Alibaba Cloud Anti-DDoS

Anti-DDoS Origin

Issue: 20200703

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 **Notice:** If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings** > **Network** > **Set network type**.
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands.	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

Contents

1 Purchase an Anti-DDoS Origin Enterprise instance

This topic describes how to purchase an Anti-DDoS Origin Enterprise instance.

Prerequisites

Anti-DDoS Origin Enterprise instances are available only after you complete enterprise real-name verification.

Context

Anti-DDoS Origin provides the Basic and Enterprise protection plans.

- Basic: provides free basic protection for Alibaba Cloud resources that have public IP addresses configured. Anti-DDoS Origin Basic provides basic protection of up to 5 Gbit/s.
- Enterprise: provides protection for Alibaba Cloud resources that have public IP addresses configured after you purchase the protection plan. These resources include Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, Elastic IP (EIP) instances, and Web Application Firewall (WAF) assets. Anti-DDoS Origin Enterprise provides basic protection of up to 20 Gbit/s and unlimited protection that is shared by all attached resources. Unlimited protection provides defense against DDoS attacks. The protection capacity is based on the total number of resources that reside in an anti-DDoS cluster. The capacity of unlimited protection increases when the overall network capacity of Alibaba Cloud increases. You do not need to pay extra expenses for the capacity increase.

  For more information about Anti-DDoS Origin pricing structures, see #unique_4.

Procedure

1. Visit the Anti-DDoS Pro official website and use your Alibaba Cloud account to log on.
2. Click **Buy Now**.
3. On the **Anti-DDoS Pro** purchase page, click the **Anti-DDoS Origin** tab.
4. On the **Anti-DDoS Origin** purchase tab, configure the required settings. The following table describes the settings of an Anti-DDoS Origin Enterprise instance.

Setting	Description
Protection Plan	Select **Enterprise**.
IP Protocol	No change is required. Only the **IPv4** protocol is available.

Setting	Description
Region	Select a region where the Anti-DDoS Origin instance resides. Available regions include China (Hangzhou), China (Shanghai), China (Qingdao), China (Beijing), China (Zhangjiakou-Beijing Winter Olympics), China (Hohhot), and China (Shenzhen). **Notice:** The region where the Anti-DDoS Origin instance resides must be the same as the region where the attached protection target resides. The protection target can contain Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and other cloud resources.
Resource Group	The resource group that hosts the Anti-DDoS Origin instance.
Clean Bandwidth	The average throughput of the business to be protected. The setting is measured in bit/s. Valid values include 100 Mbit/s, 300 Mbit/s, 500 Mbit/s, 800 Mbit/s, 1 Gbit/s, 1.5 Gbit/s, 2 Gbit/s, 2.5 Gbit/s, and 3 Gbit/s. For more information about how to select a clean bandwidth, see #unique_4/unique_4_Connect_42_section_y6r_x7v_t68.
Protected IP Addresses	The total number of IP addresses to be protected. Valid values range from 100 to 255. The default value is 100.
Quantity	The number of Anti-DDoS Origin instances that you want to purchase.
Duration	The subscription duration of your Anti-DDoS Origin instance. Valid values include 1 Year, 2 Years, and 3 Years.

5. Click **Submit Purchase Request** in the **Confirm Configuration** dialog box.
6. On the **Apply for Anti-DDoS Origin Enterprise** page, submit information about your enterprise and your contact information for approval.
7. After the request is approved, complete payment.

Result

You successfully purchase the Anti-DDoS Origin Enterprise instance. On the Instances page of the Anti-DDoS Origin console, you can view the list of instances that you have purchased.

What's next

Activate Anti-DDoS Origin to protect IP addresses from DDoS attacks

2 Quick Start

This topic describes how to view protection settings and details for each resource under an Alibaba Cloud account in the Anti-DDoS Basic console. It also provides an overview of protection against DDoS attacks. You can change protection configurations based on your business requirements.

Context

Anti-DDoS Basic is enabled by default. It provides a protection capacity of up to 5 Gbit/s for Elastic Compute Service (ECS), Server Load Balancer (SLB), and Elastic IP Address (EIP) instances. The protection against DDoS attacks for the preceding assets that belong to an Alibaba Cloud account is provided free-of-charge.

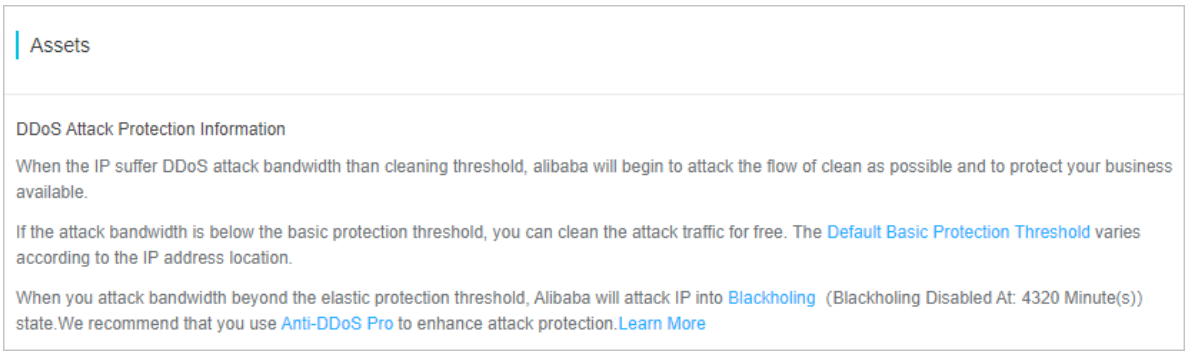
You must take note of the following items when using Anti-DDoS Basic:

- You can configure an appropriate cleaning threshold based on your business requirements. The throughput of DDoS attacks that an asset encounters may exceed the specified value of a cleaning threshold. In such cases, Anti-DDoS Basic starts cleaning attack traffic to ensure business continuity.
- You must take note of the protection capacity that is used for an instance to protect against DDoS attacks. If the bandwidth of a DDoS attack is no less than the specified cleaning threshold, Anti-DDoS Basic provides traffic cleaning free of charge. The default black hole triggering threshold for an asset changes based on the region that hosts the asset. For more information, see Default black hole triggering thresholds for Anti-DDoS Basic.
- Activate Anti-DDoS Pro based on your business requirements. If the bandwidth of a DDoS attack on an asset exceeds the default black hole triggering threshold for the asset, requests to the asset are forwarded to a black hole. We recommend that you use Anti-DDoS Pro to improve protection capacity. For more information about Anti-DDoS Pro, see What is Anti-DDoS Pro?.

Procedure

1. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the **Assets** page, select a region.

3. On the **Assets** page, view **DDoS Attack Protection Information**. The DDoS Attack Protection Information section provides the following links to specific topics.
   - Click **Default Basic Protection Threshold** to view default black hole triggering thresholds for different assets that reside in each region.
   - Click **Blackholing** to view Alibaba Cloud black hole policies.
   - Click **Anti-DDoS Pro** to go to the **Instance List** page of the Anti-DDoS Pro console. You can activate Anti-DDoS Pro based on your business requirements.



   For more information, see #unique_10.

4. You can change the value of a cleaning threshold based on your business requirements.
   a) On the **Assets** page, select the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud service for which you want to configure a cleaning threshold.
      - **ECS**: includes a list of IP addresses for ECS instances.
      - **SLB**: includes a list of IP addresses for SLB instances.
      - **EIP (including NAT)**: includes a list of IP addresses for EIP and NAT instances.

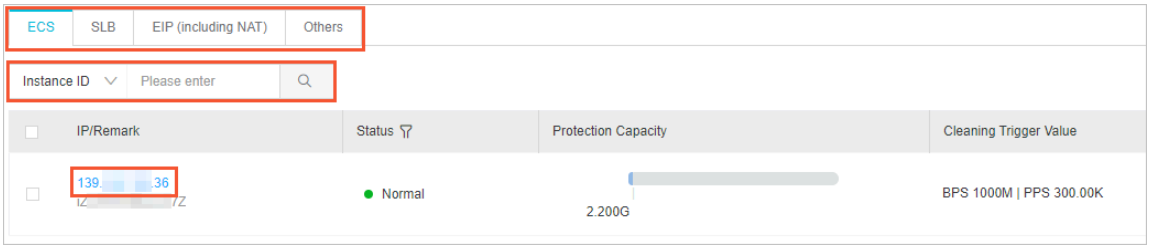
        Note:

ECS or SLB instances that have Elastic IP addresses associated are sorted into EIP instances.

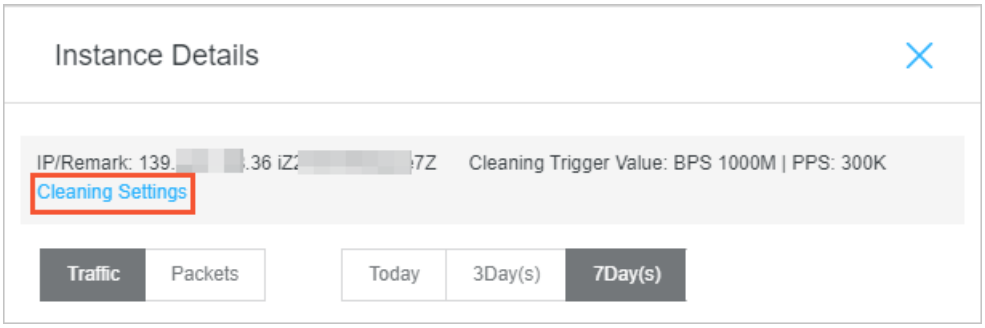
- **Others**: includes a list of IP addresses for instances that are hosted by other service providers.

b) In a list of instances, find the target instance, and click the **IP** address of the instance.

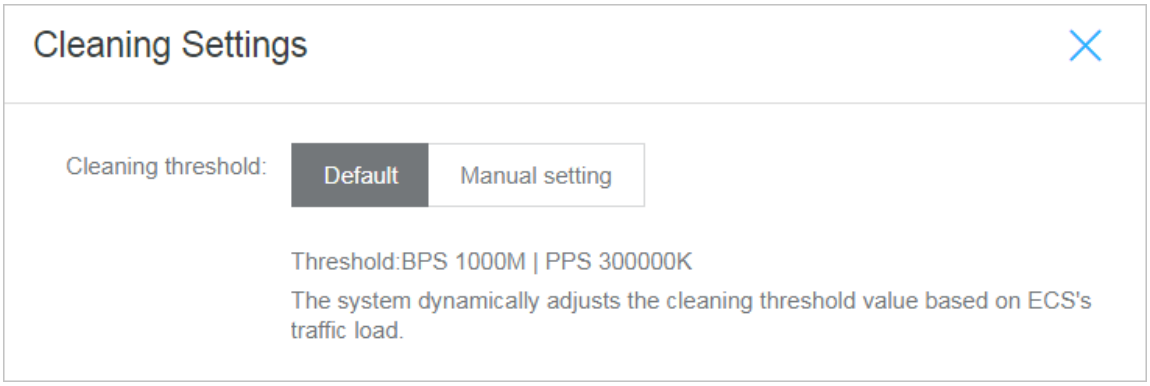
If excessive instances exist, we recommend that you search for the target instance by using the **instance ID**, **instance name**, or **instance IP** as the search condition.



Open the **Instance Details** page. The Instance Details page shows the peak daily traffic, number of daily data packets, and a list of DDoS attacks for the last seven days.



c) On the **Instance Details** page, click **Cleaning Settings**, and select **Manual Setting** or **Default** in the Cleaning Threshold field.



For more information, see Configure a cleaning threshold.

