left sidebar, and then select **CC Protection**.
2. Select an Edge Defender instance ID in the list on the left, such as "edge-xxxxxxx".



3. Click **Set** in the **CC Frequency Limit** section on the right.



4. Click **Create.
5. In the pop-up window, fill in the configuration fields and click **OK** to create a CC frequency limiting rule.



6. Now the new rule is added to the rule list. You can click **Configuration** on the right of the rule to modify it.

Service Configuration
Domain Name Rule

Last updated : 2021-09-28 15:53:26

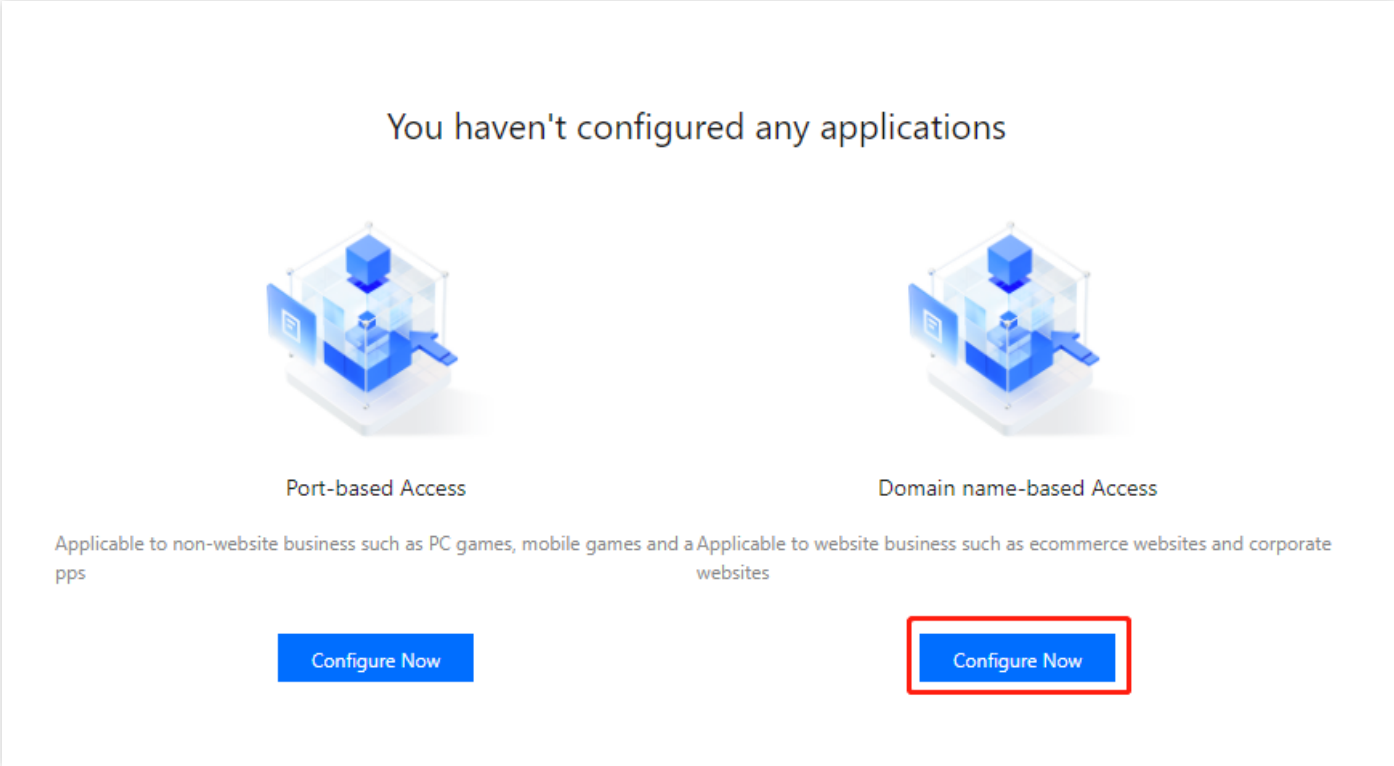
When connecting website applications to DDoS Edge Defender, you need to configure domain-based forwarding rules, which is described in this guide.

