Anti-DDoS Pro

Operation Guide

Product Documentation

Contents

Operation Guide
Operation Overview

Last updated : 2020-02-14 15:08:39

When using DDoS high defense package, you may encounter problems such as configuring DDoS high defense package instances, viewing statistical reports, viewing operation logs, and setting security event notifications. This article will introduce the common operations of using DDoS high defense package for your reference.

Instance Management

- Viewing Instance Details
- Setting Resource Name
- Configuring Elastic Protection
- Changing Protected Object IP
- Unblocking a Protected IP

Protection Configuration

- Configuring Cleansing
- Configuring Scenarios
- Managing DDoS Protection Policies
- Configuring CC Protection Policies

Statistics Reports

Viewing Statistics Reports

Operation Logs

Viewing Operation Logs

Security Event Notifications

Use Limits

Last updated : 2020-02-11 16:17:32

Applicable Services

Anti-DDoS Pro is only applicable to Tencent Cloud products, including CVM, CLB, CPM, and NAT gateway, etc.

Access Limit

Anti-DDoS Pro instances can only be bound to Tencent Cloud public IPs in the same region.

Blacklist/Whitelist

- For DDoS protection, up to 100 IP addresses can be added to the blacklist and the whitelist in total.
- For CC protection, up to 50 IPs can be added to the blacklist and 50 IPs to the whitelist.
- For CC protection, up to 50 URLs can be added to the URL whitelist.

Available Regions

Anti-DDoS Pro instances can only be bound to Tencent Cloud resources in the same region. Currently, Anti-DDoS Pro instances are available in North China (Beijing), East China (Shanghai), and South China (Guangzhou).
The following table shows the protection bandwidths that Anti-DDoS Pro provides in various regions.

Type	Region	Base Protection	Elastic Protection	Maximum Protection Capability
Single IP Instance	Guangzhou	5 Gbps - 50 Gbps	30 Gbps - 100 Gbps	100 Gbps
	Beijing	5 Gbps - 50 Gbps	30 Gbps - 100 Gbps	100 Gbps
	Shanghai	5 Gbps - 100	30 Gbps - 300	300 Gbps

		Gbps	Gbps	
Multi-IP Instance	Guangzhou	• 20 Gbps • 50 Gbps • 100 Gbps	30 Gbps - 100 Gbps	100 Gbps
	Beijing		30 Gbps - 100 Gbps	100 Gbps
	Shanghai		30 Gbps - 300 Gbps	300 Gbps

Instance Management
Viewing Instance Details

Last updated : 2020-04-22 13:28:20

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 Pro instances in the Anti-DDoS Console.

Directions

This example shows you how to view the details of the single IP instance `bgp-000006ee` in the Guangzhou region.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Pro** > **Resource List** on the left sidebar, click **Single IP Instance**, select **South China (Guangzhou)** in the region selection box, find the single IP instance named "bgp-000006ee", and click **ID/Single IP Instance Name** to view the instance information.
2. On the pop-up page, you can view the following information

Parameter description:

- **Basic Information:**

  ```
  - **Instance name**
  ```

  This is the name of the Anti-DDoS Pro 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.

  ```
  - **Region**
  ```

  This is the **region** selected when the Anti-DDoS Pro instance is purchased.

  ```
  - **Bound IP**
  ```

  This is the actual IP of the business protected by the Anti-DDoS Pro instance.

  ```
  - **Base protection bandwidth**
  ```

This is the base protection bandwidth of the Anti-DDoS Pro 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.

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

This is the current status of the Anti-DDoS Pro 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 within 7 days before the instance expires.

```
- **Tag**
```

This is the tag name of the Anti-DDoS Pro instance, which can be edited and deleted.

- **Elastic protection information**
  - **Current status**
    This indicates whether elastic protection is enabled. If it is not enabled when you purchase the Anti-DDoS Pro 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 parameter is visible only if elastic protection is enabled, which is the maximum elastic protection bandwidth of the Anti-DDoS Pro instance. You can adjust it as instructed in Configuring Elastic Protection as needed at any time.

Setting Resource Name

Last updated : 2020-04-22 13:28:20

When multiple Anti-DDoS Pro instances are used, you can set **instance names** to identify and manage instances rapidly.

Method 1

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Pro** > **Resource List** on the left sidebar, and select a region in the top-left corner.
2. Click the name in the "ID/Name" column of the target instance and 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 Pro** > **Resource List** on the left sidebar, and select a region in the top-left corner.
2. In the instance list below, click the name of the target instance in the "ID/Name" column to enter its basic information page.
3. On the basic information page of the instance, click **Modify** on the right of the basic information, enter or modify the name, and click **OK**.

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

Configuring Elastic Protection

Last updated : 2020-04-22 13:28:20

After you enable elastic protection on the Anti-DDoS Pro instance, when the attack traffic bandwidth exceeds the base protection bandwidth, Anti-DDoS Pro will continue protection based on your elastic protection bandwidth.
If elastic protection is not enabled when you purchase the Anti-DDoS Pro 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 Pro instance as needed with immediate effect.

Enabling Elastic Protection

> If elastic protection is not enabled when you purchase the Anti-DDoS Pro 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 Pro** > **Asset List**, and click **Enable Elastic Protection** next to the target instance.
2. In the **Enable Elastic Protection** box, select an appropriate **Elastic Protection Bandwidth**.
3. Click **OK**.

Modifying Elastic Protection Bandwidth

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Pro** > **Asset List**, and click the target instance to enter the basic information page of the instance.
2. In the "Elastic Protection" section, click **Modify** on the right of "Protection 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 Pro** > **Asset List**, and click **Disable Elastic Protection** next to the target instance.
2. In the **Disable Elastic Protection** box, click **OK**.

Changing Protected Object IP

Last updated : 2020-04-22 13:28:21

Operation Scenarios

Anti-DDoS Pro provides Tencent Cloud public IPs with stronger anti-DDoS capability. It supports Tencent Cloud services such as CVM, CLB, NAT, and WAF.
You can change or unbind the protected IPs bound to Anti-DDoS Pro instances based on your actual business needs.

Prerequisites

You need to purchase an Anti-DDoS Pro instance and bind a protected IP to it before you can change or unbind protected IPs

Directions

Changing the IPs to be protected

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Pro** > **Resource List** on the left sidebar, and select a region at the top.
   - For single IP instances, select the **Single IP Instance** tab.
   - For multi-IP instances, select the **Multi-IP Instance** tab.
2. Click **Change Resource** in the "Operation" column to the right of the target instance.
3. On the **Bind Resource** page, select **Resource Type** and **Resources to Associate** according to your needs.
   - A single IP instance can only be bound to one resource.
     -If your Anti-DDoS Pro instance is a multi-IP instance, you can select multiple options for **Resource Type** and **Resources to Associate**. The number of resources cannot exceed the **number of IPs** set when the instance is purchased.
4. Click **OK**.

