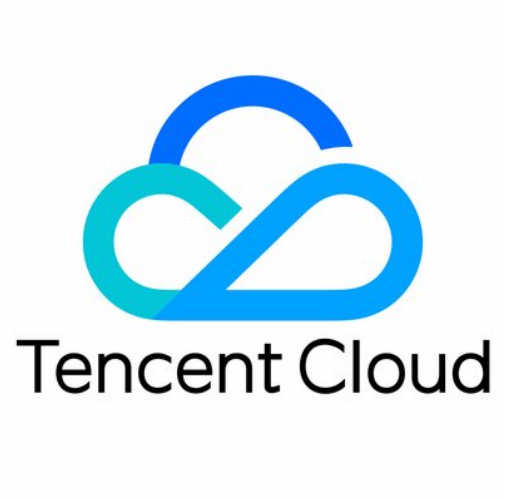
Anti-DDoS Advanced

Best Practice

Product Documentation



Contents

Best Practice
Configuration Directions and Notes on CC Protection Policy

Last updated : 2021-02-08 15:27:16

Anti-DDoS Advanced provides CC attack protection, the protection policy features protection level, cleansing threshold, precise protection, and CC frequency limit, etc. After connecting your business, you can configure CC attack protection policy as instructed in this document to use Anti-DDoS Advanced to safeguard your business.

Configuration Directions

1. Log in to the Anti-DDoS console and click **Anti-DDoS Advanced (New)** -> **Configurations** on the left sidebar.
2. Select a domain name under an instance ID from the left list, e.g., **212.64.xx.xx bgpip-000002je** -> **http:80** -> **www.xxx.com**.
3. **Set the CC protection cleansing threshold**: You can set a threshold value in the **CC Protection Policy** section.

> **Note :**
>
> - The Anti-DDoS Advanced CC protection will be enabled once you set a cleansing threshold. A value that 1.5 times your common business peak is recommended.
> - The Anti-DDoS Advanced cleansing feature will remain disabled if no threshold value is set, and the protection level, precise protection, and CC frequency limit you configured in the console will not be in effect even when your business is under CC attacks. For more information, please see Protection Level and Cleansing Threshold.

4. **Set the CC protection level**: In the **CC Protection Policy** section, set the protection level to **Loose**, **Medium**, or **Strict** as needed.

> **Note :**
>
> If the Anti-DDoS Advanced CC attack protection is enabled, the cleansing will be triggered when there is attack traffic, of which the detection strictness is the protection level. There

are three available levels for you to select based on actual attacks: **Loose**, **Medium**, and **Strict**. For more information, please see Protection Level and Cleansing Threshold.

5. **Configure the precise protection policy**:
   When your business is under attack, we recommend deriving the attack characteristics from the specific attack request information obtained through packet capture, middleware access logs, and other protection devices to configure your precise protection policy based on your business.
   You can enable precise protection to 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 that match the conditions, you can configure CAPTCHA to verify requesters or a policy to automatically discard the packets.
   ① On the **Configurations** page, click **Set** in the **Precise Protection** section to view the precise protection rule list.
   ② Click **Create**, fill in the rule fields, and click **OK** to create a new precise protection rule. For detailed configurations, please see Precise Protection.

> ⚠ **Note :**
>
> - If a policy involves multiple HTTP fields, the policy can be matched if all conditions are met.
> - Anti-DDoS Advanced supports configuring precise protection for HTTPS businesses.

Field description:

Field	Field Description
URI	The URI of an access request.
User-Agent	The identifier and other information of the client browser that initiates an access request.
Cookie	The cookie information in an access request.
Referer	The source website of an access request, from which the access request is redirected.
Accept	The data type to be received by the client that initiates the access request.

Field	Field Description
Match Condition	CAPTCHA and discard • Discard: discards packets without verifying the requester. • CAPTCHA: verifies the requester through algorithms.

6. **Set the CC frequency limit**:
   Anti-DDoS Advanced 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.
   i. On the **Configurations** page, click **Set** in the **CC Frequency Limit** section to view the frequency limit rule list.
   ii. Click **Create**, fill in the rule fields, and click **OK** to create a new rule. For detailed configurations, please see CC Frequency Limit.

