Anti-DDoS Advanced

Operation Guide

Product Documentation

Tencent Cloud

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

Operation Guide

Operation Overview

Last updated：2020-05-13 19:36:21

When you use Anti-DDoS Advanced, you may need to configure Anti-DDoS Advanced instances, view statistical reports, view operation logs, and set security event notifications. This document describes common operations in Anti-DDoS Advanced for your reference.

Instance Management

- Viewing instance details
- Setting resource name
- Configuring elastic protection
- Adjusting Anti-DDoS Advanced instance specification
- Unblocking protected IP

Protection Configuration

- Configuring scenario
- Configuring cleansing threshold and protection level
- Managing advanced DDoS protection Policy
- Configuring CC protection level
- Managing CC protection policy
- Configuring health check
- Configuring session persistence

Statistical Report

Viewing statistical report

Operation Log

Viewing operation log

Security Event Notification

Usage Limits

Last updated：2020-07-30 11:32:26

Scenario

Anti-DDoS Advanced can protect your IPs/domain names that are not deployed on Tencent Cloud. Both website and non-website applications are supported.

Capability

By default, each Anti-DDoS Advance instance supports up to 60 forwarding rules, and each rule supports up to 20 real server IPs/domain names.

Blocklist/Allowlist

- Up to 120 IPs allowed for one DDoS IP blocklist/allowlist
- Up to 50 IPs allowed for one CC IP blocklist/allowlist
- Up to 50 URLs allowed for one CC URL allowlist

Region availability

Anti-DDoS Advanced is available in the following regions:

- Mainland China: South China (Guangzhou), East China (Shanghai), North China (Beijing).
- Outside Mainland China: South China (Hong Kong), Asia-Pacific (Singapore, Seoul, Bangkok, India, Japan), Western U.S. (Silicon Valley), Eastern U.S. (Virginia), North America (Toronto), Europe (Frankfurt, Moscow).

Below is the protection bandwidth range in different regions.

Region	Base Protection	Elastic Protection	Maximum Protection Bandwidth
Guangzhou	20-50 Gbps	30-100 Gbps	100 Gbps
Beijing	20-50 Gbps	30-100 Gbps	100 Gbps
Shanghai	20-100 Gbps	30-300 Gbps	300 Gbps

Region	Base Protection	Elastic Protection	Maximum Protection Bandwidth
Outside Mainland China	10-100 Gbps	30-400 Gbps	400 Gbps

Protection Configuration

Configuring Scenarios

Last updated：2020-05-13 19:50:59

Use Cases

Anti-DDoS Advanced supports custom advanced DDoS protection policies. You can customize protection policies according to your business characteristics or the nature of attacks. In general, you can associate at most one advanced DDoS protection policy with an Anti-DDoS Advanced instance. If you have multiple instances, you can configure up to 5 advanced DDoS protection policies.

You may need to continuously optimize the policies to keep up with actual business needs and ever-changing attacks. To streamline the management of refined DDoS protection, Anti-DDoS Advanced allows you to create scenarios. You can create scenarios, and the backend can collect, identify, and automatically generate advanced protection policies for flexible configuration or maintenance of policies.

Creating Scenario

- **Method 1:**
  If you have not configured any scenario for your Anti-DDoS Advanced instance yet, when you log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar, you will see a message as shown below. Click **Create Now** to create a scenario.

> You can create up to 5 scenarios.

- **Method 2:**

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar. Select the **Advanced DDoS Protection Policy** tab and click **Create Scenario**.

2. On the scenario creation page, configure the following parameters according to your business characteristics and click **OK** to complete the configuration.

   - **Scenario Name:** required; enter a scenario name containing 1–32 characters of any type.

- **Platform:** select the development platform of your business. The options include PC client, mobile, TV, and CVM.
- **Category:** select a service category. The options include game, application, website, and others.
- **Basic Information:**
  - **Users outside China**
    Select **Yes**, **No**, or **Unknown**, indicating disabling or enabling **Reject traffic from outside China**.
  - **Actively initiate outbound TCP requests**
    Select **Yes**, **No**, or **Unknown**. If you select **Yes**, you need to enter the ports that initiate outbound TCP requests. Use commas (,) to separate multiple ports.
  - **Actively initiate outbound UDP requests, such as DNS, NTP requests**
    Select **Yes**, **No** or **Unknown**. If you select **Yes**, you need to enter the ports that initiate outbound UDP requests. Use commas (,) to separate multiple ports.
- **Other Info**: click **Expand** to configure more parameters.
  - **UDP payload with fixed characteristic**
    Select **Yes** or **No**. **No** is selected by default. If you select **Yes**, you need to enter the UDP payload characteristic.
  - **TCP payload with fixed characteristic**
    Select **Yes** or **No**. **No** is selected by default. If you select **Yes**, you need to enter the TCP payload characteristic.
  - **Web API application (separated with comma ",")**
    Select **Yes** or **No**. **No** is selected by default. If you selected **Yes**, you need to enter the API service URL(s). Use commas (,) to separate multiple URLs.

3. The backend will analyze the scenario you created and then automatically generate an advanced protection policy named in the format of `scenario name_policy_number`, such as `test_policy_1`. You can then configure or modify the protection policy as needed.

> - If you **have only one Anti-DDoS Advanced instance (resource)** and **have created only one scenario**, **the generated advanced protection policy will be automatically associated with the instance (resource)**.

- **If you modify the scenario information, the related configuration items in the corresponding advanced protection policy will be automatically modified to keep up with the changes to the scenario.** However, changes to the advanced policy will not be synchronized to the corresponding scenario.

> - When one or more instances (resources) are bound to an advanced protection policy named "scenario name_policy_number.", if the forwarding rule parameters (such as the following parameters) of one instance (resource) are modified, **the corresponding configuration item information in the advanced protection policy will be automatically synced**.
> - (Layer-4) Non-website business: TCP/UDP protocols; forwarding port range.
> - (Layer-7) Website business: HTTP/HTTPS protocols; the forwarding ports are 80/443 by default.

Modifying and Deleting Scenario

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar.
2. Click **Advanced DDoS Protection Policy** and click **Configure** or **Delete** on the right of the target scenario to modify or delete the scenario.

> If a scenario is deleted, the advanced protection policy corresponding to the scenario will also be deleted.

For more information, please see Managing Advanced DDoS Protection Policy.

Configuring Cleansing Threshold and Protection Level

Last updated：2020-07-30 11:59:28

Use Cases

Anti-DDoS Advanced allows you to adjust protection policies and provides three protection levels against DDoS attacks. The protection operations at each level are as described below:

> If you need to use the UDP protocol, please contact Tencent Cloud Technical Support to customize a policy and avoid impact on business operations when in strict mode.

Protection Level	Protection Operation	Description
Loose	• Filters SYN and ACK data packets with explicit attack characteristics. • Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specification. • Filters UDP data packets with explicit attack characteristics.	This cleansing policy is loose and only protects against explicit attack packets. You are recommended only to use this mode when requests are blocked mistakenly. Attack packets may pass through the security system in case of complex attacks.
Normal	• Filters SYN and ACK data packets with explicit attack characteristics. • Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specification. • Filters UDP data packets with explicit attack characteristics. • Filters common attack UDP data packets.	This cleansing policy applies to most businesses and effectively protects against common attacks. The normal mode is configured by default.

	• Actively verifies the source IPs of certain access requests.	
Strict	• Filters SYN and ACK data packets with explicit attack characteristics. • Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specification. • Filters UDP data packets with explicit attack characteristics. • Filters common attack UDP data packets. • Actively verifies the source IPs of certain access requests. • Filters ICMP attack packages. • Filters common UDP attack data packets. • Strictly checks UDP data packets.	This cleansing policy is strict. You are recommended to use this mode when attack packets pass through the security system in Normal mode.

By default, your purchased Anti-DDoS Advanced instance uses the Normal protection level, which can be changed based on your actual business needs. In addition, you can customize the cleansing threshold. If the attack traffic exceeds the threshold, the cleansing policy will be automatically triggered.

Configuration Samples

This section takes instance "bgpip-000002ai" in South China (Guangzhou) as an example to describe the configurations.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List** on the left sidebar, and click **South China (Guangzhou)** in the region selection box.
2. Find the Anti-DDoS Advanced instance whose ID is "bgpip-000002ai" and click **Protection Configuration** in the "Operation" column on the right.

3. In the pop-up Anti-DDoS configuration page, enable **Protection Status** to set the cleansing threshold and protection level.

> The configuration items are visible only when **Protection Status** is ●. If you disable the protection, the configuration items will be hidden and will not take effect. After you enable the protection again, the items will be visible again and retain the original configurations.
> **Configuration parameter descriptions:**

- **Protection status**
  Protection is enabled by default. You can enable or disable it as needed and set the duration for disablement. Currently, the duration can only be 1–6 hours. The Anti-DDoS Advanced instance will automatically enable protection after the set duration elapses or when the attack traffic bandwidth exceeds 1 million pps or 2 Gbps.
  - **Cleansing threshold**
- It indicates the threshold to trigger cleansing. If the traffic is below the threshold, no cleansing operation will be executed even if attacks are detected.
- After protection is enabled, the Anti-DDoS Advanced instance, if just connected to your business, will use the default cleansing threshold value by default. As the business traffic changes, the system will automatically learn to calculate a baseline value. You can set the cleansing threshold based on your business protection needs at any time.
  If you have a clear concept about the threshold, set it as needed; otherwise, please use the default value. Anti-DDoS will automatically learn through AI algorithms and calculate the default threshold for you.