Unbinding protected IPs

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Pro** > **Resource List** on the left sidebar, and select a region at the top.

- For single IP instances, select the **Single IP Instance** tab.
- For multi-IP instances, select the **Multi-IP Instance** tab.

2. Click **More** > **Unbind** in the "Operation" column to the right of the target instance and click **OK** in the pop-up dialog box.

Unblocking a Protected IP

Last updated : 2020-04-22 13:28:21

Anti-DDoS Pro allows you to unblock blocked IPs in a self-service manner in the Anti-DDoS Console.

Chances for Self-Service Unblocking

Only **three** chances of self-service unblocking are provided for Anti-DDoS Pro every day. The system resets the chance counter daily at midnight. Unused chances cannot be accumulated for the next day.

- The unblocking may fail for risk management reasons. A failed attempt does not count as a chance. Please wait for a while and then try again.
- Before unblocking the IP, please check the predicted unblocking time which may be affected by some factors and will be postponed. If you accept the predicted time, you do not need to operate manually.
- If the chances are used up for the day, you can upgrade the base protection capability or the elastic protection capability to defend against high-traffic attack and avoid continuous blocking.

Directions to Self-Service Unblocking

Log in to the Anti-DDoS Console, select **Self-Service Unblocking** > **Unblock Blocked IP**, find the protected IP you want to unblock, and click **Unblock** in the **Operation** column. Click **OK** in the **Unblock Blocked IP** dialog box.

- If the unblocking fails, you will receive a failure message. Please wait for a while and then try again.
- If you receive a notification indicating successful unblocking, the IP has been successfully unblocked. You can refresh the page to check whether the protected IP is in running status.

Unblocking Operation Records

Log in to the Anti-DDoS Console, select **Self-Service Unblocking** > **Unblocking History**. You can check all unblocking records in the specified period, including records of automatic unblocking and manual self-service unblocking.

Protection Configuration
Configuring Cleansing

Last updated : 2020-04-22 13:28:21

Use Cases

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

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. • Actively verifies the source IPs of certain	• This cleansing policy applies to most businesses and effectively protects against common attacks. • The normal mode is configured by default.

	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.

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.

By default, your purchased Anti-DDoS Pro 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 Sample

This section takes instance "bgp-000006ee" in South China (Guangzhou) as an example to describe the configurations.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Pro** > **Resource List** on the left sidebar, click **Single IP Instance**, select **South China (Guangzhou)** in the region selection box, find the single IP instance named "bgp-000006ee", and click **Protection Configuration** on the right.
2. 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 Pro 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 Pro 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 Pro 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**

- **Scenario**
  You can select and modify a matched scenario from the created ones as needed. When a scenario

is selected, the corresponding "advanced policy" will be automatically generated accordingly. For more information on how to create a scenario, please see Configuring 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 Advanced Anti-DDoS Protection Policies.
- **Alarm threshold for DDoS attacks**
  You can configure an alarm threshold for new 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 Pro 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 Pro 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 users in the whitelist.

Configuring Scenarios

Last updated : 2020-04-22 13:28:21

Use Cases

Anti-DDoS Pro 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 Pro 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 Pro 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 a Scenario

- **Method 1:**
  If you have not configured any scenario for your Anti-DDoS Pro instance yet, when you log in to the Anti-DDoS Console and select **Anti-DDoS Pro** > **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 Pro** > **Protection Configuration** on the left sidebar. Select the **Advanced DDoS Protection Policy** tab and click **Create Scenario**.
2. In the **Create Scenario** box, 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:**
  - **Current Protocol:** select the protocol currently in use. The options include ICMP, TCP, UDP, and others.

    > If you select TCP or UDP, you will need to enter the TCP/UDP service port range (1–65535). You will also see an item in the **Other Information** section where you can configure the length of TCP/UDP service packet (optional; the length range is 0–1500).

  - **Users outside China**
    Select **Yes** or **No**, indicating disabling or enabling **Reject traffic from outside China**.
  - **Actively initiate outbound TCP requests**
    Select **Yes** or **No**. 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** or **No**. 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**
    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.
  - **VPN application**
    Select **Yes** or **No**. **No** is selected by default. If you select **Yes**, "Other protocols" will not be disabled.

    > If "Other protocols" in "Current Protocol" or **Yes** in "VPN application" is selected, then "Other protocols" will not be disabled.

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 Pro instance and have created only one scenario, the generated advanced protection policy will be automatically associated with the instance.
   - 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.

Modifying and Deleting a Scenario

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Pro** > **Protection Configuration** on the left sidebar.
2. In the **Advanced DDoS Protection Policy** tab, click **Configure** or **Delete** to 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 Policies.

Managing DDoS Protection Policies

Last updated : 2020-04-22 13:28:21

Anti-DDoS Pro provides advanced protection policies against DDoS attacks. You can adjust and optimize the DDoS protection policy as required through blacklists/whitelists, disabling protocols and ports, packet characteristic filtering, connection flood protection, and watermark protection.

Configuration Item Overview

Configuration Item	Description	Effective Time
Blacklist/whitelist	It is IP-based protection. • It always allows requests from IPs in the whitelist. • It always blocks requests from IPs in the blacklist.	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 Pro cluster will cleanse the traffic under the protocol.	It takes effect immediately when the protected IPs are under attack.
Disabled port	It disables a port not used by the business. If attacks are detected, the Anti-DDoS Pro cluster will cleanse traffic from the disabled ports.	It takes effect immediately when the protected IPs are under attack.

Configuration Item	Description	Effective Time
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.
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.
Null session protection	It protects against null session attacks.	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 the IPs protected by Anti-DDoS Pro to protect against light traffic connection attacks.	It takes effect immediately when the protected IPs are under attack.

Configuration Item	Description	Effective Time
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 blacklist 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 Pro 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 Pro 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 Pro** > **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.

- **Blacklist/Whitelist**

- If you need to set a blacklist, click **Add**, select **Blacklist**, enter IPs to block, and then click **OK**. Separate multiple IPs with carriage returns.
- If you need to set a whitelist, click **Add**, select **Whitelist**, 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 blacklist and whitelist. The number of IPs to be added in batches cannot exceed the current available quota.

- **Disabled Protocol**
  Select the protocol you want to disable.

- **Disabled Port**
  Select a protocol and port type, and then enter the ports to be disabled. If you only need to disable one port in an entry, enter the same number for the starting and ending ports. Click **Add** under the list to add more entries. Protocols include TCP and UDP. Port types include destination port, source port, and destination/source port.

- **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 Pro 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.