Prerequisites

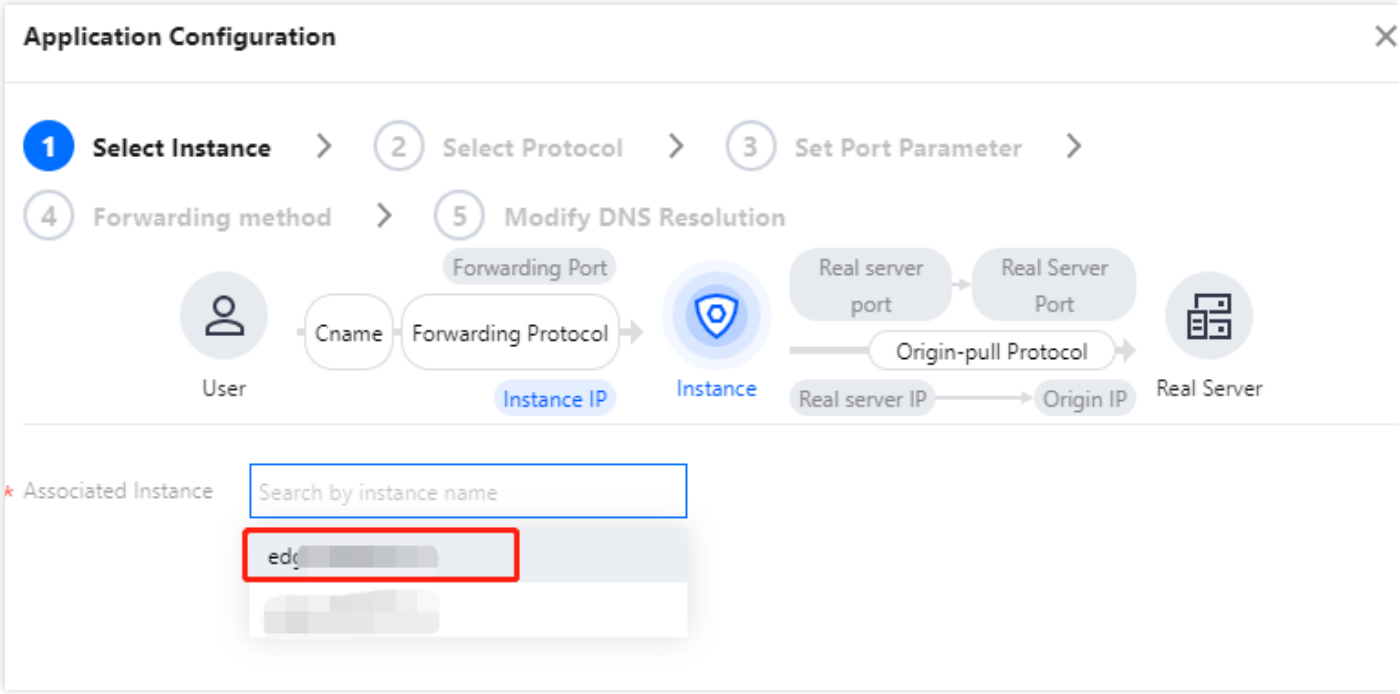
You have purchased a DDoS Edge Defender instance.