3 Configure a cleaning threshold

This topic describes how to configure a cleaning threshold in the Anti-DDoS Basic console.

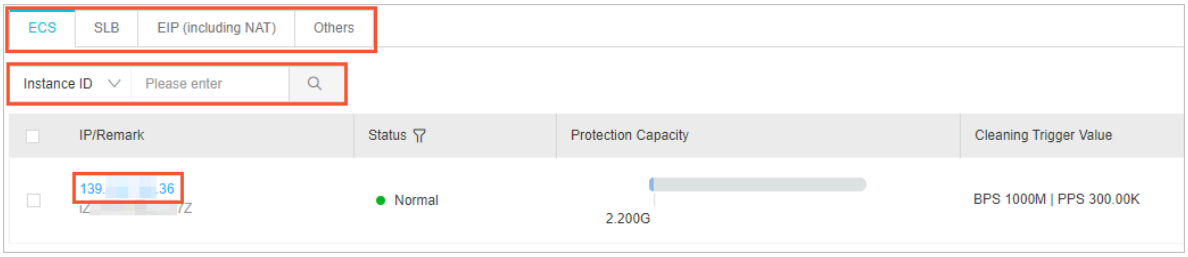
Context

Anti-DDoS Basic is applied to protect Alibaba Cloud assets by default. The service is provided free of charge after each asset is activated. The assets include Elastic Compute Service, Server Load Balancer, and Elastic IP Address instances. The maximum throughput of DDoS attacks that an asset encounters may exceed the specified cleaning threshold. In such cases, Anit-DDoS cleans attack traffic and performs other counter measures to ensure business continuity.

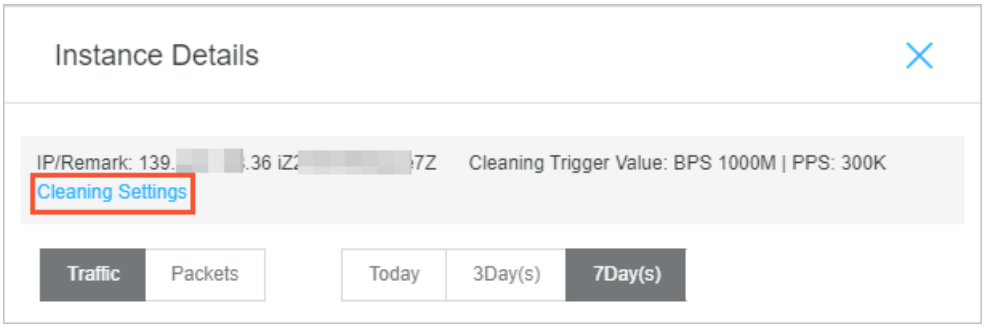
Procedure

1. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the **Assets** page, select a region.
3. Select the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud service for which you want to configure a cleaning threshold.
4. In a list of instances, find the target instance and click the **IP** address of the instance.

   If excessive instances exist, we recommend that you search for the target instance by using the **instance ID**, **instance name**, or **instance IP** as the search condition.



5. In the **Instances Details** dialog box, click **Cleaning Settings**.

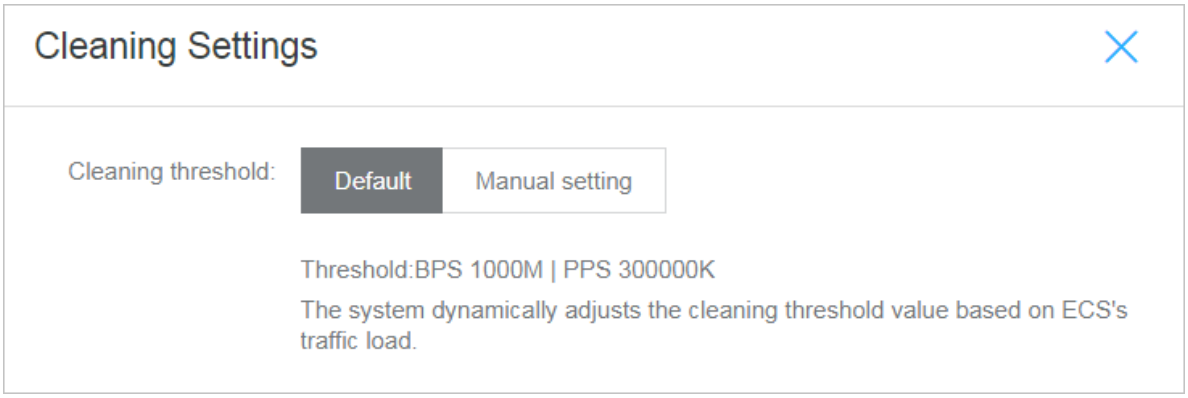


6. In the **Cleaning Settings** dialog box, select **Default** or **Manual Setting** in the Cleaning Threshold field.

   - **Default**: Anti-DDoS Basic dynamically adjusts the cleaning threshold based on the traffic load of an asset.
   - **Manual setting**: You can select a specific threshold that includes two values. One indicates the minimum throughput and the other indicates the mininum packets per second (PPS).

   Recommendations:

   - Configure a cleaning threshold of which the value is slightly greater than the maximum bandwidth for actual incoming requests. If the specified value of a threshold is greater than expected, the effect of protection is compromised. If the specified value of a threshold is less than expected, legitimate access may be affected when traffic cleaning is triggered.
   - If legitimate access is affected, we recommend that you increase the value of the cleaning threshold.
   - During large promotions or activities for a website, we recommend that you increase the specified value of a cleaning threshold.



Result

The cleaning threshold is configured. When the maximum throughput of incoming requests that a website can serve reaches the specified cleaning threshold, Anti-DDoS Basic launches traffic cleaning.

4 Cancel traffic cleaning

Anti-DDoS Basic provides default protection against distributed denial of service (DDoS) attacks for Alibaba Cloud instances. Anti-DDoS Basic automatically detects attacks and cleans excessively high traffic for instances that experience flood attacks. You can cancel traffic cleaning for IP-bound assets that are in an abnormal state such as cleaning.

Context

Cleaning refers to real-time monitoring that Anti-DDoS Basic performs on incoming data traffic of instances. Based on the monitoring result, Anti-DDoS identifies suspicious traffic such as DDoS attacks. On the premises of business continuity, Anti-DDoS Basic cleans excessively high traffic and redirects suspicious traffic from original routes to a cleaning module. Then, the cleaning module identifies and strips malicious content from suspicious traffic. After the filtering process, legitimate traffic is returned to the original routes and then forwarded to target systems.

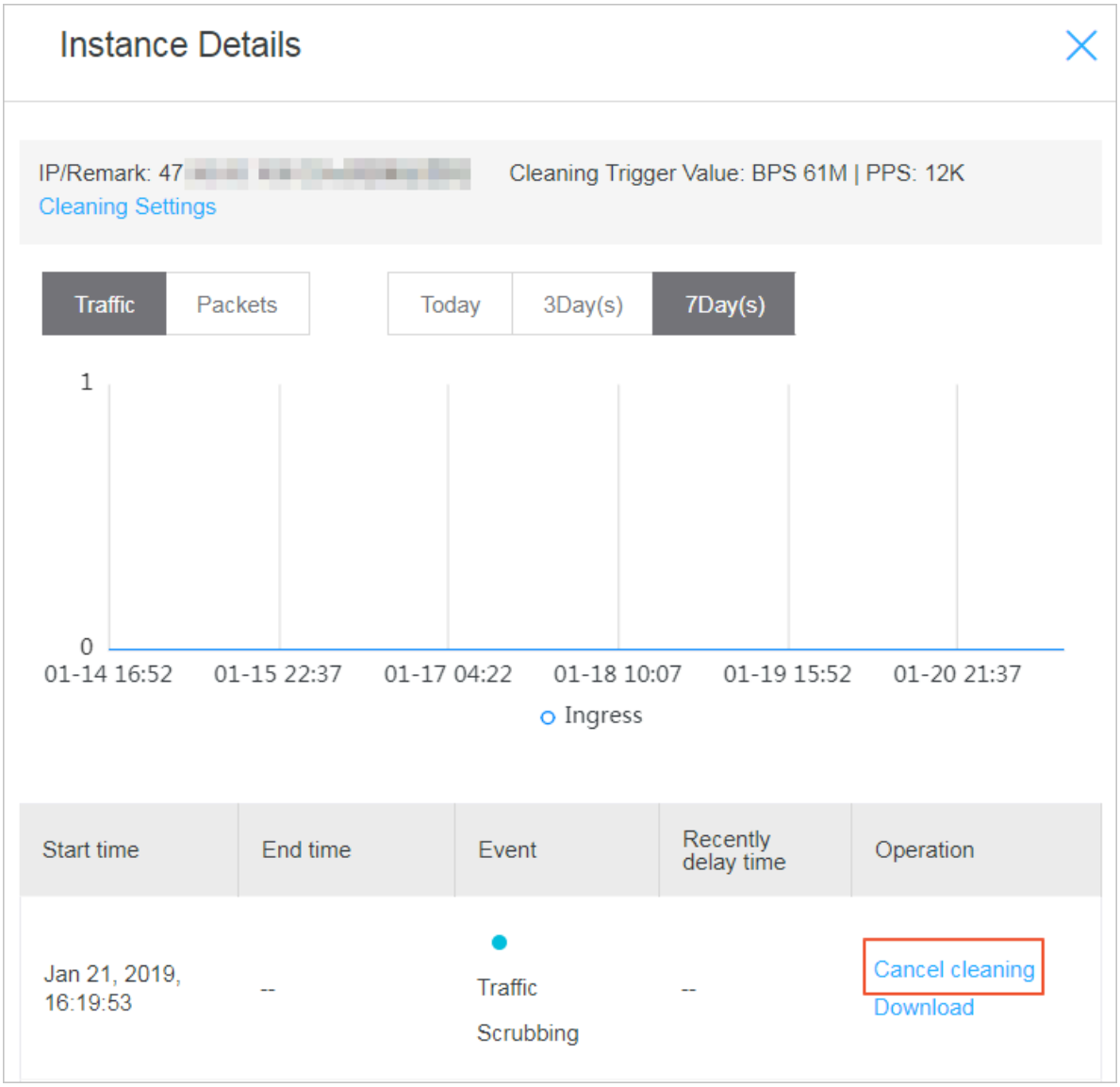
Note:
You can cancel cleaning a maximum of three times a day for each account.

Procedure

1. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the **Assets** page, select a region.
3. Select the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud service for which you want to configure a cleaning threshold.
4. In a list of instances, find an instance of which the **Status** is **Cleaning**, and click the **IP** of the instance.
5. On the **Instance Details** page, find an entry of which the **Event** is **Traffic Scrubbing** and the **End Time** is empty and click **Cancel cleaning** in the Operation column.

Note:

If no traffic scrubbing event exists, the **cancel cleaning** operation is unavailable.



Result

The traffic cleaning operation is canceled.

What's next

After you cancel traffic cleaning, we recommend that you increase cleaning thresholds in specific scenarios, such as scenarios with a sharp increase in traffic during large activities or promotions. This action avoids triggering traffic cleaning again. For more information, see Configure a cleaning threshold.

Note:

The maximum cleaning threshold for each instance of a cloud service changes based on the instance type. If the maximum cleaning threshold that you can configure cannot meet

your requirements, we recommend that you upgrade the specified instance type of the cloud service.

5 Black hole policies

5.1 View the duration of a black hole

A server may encounter a distributed denial of service (DDoS) attack. After a black hole is triggered due to the attack, access from clients to the public IP address of the server is blocked for a period of time. The access is unblocked after the duration of the black hole expires. The default black hole duration for an asset changes based on the region where the asset resides. You can view the duration of a black hole for an asset in the Anti-DDoS Basic console.