Binding and Unbinding Resources

Log in to the Anti-DDoS Console and select **Anti-DDoS Pro** > **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 Pro** > **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 a Watermark Key

Log in to the Anti-DDoS Console and select **Anti-DDoS Pro** > **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 a Policy

Log in to the Anti-DDoS Console and select **Anti-DDoS Pro** > **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
- Blacklist/Whitelist
- Disabled Protocol
- Disabled Port
- Packet Filter Characteristic
- Reject Traffic from Outside china
- Connection Flood Protection
- Exceptional Connection Detection
- Watermark Protection

Deleting a Policy

- You can directly delete a policy without bound resources. To delete a policy with bound resources, unbind the resources first. 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 Pro** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Delete** next to the target policy. In the pop-up dialog box, click **OK**.

Configuring CC Protection Policies

Last updated : 2020-04-02 10:00:57

Operation Scenarios

Anti-DDoS Pro supports the CC protection function. When the HTTP request amount calculated by Anti-DDoS Pro exceeds the set **HTTP Request Threshold**, CC protection is automatically triggered. Meanwhile, Anti-DDoS Pro supports URL whitelist, IP whitelist, and IP blacklist policies:

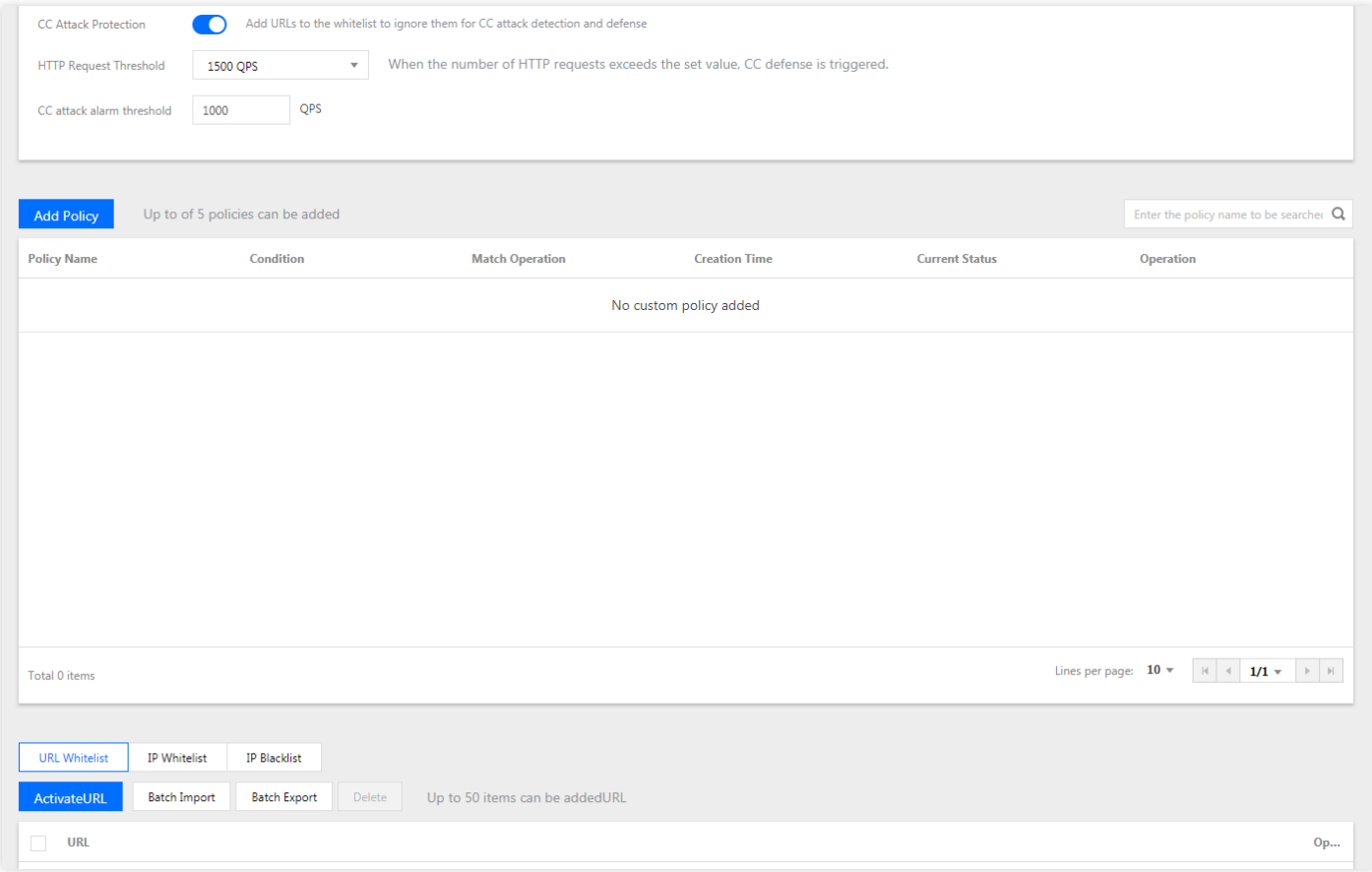
- For URLs in the whitelist, their access requests do not require CC attack detection and can pass directly.
- For IPs in the whitelist, their HTTP access requests do not require CC attack detection and can pass directly.
- For IPs in the blacklist, their HTTP access request will be directly denied.

You can custom the protection policy according to the features and protection needs of your business to block CC attacks more accurately.

Directions

1. Log in to Anti-DDoS Console and choose **Anti-DDoS Pro** -> **Protection Configuration**. On the **CC Protection** tab, select the target region and Anti-DDoS Pro instance to configure CC

protection.