Directions

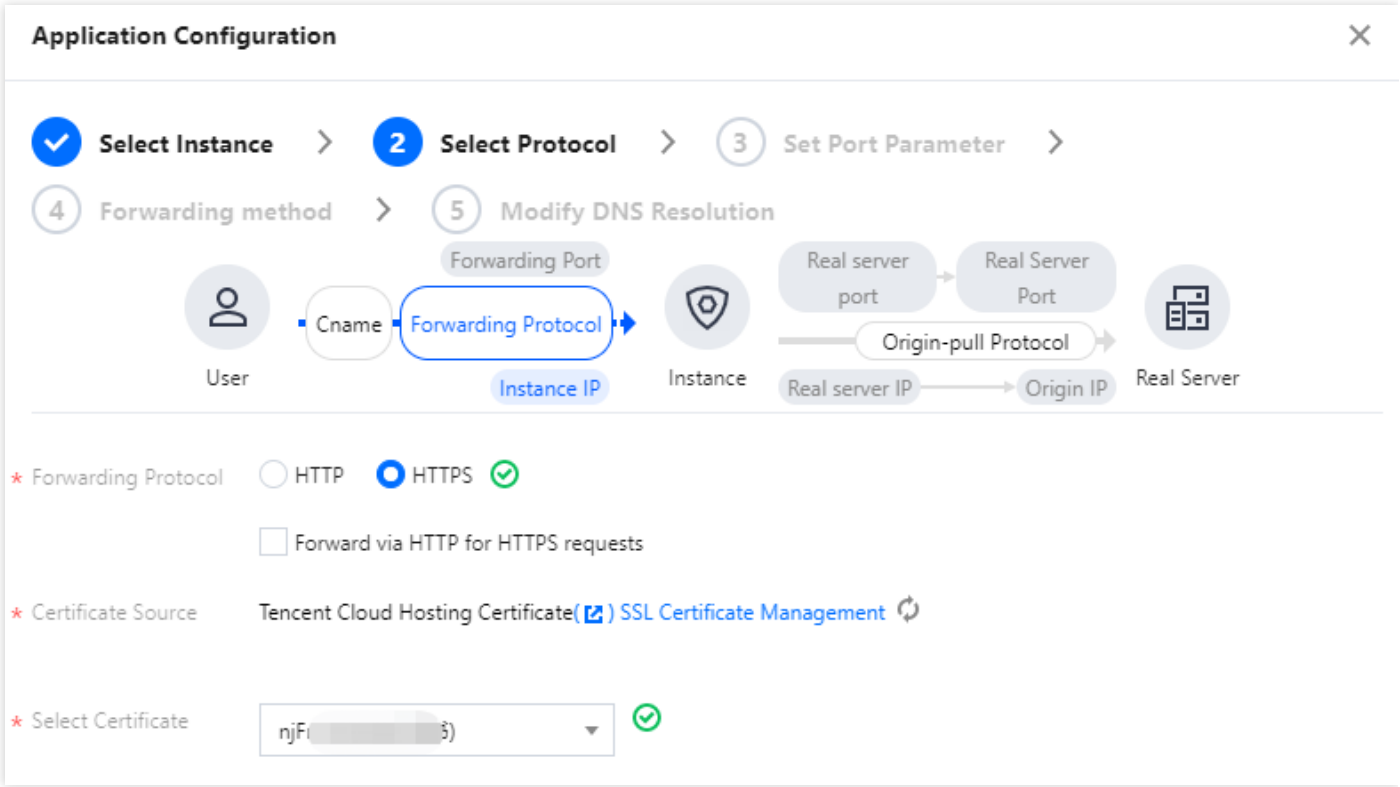
1. Log in to the DDoS Edge Defender Console, click **Applications** on the left sidebar, and then click **Configure Now** at the bottom of the domain-based access page.