> - **Protection level**
>   After protection is enabled, the Anti-DDoS Advanced instance, if just connected to your business, will use the Normal protection level by default. You can adjust the level based on your business protection needs at any time.

- **Other configuration items**
- **Business scenario**
  You can select and modify a matched business scenario from the created ones as needed. When a business scenario is selected, the corresponding "advanced policy" will be automatically generated accordingly. For more information on how to create a business scenario, please see Configuring Business Scenarios.
  - **Advanced policy**
    You can select and modify a matched advanced policy from the created ones based on your business protection

characteristics. For more information on how to create an advanced policy, please see Managing Anti-DDoS Advanced Policies.

- **Alarm threshold for DDoS attacks**

  You can configure an alarm threshold for DDoS attacks. If the detected metric exceeds the set threshold, an alarm will be triggered and alarm notifications will be pushed to you. For more information on how to set an alarm threshold, please see Configuring Attack Alarm Thresholds.

- **AI-based enhanced protection for TCP business**

  For layer-4 TCP business, Anti-DDoS Advanced provides AI-based enhanced protection. After this feature is enabled, through self-learning of business routine characteristics with the aid of AI models, Anti-DDoS Advanced can automatically distinguish between business traffic and attack traffic, effectively defending your business against layer-4 CC attacks.

  Currently, AI-based enhanced protection for TCP business is only available to allowed users.

Manage DDoS advanced protection strategy

Last updated：2020-07-30 12:03:25

Anti-DDoS Advanced provides advanced protection policies against DDoS attacks. You can adjust and optimize the DDoS protection policy as required through blocklists/allowlists, disabling protocols, disabling (discarding) or opening ports, packet characteristic filtering, connection flood protection, and watermark protection.

Configuration Item Overview

Configuration Item	Description	Effective Time
Blocklist/Allowlist	It is IP-based protection. • It always allows requests from IPs in the allowlist. • It always blocks requests from IPs in the blocklist.	It takes effect immediately when the protected IPs are under attack.
Disabled protocol	It disables a protocol not used by the business. If attacks are detected, the Anti-DDoS cluster will cleanse the traffic under the protocol.	It takes effect immediately when the protected IPs are under attack.
Disabled (discarded) or passed port	You can disable or pass traffic from the specified type of ports.	When an attack is detected, the Anti-DDoS cluster will cleanse (or pass) the traffic on the specified port or specified port range.
Packet filter characteristic	It combines multiple criteria to set policy operations, such as the protocol, port range, packet range, whether to detect load, offset, detection depth, and whether to include characteristic strings based on the business or attack packets. If the packets match the policy criteria, operations such as direct forwarding, discarding, source IP blocking, or disconnecting can be executed.	It takes effect immediately when the protected IPs are under attack.
Speed limit	It is IP-based protection and limits the speed of the access protocol.	It takes effect immediately when the protected IPs are under attack.

Configuration Item	Description	Effective Time
Reject traffic from outside China	It rejects TCP traffic requests from outside China (including Mainland China, Hong Kong, Macao, and Taiwan).	It takes effect when the protected IPs are under attack.
Connection flood protection	It is IP-based protection, which limits the speed, packet length, and other parameters of connections accessing non-website IPs protected by Anti-DDoS Advanced to protect against light traffic connection attacks.	It takes effect immediately when the protected IPs are under attack.
Exceptional connection detection	When a source IP receives a TCP connection meeting the configured parameter characteristics, the connection will be regarded as exceptional. If the amount of exceptional connections received by the source IP exceeds the maximum allowable number, the IP will be added to the blocklist for a certain period and will not be accessible.	It takes effect immediately when the protected IPs are under attack.
Watermark protection	It supports UDP and TCP packets. Watermark detection and stripping will be executed for the payloads within the configured port range. Watermark protection can protect against layer-4 CC attacks, such as forged business packet attacks and replay attacks. • Customer client and Tencent Cloud Anti-DDoS Advanced system share the same watermark algorithm and key. • Each packet sent by the client is embedded with watermark characteristic which attack packets do not have. • The Anti-DDoS Advanced system will identify and discard attack packets.	It takes effect immediately when the protected IPs are under attack.

Adding Policies

> Configuration of advanced protection policy requires technical expertise. You are recommended to read the operation guide before configuring policies as needed.

Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Add Policy**. Configure the following parameters as needed and click **OK**.

- **Policy Name**
  Enter a policy name containing 1–32 characters of any type.

- **Blocklist/Allowlist**
  - If you need to set a blocklist, click **Add**, select **Blocklist**, enter IPs to block, and then click **OK**. Separate multiple IPs with carriage returns.
  - If you need to set a allowlist, click **Add**, select **Allowlist**, enter the IP to allow directly, and then click **OK**. Separate multiple IPs with carriage returns.

  > You can add up to 100 IPs for the blocklist and allowlist. The number of IPs to be added in batches cannot exceed the current available quota.

- **Disabled Protocol**

- Select the protocol to be disabled. The speed of ICMP, TCP, UDP and other protocols can be limited.

- **Port Number**
  Select the protocol and port type, enter the corresponding port, and choose the discarding or passing action according to your business needs. If you need to configure a continuous port range, you can use the "start port-end port" format.

- **Packet Filter Characteristic**
  Set conditions such as the protocol, port range, packet length, payload detection, offset, detection depth, and characteristic strings and configure the action to be taken for immediate effect.

  > - Offset: specifies the start position of the matched characteristics in the packet.
  > - Detection depth: specifies the packet length from the position set by the offset to the end of the matching content. It is used with the offset.
  > - Policy:
  >   - "Discard packet": discards the data packet matching the packet filter characteristic.
  >   - "Discard packet and block source IP": discards the data packet matching the packet filter characteristics and temporarily blocks the source IP.
  >   - "Discard packet and disconnect": discards the data packet matching the packet filter characteristics and closes the TCP connection.

- **Discard packet, disconnect, and block source IP**: discards the data packet matching the packet filter characteristics, closes the TCP connection, and temporarily blocks the source IP.
- **Directly forward**: directly forwards the data packets matching the packet filter characteristics.

- **Speed Limit**
  Click **Add**, select the protocol for speed limit, and then set the limit threshold. The speed of ICMP, TCP, UDP, and other protocols can be limited.

- **Reject Traffic from Outside China**
  Select "Enable" or "Disable". The protection engine of Anti-DDoS Advanced is embedded with an IP library containing IPs from outside China. If you enable this feature, source IPs in the library will be rejected. The **Enable** operation takes effect when attacks occur. The **Disable** operation takes effect immediately.

- **Connection Flood Protection**
  - **Null Session Protection**: select "Enable" or "Disable". The **Enable** operation takes effect when attacks occur. This feature is implemented based on TCP proxy and may affect the initial business access.
  - **Source New Connection Limit**: select "Enable" or "Disable". After selecting **Enable**, you need to set the rate threshold (unit: connection/sec) in the range of 0–∞. It specifies the number of new connections established by a source IP per second. New connections exceeding the upper limit will be discarded.
  - **Source Concurrent Connection Limit**: select "Enable" or "Disable". After selecting **Enable**, you need to set the quantity threshold in the range of 0–∞. It specifies the maximum allowed number of concurrent connections of a source IP. Concurrent connections exceeding the upper limit will be discarded.
  - **Destination New Connection Limit**: select "Enable" or "Disable". After selecting **Enable**, you need to set the rate threshold (unit: connection/sec) in the range of 0–∞. It specifies the maximum number of new connections established by a destination IP per second. New connections exceeding the upper limit will be discarded. Due to cluster-based deployment of the protection devices, deviation exists for the speed limit of new connections.
  - **Destination Concurrent Connection Limit**: select "Enable" or "Disable". After selecting **Enable**, you need to set the quantity threshold in the range of 0–∞. It specifies the maximum number of concurrent connections of a destination IP. Concurrent connections exceeding the upper limit will be discarded. Due to cluster-based deployment of the protection devices, deviation exists for the speed limit of concurrent connections.

- **Exceptional Connection Detection**
  - **Maximum Exceptional Source IP Connections**: click **Enable** and enter the maximum allowed number of exceptional source IP connections in the range of 0–∞. It specifies the maximum number of exceptional connections allowed for a source IP. If the number exceeds the threshold, the source IP will be identified as exceptional and will be blocked for a while.

> The following parameters can be configured only if **Maximum Number of Exceptional Source IP Connections** is enabled.

- **Syn Packet Ratio Detection**: select "Enable" or "Disable". After selecting **Enable**, you need to set the Syn packet ratio in the range of 0–100. It specifies the threshold ratio of Syn packets and Ack packets for a TCP connection to be identified as exceptional.
- **Syn Packet Number Detection**: select "Enable" or "Disable". After selecting **Enable**, you need to set the maximum allowed number of packets in the range of 0–65535. It specifies the threshold number of Syn packets for a TCP connection to be identified as exceptional.
- **Connection Timeout Detection**: select "Enable" or "Disable". After selecting **Enable**, you need to set the detection cycle (unit: second) in the range of 0–65535. It specifies the threshold period during which no packets are transmitted for an established TCP connection to be identified as exceptional.
- **Exceptional Null Session Detection**: select "Enable" or "Disable". It specifies that an established TCP connection will be identified as exceptional if it has no packets with payload.

- **Watermark Protection**
  Click **Enable** to configure watermark protection. Enter a specified TCP protection port and UDP protection port, and then click **OK** to make the watermark protection take effect. Adding an advanced DDoS protection policy will automatically generate a key. You need to add the watermark configuration to the client offline.