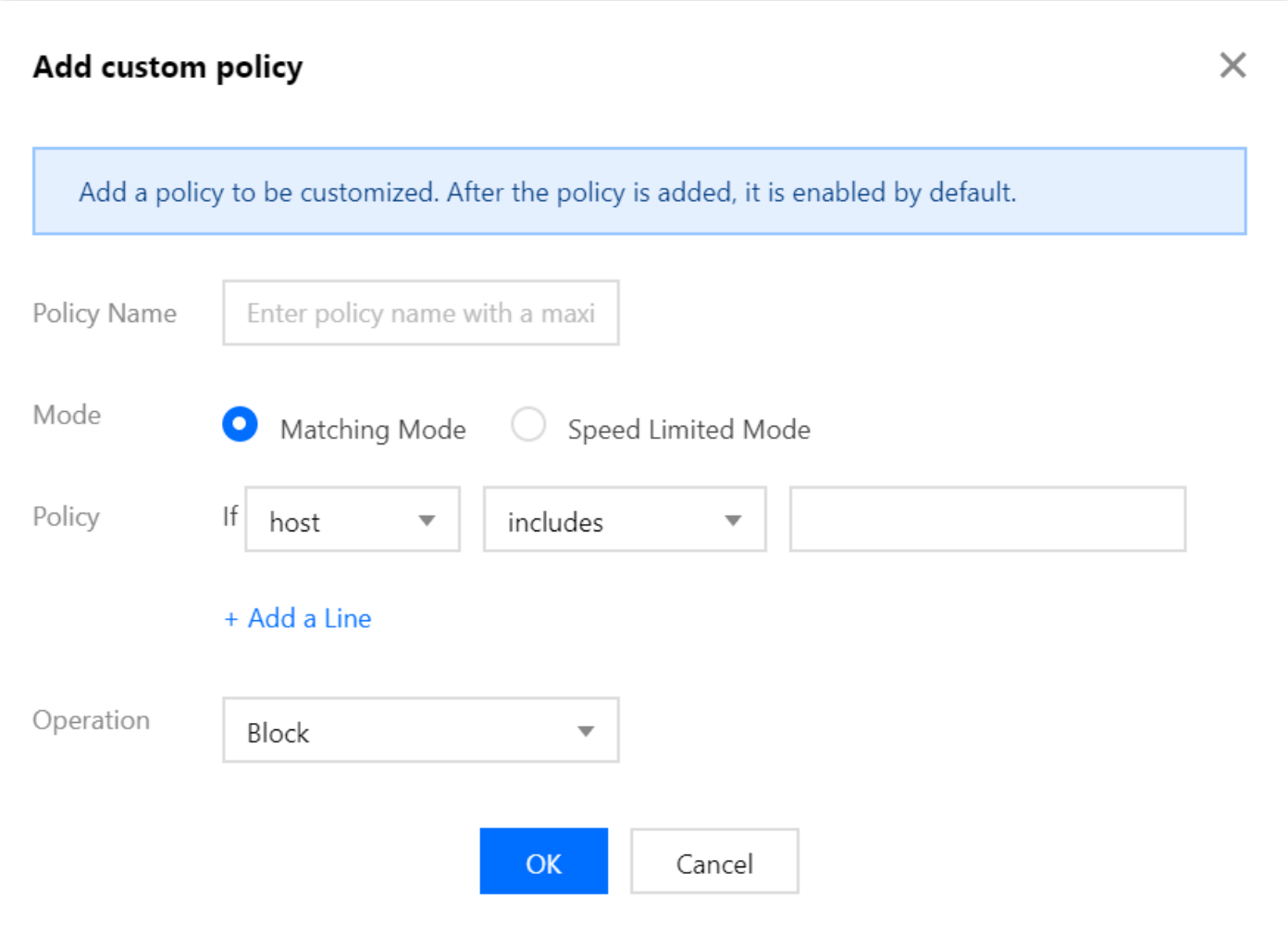
2. Click next to **CC Protection** to enable it.

   - By default, CC Protection is disabled.
   - You can set the HTTP request amount threshold, custom CC protection policy and blacklist/whitelist when you enable CC protection.

3. Click the drop-down list right to the **HTTP Request Threshold** to select a proper threshold.

4. Click **Add Access Control Policy**, and then set the following parameters according to the actual business demand in the **Add Access Control Policy** pop-up box. Click **OK** to complete the

configuration.



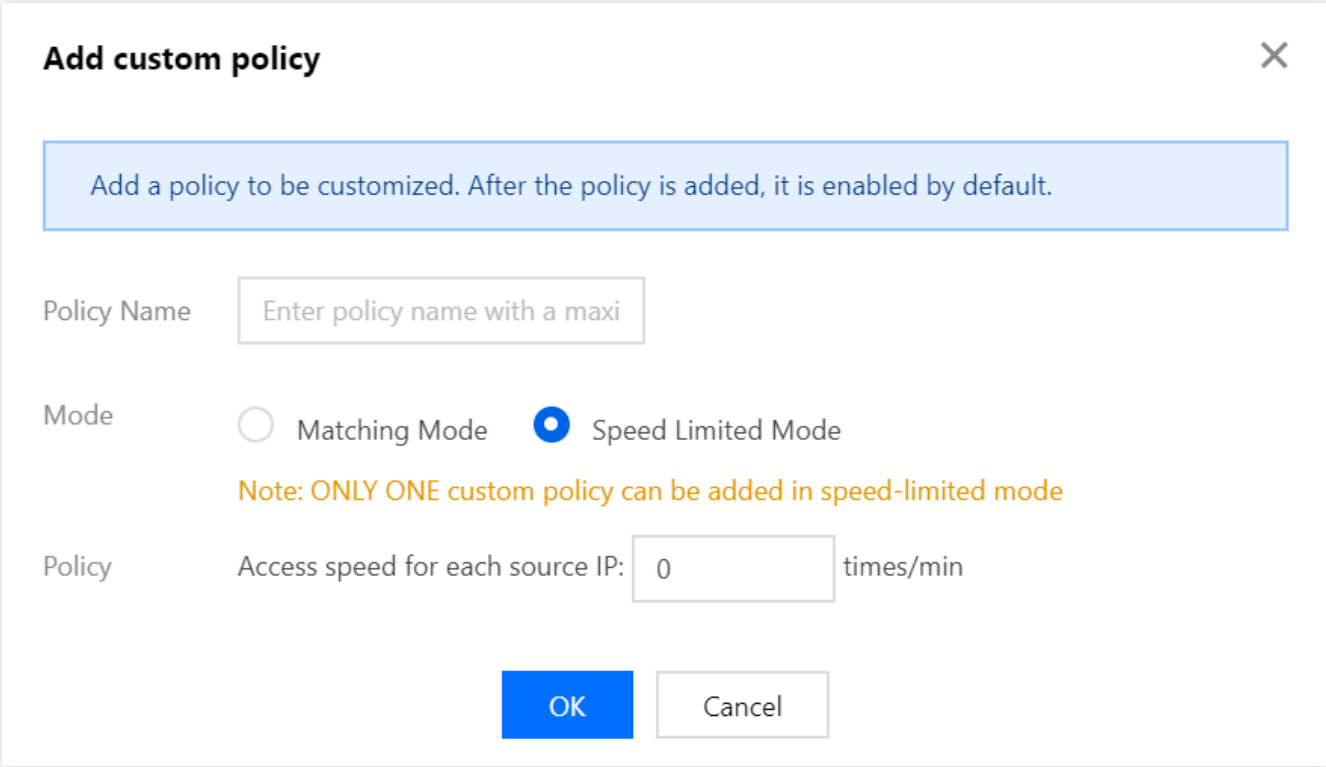
- **The custom policy takes effect only when Anti-DDoS Pro is under attack.**
- **Match mode**: Each custom policy may have up to **4** conditions for feature control, and these conditions have “and” relation, which means all conditions must be matched before the policy takes effect.
- **Speed limit mode**: Each custom policy only allows for setting **1** policy condition.
- **Policy Name**
  Enter policy name, which consists of 1-20 characters. Character type is not restricted.
- **Mode**

- Match Mode: When it detects requests matched the corresponding HTTP field, it will block the request or require human-machine recognition.
- Speed Limit Mode: Limits the speed of source IP access.