2. On the instance setting page, select an associated instance ID and then click **Next: Select Protocol**.



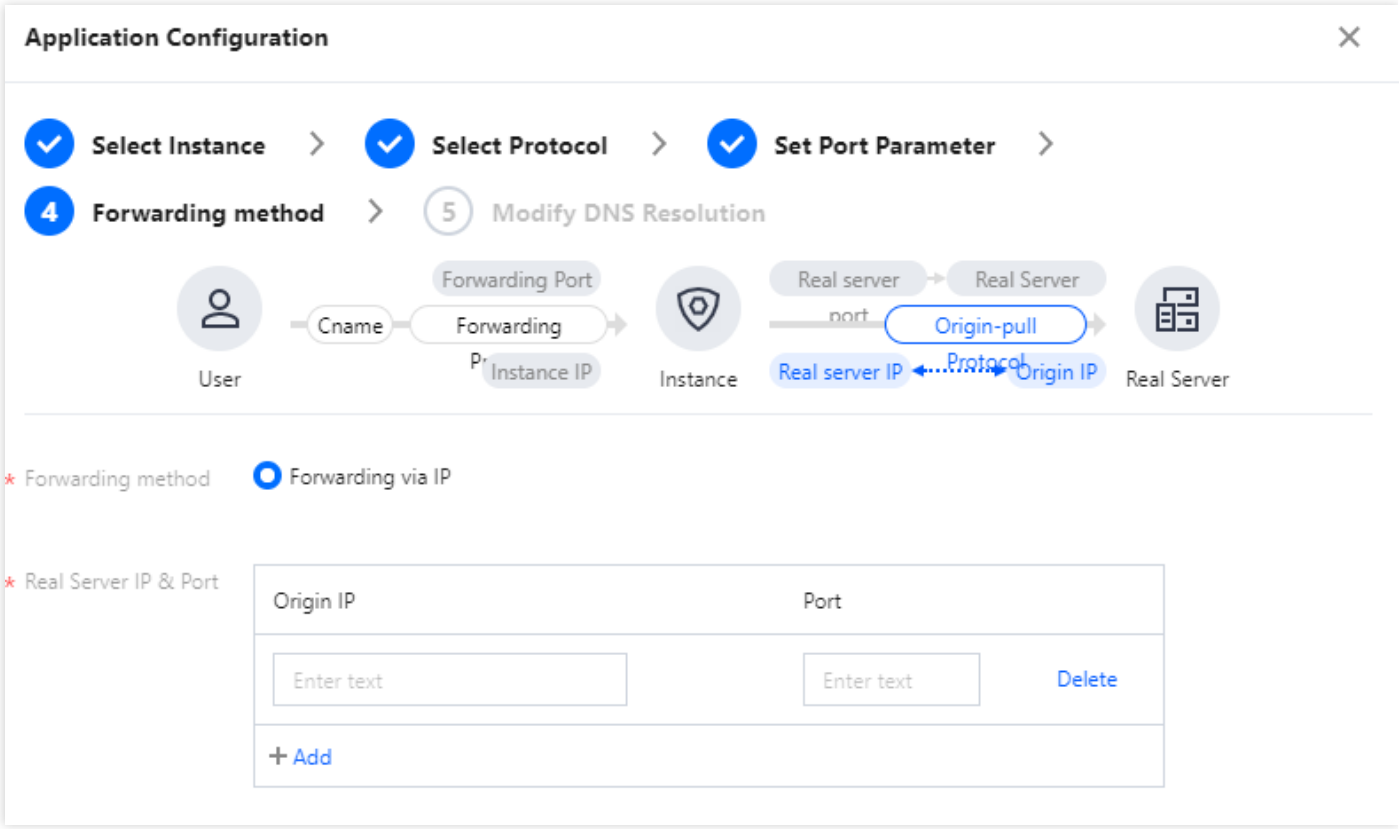
3. On the protocol setting page, select a forwarding protocol prior to clicking **Next: Set Port Parameter**. If you select HTTP, you need to specify the relevant certificate.



4. On the port parameter setting page, enter your application domain, and click **Next: Set Forwarding Method**.

Note :
The domain name can contain up to 67 characters.