Context

The default duration of a black hole is 2.5 hours and you cannot disable the black hole during the period. In practical scenarios, the black hole duration depends on the attack situation and may range from 30 minutes to 24 hours. The duration of a black hole changes based on the following factors:

- The duration of attacks. If attacks continue, the black hole duration is extended.
- The frequency of attacks. If an asset experiences attacks for the first time, the black hole duration automatically decreases. Otherwise, assets that experience frequent attacks have a high probability to encounter continuous attacks. In such cases, the black hole duration is automatically extended.

You can refer to the Anti-DDoS Pro console for more details about the black hole triggering threshold and black hole duration.

Note:

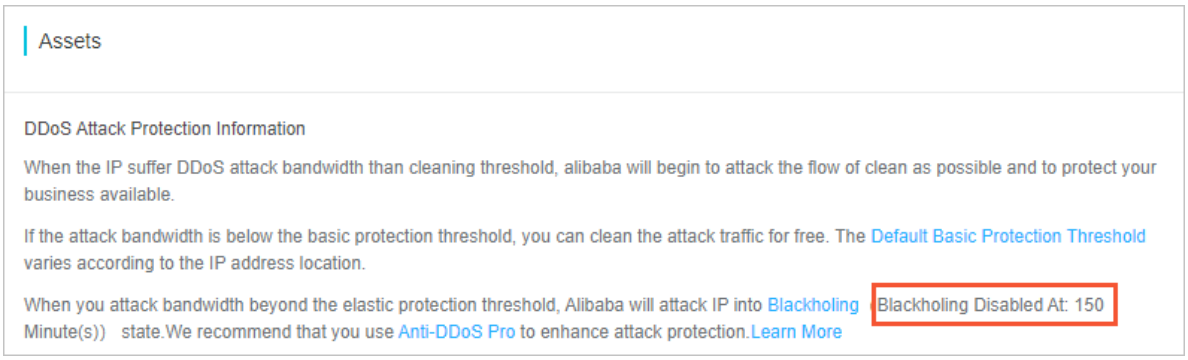
- If excessive breaches of the black hole threshold occur on an asset, Alibaba Cloud reserves the right to extend the black hole duration and decrease the black hole threshold for the asset.
- Blackhole filtering is a service that Internet service providers (ISPs) provide for Alibaba Cloud. Specific black hole triggering thresholds are predefined by ISPs. In most cases, the duration of a black hole is greater than or equal to 30 minutes. The duration of each black hole for an account changes based on the security credits of the account.

For more information about black hole policies that Alibaba Cloud provides, see #unique_8.

Procedure

1. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the **Assets** page, select a region.
3. On the top of the Assets page, view **DDoS Attack Protection Information**.

   The duration after **Blackholing Disabled At** in the DDoS Attack Protection Information section refers to the black hole duration for an asset in the specified region.



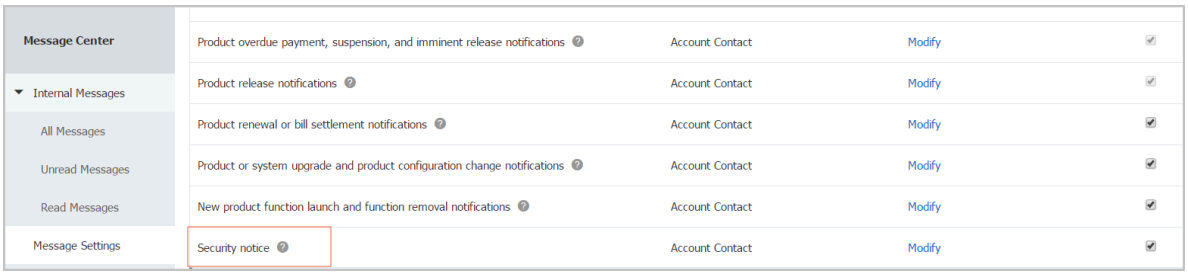
5.2 Configure DDoS Protection notification settings

Alibaba Cloud provides DDoS Protection notifications. When a server under your account suffers DDoS attacks, triggers traffic scrubbing or the blackhole mechanism, the system sends notifications by specified methods to specified receivers.

Manage message recipients

To configure the notification methods (Internal Messages, Email, and Text message) and recipients for Security Notice, follow these steps:

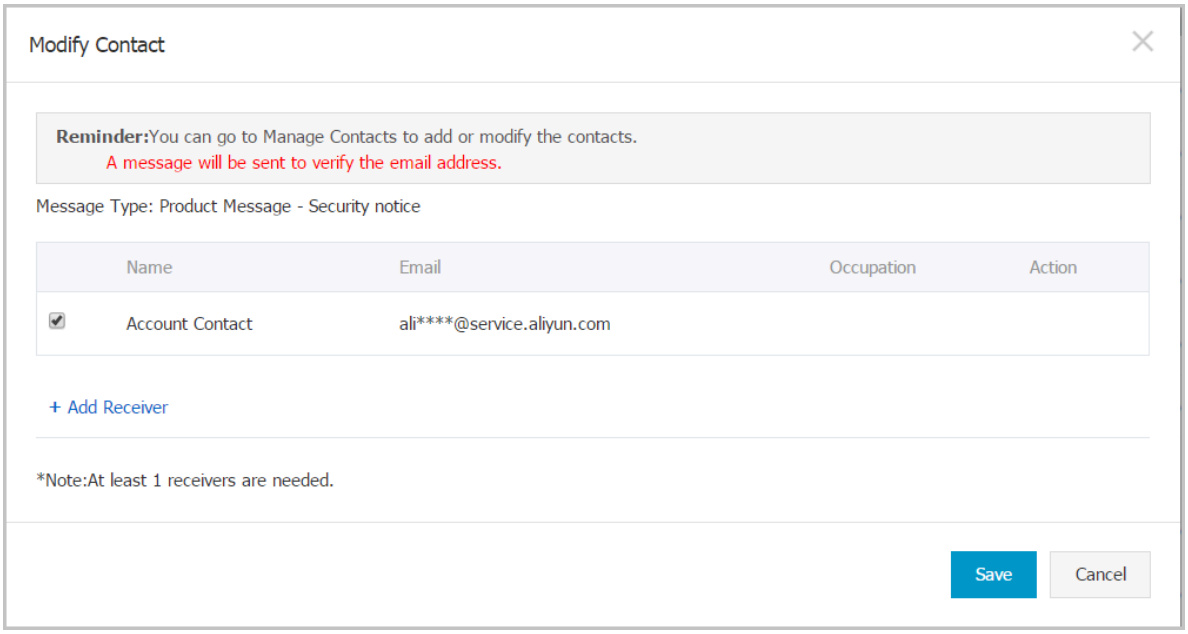
1. Log on to the Message Center console.
2. Click **Message Settings** and locate to **Security Notice**.



3. Click **Modify** and select the message recipient.

Note:

To add a new message recipient, click **Add Receiver**.



5.3 View the time when a black hole is enabled for an instance and the reason for enabling the black hole

In the Anti-DDoS Pro console, you can view a list of black hole events for all assets that belong to an account. For example, you can view the time point when a black hole is enabled for an asset and a list of IP addresses from which attacks originate.

Context

The public IP address of an Elastic Compute Service (ECS) or Server Load Balancer (SLB) instance may experience a large number of distributed denial of service (DDoS) attacks. If the throughput of these attacks exceeds the predefined black hole triggering threshold, all traffic to the public IP address is routed to a black hole. Your businesses are no longer accessible by clients because all exterior traffic is dropped.

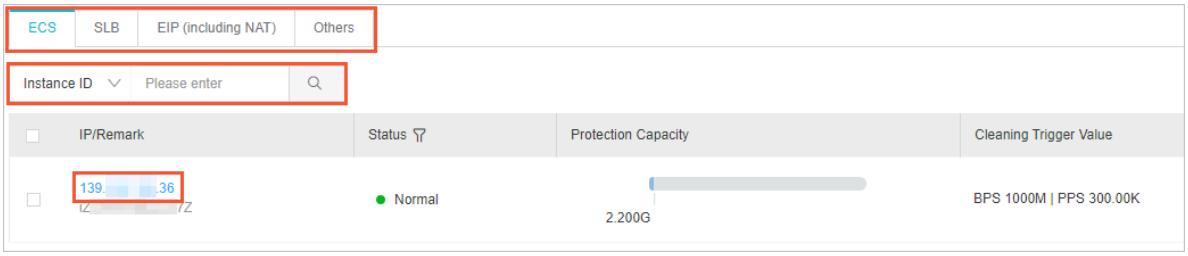
The black hole triggering threshold for an instance changes based on the region where the instance resides. For more information about black holes, see #unique_8.

Procedure

1. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the **Assets** page, select a region.
3. Select the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud service for which you want to configure a cleaning threshold.

4. In a list of instances, find the target instance and click the **IP** address of the instance.

   If excessive instances exist, we recommend that you search for the target instance by using the **instance ID**, **instance name**, or **instance IP** as the search condition.



5. On the **Instance Details** page, view a list of historical black hole events where the **Event** is **Black Hole** and view the peak traffic for each attack.

   The **Start time** and **End time** of a black hole event are displayed.

> **Note:**
> If no black hole or scrubbing event for an asset exists, no result is displayed in the event list.

6. Optional: In the Operation column of the target event, click **Download**. You can use the downloaded packet file for the attack event as evidence of criminal activity. You can send the evidence to the Internet Crime Reporting Center.

5.4 Connect to a server whose IP address is thrown into the black hole

If your server suffers from a heavy traffic attack and its IP address is thrown into the black hole, then all external traffic to the server is discarded. However, you can still access this server from Alibaba Cloud services within the same region as that of this server.

> **Note:**
> During the black hole period, external access requests sent to this server are blocked.

You can use an Alibaba Cloud ECS instance to connect to your server, even when its IP address is thrown into the black hole.

1. Connect to an Alibaba Cloud ECS instance that can be normally accessed and is within the same region as this server.

> **Note:**

This ECS instance must be connectable to the server under black hole status. They must belong to the same VPC environment, and the connection is not blocked by any security group access control rules.

2. Use a tool or command line to connect from the ECS instance to the server under black hole status.

After successfully connecting to the server from the ECS instance, you can transfer files from the server to the ECS instance and modify the configuration files on this server.

5.5 Black hole triggering thresholds in Anit-DDoS Basic

The following table lists the default thresholds at which Anti-DDoS automatically triggers black holes in each region. These thresholds are measured in bit/s.

Note:

- Anti-DDoS can automatically trigger black holes for Elastic Compute Service (ECS), Server Load Balancer (SLB), Elastic IP Address (EIP), and Web Application Firewall (WAF) instances. This feature is available for IPv4 networks in all regions and for IPv6 network only in specific regions. In the following table, a check sign (√) in the Support IPv6 column indicates that the automatic black hold trigger feature is supported for IPv6 in the region and the thresholds are applicable to both IPv4 and IPv6. A cross sign (×) indicates that the feature is not supported for IPv6 in the region and the thresholds are applicable only to IPv4 networks.
- Practical black hole triggering thresholds for ECS, SLB, and EIP instances change based on the instance type and bandwidth that you purchase. You can refer to the **Assets** page of the Anti-DDoS Basic console for more details. For more information, see #unique_10.
- In each region, the same threshold to trigger black holes is applied for WAF, SLB, and EIP instances.