- **Policy**
  - When you select **Match Mode**, it supports a combination of multiple features such as `host`, `CGI`, `Referer`, and `User-Agent` from HTTP messages. The combination logic includes contain, not contain, and equal to. You can set up to 4 policy conditions for feature control as described below:

Field	Description	Logic
host	Domain name of the access request	contain, not contain, equal to
CGI	URL of the access request	contain, not contain, equal to
Referer	Source website of the access request, which means at which webpage the access request is generated	contain, not contain, equal to
User-Agent	Information like browser identifier of the requester client	contain, not contain, equal to

  - When you select **Speed Limit Mode**, you limit the speed of each source IP access. You are allowed to set only one policy condition.



5. Click **URL Whitelist**, **IP Whitelist**, or **IP Blacklist** tab for blacklist/whitelist configuration. Addition and deletion are allowed.

> When you add a URL to the Anti-DDoS Pro whitelist, the HTTP protocol header is optional. But Anti-DDoS Pro supports only HTTP protocol. Example: `http://test.com/index.php` or `www.test.com/index.php` .

Configuring Attack Alarming Threshold

Last updated : 2020-04-02 10:00:57

Introduction

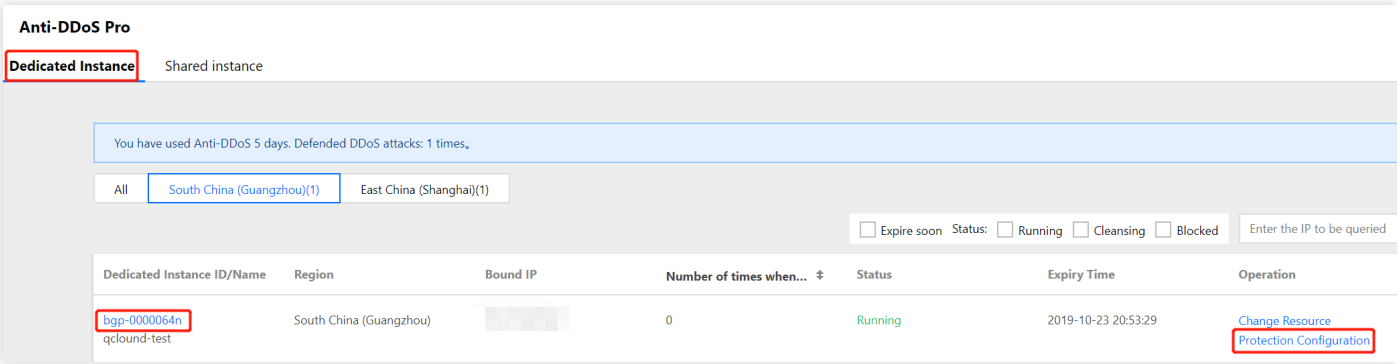
When attacks against your Anti-DDoS Pro resources start/end, and your Anti-DDoS Pro IPs are blocked/unblocked, you will get notifications in Message Center or via SMSs or emails. Configuring proper alarm thresholds can help you know about the attack instantly. And this feature can also help prevent mis-alarming caused by normal business operations that bring traffic rush (for example, data synchronization). For more information about how you can receive the alarm messages, please refer to Security Event Notification Settings.

Configuring DDoS Attack Alarm Threshold

Scenario: When Anti-DDoS Pro detects that the inbound traffic bandwidth of the Single IP instance “bgp-000005w1” is over 1,000 Mbps, the system will send DDoS attack alarm message to the specific user group.

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

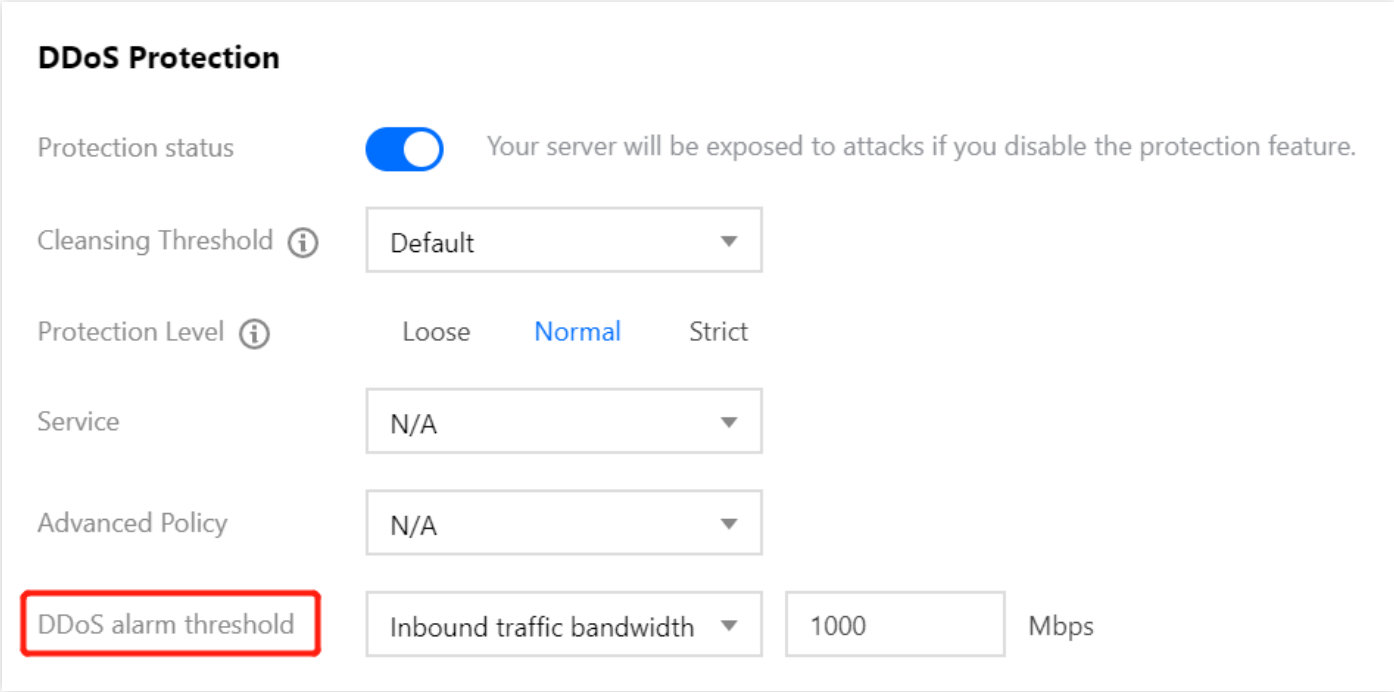
1. Log in to the Anti-DDoS Console and choose **Anti-DDoS Pro** -> **Resource List** in the left sidebar to enter the Anti-DDoS Pro page. Click **Single IP Instance** to find the instance “bgp-000005w1”, and then click **Protection Configuration** in the line of the instance.