5. On the forwarding method setting page, enter the configuration parameters, and click *Next: *Modify Resolution*.



6. Modify the DNS resolution to complete the whole configuration.

Port Rule

Last updated : 2021-09-28 15:53:27

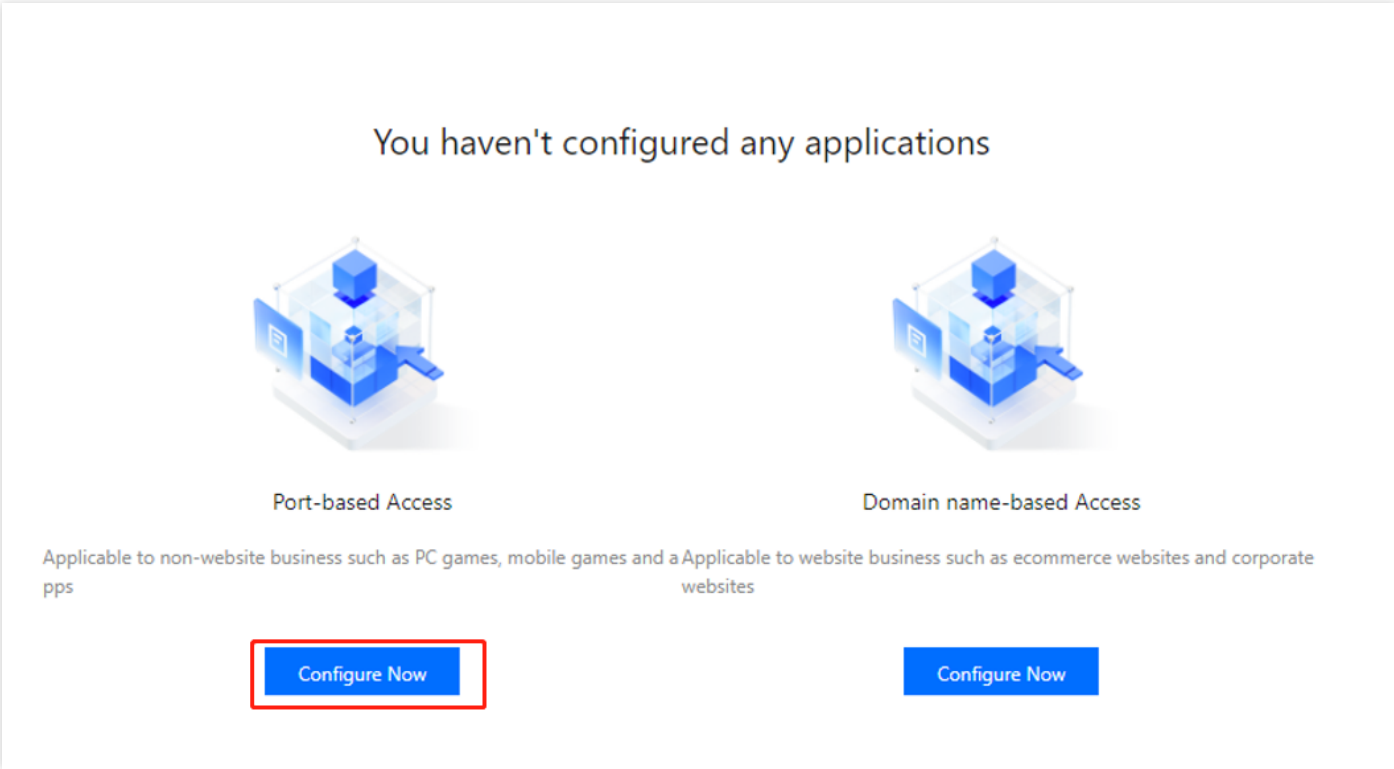
When connecting non-website applications such as PC games, mobile games and apps to DDoS Edge Defender, you need to configure port-based forwarding rules, which is described in this guide.

Prerequisites

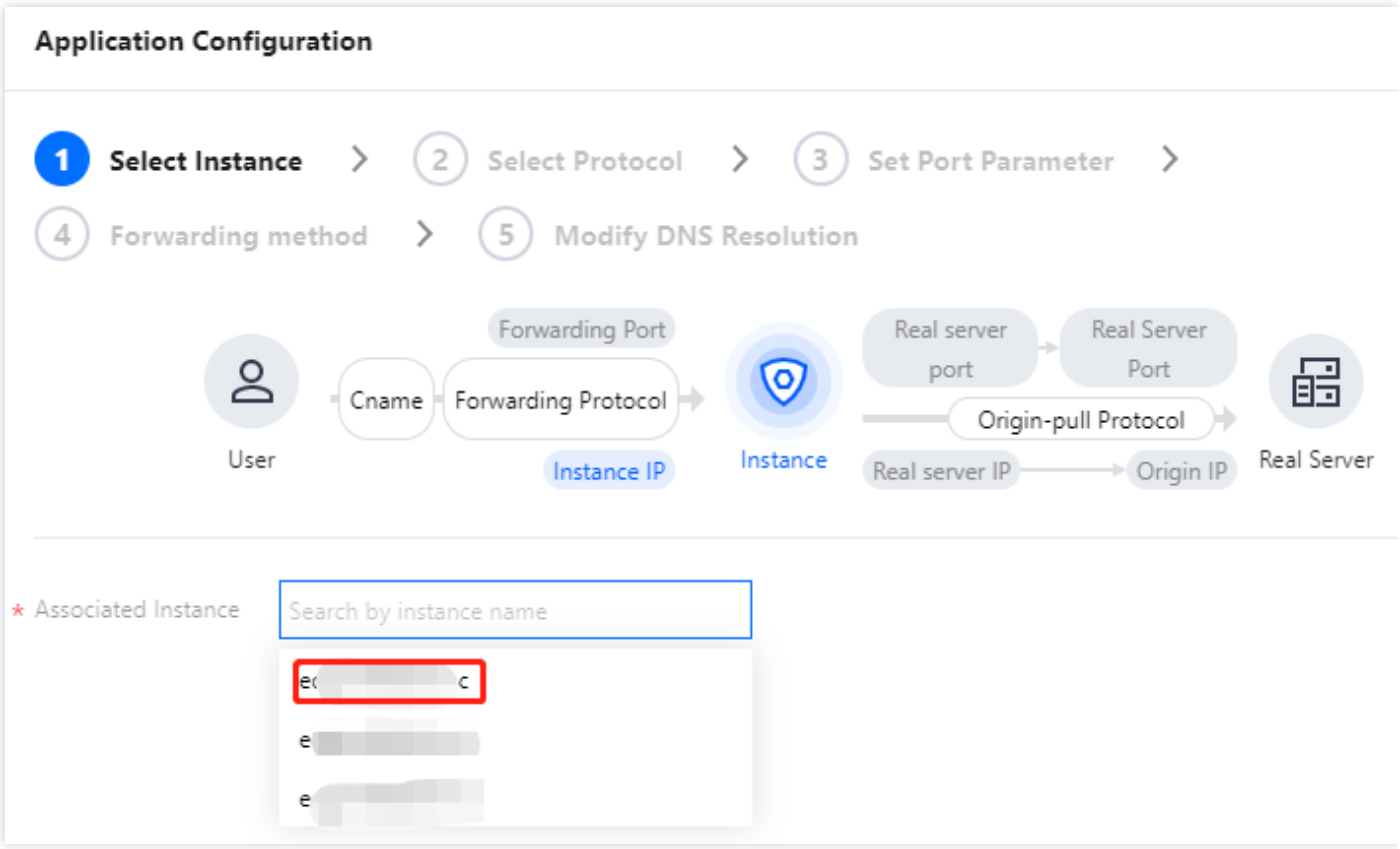
You have purchased a DDoS Edge Defender instance.