Region	Support IPv4	Support IPv6	ECS instances with one vCPU	ECS instances with two vCPUs	ECS instances with more than four vCPUs	SLB, EIP (includes public IP addresses of NAT gateways), and WAF instances
China (Hangzhou)	√	√	500 Mbit/s	1 Gbit/s	5 Gbit/s	5 Gbit/s
China (Shanghai)	√	√	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Qingdao)	√	×	500 Mbit/s	1 Gbit/s	5 Gbit/s	5 Gbit/s
China (Beijing)	√	√	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Zhangjiakou-Beijing Winter Olympics)	√	√	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Hohhot)	√	√	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Shenzhen)	√	√	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Heyuan)	√	√	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Chengdu)	√	×	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
China (Hong Kong)	√	√	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
Singapore	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
Australia (Sydney)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
Malaysia (Kuala Lumpur)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
Indonesia (Jakarta)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
Japan (Tokyo)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
Germany (Frankfurt)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s

Region	Support IPv4	Support IPv6	ECS instances with one vCPU	ECS instances with two vCPUs	ECS instances with more than four vCPUs	SLB, EIP (includes public IP addresses of NAT gateways), and WAF instances
UK (London)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
US (Silicon Valley)	√	×	500 Mbit/s	1 Gbit/s	2 Gbit/s	2 Gbit/s
US (Virginia)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s
India (Mumbai)	√	×	500 Mbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s
UAE (Dubai)	√	×	500 Mbit/s	500 Mbit/s	500 Mbit/s	500 Mbit/s

The default black hole duration is 2.5 hours. During this period, blackholing is enabled and cannot be disabled. The actual black hole duration changes based on the type of attack, ranging from 30 minutes to 24 hours. The black hole duration is based on the following factors:

- The duration of attacks: If attacks continue, the black hole duration is extended. The next black hole duration is set to zero and starts at the time when the last black hole duration is extended.
- The frequency of attacks: If an asset experiences attacks for the first time, the black hole duration automatically decreases. Otherwise, assets that experience frequent attacks have a high probability to encounter continuous attacks. In such cases, the black hole duration is automatically extended.

Note:

If excessive breaches of the black hole threshold occur on an asset, Alibaba Cloud reserves the right to extend the black hole duration and decrease the black hole threshold for the asset. You can refer to the Anti-DDoS console for more details about the black hole triggering threshold and black hole duration.

5.6 Anti-DDoS Basic black hole threshold for web hosting

The default black hole threshold for web hosting is as follows (unit: bps).

Note:
For shared web hosting, the specific black hole threshold cannot be defined as multiple web hosting may share one IP address. Additionally, the actual threshold must be lower than the default threshold value. When a shared web hosting server triggers the black hole, all the other servers that share IP address with this server becomes inaccessible. We strongly recommend that you buy ECS instance if you give utmost importance to the security.

Region	Web hosting threshold
China (Hangzhou)	5 G
China (Qingdao)	5 G
China (Shenzhen)	2 G
China (Beijing)	2 G
China (Shanghai)	2 G
Hong kong	500 M
US West	500 M
Singapore	500 M

The black hole duration is the amount of time the triggered back hole lasts, 2.5 hours by default. The actual black hole duration varies from 30 minutes to 24 hours, depending on attack intensity. Additionally, the following factors are considered:

- Attack Continuity. The black hole duration is extended, if the attack continues.
- Attack Frequency. The black hole duration is shortened automatically when the ECS instance is attacked for the first time, but can be prolonged accordingly, if under frequent attacks.

Note:
If an ECS instance triggers too many black holes, Alibaba Cloud Security reserves the right to extend the black hole duration and lower its threshold. You can check the actual duration and threshold information in Alibaba Cloud Anti-DDoS Basic console.

To get more powerful DDoS mitigation capacities, see Alibaba Cloud Anti-DDoS Pro.

5.7 Deactivate a black hole

This topic describes how to deactivate a black hole that is applied to the IP address of a protection target.

Context

After you purchase an Anti-DDoS Origin Enterprise instance, you can deactivate a black hole 100 times each month.

> **Note:**
> At the end of each month, the unused quota becomes invalid.

Before you manually deactivate a black hole, we recommend that you check the auto-deactivation time of the black hole in the Anti-DDoS Origin console. If the auto-deactivation time meets your requirements, we recommend that you wait for the black hole to automatically deactivate. For more information, see View the duration of a black hole.

Procedure

1. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the page, select a region where the instance resides.
3. In the **Anti-DDoS Origin console**, find the instance whose operations logs that you want to view, and click **Deactivate Black Hole** in the Actions column of the instance.

   > **Note:**
   > You can **deactivate a black hole**. If **an abnormal IP address** exists in the instance, it indicates that the related protection target is in the blackholing state.

4. On the **Protection Target** tab, find a protection target that is in the **Blackholing** state, and click **Deactivate Black Hole** in the Actions column of the protection target.
5. The **Deactivate Black Hole** dialog box shows the remaining times that you can deactivate a black hole. Click **OK**.

   > **Note:**
   > You may fail to deactivate a black hole due to the predefined policies for risk management of a backend system of Alibaba Cloud. The number of remaining times does not decrease when you fail to deactivate a black hole.

Result

If you fail to deactivate a black hole, you will receive a notification. We recommend that you wait a few minutes and try again. If you do not receive a failure message, it means that the black hole is deactivated.

6 Add a protection target

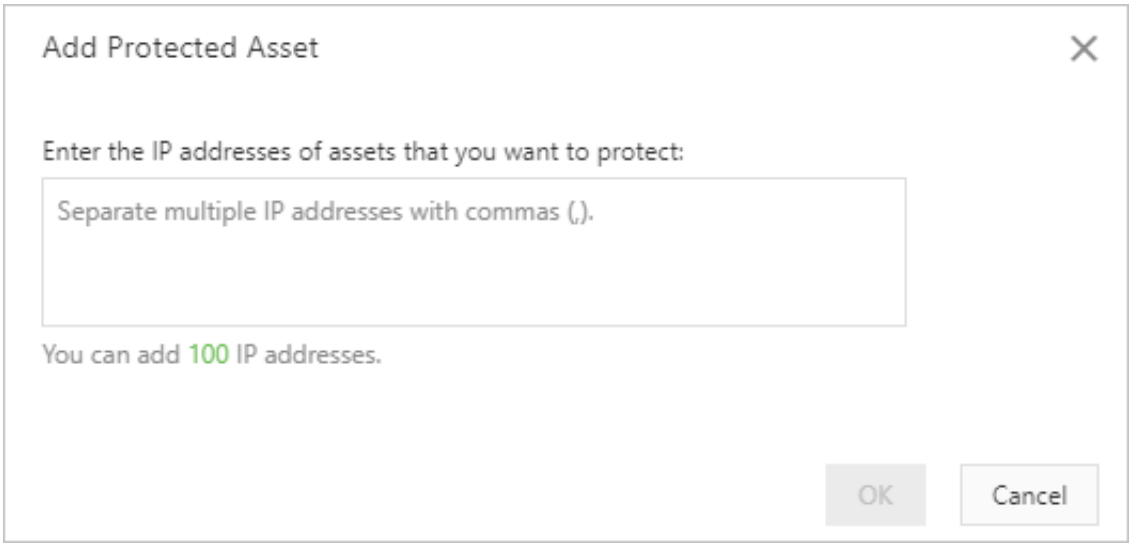
After activating Anti-DDoS Origin Enterprise, you can add IP addresses that you want to protect to an Anti-DDoS Origin Enterprise instance.

Procedure

1. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the page, select a region where the instance resides.
3. On the **Anti-DDoS Origin**, find the target instance, and click **Add Protection Target** in the Actions column of the instance.

4. Optional: If you are a first-time user of Anti-DDoS Origin Enterprise, we recommend that you follow the instructions that are provided on the page to authorize the instance to protect other cloud resources under your account. If authorization is complete, no notification appears.

5. In the **Add Protection Target** dialog box, add the IP address of a cloud resource to be protect, and click **OK**.



When you add an IP address, you may receive an error showing **The specified IP address is invalid**. For more information about the error, see Troubleshoot issues related to invalid IP addresses.

Result

After the configuration is complete, Anti-DDoS Origin provides protection for the IP address that is added to the instance.

What's next

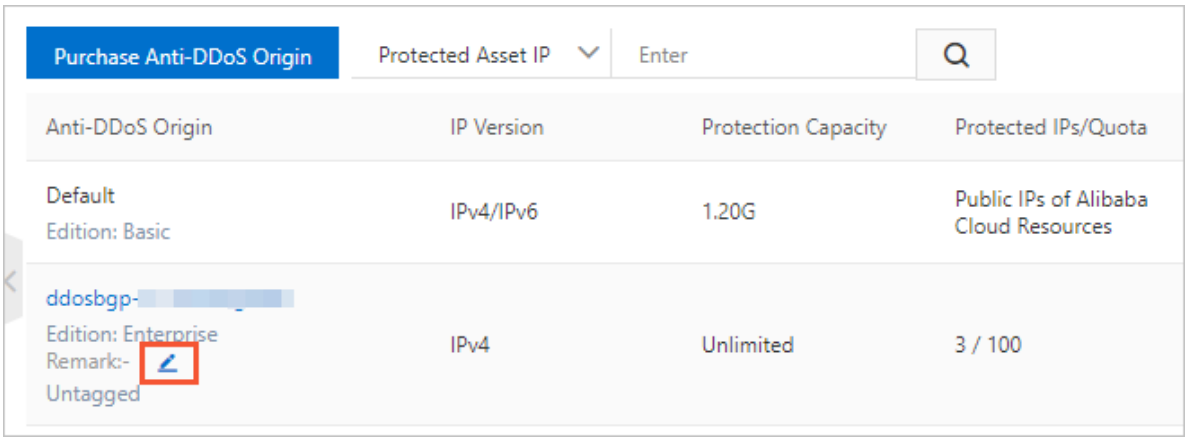
- View security reports
- Deactivate a black hole

7 Specify an alias

You can specify an alias for an Anti-DDoS Origin instance. If multiple Anti-DDoS Origin instances exist, you can configure an alias for each instance based on the characteristics of the instances. The characteristics include the applicable target, scenario, and scope. You can use aliases to differentiate instances to simplify identification and management of your instances.

Procedure

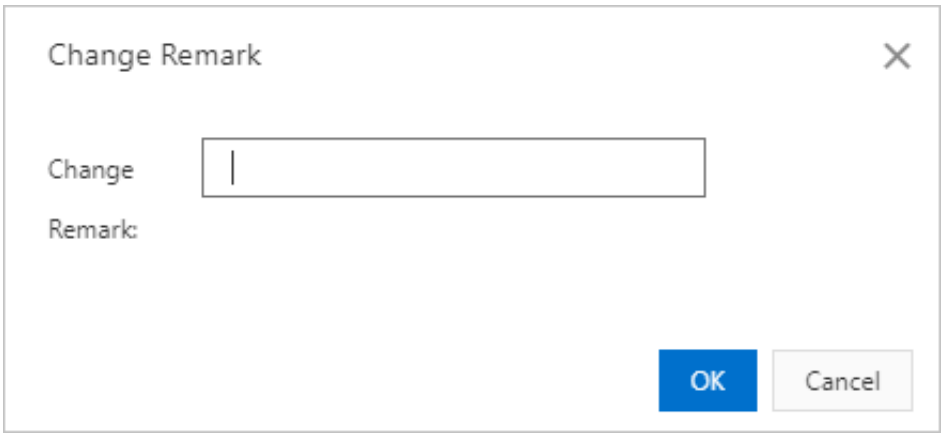
1. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the page, select a region where the instance resides.
3. In the **Anti-DDoS Origin** console, find the target instance, and click the Edit icon next to the alias of the instance.