- **TCP Protection Port and UDP Protection Port**
  A TCP/UDP protection port can be configured with up to 5 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.

> Only when the UDP protocol port range is configured can UDP watermark be removed. You can also specify the offset of the watermark tag in the UDP packet.

- **UDP Watermark Removal**
  Select **Automatically Remove UDP Packet Watermark**. After the data packet passes through the security protection system, the watermark in a UDP packet will be automatically removed and then transferred to the real server.

> If the Anti-DDoS system is not required to remove the UDP watermark, then the client needs to be modified for watermark removal.

- **Offset**
  Specify the offset of the watermark tag in the UDP packet. The default value is 0, and the value range is 0–99. The offset only works after UDP watermark removal is enabled.

Binding and Unbinding Resource

Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Bind Resource** next to the target policy.

- Bind Resource: in the pop-up **Bind Resource** dialog box, select one or more resources as needed and click **OK**.
- Unbind Resource: in the pop-up **Bind Resource** dialog box, click ✕ to the right of a resource in the **Selected** section and click **OK**.

Adding Watermark to Client

Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Download Client Watermark File** next to the target policy to add the watermark to the client offline.

Adding, Deleting, or Disabling/Enabling Watermark Key

Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Watermark Key Configuration** next to the target policy.

- **Add Key**: in the pop-up **Key Information** dialog box, click **Add Key** to generate a key.
- **Disable**/**Enable Key**: you can disable or enable a key. In the pop-up **Key Information** dialog box, click **Disable** next to the target key. If you need to enable it again, click **Enable**.
- **Delete Key**: you can delete a disabled key. In the pop-up **Key Information** dialog box, click **Delete** next to the target key.

> At most 2 keys can exist at one time. If you need to add more keys, please delete an existing one first. If only one key is activated, you cannot disable or delete it.

Configuring Policy

Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Configuration** next to the target policy. Update the following parameters as required, and then click **OK**.

> You cannot modify a policy name in the "scenario name_policy_No." format.

- Policy Name
- Blocklist/Allowlist
- Disabled Protocol
- Port Number
- Packet Filter Characteristic
- Reject Traffic from Outside china
- Connection Flood Protection
- Exceptional Connection Detection
- Watermark Protection

Deleting Policy

- You can directly delete a policy without bound resources. To delete a policy with bound resources, unbind the resources first.
- If UDP watermark removal is enabled, deleting the policy will disable UDP watermark removal at the same time. Verify whether corresponding configuration or change has been completed on both the client and server first before deleting the policy.
- A deleted policy cannot be recovered.
- **You cannot delete an advanced protection policy automatically generated for your created scenario.**

Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Delete** next to the target policy. In the pop-up dialog box, click **OK**.

Configure CC protection level

Last updated：2021-01-27 11:11:39

Protection Description

In order to improve the protection effect and reduce the risk of false blocking during protection, Anti-DDoS Advanced has three protection levels for CC attacks for your choice, and the "normal" level is used by default.

- **Loose**: this level can be used when the protected website has no obviously exceptional traffic. It performs a looser human-machine recognition algorithm check on all requests made to the protected website, that is, each visitor is verified and only successfully authenticated visitors are allowed to access the website. As the CC protection policy at this level is relatively loose, there may be a risk of passing through a small number of exceptional requests.
- **Normal**: this level is the default CC protection level. It is recommended if you find that the protected website is under CC attacks. Compared with the loose level, the normal level of CC protection can cover most of attack scenarios and defend against most of CC attacks. In addition, it performs a human-machine recognition algorithm check on all requests made to the protected website, that is, each visitor is verified and only successfully authenticated visitors are allowed to access the website.
- **Strict**: the CC attack protection policy is stricter at this level and can defend against more complex CC attacks. In addition, it performs a strict human-machine recognition algorithm check on all requests made to the protected website, that is, each visitor is verified and only successfully authenticated visitors are allowed to access the website. Due to the strict authentication mechanism in this mode, some normal requests may be blocked by mistake.

  - The protection algorithms used at the above three CC protection levels are only applicable to webpages and HMTL5 pages.
  - If the business of the visited website is an API or a native app, as such businesses generally cannot respond to algorithm-based authentication normally, there is a great risk of false blocking.
  - If you need CC protection for API or native app businesses, please submit a ticket for protection policy customization.

Directions

By default, the normal level of CC protection is used for domain names of websites protected by Anti-DDoS Advanced instances. You can freely adjust the protection mode according to your actual business needs.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar, and click **CC Protection** on the protection policy page.
2. On the CC protection page, find the HTTP CC protection and HTTPS CC protection section at the bottom of the page, select the domain name that requires CC protection under the corresponding protocol, and set the CC protection level.

    - The CC protection level policy only takes effect for domain names with the access configured as website business (layer-7 access).
    - If you haven't connected the website domain name to be configured to an Anti-DDoS Advanced instance, please connect it first as instructed in Connecting Website Business.

For more information, please see Managing CC Protection Policy.

Manage CC protection policies

Last updated：2020-07-30 12:00:19

Anti-DDoS Advanced supports HTTP/HTTPS CC protection. When the number of HTTP/HTTPS requests recorded by Anti-DDoS Advanced exceeds the set **maximum number of HTTP/HTTPS requests**, HTTP/HTTPS CC protection will be automatically triggered.

Anti-DDoS Advanced allows you to set an ACL. By enabling HTTP/HTTPS CC protection, you can use common HTTP/HTTPS packet fields (such as host, CGI, Referer, and User-Agent parameters) to set matching conditions, so as to control access requests from internet users, i.e., blocking requests that hit the conditions or triggering CAPTCHA verification. You can also set speed limit rules to limit the speed of access IPs.

Anti-DDoS Advanced also allows you to configure URL allowlist, IP allowlist, and IP blocklist.

- For URLs in the allowlist, their access requests do not require CC attack detection and can pass directly.
- For IPs in the allowlist, their HTTP/HTTPS access requests do not require CC attack detection and can pass directly.
- For IPs in the blocklist, their HTTP/HTTPS access request will be directly denied.

Enabling CC Protection

HTTP CC protection

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar. On the protection configuration page, click **CC Protection** and select the target instance.
2. In the **HTTP CC Protection** section, click on the right of **Protection Status** to enable HTTP CC protection. Then, click the drop-down list on the right of **Maximum Number of HTTP Requests** to select an appropriate upper limit.

> CC protection is disabled by default. Only after it is enabled can the maximum number of HTTP requests be set.

HTTPS CC protection

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar. On the protection configuration page, click **CC Protection** and select the target instance.
2. In the **HTTPS CC Protection** section, select a protected domain name and click on the right of **Protection Status** to enable HTTPS CC protection. Then, click the drop-down list on the right of **Maximum Number of**

HTTPS Requests to select an appropriate upper limit.

> CC protection is disabled by default. Only after it is enabled can the HTTPS requests threshold be set.

Customizing CC Protection Policies

- **Only after HTTP/HTTPS CC protection is enabled can you customize CC protection policies. Up to 5 policies can be added.**
- **A custom policy will take effect only when your Anti-DDoS Advanced instance is under attack.**
- In **match mode**, each custom policy may have up to **four** conditions for characteristic control, and the logical relationship between these conditions is "AND", which means all conditions must be matched before the policy will take effect.
- In **speed limit mode**, each custom policy can have only **one** condition.

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar to enter the protection configuration page. Click **CC Protection**, select the region, line, and target instance, and click **Add ACL**.
2. In the **Add ACL** pop-up window, set the following parameters as needed and click **OK**.

- Policy Name
  Enter the policy name, which can contain 1–20 characters of any type.
- Protocol
  Currently, HTTP and HTTPS are supported.
- Protected Domain Name
  Only when HTTPS is selected can a protected domain name be selected accordingly. You can select the protected domain name range, i.e., HTTPS website domain names in the configured forwarding rules.
- Mode
- Match mode: if an HTTP/HTTPS request with the specified field header is detected, it will be blocked or processed for CAPTCHA verification.
- Speed limit mode: the speed of access requests from the source IP will be limited. **This mode is not supported for HTTPS.**

- Policy
- **If the **match mode** is selected and the protocol is HTTP**, multiple fields of an HTTP packet, namely, host, CGI, Referer, and User-Agent parameters, can be combined in various logical relationships such as "INCLUSIVE", "EXCLUSIVE", and "EQUAL TO", and you can set up to four policy conditions to combine the fields. **If the protocol is HTTPS**, multiple fields of an HTTPS packet, namely, CGI, Referer, and User-Agent parameters, can be combined in various logical relationships such as "INCLUSIVE", "EXCLUSIVE", and "EQUAL TO", and you can set up to three policy conditions to combine the fields. The fields are as described below:

Matched Field	Description	Applicable Logical Operators
host	Domain name of the access request.	INCLUSIVE, EXCLUSIVE, and EQUAL TO
CGI	URI of the access request.	INCLUSIVE, EXCLUSIVE, and EQUAL TO
Referer	Source website address of the access request, indicating the page from which the access request is generated.	INCLUSIVE, EXCLUSIVE, and EQUAL TO
User-Agent	Information such as browser identifier of the client that initiates the access request.	INCLUSIVE, EXCLUSIVE, and EQUAL TO

- When you select the **speed limit mode**, the speed of each source IP access request will be limited. You are allowed to set only one policy condition.
- Run
  This parameter is required only when the **match mode** is selected, indicating the action that needs to be performed after a policy is matched, such as blocking or CAPTCHA verification.