Directions

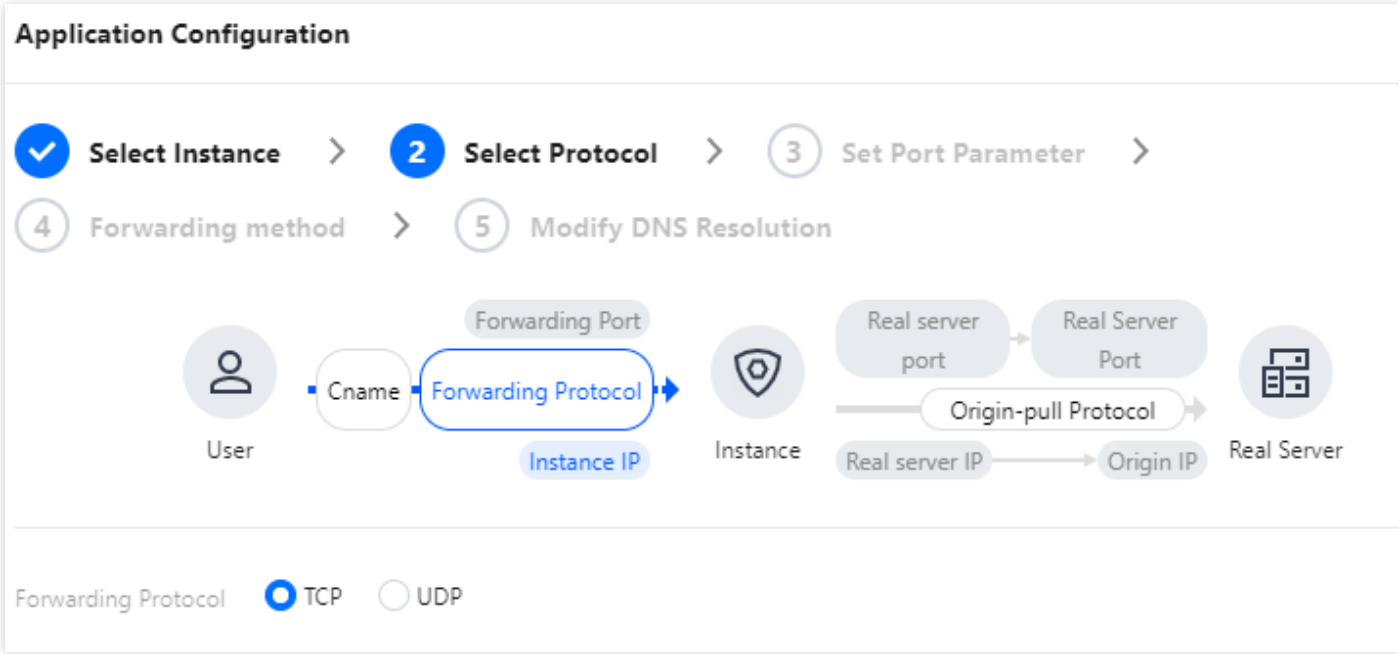
1. Log in to the DDoS Edge Defender Console, click **Applications** on the left sidebar, and then click **Configure Now** at the bottom of the port-based access page.