2. Enter the **DDoS Protection** page, select the alarm metric **Inbound Traffic Bandwidth** in the drop-down list to the right of the DDoS attack alarm threshold, and set the threshold to 1000

Mbps.

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



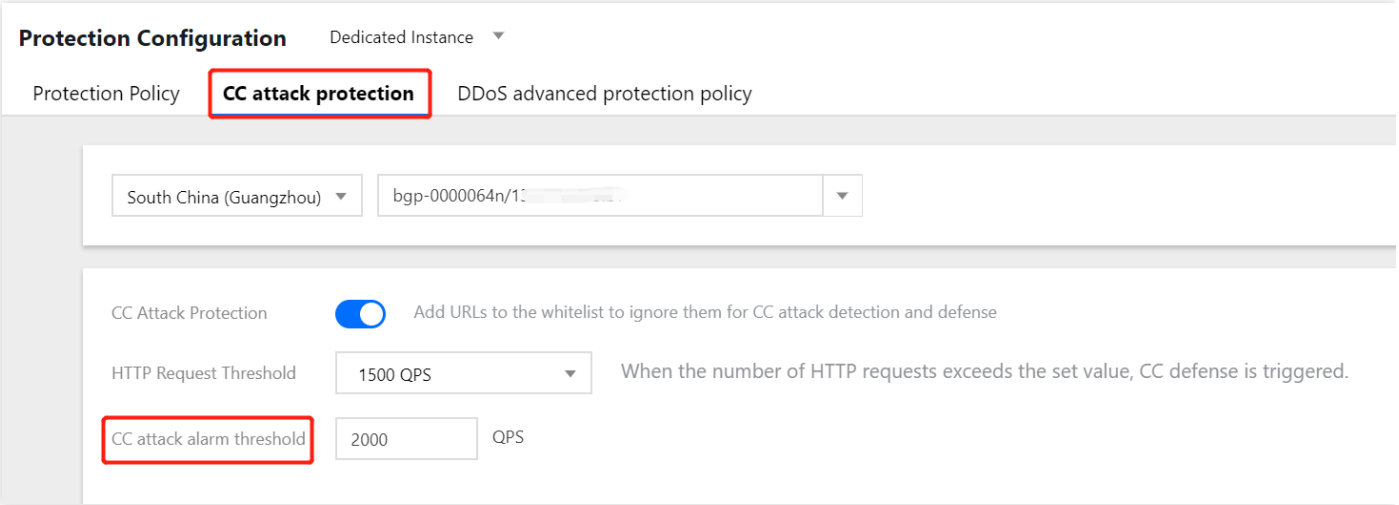
Configuring CC Attack Alarm Threshold

Scenario: CC Protection is enabled for the Single IP instance “bgp-000006i9”. When the CC protection bandwidth exceeds 2000 QPS, alarm messages will be sent to the specific user group.

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

1. Log in to Anti-DDoS Console and choose **Anti-DDoS Pro** -> **Protection Configuration**. On the **CC Protection** tab, select **Single IP Instance** -> **CC Protection**.

. Click **CC Protection** and set the threshold to 2,000 QPS for the CC attack alarm threshold.



Configuring Intelligent Scheduling

Last updated : 2020-04-02 10:00:58

Introduction

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), Anti-DDoS Advanced and Anti-DDoS Ultimate 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.

Samples

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 or Connecting Website Application.

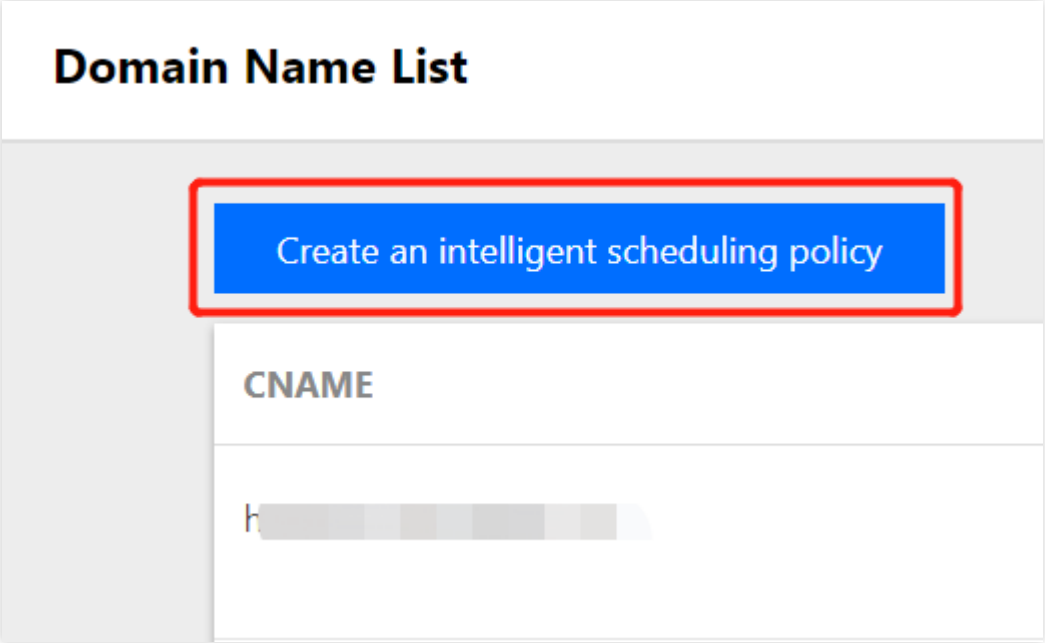
- To modify the DNS resolution, you need to purchase the domain name resolution product.

Setting Line Priority

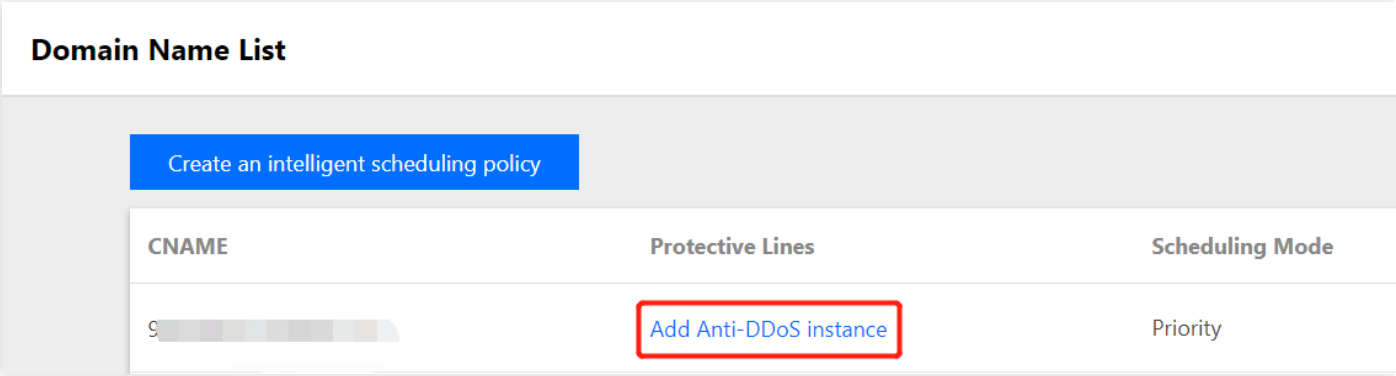
Please follow the steps below to set priorities for your protective lines based on your scheduling scheme.