Setting Blocklist/Allowlist

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar to enter the protection configuration page. Click **CC Protection** and select the region, line, and target instance.
2. Select **HTTP** or **HTTPS** on the right of the page and select **URL allowlist**, **IP allowlist**, or **IP blocklist** to set the blocklist/allowlist. You can add or modify entries or export/import them in batches.

Configure Health check

Last updated：2020-05-13 19:51:00

Operation Scenarios

Anti-DDoS Advanced can automatically identify the running status of your real servers and isolate exceptional ones through health checks. This reduces the impact of real server exceptions on your overall business availability.

- **Non-website business (layer-4) health check**
  The health check mechanism for non-website business protection in Anti-DDoS Advanced is as follows: an Anti-DDoS cluster node initiates access requests to the server port specified in the configuration. If access to the port is normal, the real server will be considered healthy; otherwise, it will be considered exceptional.
  Under the TCP protocol, it detects whether the port can be connected. Under the UDP protocol, it uses ping for reachability check.
- **Website business (layer-7) health check**
  The health check mechanism for website business protection in Anti-DDoS Advanced is as follows: the Anti-DDoS forwarding cluster sends HTTP requests to the real server, and the Anti-DDoS system judges whether the server is normal according to the returned HTTP status codes.
  You can customize the status represented by the response code. For example, in a certain scenario, if HTTP returned values include http_1xx, http_2xx, http_3xx, http_4xx, and http_5xx, and you define http_1xx and http_2xx as normal status based on your business needs, then when a response code between http_3xx to http_5xx is returned, you can know that the server is exceptional.

> When configuring a layer-4 or layer-7 forwarding rule, if only one real server IP is configured in the rule, the health check feature will not be enabled, as it is suitable for scenarios with multiple real server IPs.

Directions

Health check configuration for non-website business

The following describes how to configure a health check rule for non-website business protection in Anti-DDoS Advanced.

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Access Configuration** to enter the management page.

2. Click **Non-Website Business**, select the target Anti-DDoS Advanced instance and corresponding rule, and click **Edit** in the "Health Check" column.

3. On the health check editing page, click **Show Advanced Options** to set the configuration items and click **OK**.

> - Health check is enabled by default.
> - When configuring health check, you are recommended to use the default values.
> - The health check configuration information can be imported and exported in batches. After import, the system will match the rules one by one according to the imported "forwarding protocols and forwarding ports", and the "forwarding ports" must have rules configured.

Health check configuration for website business

The following describes how to configure a health check rule for website business protection in Anti-DDoS Advanced.

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Access Configuration** to enter the management page.

2. Click **Website Business**, select the target Anti-DDoS Advanced instance and corresponding rule, and click **Edit** in the "Health Check" column.

3. On the health check editing page, click to enable health check and click **Show Advanced Options** to set the configuration items. After confirming that everything is correct, click **OK**.

```
- Health check is disabled by default.
- When configuring health check, you are recommended to use the default values.
- The health check configuration information can be imported and exported in batc
hes. After import, the system will match the rules one by one according to the im
ported "forwarding protocols and business domain names", and the "business domain
names" must have rules configured.
```

Configuration Item Description

Layer-4 health check

Configuration Item	Description
Response timeout period	Maximum response timeout period for health check. If a real server fails to respond properly within the timeout period, the health check will be considered as failed.
Check interval	Interval between two health checks.
Unhealthy threshold	When the health check status is "succeeded", if the health check "failed" status is received for n times (n is the entered number) in a row, the real server will be considered as unhealthy, and an exception will be displayed in the console.
Healthy threshold	When the health check status is "failed", if the health check "succeeded" status is received for n times (n is the entered number) in a row, the real server will be considered as healthy, and nothing will be displayed in the console.

Layer-7 health check

Configuration Item	Description
Check interval	Interval between two health checks, which is 15 seconds by default.
Unhealthy threshold	When the health check status is "succeeded", if the health check "failed" status is received for n times (n is the entered number) in a row, the real server will be considered as unhealthy, and an exception will be displayed in the console.
Healthy threshold	When the health check status is "failed", if the health check "succeeded" status is received for n times (n is the entered number) in a row, the real server will be considered as healthy, and nothing will be displayed in the console.
HTTP request method and check path URL	The HEAD method is used by default, and the server will return only the header of the response packet. If the GET method is used, the server will return the complete response packet. The corresponding real server needs to support HEAD and GET. • If the page used for health check is not the default homepage of the application server, you need to specify a specific check path. • If the `host` field parameter is specified in the HTTP HEAD request, you need to specify the check path, i.e., the URI of the page file used for the health check.
HTTP status code detection	The HTTP status code used to determine whether the server is normal during health check. By default or if no selection is made, this value is http_1xx, http_2xx, http_3xx, and http_4xx. If the returned HTTP status code is not the default status value, the server will be considered as unhealthy. This value can be modified.

Configure Session to keep

Last updated：2020-05-13 19:51:00

Operation Scenarios

The non-website business protection service of Anti-DDoS Advanced provides IP-based session persistence to support forwarding requests from the same IP address to the same real server for processing.
Layer-4 forwarding supports simple session persistence. The session persistence duration can be set to any integer between 30 and 3600 seconds. If the time threshold is exceeded and the session has no new request, the connection will be automatically closed.

Directions

The following describes how to configure a session persistence rule for non-website business protection in Anti-DDoS Advanced.

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Access Configuration** on the left sidebar to enter the management page.

2. On the **Non-Website Business** tab, select the target Anti-DDoS Advanced instance and the corresponding rule, and click **Edit** in the "Session Persistence" column.

3. On the **Edit Session Persistence** page, click to enable session persistence, set the persistence duration, and click **OK**.

> - Session persistence is disabled by default.
> - When setting the persistence duration, you are recommended to use the default value.
> - The session persistence configuration information can be imported and exported in batches. After import, the system will match the rules one by one according to the imported "forwarding protocols and forwarding ports", and the "forwarding ports" must have rules configured.

Configuring Intelligent Scheduling

Last updated：2019-12-05 19:09:10

Use Cases

Each account can have multiple Anti-DDoS instances, and each instance has at least one protective line; therefore, there can be multiple protective lines under one account. Once your business is added to an Anti-DDoS instance, a protective line will be configured for it. If multiple protective lines have been configured, you need to choose the optimal business traffic scheduling method, i.e., how to schedule business traffic to the optimal line for protection while ensuring high business access speed and availability.
Anti-DDoS features priority-based CNAME intelligent scheduling, where you can select an Anti-DDoS instance and set the priority of its protective line as needed.

> Anti-DDoS Pro (includes single-IP and multi-IP instances) and Anti-DDoS Advanced instances support setting resolution.

Priority-based Scheduling

This refers to using the protective line of the highest priority to respond to all DNS requests, i.e., all access traffic will be scheduled to the protective line of the currently highest priority. You can adjust the priority value of protective line, which is 100 by default. The smaller the value, the higher the priority. The specific scheduling rules are as follows:

- If the protective instance configured for your business contains multiple protective lines from different ISPs and of the same priority, response will be made based on the ISP of the specific DNS request. If one of the lines is blocked, access traffic will be scheduled in the order of BGP > China Telecom > China Unicom > China Mobile > ISP outside Mainland China.
- If all the lines of the same priority are blocked, access traffic will be automatically scheduled to the currently available protective line of the second-highest priority.

  > If no protective lines of the second-highest priority are available, automatic scheduling cannot be completed, and business access will be interrupted.

- If the protective instance configured for your business contains multiple protective lines from the same ISP and of the same priority, access traffic will be scheduled by way of load balancing, i.e., evenly distributed to such lines.

Example

Assume that you have the following Anti-DDoS instances: BGP protective IPs 1.1.1.1 and 1.1.1.2, China Telecom protective IP 2.2.2.2, and China Unicom protective IP 3.3.3.3, of which the priority of 1.1.1.2 is 2 and that of the rest is 1. Normally, all traffic will be scheduled to the protective lines with the current priority of 1. Specifically, traffic from China Unicom will be scheduled to 3.3.3.3, that from China Telecom to 2.2.2.2, and that from other ISPs to 1.1.1.1. If 1.1.1.1 is blocked, access traffic under this IP will be automatically scheduled to 2.2.2.2. If both 1.1.1.1 and 3.3.3.3 are blocked, traffic supposed to be scheduled to them will be distributed to 2.2.2.2, and if 2.2.2.2 is blocked too, traffic will be scheduled to 1.1.1.2.