4. In the **Edit Alias** dialog box, enter an alias, and click **OK**.

Note:

The alias must be 2 to 50 characters in length and can contain letters, digits, and underscores (_).



Result

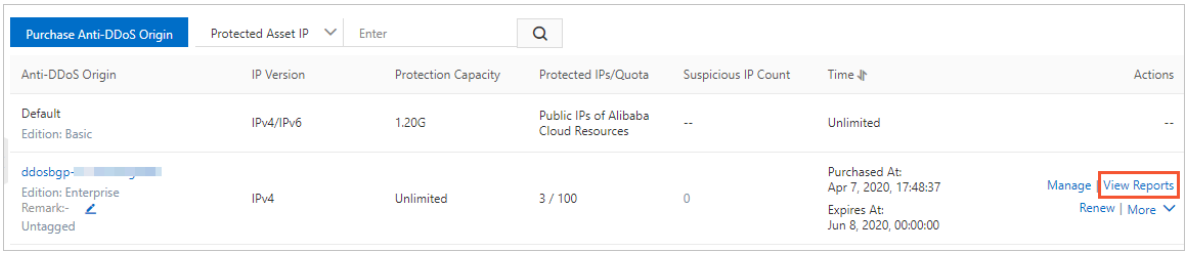
After you edit an alias, the alias is displayed under the ID of the instance. You can follow the preceding steps to edit the alias of an Anti-DDoS Origin instance at any time based on your business requirements.

8 View security reports

This topic describes how to view the total traffic of an instance, traffic of each IP address, and a list of event logs for DDoS attacks after you add a protection target to the instance.

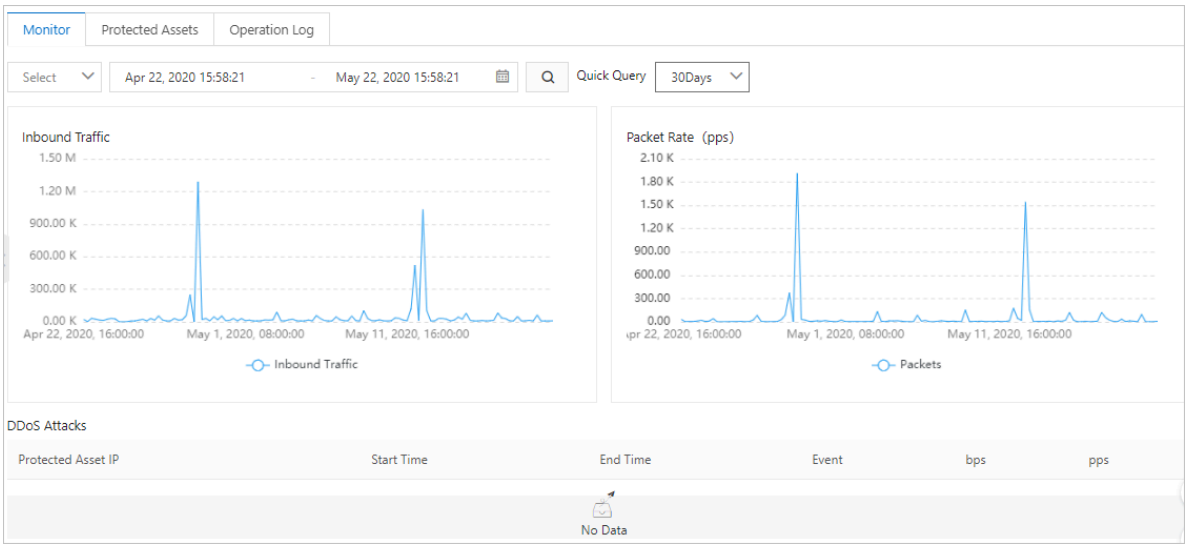
Procedure

1. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the page, select a region where the instance resides.
3. In the **Anti-DDoS Origin** console, find the instance whose operations log that you want to view, click **View Report** in the Actions column of the instance.



4. On the **Monitoring** tab, select a protection target and a time range. The console shows the trend of network traffic and event logs of DDoS attacks. The network traffic metric includes the inbound traffic and number of received data packets.

> **Note:**
> You can query data of the last 30 days.

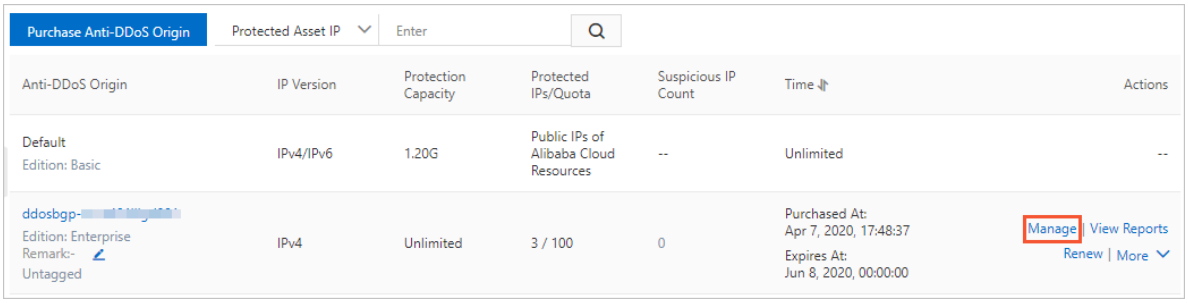


9 View operations logs

This topic describes how to view the operations logs of Anti-DDoS Origin instances. In the Anti-DDoS Origin console, you can trace configuration changes of each instance.

Procedure

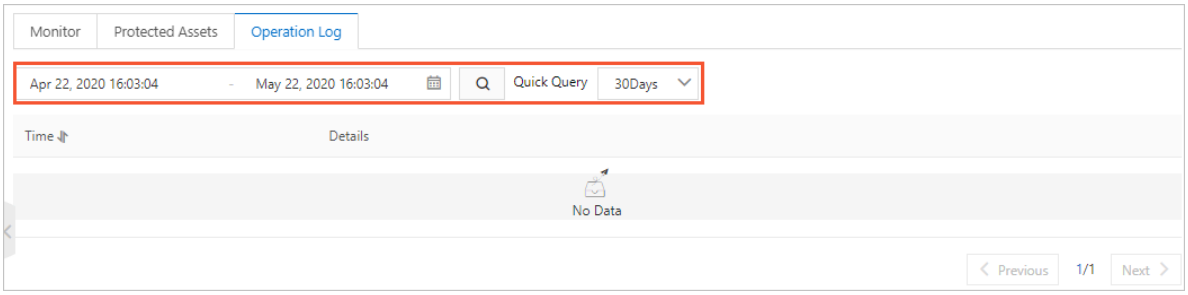
1. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the page, select a region where the instance resides.
3. On the **Instances** page, find the instance whose operations logs that you want to view, and click **Manage** in the Actions column of the instance.



4. On the Instance Details page, click the **Operations Log** tab.
5. On the **Operations Log** tab, specify a time range and query operations logs that are generated within the time range. Each operations log includes the operation time and a description.

Note:

You can view operations logs of the last 30 days.



10 Upgrade Anti-DDoS Origin to Anti-DDoS Pro

This topic describes how to improve protection capacity by upgrading Anti-DDoS Origin to Anti-DDoS Pro. Given the design of Anti-DDoS Origin, the effect of protection may be compromised or the protection capacity cannot meet your business requirements. In such cases, we recommend that you upgrade Anti-DDoS Origin to Anti-DDoS Pro.

Context

For more information about scenarios to which Anti-DDoS Origin is applicable, see Scenarios.

If you encounter one of the following issues when using Anti-DDoS Origin, we recommend that you upgrade Anti-DDoS Origin to Anti-DDoS Pro.

- A protection target encounters continuous DDoS attacks that last for a long period of time.
- A protection target encounters HTTP flood attacks. However, Anti-DDoS Origin cannot defend against these types of attacks.
- Other specific issues.

Note:
Alibaba Cloud will refund you the remaining balance of a paid Anti-DDoS Origin instance.

Procedure

1. Contact Alibaba Cloud Technical Support by using DingTalk.

   To join the DingTalk group, scan the following QR code.

   Note:
   If you have any questions when you upgrade Anti-DDoS Origin to Anti-DDoS Pro, contact Alibaba Cloud Technical Support by using DingTalk.

2. Alibaba Cloud support engineers will evaluate your environment to determine whether you can upgrade to Anti-DDoS Pro.

3. If all conditions are met, Alibaba Cloud will refund you the remaining balance of a paid Anti-DDoS Origin instance. The amount of the refund changes based on the specifications and remaining subscription duration of the Anti-DDoS Origin instance.
4. Purchase an Anti-DDoS Pro instance and add your assets to the instance for protection.

11 Activate Anti-DDoS Origin to protect IP addresses from DDoS attacks

By default, Alibaba Cloud provides basic protection capacity for resources that have public IP addresses configured. These resources include Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, Elastic IP (EIP) instances, and Web Application Firewall (WAF) assets. If the throughput of a DDoS attack is more than the default protection capacity of the resource, we recommend that you purchase Anti-DDoS Origin Enterprise instance. Anti-DDoS Origin Enterprise uses all protection capacity of a region where the public IP address resides to defense against the attacks. This ensures business continuity.

Context

Anti-DDoS Origin Enterprise provides unlimited protection. When DDoS attacks are detected, Anti-DDoS Origin Enterprise automatically uses all the protection capacity of a region where an instance resides to defend against the DDoS attacks.

Prerequisites

Before activating Anti-DDoS Origin Enterprise, you need to confirm the following informatio n:

- The IP address that you want to protect.
- The region where the IP address resides.

> **Note:**
> Anti-DDoS Origin is not available in all regions. Before you activate Anti-DDoS Origin, ensure that Anti-DDoS Origin is available in the region where an IP address that you want to protect resides. For more information about supported regions where you can activate Anti-DDoS Origin Enterprise, see #unique_27.

Procedure

1. For more information about how to purchase an Anti-DDoS Origin Enterprise instance, see Purchase an Anti-DDoS Origin Enterprise instance.

   > **Note:**
   > Ensure that the region where an Anti-DDoS Origin instance resides is the same as the region where resources that are protected by the instance reside. The resources include

Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and Elastic IP (EIP) instances.

2. Log on to the Anti-DDoS Basic console.
3. On the **Anti-DDoS Origin** page, find the target instance, and click Add a protection target to add the addresses that you want to protect to the instance.

Result

After you add an IP address to an Anti-DDoS Origin instance, the protection capacity of the instance applies to the IP address. On the **Assets** page, you can find that the protection capacity of the IP address increases to the protection capacity of the instance.

12 Best Practices

12.1 Best practices for automatic deactivation of black holes

To ensure business continuity, you must learn how to recover your business by deactivating a black hole that is applied to the IP address of a protection target. A black hole may still be activated if the protection target encounters an instantaneous amount of high-traffic DDoS attacks. Anti-DDoS Origin Enterprise supports automatic deactivation of black holes in response to such requirements.

Prerequisites

The solution applies to only Anti-DDoS Origin Enterprise instances. This is because you must call an Anti-DDoS Origin API operation to complete auto-deactivation. Before implementing the solution, make sure that the IP address of the required protection target is added to an Anti-DDoS Origin Enterprise instance. For more information, see Add a protection target.

Context

Anti-DDoS Origin allows you to deactivate black holes manually or automatically. However, manual deactivation may result in delays and unexpected errors. For more information, see Deactivate a black hole. If your business requires a high level of stability and continuity, you can use the following method to set up automated responses and deactivation for black holes.

1. Create an alarm rule in the CloudMonitor console to monitor the blackhole events of an Anti-DDoS Origin Enterprise instance.