> **⚠ Note :**
>
> - When configuring a CC frequency limit policy targeting the URI field, you need to configure a frequency limit on the directory `/` first and the match mode must be "equals to". Then you can configure the URI access frequency limit on other directories.
> - If a source IP accesses the `/` directory of the domain name for more than the set number of times in the set period, the set action (**CAPTCHA** or **Discard**) will be triggered.
> - If a frequency limit policy is configured for the `/` directory of a domain name, then the frequency of the domain name's other directories must be the same.
> - If the request URI contains any unfixed string, you can set the match mode to "include", so that URIs with the set prefix will be matched.

Field description:

Field	Field Description
Cookie	The cookie information in an access request.
User-Agent	The identifier and other information of the client browser that initiates an access request.
URI	The URI of an access request.

Field	Field Description
Frequency limit policy	CAPTCHA and discard • Discard: discards packets without verifying the requester. • CAPTCHA: verifies the requester through algorithms.
Check Condition	Set the access frequency based on your business, for which a value 2 to 3 times the common number of access requests is recommended. For example, if your website is accessed averagely 20 times per minute, you can configure the value to 40 to 60 times per minute or adjust it according to the attack severity.
Punishment Time	The longest period is a whole day.

Quickly Syncing Forwarding Rules for New Anti-DDoS Advanced Instances

Last updated : 2021-02-08 15:29:34

This document describes how to quickly sync forwarding rules when configuring multiple Anti-DDoS Advanced instances or CTCC/CUCC/CMCC Anti-DDoS Advanced instances.

Operation Directions

1. Log in to the Anti-DDoS console, click **Anti-DDoS Advanced (New)** -> **Application Accessing** on the left sidebar, and open the **Access via ports** tab.
2. Click **Batch Export**.
3. Enter IPs in the search bar and select Anti-DDoS Advanced forwarding rules to be exported, then you can see the forwarding rules configured for the Anti-DDoS Advanced instance, click **Copy**.
4. Click **Batch Import**.
5. Enter the new Anti-DDoS Advanced instance (with no forwarding rules configured) in the **Anti-DDoS Advanced** input box, paste the content in the input box below, and click **OK**.
6. Now you can view the forwarding rules in the list.

Smart Scheduling CTCC/CUCC/CMCC Traffic

Last updated : 2021-02-08 15:34:27

This document describes how to schedule traffic from CTCC, CUCC, and CMCC through smart scheduling.

Overview

With a CTCC/CUCC/CMCC Anti-DDoS Advanced instance, business traffic can be forwarded according to the source ISP of DNS requests, which is a common traffic scheduling method. You can configure smart scheduling to schedule the traffic from CTCC, CUCC, CMCC, or other ISPs to the Anti-DDoS Advanced instances of CTCC, CUCC, CMCC, and other ISPs respectively.

Prerequisites

- Before enabling smart scheduling, please connect your business to your Anti-DDoS instance.

> **Note :**
>
> - If you need to add the IP of your protected Tencent Cloud product to an Anti-DDoS Pro instance, please see Getting Started.
> - If you need to connect your layer-4 or layer-7 business to an Anti-DDoS Advanced instance, please see Anti-DDoS Advanced documents Port Connection or Domain Name Connection.

- To modify the DNS resolution, you need to purchase a domain name resolution product.

Operation Directions

1. Log in to the Anti-DDoS console, select **Anti-DDoS Advanced (New)** -> **Smart Scheduling** on the left sidebar to view the policy list, and click **New Scheduling Policy** to automatically generate a CNAME record.
2. Click **Add Anti-DDoS instance** of the CNAME record to enter the smart scheduling editing page.

3. The TTL value defaults to **60 seconds** and ranges from 1 to 3,600 seconds. The default scheduling mode is **Priority**.
4. Click **Add Anti-DDoS IP**, tick the target Anti-DDoS instance and IP, and click **OK**.
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.

Note :

- The priority of the three ISPs must be the same to guarantee that DNS requests can receive responses according to source ISPs.
- For smart scheduling configurations, please see Configuring Smart Scheduling.