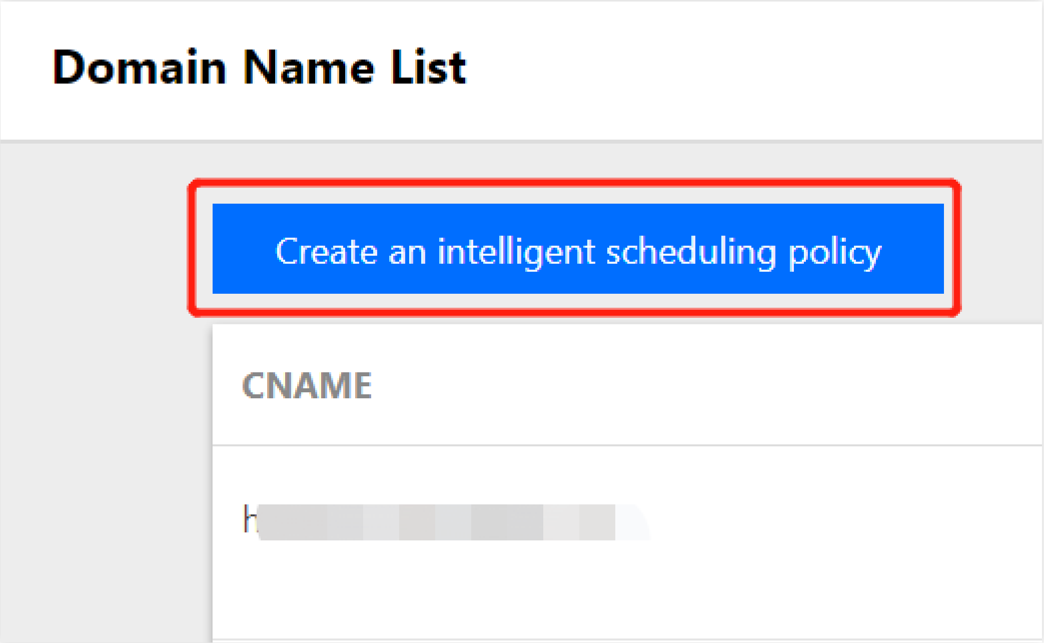
Prerequisites

- Before enabling intelligent scheduling, please connect your business to be protected to your Anti-DDoS instance.
    - If you need to add the IP of your protected Tencent Cloud product to a purchased Anti-DDoS Pro instance, please see Getting Started with Anti-DDoS Pro.
    - If you need to connect your layer-4 or layer-7 application to a purchased Anti-DDoS Advanced instance, please see Anti-DDoS Advanced documents Connecting Non-website Application.
- Before modifying DNS information, you need to purchase a domain name resolution product.

Setting Line Priority

Please follow the steps below to set priorities for your protective lines based on your scheduling scheme.

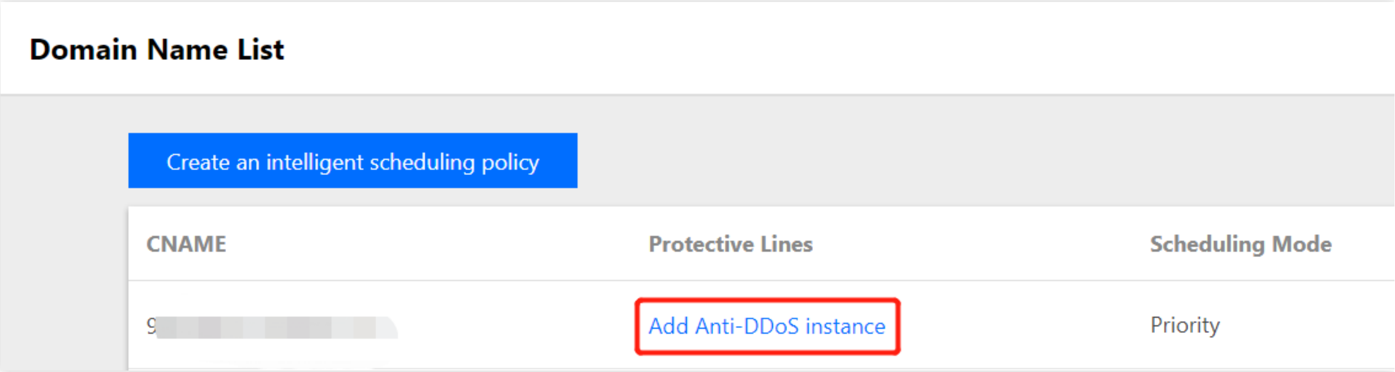
1. Log in to the Anti-DDoS Console, select **Intelligent Scheduling** > **Domain Name List** on the left sidebar, and click **Create Intelligent Scheduling**. Then, a CNAME record will be generated automatically by the system.



Domain Name List

CNAME
[redacted]

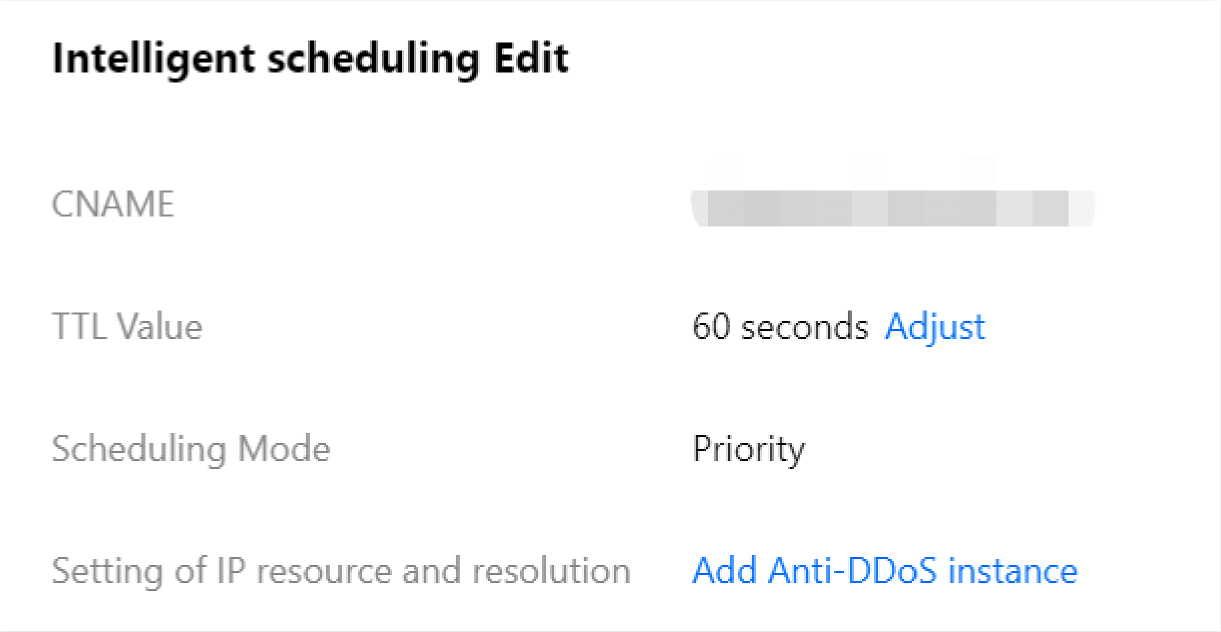
2. Locate the row of the CNAME record and click **Add Anti-DDoS Instance** to enter the intelligent scheduling editing page.



Domain Name List

CNAME	Protective Lines	Scheduling Mode
[redacted]	Add Anti-DDoS instance	Priority

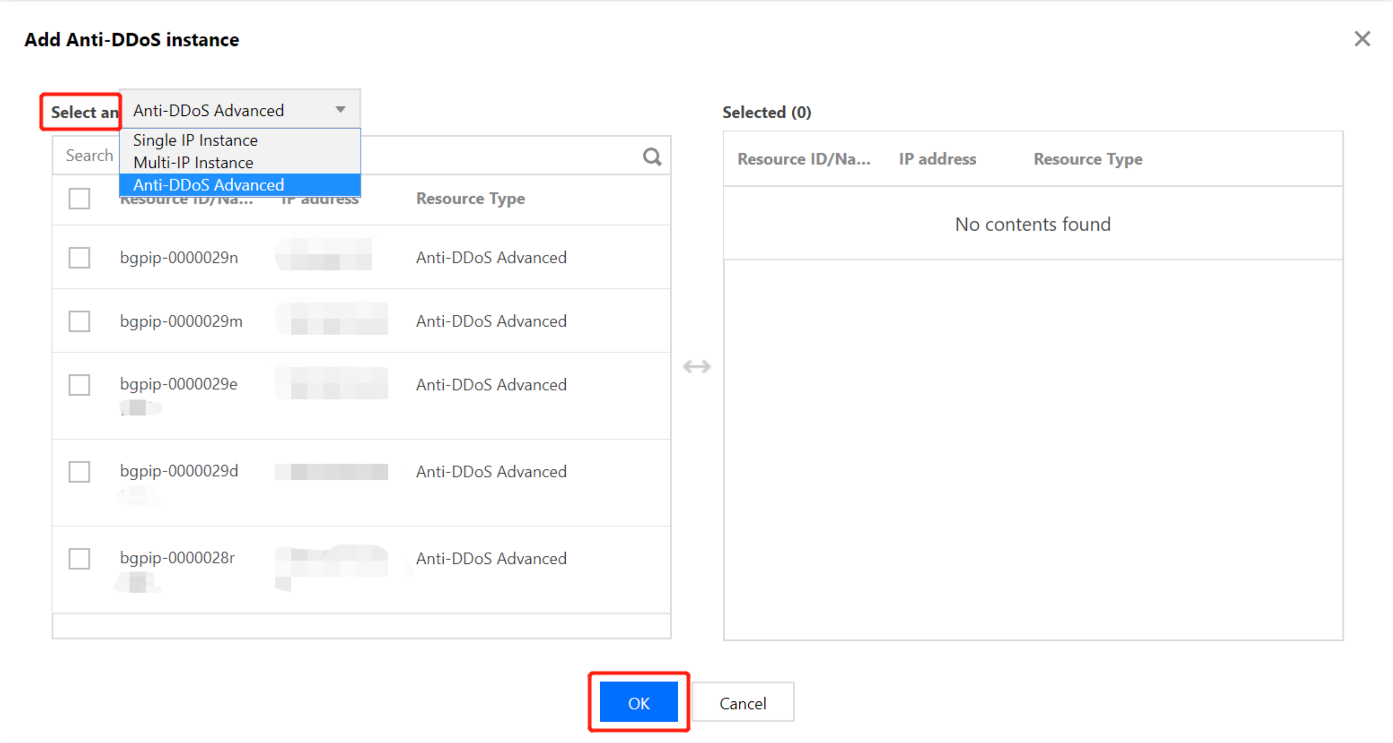
3. On the intelligent scheduling editing page, the TTL value is 60s by default, which can range from 1s to 3,600s, and the default scheduling method is priority-based.