   Note:
   Only if blackhole events occur on the protected IP addresses, CloudMonitor sends messages. You must add IP addresses that you want to protect to the instance as protection targets.

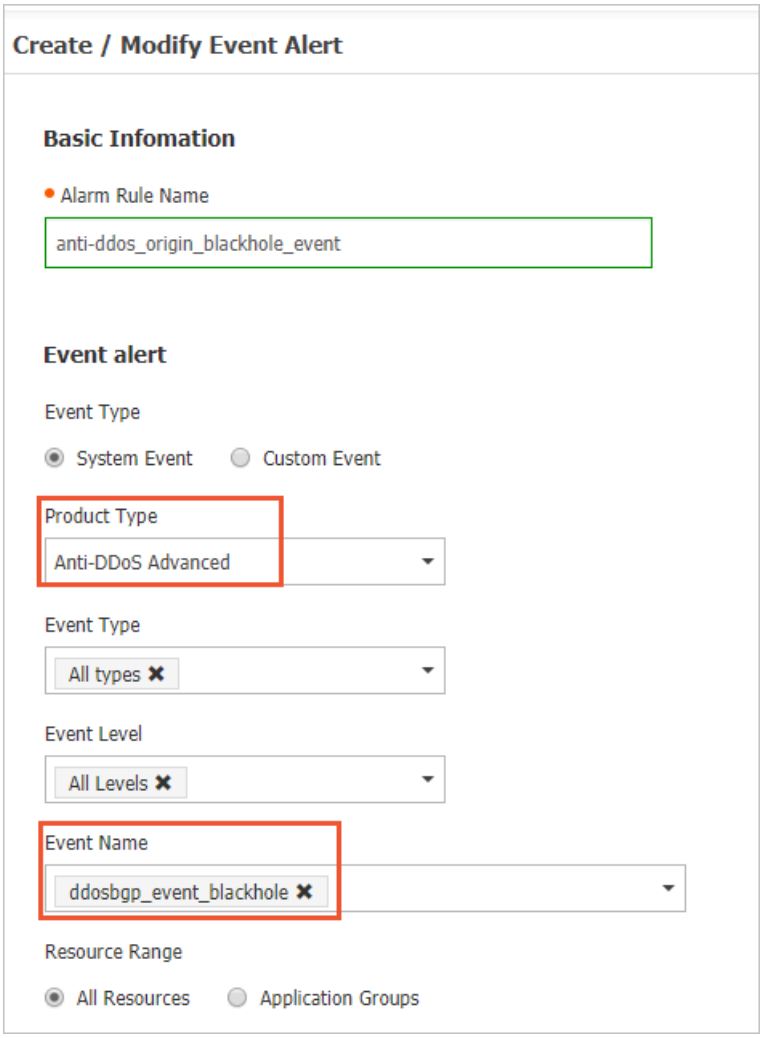
2. Create an alarm rule and specify an action of calling the #unique_30 API operation of Anti-DDoS Origin to deactivate the black holes.

Likewise, the preceding method also allows you to automatically call an API operation of Alibaba Cloud DNS. The operation helps change DNS records for a domain that is under

DDoS attacks and associate the name of the domain with the IP address of an Anti-DDoS Pro instance.

Procedure

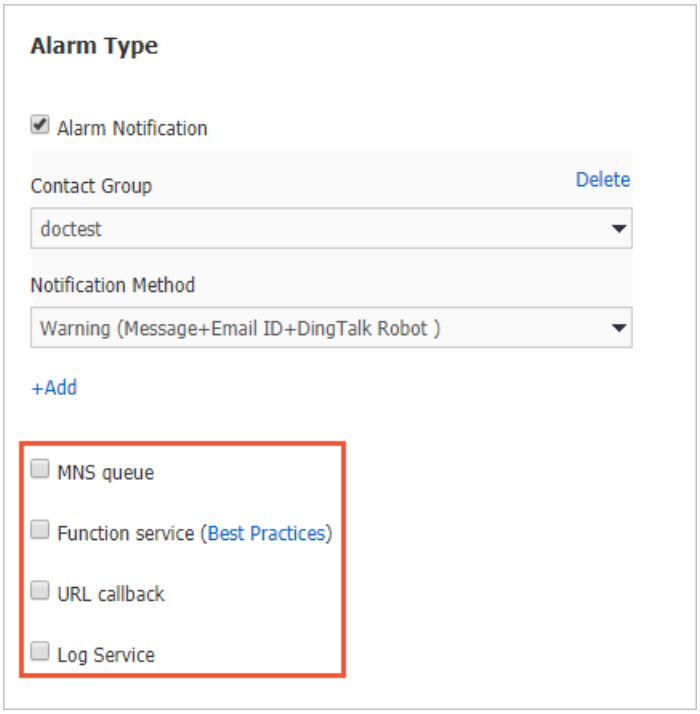
1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, choose **Alarms** > **Alarm Rules**.
3. On the **Alarm Rules** page, select the **Event Alarm** tab.
4. Click **Create Event Alert** to create a rule for blackholing events.
   - In the **Product Type** field, select **Anti-DDoS Advanced**.
   - In the **Event Name** field, select **ddosbgp_event_blackhole**.



5. In the event alarm, select alarm types based on your business requirements and click **OK**.

   CloudMonitor supports the following alarm types:

   - **MNS queue**
   - **Function Compute**
   - **URL callback**
   - **Log Service**



After you create the event alarm, the alarm automatically triggers a response to any blackhole events. Then, CloudMonitor sends an alarm message to the target that you specified in the Alarm Type section. The following shows a sample alarm message.

Sample alarm message

```
{
   "action": "add", //The action. The value of add indicates that an event begins, and the value of del indicates that an event ends.
   "bps": 0, //The throughput of a DDoS attack. Unit: Mbit/s.
   "pps": 0, //The packet forwarding rate of a DDoS attack. Unit: packets per second (PPS).
   "instanceId": "ddosbgp-cn-78v17******", //The ID of an Anti-DDoS Origin instance.
   "ip": "47. *. *. *", //The IP address to which a black hole is applied.
   "regionId": "cn-hangzhou", //The ID of a region where the Anti-DDoS Origin instance resides.
   "time": 1564104493000, //The time when the event begins. Unit: milliseconds.
   "type": "blackhole"  //The event type. The value of defense indicates a cleaning event, and the value of blackhole indicates a blackholing event.
```

```
}
```

6. Specify an alarm action that calls the #unique_30 API operation to deactivate black holes.

12.2 Integrate Anti-DDoS Origin with Anti-DDoS Pro

This topic describes how to integrate Anti-DDoS Origin with Anti-DDoS Pro. The integration provides effective protection for your business data against distributed denial of service (DDoS) attacks without compromising business continuity. To integrate Anti-DDoS Origin with Anti-DDoS Pro, create a scheduling rule for Sec-Traffic Manager of Anti-DDoS Pro.

Background information

Anti-DDoS Origin is a security service that provides protection against DDoS attacks for specific Alibaba Cloud services. These services include Elastic Compute Service (ECS), Server Load Balancer (SLB), Elastic IP Address (EIP), and Web Application Firewall (WAF). Compared with Anti-DDoS Pro, Anti-DDoS Origin attaches protection capabilities to cloud services. You do not need to change the IP addresses of resources that you want to protect. You also do not need to limit the number of Layer 4 ports and the number of Layer 7 domain names for a protection target. Anti-DDoS Origin provides out-of-the-box deployment and elastic protection. If your business encounters large-scale DDoS attacks, Anti-DDoS Origin uses all resources that reside in a region to provide unlimited protection. Anti-DDoS Origin provides protection against DDoS attacks whose bandwidth can be up to hundreds of gigabits per second.

Anti-DDoS Pro provides eight-line bandwidth resources of the Border Gateway Protocol (BGP) type at the terabit level. This is only available for regions inside mainland China. Anti-DDoS Pro provides a protection bandwidth of up to 1.5 Tbit/s. This allows you to defend against volumetric DDoS attacks of the terabit level. Anti-DDoS Pro routes DDoS attack traffic to scrubbing centers based on DNS records. Anti-DDoS Pro provides high-quality BGP bandwidth resources for China Telecom, China Unicom, China Mobile, China Education and Research Network (CERNET), and other Internet service providers (ISPs) inside mainland China with an average latency of about 20 ms.

To enable interaction between Anti-DDoS Origin and Anti-DDoS Pro, you can create a scheduling rule for Sec-Traffic Manager of Anti-DDoS Pro. This rule allows you to use Anti-DDoS Origin for daily protection against low-traffic DDoS attacks and switch traffic over to Anti-DDoS Pro in the event of heavy-traffic DDoS attacks.

Overview

The integration solution allows you to use both Anti-DDoS Origin and Anti-DDoS Pro. The integration solution provides cost controllability, protection for full-scale assets, and transparent deployment without extra latencies from Anti-DDoS Origin as well as protection against volumetric DDoS attacks from Anti-DDoS Pro.

The integration solution allows you to purchase an Anti-DDoS Origin Enterprise instance. This allows you to protect a maximum of 255 IP addresses of a specific region. With unlimited protection, Anti-DDoS Origin Enterprise provides a protection capability that ranges from 100 Gbit/s to 300 Gbit/s based on the region. Besides the protection of Anti-DDoS Origin, you can purchase another Anti-DDoS Pro instance as a backup to defend against DDoS attacks whose bandwidth is greater than 300 Gbit/s. After you create a scheduling rule, all resources are consolidated into Sec-Traffic Manager for centralized management. If a black hole is triggered by Anti-DDoS Origin, Sec-Traffic Manager automatically switches traffic over to Anti-DDoS Pro.

The integration solution provides the following features:

- Anti-DDoS Origin Enterprise provides multi-region account-level protection without extra latencies. You do not need to change the IP addresses of resources and business structures.
- Anti-DDoS Origin provides unlimited protection that ranges from 100 Gbit/s to 300 Gbit/s based on the region. Anti-DDoS Pro is used to defend against DDoS attacks whose bandwidth is greater than 300 Gbit/s.
- If a black hole is triggered, a switchover is automatically performed from Anti-DDoS Origin to Anti-DDoS Pro based on DNS records. A switchover requires 1 to 3 minutes or 5 to 10 minutes to complete based on the response time of local DNS servers.
- Dedicated circuits are provided for back-to-origin traffic. This eliminates the effect of black holes on traffic.

After you integrate Anti-DDoS Origin with Anti-DDoS Pro, SLB instances, ECS instances, or WAF assets are under the protection of Anti-DDoS Origin Enterprise without extra latencies. If an attack bandwidth exceeds the threshold, a black hole is triggered by Anti-DDoS Origin. In this case, Sec-Traffic Manager switches traffic over to Anti-DDoS Pro, which forwards inbound traffic to a scrubbing center but has a latency of about 20 ms. If the attack stops, inbound traffic is rerouted to SLB instances, ECS instances, or WAF assets, and Anti-DDoS Origin starts to provide protection capabilities.

- If a switchover is triggered, the process requires 5 to 10 minutes to complete based on the response time of local DNS servers that are deployed inside mainland China.

  Note:
  It requires about 5 to 10 minutes for DNS servers that are deployed inside mainland China to respond. It requires about 1 to 3 minutes for DNS servers that are deployed outside mainland China to respond.
- If protection is switched over to Anti-DDoS Pro, the black hole triggering threshold is limited to the maximum protection capability of Anti-DDoS Pro. Anti-DDoS Pro provides basic protection of up to 30 Gbit/s and elastic protection of up to 300 Gbit/s. However, you can submit a ticket to upgrade the protection capability to 1 Tbit/s or higher.
- After protection is switched over to Anti-DDoS Pro, an immediate switchover back to Anti-DDoS Origin will not occur even if the attack stops. You can configure the intervals at which Sec-Traffic Manager performs switchovers. The default interval is 120 minutes (two hours). This configuration allows you to avoid frequent switchovers due to continuous attacks and ensures business continuity.