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

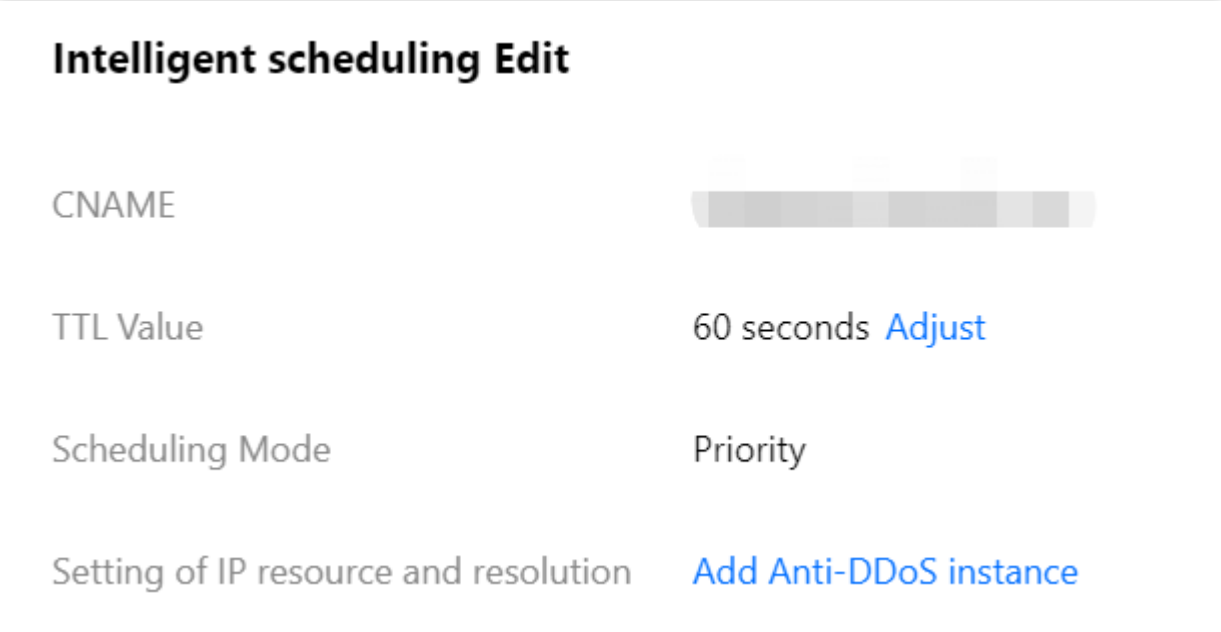
automatically by the system.



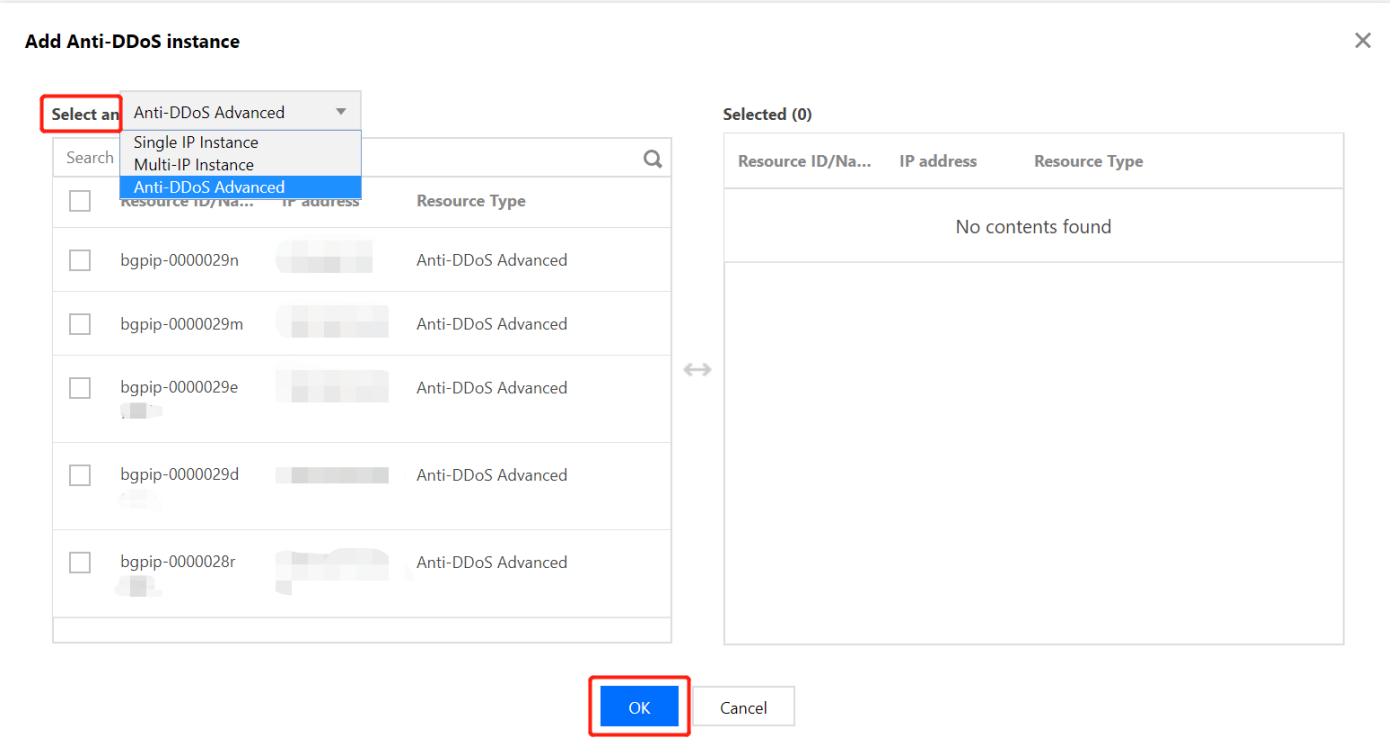
2. Locate the row of the CNAME record and click **Add Anti-DDoS Instance** to enter the intelligent scheduling editing page.