Intelligent scheduling Edit

CNAME	[redacted]
TTL Value	60 seconds Adjust
Scheduling Mode	Priority
Setting of IP resource and resolution	Add Anti-DDoS instance

4. Go to the "Add Anti-DDoS Instance" page, select an instance (Single IP, Multi-IP, or Anti-DDoS Advanced instance) for which you want to set line priority, and then click **OK**.



Add Anti-DDoS instance

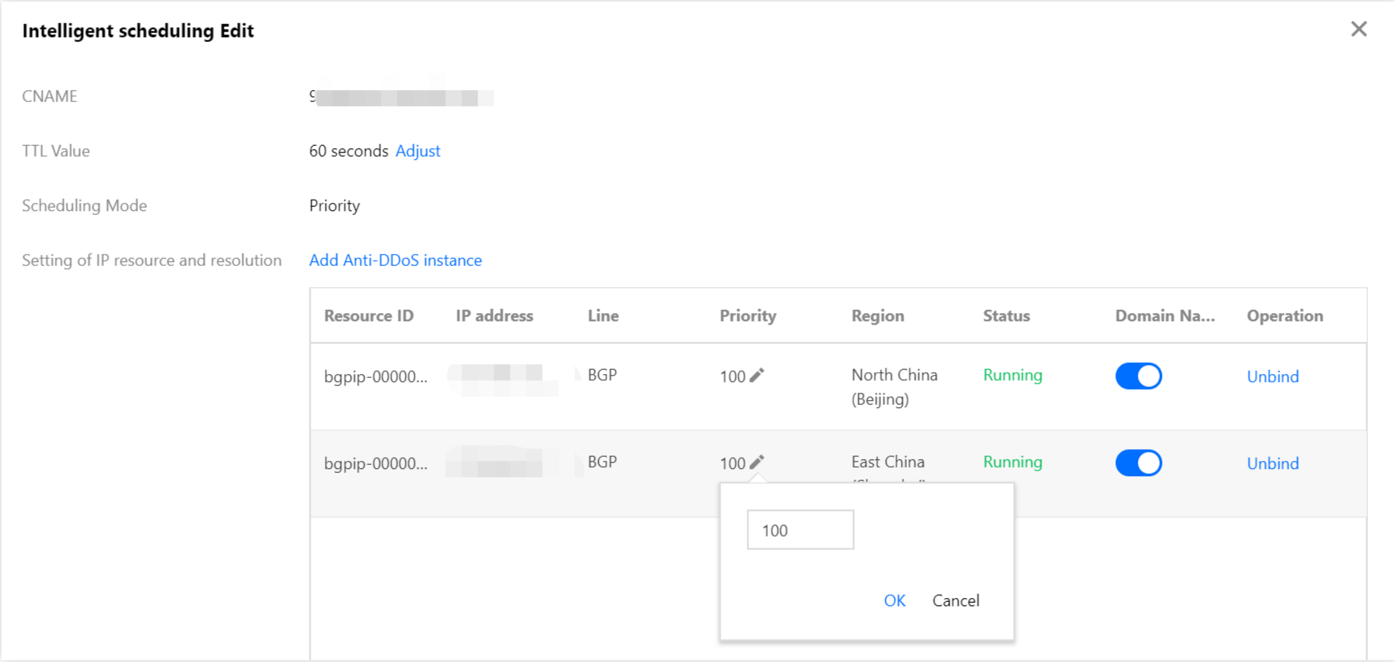
Select an: Anti-DDoS Advanced

□	Resource ID/Na...	IP address	Resource Type
□	bgpip-0000029n	[redacted]	Anti-DDoS Advanced
□	bgpip-0000029m	[redacted]	Anti-DDoS Advanced
□	bgpip-0000029e	[redacted]	Anti-DDoS Advanced
□	bgpip-0000029d	[redacted]	Anti-DDoS Advanced
□	bgpip-0000028r	[redacted]	Anti-DDoS Advanced

Selected (0)

Resource ID/Na...	IP address	Resource Type
No contents found		

5. After the instance is selected, DNS will be enabled for its protective line by default. At this point, you can set the line priority.



Intelligent scheduling Edit

CNAME [redacted]

TTL Value 60 seconds Adjust

Scheduling Mode Priority

Setting of IP resource and resolution Add Anti-DDoS instance

Resource ID	IP address	Line	Priority	Region	Status	Domain Na...	Operation
bgpip-00000...	[redacted]	BGP	100	North China (Beijing)	Running	●	Unbind
bgpip-00000...	[redacted]	BGP	100	East China	Running	●	Unbind

Modifying DNS

Before using a CNAME record for intelligent scheduling, you are recommended to change the CNAME record of your business domain name DNS to the CNAME record automatically generated by the intelligent scheduling system of Tencent Cloud Anti-DDoS, to which all access traffic will be directed.

Configure attack alarm threshold

Last updated：2020-05-13 19:51:00

Use Cases

When attacks against your Anti-DDoS Advanced resources start/end and your protected IPs are blocked/unblocked, you will get notifications through internal message, SMS, or email. Configuring proper attack alarm thresholds can help you know more about attacks instantly. This feature can also help prevent false alarming caused by normal business operations that bring traffic surges (such as data sync). For more information on how to receive alarm messages, please see Setting Security Event Notification.

Configuring DDoS Attack Alarm Threshold

This configuration example can achieve the following effect: after the attack traffic to the Anti-DDoS Advanced instance "bgpip-0000021y" exceeds the cleansing threshold and triggers DDoS attack cleansing, when the cumulative cleansed traffic (value) exceeds 1,000 Mbps, DDoS attack alarm messages will be sent to the specified user group.

> To set the attack alarm threshold, make sure that you have enabled DDoS protection.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Resource List** on the left sidebar to enter the Anti-DDoS Advanced page, find the instance "bgpip-0000021y", and click **Protection Configuration** in the "Operation" column.

2. Enter the DDoS protection configuration page, select the alarm metric **Cleansed Traffic** in the drop-down list on the right of the DDoS attack alarm threshold, and set the threshold to 1,000 Mbps.

   > The DDoS attack alarm threshold is **Not Set** by default. Available alarm metrics include **Inbound Traffic Bandwidth** and **Cleansed Traffic**.

Configuring CC Attack Alarm Threshold

This configuration example can achieve the following effect: after the Anti-DDoS Advanced instance "bgpip-0000021y" triggers CC protection, when the HTTP CC protection bandwidth exceeds 2000 QPS, CC attack alarm messages will be sent to the specified user group.

> To set the attack alarm threshold, make sure that you have enabled HTTP CC protection.

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the protection configuration page, click **CC Protection**.
2. On the CC protection page, find the "HTTP CC Protection" section at the bottom of the page, and set the threshold to 2,000 QPS in "HTTP CC Attack Alarm Threshold".

Instance Management

Viewing Instance Details

Last updated：2020-04-25 11:34:54

Operation Scenarios

You can view the basic information (such as the base protection bandwidth and running status) and configure elastic protection of all purchased Anti-DDoS Advanced instances in the Anti-DDoS Console.

Directions

This document uses the Anti-DDoS Advanced instance "bgpip-0000020n" in Guangzhou as an example to describe how to view instance details.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List** on the left sidebar, and click **South China (Guangzhou)** in the region selection box. In the list below, click the Anti-DDoS Advanced instance whose ID is "bgpip-0000020n" to view its information.
2. On the pop-up page, you can view the following information:

Parameter description:

- **Basic information:**

  ```
  – **Name**
  ```

  This is the name of the Anti-DDoS Advanced instance for easier instance identification and management. You can set a custom instance name containing 1–20 character of any type as desired. For detailed directions, please see Setting Resource Name.

  - **IP**
    This is the protective IP provided by the Anti-DDoS Advanced instance, which is used as the frontend IP of the real server to provide services.
  - **Region**
    This is the **region** selected when the Anti-DDoS Advanced instance is purchased.
  - **Forwarding target**
    This is the location of the real business server protected by the Anti-DDoS Advanced instance.
  - **Base DDoS protection bandwidth**
    This is the base protection bandwidth of the Anti-DDoS Advanced instance, i.e., the **base protection**

bandwidth selected when the instance is purchased. If elastic protection is not enabled, this will be the maximum protection bandwidth of the instance.

  - **CC protection bandwidth**

    This is the capability of the Anti-DDoS Advanced instance to defend against sudden CC attacks.
  - **Current status**

    This is the current status of the Anti-DDoS Advanced instance, such as **Running**, **Cleansing**, and **Blocked**.
  - **Expiration time**

    This is calculated based on the **purchase duration** selected when the instance is purchased and the order is paid, which is accurate to second. Tencent Cloud will send expiration and renewal reminders to the account creator and all collaborators through internal message, SMS, and email 7 days before the instance expires.
  - **Intermediate IP range**

    This is the information of the intermediate IP range in the region of the current Anti-DDoS Advanced instance.