2. On the instance setting page, select an associated instance ID and then click **Next: Select Protocol**.

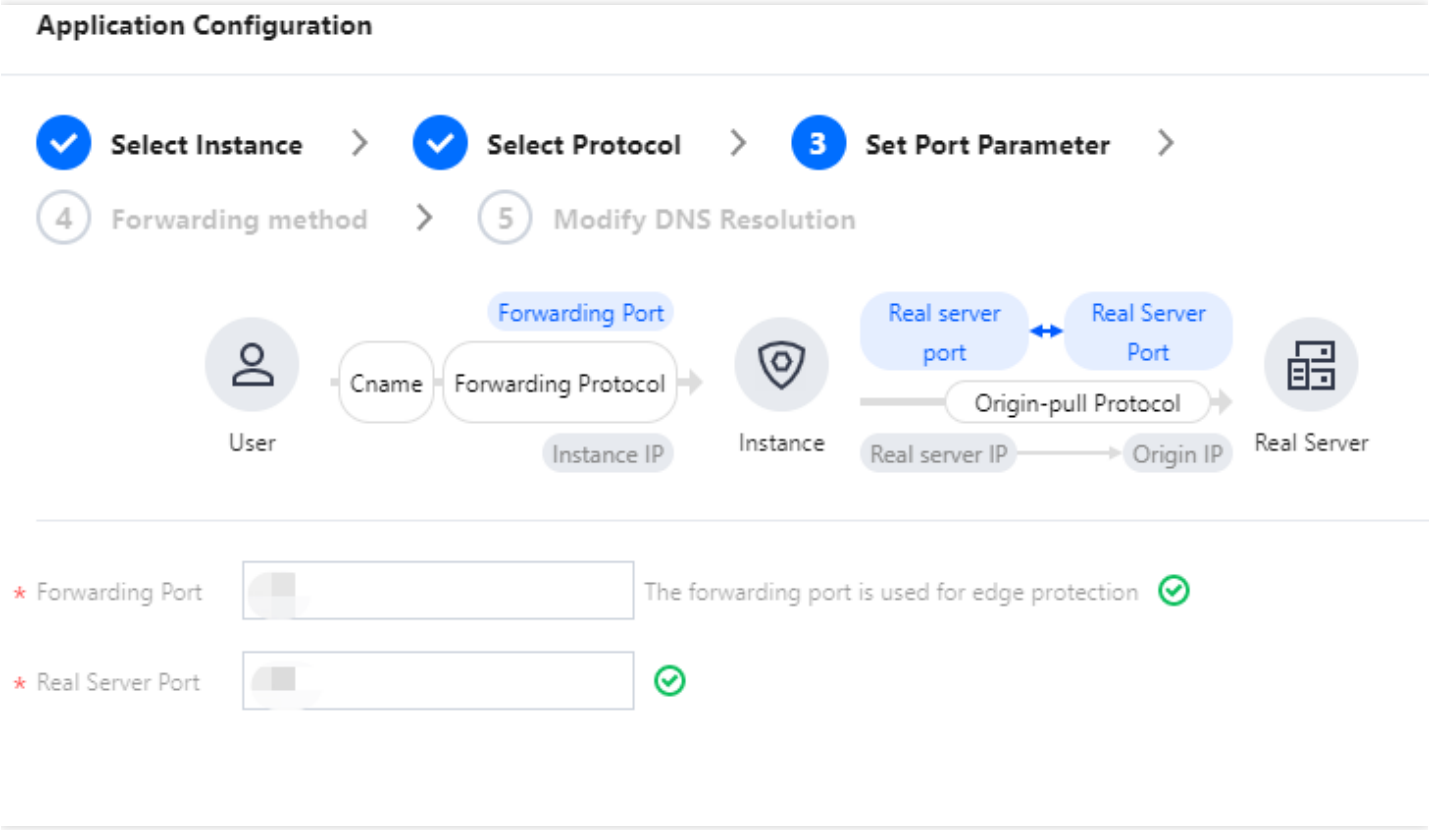


3. On the protocol setting page, select a forwarding protocol prior to clicking **Next: Set Port Parameter**.

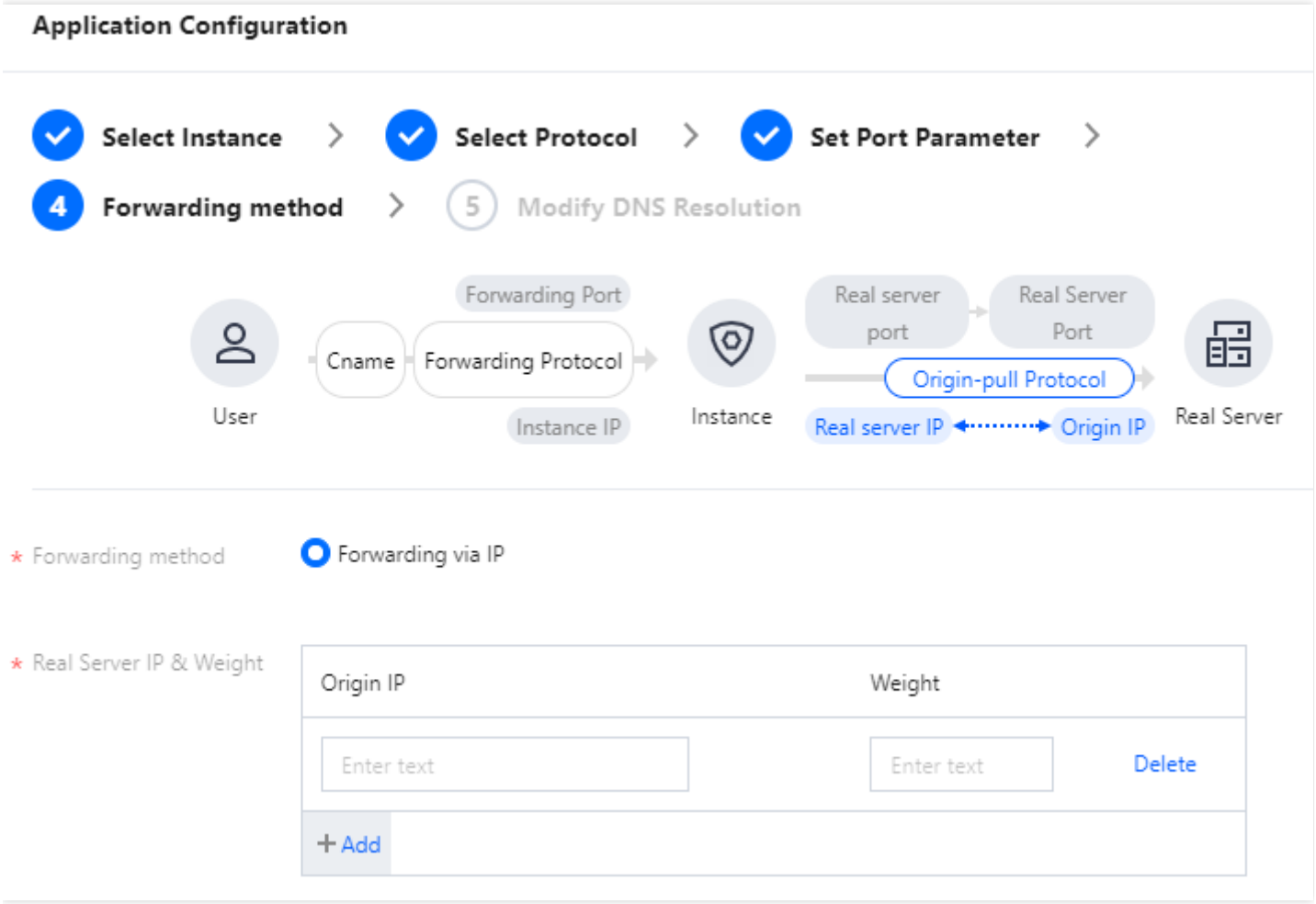


4. On the port parameter setting page, enter your application domain, and click **Next: Set Forwarding Method**.

Note :
The forwarding port and real server port must be an integer in the range 1–65535.



5. On the forwarding method setting page, enter the configuration parameters, and click *Next: *Modify Resolution*.



6. Modify the DNS resolution to complete the whole configuration.