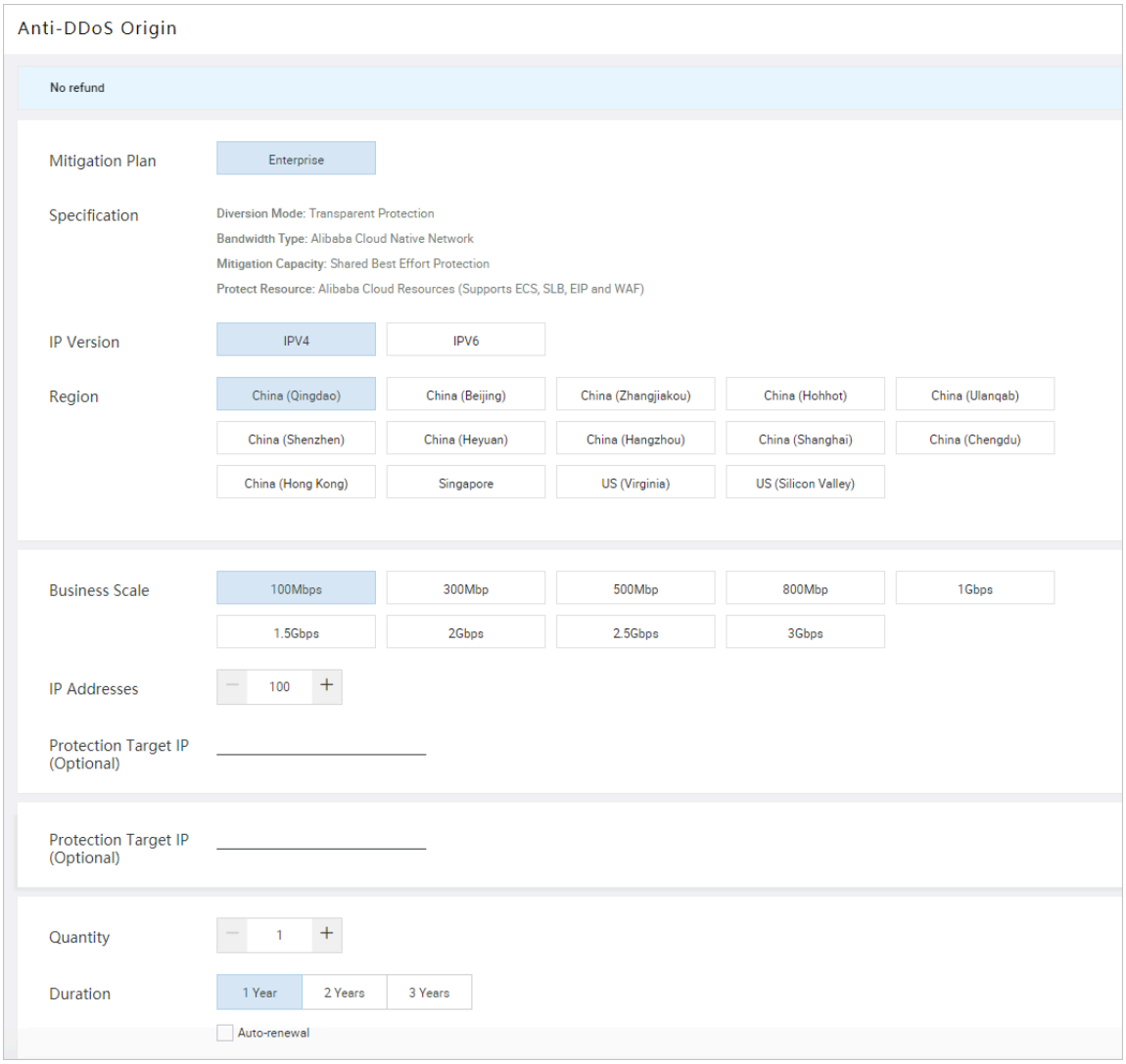
Activate and configure Anti-DDoS Origin

Create an Anti-DDoS Origin Enterprise instance and add resources to the instance as protection targets. Make sure that these resources and the instance are located in the same region. These resources include ECS instances, SLB instances, Elastic IP addresses, and WAF assets.

Notice:

- If the public IP addresses of resources are used to serve clients, make sure that the network specifications and specified scrubbing threshold that is related to each service meet your business requirements. You can view the scrubbing threshold for each service in the Anti-DDoS Basic console.
- Before sales promotions, you must estimate the peak bandwidth and inform Alibaba Cloud technical support. This allows you to avoid traffic scrubbing or throttling by mistake and reduces the impact on your business.

1. Create an Anti-DDoS Origin Enterprise instance. If an instance is available, skip this step.
   a) Log on to the Alibaba Cloud Anti-DDoS console.
   b) On the **Manage Instances** page, click **Purchase Anti-DDoS Origin**.
   c) On the **Anti-DDoS Origin** buy page, specify the required parameters and click **Buy Now**. The parameters are described as follows:
      - **Mitigation Plan**: specifies a protection plan. Select **Enterprise Edition**.
      - **Region**: specifies a region where the resources that you want to protect reside.
      - **Business Scale**: specifies the bandwidth of the business that you want to protect.

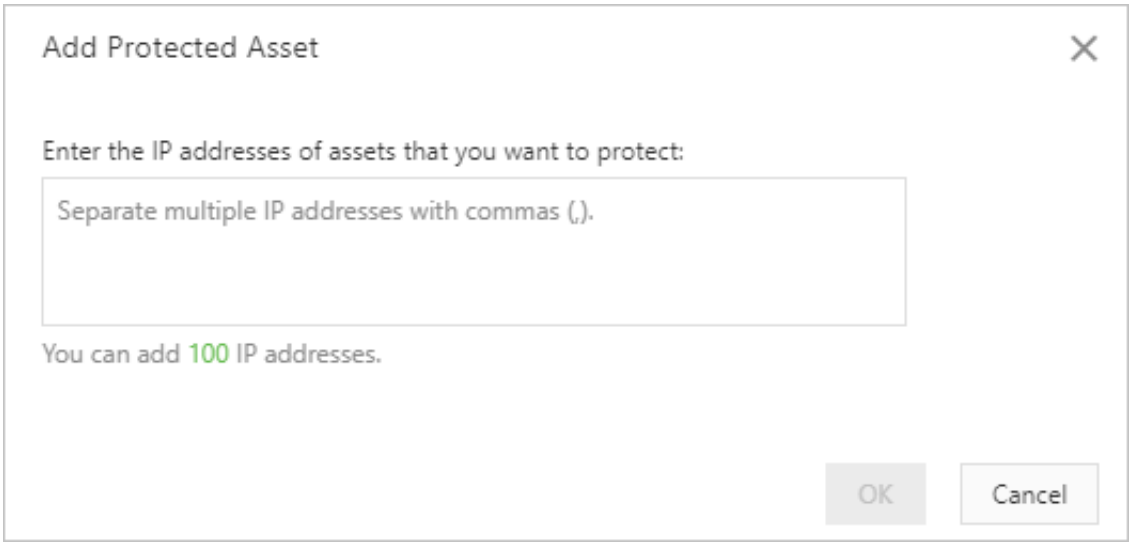


Note:

For more information, see Purchase an Anti-DDoS Origin Enterprise instance.

   d) Confirm the parameters and complete the payment.

2. Add a protection target to the Anti-DDoS Origin Enterprise instance.
   a) Log on to the Alibaba Cloud Anti-DDoS console.
   b) On the **Manage Instances** page, find the target instance and click **Add Protected Asset** in the Actions column.
   c) In the **Add Protected Asset** dialog box, enter one or more IP addresses that you want to protect and click **OK**.

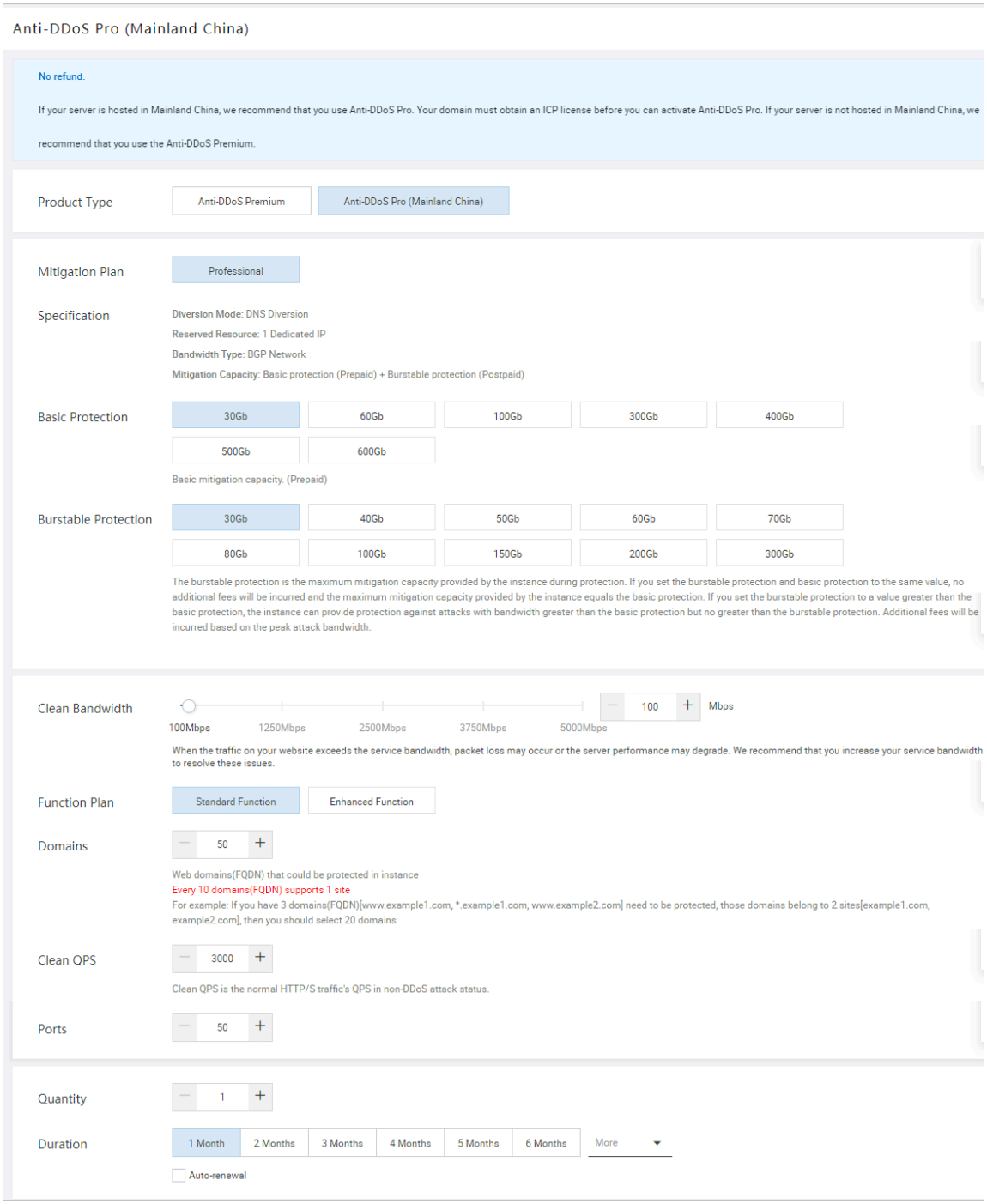


Note:
For more information, see Add a protection target.