- **Elastic protection information**

  ```
  - **Current status**
  ```

  This indicates whether elastic protection is enabled. If it is not enabled when you purchase the Anti-DDoS Advanced instance, you can enable it in a self-service manner when using the instance. For detailed directions, please see Configuring Elastic Protection.

  - **Elastic bandwidth**

    This is the maximum elastic protection bandwidth of the Anti-DDoS Advanced instance. You can adjust it as needed at any time.

    > This parameter is visible only after elastic protection is enabled.

Setting Resource Name

Last updated：2020-04-25 11:34:54

When multiple Anti-DDoS Advanced instances are used, you can set **resource names** to quickly identify and manage them.

Method 1

Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List**, select the region and line, click the name of the target instance in the **ID**/**Name** column, and then enter a name.

> The name can contain 1–20 characters of any type.

Method 2

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List**, and select a region in the top-left corner.
2. In the list below, click the ID of the target instance in the "ID/Name" column. In the **Basic Instance** section on the pop-up page, click **Modify**, enter or modify the name, and click **OK**.

   > The name can contain 1–20 characters of any type.

Configuring Elastic Protection

Last updated：2020-04-25 11:34:55

After you enable elastic protection on the Anti-DDoS Advanced instance, when the attack traffic bandwidth exceeds the base protection bandwidth, Anti-DDoS Advanced will continue protection based on your elastic protection bandwidth.

If elastic protection is not enabled when you purchase the Anti-DDoS Advanced instance, you can enable it when using the instance. If elastic protection is not triggered on a day, no relevant fees will be incurred. When elastic protection is triggered (i.e., the attack bandwidth exceeds the base protection bandwidth), fees will be charged based on the billing tier corresponding to the actual attack bandwidth peak on the day and a bill will be generated the next day. You can modify the elastic protection bandwidth of the Anti-DDoS Advanced instance as needed with immediate effect.

Enabling Elastic Protection

> If elastic protection is not enabled when you purchase the Anti-DDoS Advanced instance, you can enable it when using the instance and set the elastic protection bandwidth to higher than the highest historical attack traffic bandwidth. This helps avoid potential IP blockage in case of excessive attacks.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List**, and click **Enable Elastic Protection** next to the target instance.
2. In the **Enable Elastic Protection** box, select the needed **Elastic Protection Bandwidth**.
3. Click **OK**.

Modifying Elastic Protection Bandwidth

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List**, and click the target instance ID to enter the basic information page of the instance.

2. In the "Elastic Protection" section, click **Modify** on the right of "Elastic Bandwidth".

3. In the **Modify Elastic Protection** box, select an appropriate **Elastic Protection Bandwidth**.

- You can increase or reduce the elastic protection bandwidth. The protection capability varies by region. For more information, please see Product Overview.
- Modification of the elastic protection bandwidth takes effect immediately.

4. Click **OK**.

Disabling Elastic Protection

If you disable elastic protection, the maximum protection bandwidth will degrade to the base protection bandwidth. Please ensure that the base protection bandwidth meets your actual needs before disabling elastic protection.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List**, and click **Disable Elastic Protection** next to the target instance.
2. In the **Disable Elastic Protection** box, click **OK**.

Adjust the specification of DDoS High Defense IP instance

Last updated：2020-05-13 19:50:59

Operation Scenarios

When using Anti-DDoS Advanced, if you find that the current specification (such as the base protection bandwidth, number of forwarding rules, or service bandwidth) cannot meet your actual business needs, you can upgrade the Anti-DDoS Advanced instance specification to improve the protection capabilities.
Specification adjustment in Anti-DDoS Advanced supports increasing the base protection bandwidth, the number of forwarding rules (protected domain names or ports), and the service bandwidth.

> Currently, specification downgrade of purchased Anti-DDoS Advanced instances is not supported.

Upgrading Anti-DDoS Advanced instance specification incurs additional fees. After the payment is made, the instance specification upgrade will take effect immediately.

Directions

1. Log in to the Anti-DDoS Console.
2. Select **Anti-DDoS Advanced** > **Resource List**.
3. Click **Upgrade** in the "Operation" column in the row of the target instance.
4. Set **Upgrade Base Protection**, **Upgrade Service Bandwidth**, or **Upgrade Forwarding Rule Quantity** as needed.
5. Click **Upgrade Now** to enter the **Check Information** page.
6. After confirming that everything is correct, determine whether to use vouchers according to your actual needs, and then click **Purchase**.
7. After making the payment, return to the Anti-DDoS Advanced resource list and you can see that the specification adjustment has taken effect.

Viewing Statistics Reports

Last updated：2020-04-25 11:34:56

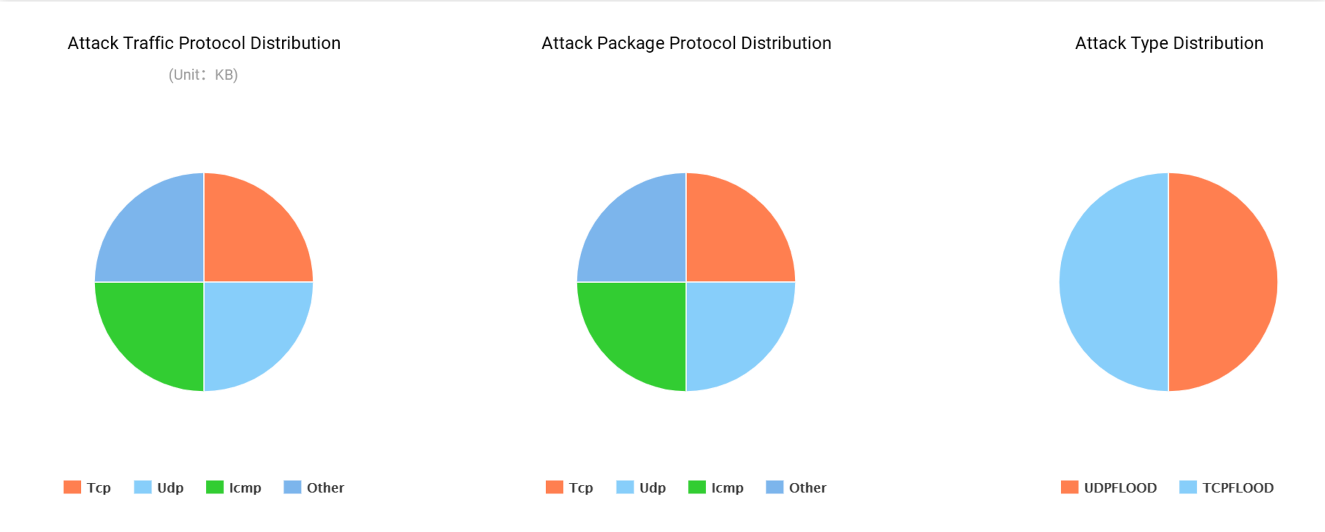
When you receive a DDoS attack alarm message or notice any issue with your business, you need to view details of the attacks, including the traffic and current protection effect. Enough information is critical for you to take measures in time to keep your business running smoothly.
The statistical reports in the Anti-DDoS Advanced Console provide rich information to help you easily stay up to date with the current business and attack conditions.

Viewing DDoS Protection Details

1. Log in to the Anti-DDoS Console.
2. Select **Anti-DDoS Advanced** > **Statistical Report**.
3. On the **DDoS Protection** tab, set the query period and select the region, line, target instance, and protected IP to check whether the instance has been attacked.

   > You can query the attack traffic and DDoS attack events in the last 180 days.

   - View the information of attacks suffered by the selected Anti-DDoS Advanced instance within the queried period, such as the trends of **attack traffic bandwidth/attack packet rate**. When the instance is under attack, you can intuitively view the attack bandwidth peak in the bandwidth trend diagram.
   - View how the attacks distribute across different attack traffic protocols, attack packet protocols, and attack types.
     - **Attack Traffic Protocol Distribution** displays how the attacks suffered by the selected Anti-DDoS Advanced instance distribute across different attack traffic protocols within the queried period.
     - **Attack Packet Protocol Distribution** displays how the attacks suffered by the selected Anti-DDoS Advanced instance distribute across different attack packet protocols within the queried period.
     - **Attack Type Distribution** displays how the attacks suffered by the selected Anti-DDoS Advanced instance distribute across different attack types within the queried period.



  - **Attack Source Distribution**: in the **Attack Source Distribution** section, you can view the distribution of DDoS attack sources in and outside Mainland China within the queried period, so that you can take further protective measures based on the displayed information.
- In **DDoS Attack Records**, you can view details of the DDoS attack events within the queried period, including the start time, duration, type, and status of each attack event.
  - You can download DDoS attack packets to analyze and trace the attacks.
  - Click **Attack Details** to view the maximum packet rate, maximum attack traffic bandwidth, and total amount of traffic cleansed during the DDoS attack event.
  - Click **Attack Source Info** to view the attack source IP addresses, source regions, generated attack traffic, and attack packet size.

> Attack source information is sampled data, which is randomly collected for statistics. The data will be displayed around 2 hours after an attack ends.

Viewing CC Protection Conditions

1. Log in to the Anti-DDoS Console.

2. Select **Anti-DDoS Advanced** > **Statistical Report**.

3. Click the **CC Protection** tab, set the query period, and select the region, line, target instance, and protected IP to check whether the instance has been attacked.