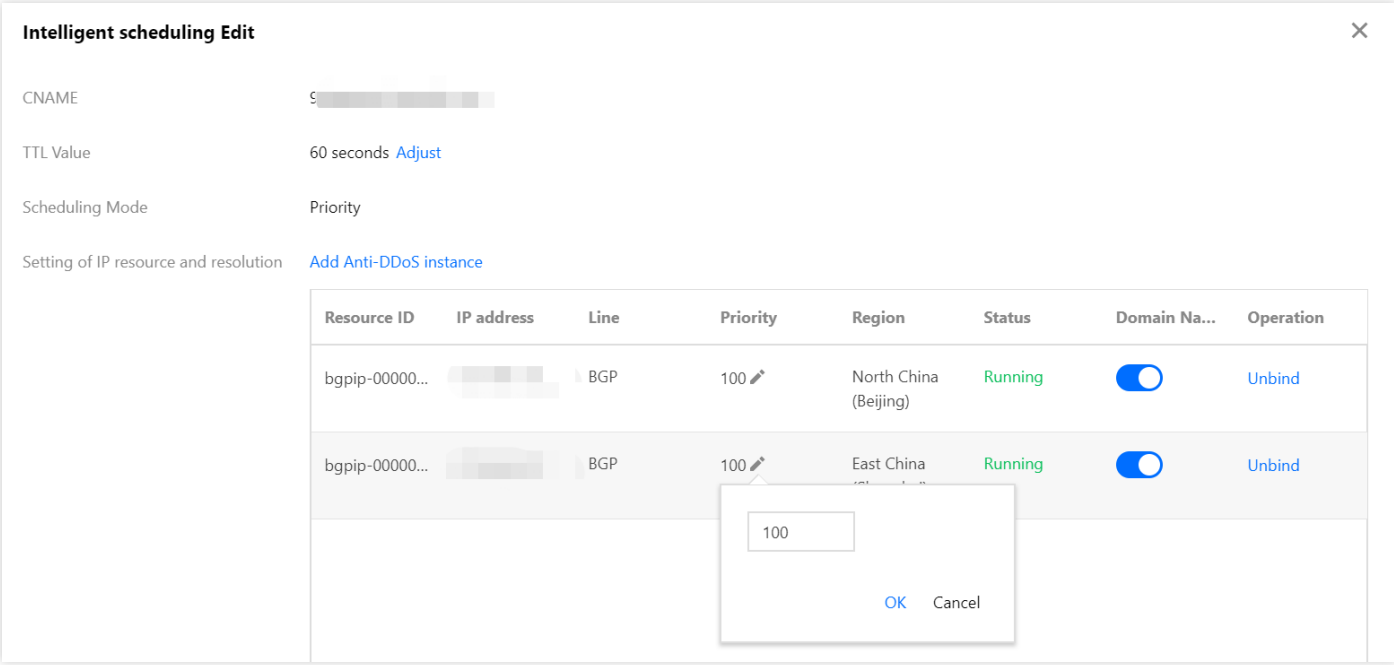
3. On the intelligent scheduling editing page, the TTL value is 60s by default, which can range from 1s to 3,600s, and the default scheduling method is priority-based.



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



Samples

Assume that you want to implement the following scheme: The business traffic will be scheduled to a BGP protective line first; if it is blocked due to attacks, the traffic will be automatically scheduled to a China Telecom protective line; if it is blocked too, the traffic will be scheduled to a China Unicom protective line; and after the BGP protective line is unblocked, the traffic will be scheduled to it automatically.

To implement this scheduling scheme, set the priority of the BGP line in the protective instance to 1 and that of the China Telecom line to 2, and keep the priority of the China Unicom line unchanged.

If you do not want the China Unicom protective line to be in the traffic scheduling scheme, click  to disable DNS for it, and you can enable DNS again and set its priority when necessary. If you want to delete it from the current scheduling scheme, you can locate the row of its corresponding instance and click **Unbind**.

Viewing Statistics Reports

Last updated : 2020-04-22 13:28:21

After an IP address is bound to an Anti-DDoS Pro instance, when you receive a DDoS attack alarm message or notice any issue with your business, you need to view details of the attacks in the console, including the attack traffic and current protection effect. Enough information is critical for you to take measures in time to keep your business running smoothly.

Viewing DDoS Protection Details

1. Log in to the Anti-DDoS Console.
2. Select **Anti-DDoS Pro** > **Statistical Report** and click **Single IP Instance**.
   Note: if you select **Multi-IP Instance**, you will be able to view DDoS protection details of each IP protected by your Anti-DDoS Pro instance.
3. In the **DDoS Protection** tab, select a query period, target region, and instance 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 Pro instance within the queried period, such as the trends of **attack traffic bandwidth/attack packet rate**.

- 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 A
nti-DDoS Pro instance distribute across different attack traffic protocols within the queried
period.
- **Attack Packet Protocol Distribution** displays how the attacks suffered by the selected An
ti-DDoS Pro instance distribute across different attack packet protocols within the queried pe
riod.
- **Attack Type Distribution** displays how the attacks suffered by the selected Anti-DDoS Pro
instance distribute across different attack types within the queried period.
```

  - 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, generat
ed 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 Pro** > **Statistical Report** and click **Single IP Instance**.
   Note: if you select **Multi-IP Instance**, you will be able to view CC protection details of each IP protected by your Anti-DDoS Pro instance.
3. In the **CC Protection** tab, select a query period, target region, and instance 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 Pro 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 Pro instance receives when the attack occurs.
  - **Attack request peak**: the peak number of requests blocked by the instance when the attack occurs.

Viewing Operation Logs

Last updated : 2020-04-02 10:00:58

Operation Scenarios

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

- Logs of protected objects' IP replacement
- Logs of Anti-DDoS advanced protection policy change operations
- Logs of cleansing threshold adjustment
- Logs of protection level change
- Logs of Anti-CC protection policy change operations
- Logs of elastic protection bandwidth adjustment
- Modification logs of resource name

Direcitons

1. Log in to Anti-DDoS Pro Console.
2. Choose **Operation Logs** to enter the log query page.
3. Set the time range. View the corresponding operation history by filtering **Single IP Instance** or **Multi-IP Instance** in **Product Type**.

> - Single IP instance: Refers to Anti-DDoS Pro instance providing one IP with dedicated anti-DDoS protection.
> - Multi-IP instance: Refers to Anti-DDoS Pro instance providing multiple IP with shared anti-DDoS protection.

Setting Security Event Notifications

Last updated : 2020-04-22 13:28:22

Operation Scenarios

Alarm messages for Anti-DDoS Pro 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.

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