Configure Anti-DDoS Pro and Sec-Traffic Manager

Create an Anti-DDoS Pro instance of the Professional plan, add a forwarding rule, and create a scheduling rule for Sec-Traffic Manager. After the configuration is complete, inbound traffic is mapped to the CNAME record assigned by Sec-Traffic Manager.

1. Create an Anti-DDoS Pro instance of the Professional plan. If an instance is available, skip this step.
   a) Log on to the Alibaba Cloud Anti-DDoS Pro console.
   b) In the left-side navigation pane, click **Assets** and then **Instances**. On the page that appears, click **Purchase Instances** in the upper-right corner.
   c) On the **Anti-DDoS Pro (Mainland China)** buy page, specify the required parameters and click **Buy Now**. The parameters are described as follows:
      - **Mitigation Plan**: specifies a protection plan. The value can only be **Professional**.
      - **Basic Protection**: specifies basic protection. Select 30Gb.
      - **Burstable Protection**: specifies burstable protection. Select 300Gb.
      - **Clean Bandwidth**: specifies a clean bandwidth that you require.



Note:

For more information, see #unique_32.

d) Confirm the parameters and complete the payment.

2. Add a domain to the Anti-DDoS Pro instance of the Professional plan.

   a) Log on to the Alibaba Cloud Anti-DDoS Pro console.

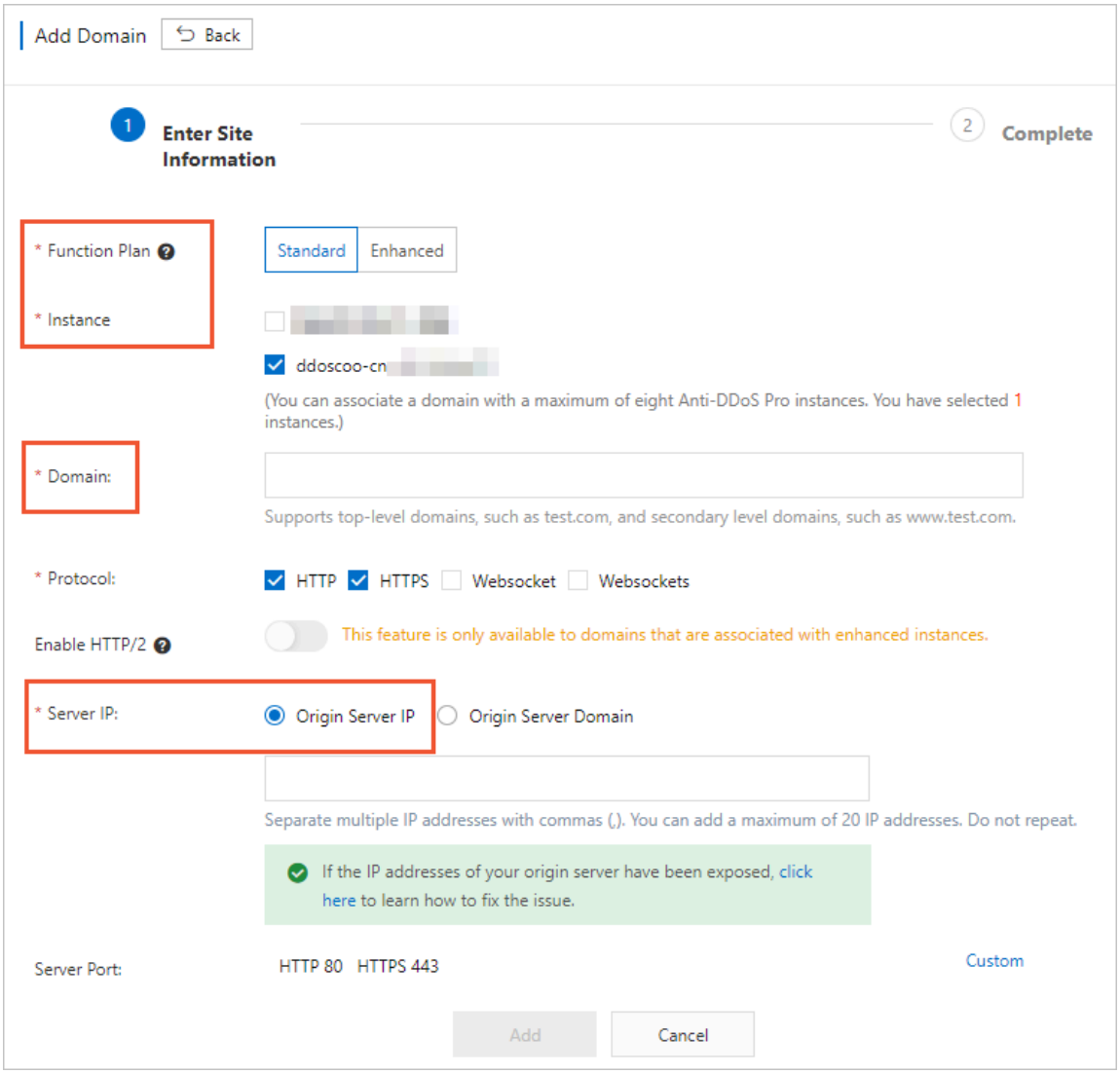
   b) In the left-side navigation pane, click **Provisioning** and then **Website Config**. The **Add Domain** page appears.

   c) In the **Enter Site Information** step, specify the required parameters and click **Add**. The parameters are described as follows:

   - **Function Plan** and **Instance**: specifies a function plan and an instance that you want to use.
   - **Domain**: specifies the domain name of the website that you want to protect.
   - **Server IP**: specifies a method for accessing an origin server. Select **Origin Server IP**.

    **Note:**

For more information, see Add a domain.



After you add the forwarding rule for a website, you do not need to follow the instructions to modify DNS records.

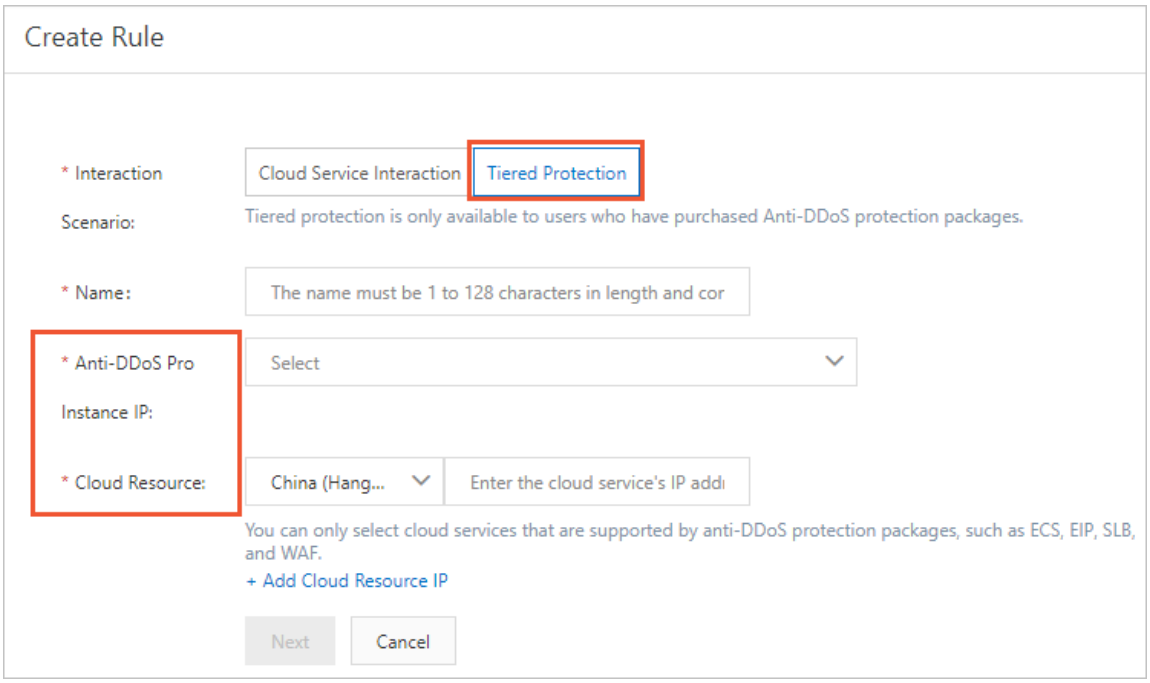
3. Create a scheduling rule for Sec-Traffic Manager.

   a) Log on to the Alibaba Cloud Anti-DDoS Pro console.

   b) In the left-side navigation pane, click **Provisioning** and then **Sec-Traffic Manager**. On the page that appears, click the Cloud Service Interaction tab. On the **General** tab, click **Create Rule**.

   c) In the **Create Rule** pane, specify the required parameters of a tiered protection rule and click **Next**. The parameters of the tiered protection rule are described as follows:

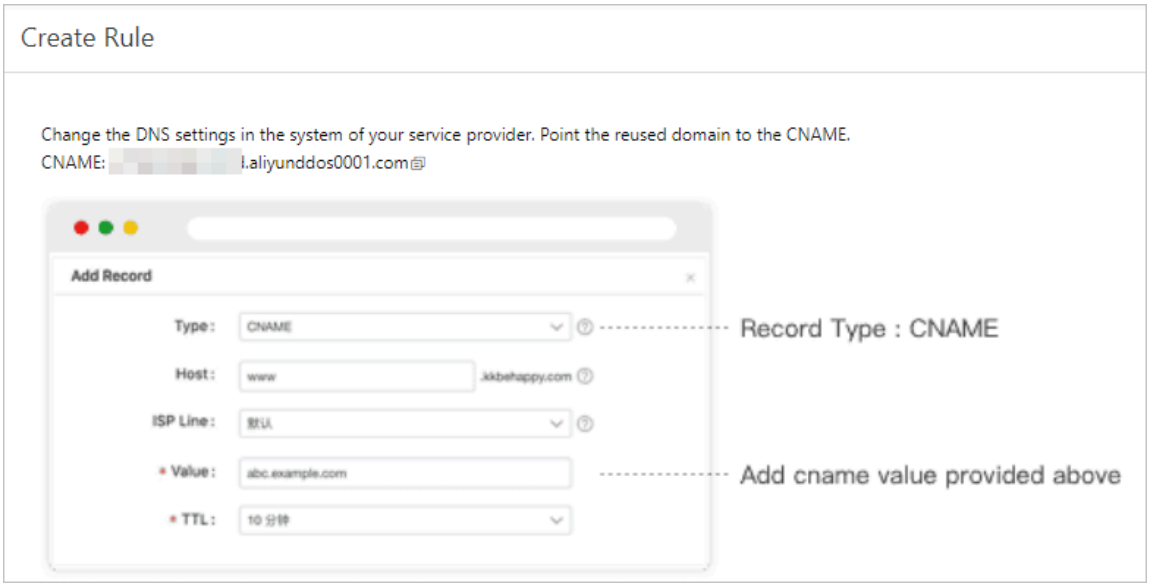
   - **Interaction Scenario**: specifies a scenario. Select **Tiered Protection**.
   - **Anti-DDoS Instance IP**: specifies an Anti-DDoS Pro instance. Select the instance that you configure in the domain.
   - **Cloud Resource**: specifies an origin server.



Note:

For more information, see #unique_34.

After you create the rule, you can obtain a CNAME address assigned by Sec-Traffic Manager.



4. Update the DNS record of your domain. Specifically, visit the website of your DNS provider to modify DNS resolution and change the mapped CNAME record to the CNAME record assigned by Sec-Traffic Manager.