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

- You can select **Today** to view the trend in the number of attack requests to the selected Anti-DDoS Advanced instance. 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.
- If the protected IP is under CC attack, the system will record the attack start time, end time, attacked domain names, attacked URLs, total request peak, attack request peak, and attack sources.
  - **Total request peak**: the peak of the total request traffic the Anti-DDoS Advanced instance receives when the attack occurs.
  - **Attack request peak**: the peak number of requests blocked by the instance when the attack occurs.

Viewing Business Traffic Conditions

1. Log in to the Anti-DDoS Console.
2. Select **Anti-DDoS Advanced** > **Statistical Report**.
3. Click the **Scenarios** tab, set the query period, and select the region, line, target instance, and protected IP to view the **inbound/outbound business traffic bandwidth trend**, **inbound/outbound business packet rate trend**, and **new connections or concurrent connections trend** in the selected period. In addition, you can view the peaks of inbound/outbound business traffic bandwidth and inbound/outbound business packet rate.
   - **Number of concurrent connections**: the total number of connections that exist in the system at a time point.
   - **Number of new connections**: the number of TCP connections that are established in the system in one second.

   You can query the business information in the last 180 days.

Viewing Operation Logs

Last updated：2020-05-13 19:36:22

Operation Scenarios

Anti-DDoS Advanced allows you to view important operation logs of the last 90 days. You can log in to the Anti-DDoS Console to view operation logs. Viewable logs include the following categories:

- Logs of forwarding policy change
- Logs of advanced DDoS protection policy change
- Logs of cleansing threshold adjustment
- Logs of protection level change
- Logs of CC protection policy change
- Logs of elastic protection bandwidth adjustment
- Logs of resource name change

Directions

1. Log in to the Anti-DDoS Console.
2. Select **Operation Logs** to enter the log query page.
3. Set the time range. View the corresponding operation history by filtering **Anti-DDoS Advanced** in **Product Type**.

Setting Security Event Notifications

Last updated：2020-04-25 11:34:56

Operation Scenarios

Alarm messages for Anti-DDoS Advanced will be sent to you through internal message, SMS, or email in the following conditions:

- An attack starts.
- An attack ended 15 minutes ago.
- An IP is blocked.
- An IP is unblocked.

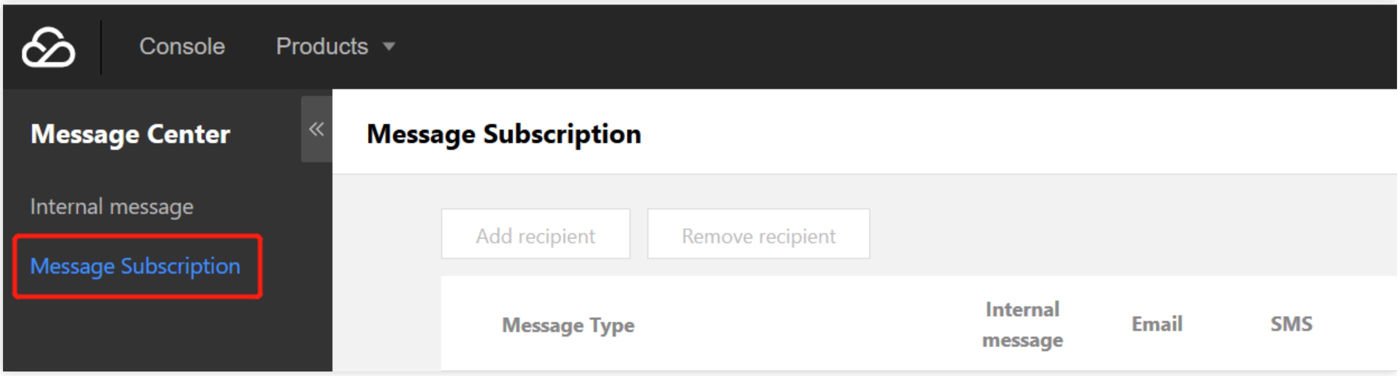
You can modify the recipients and how they receive the alarm messages as needed.

Directions

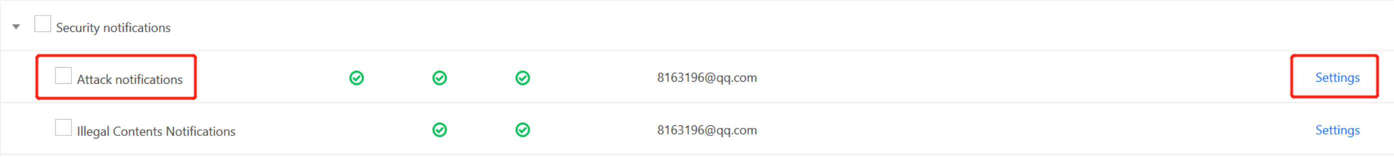
1. Log in to your Tencent Cloud account and go to the Message Center.

> Alternatively, you can log in to the console, click ✉ in the top-right corner, and then click **Enter Message Center** at the bottom of the page.

2. Click **Message Subscription** on the left sidebar to enter the message list.

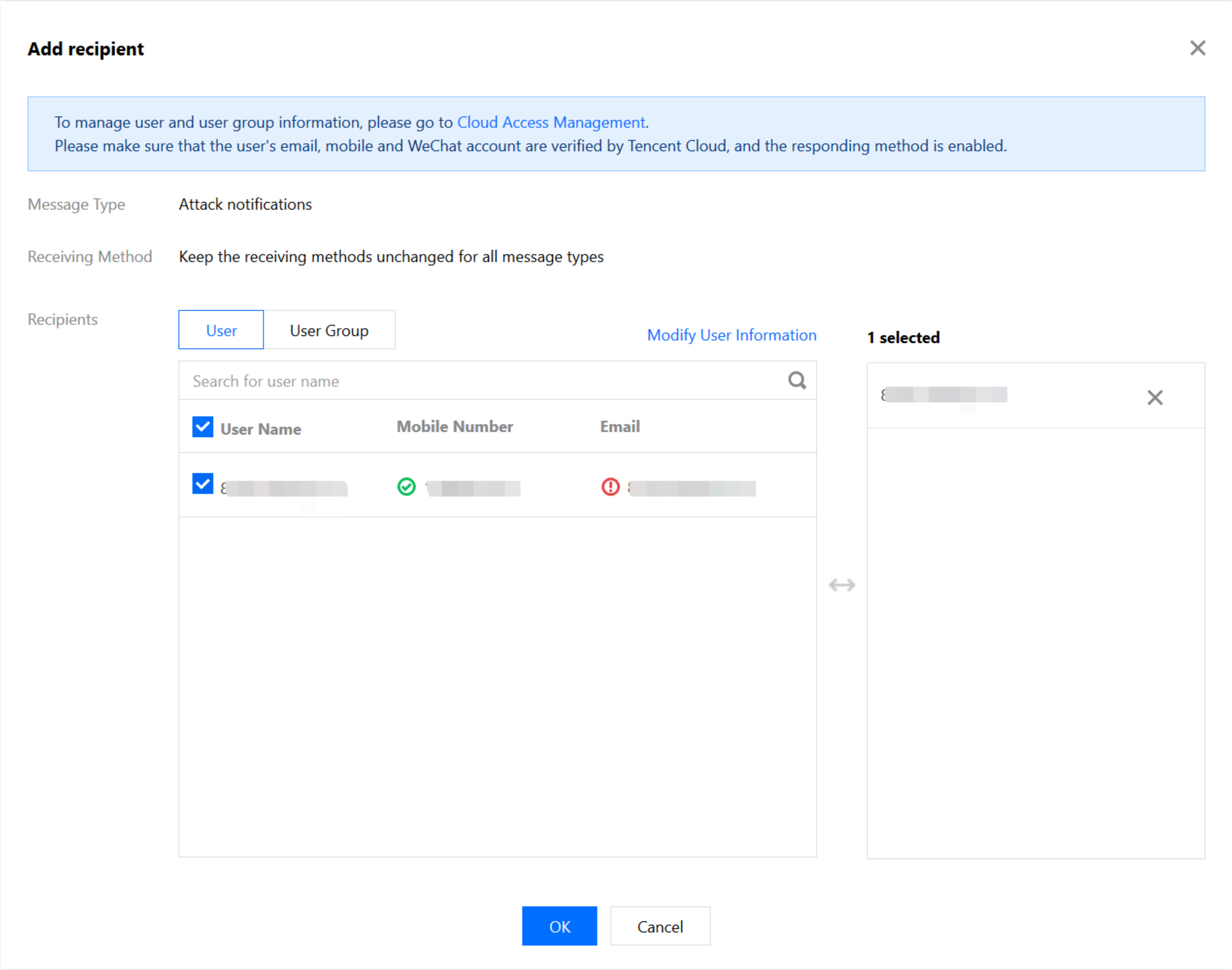


3. In the message list, click **Settings** on the row of **Security Event Notifications** to enter the settings page.



□ Security notifications					
□ Attack notifications	✓	✓	✓	8163196@qq.com	Settings
□ Illegal Contents Notifications		✓	✓	8163196@qq.com	Settings

4. Select recipients and receiving methods and then click **OK**.



Add recipient

To manage user and user group information, please go to Cloud Access Management.
Please make sure that the user's email, mobile and WeChat account are verified by Tencent Cloud, and the responding method is enabled.

Message Type: Attack notifications

Receiving Method: Keep the receiving methods unchanged for all message types

Recipients: User | User Group

Modify User Information

Search for user name

☑ User Name	Mobile Number	Email
☑ [redacted]	✓ [redacted]	! [redacted]

1 selected

[redacted]