ALIBABA CLOUD

Alibaba Cloud

Anti-DDoS

Anti-DDoS Pro & Premium User Guide

Document Version: 20220629

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

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

Table of Contents

1.Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance

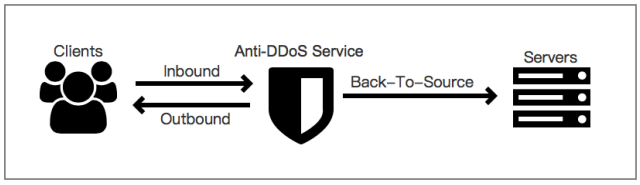
- Notice
  -
  - What are Anti-DDoS Pro and Anti-DDoS Premium?
-
-
  - Note Configure Anti-DDoS Premium Sec-MCA
  - Note Overview
-
-

Note

Billing methods of Anti-DDoS Pro

Notice

1.
2.

	○ ■ ■ ■ ■ ■ ■ ■ ○ ■ ■ ■ ■ ○ ○ Modify the burstable protection bandwidth of an instance
	Warning 
	Function plan
	Warning
	Create a resource group
	○ ○ Enable auto-renewal

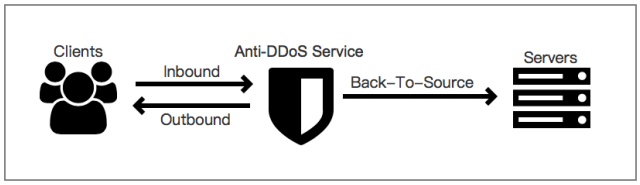
3.

4.

Billing methods of the Insurance and Unlimited mitigation plans

Notice

1.
2.

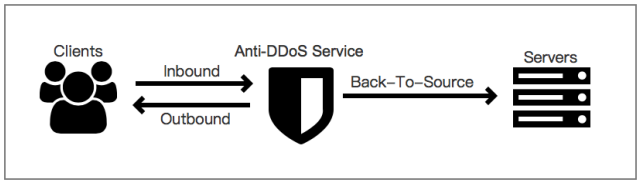
	Billing methods of the Insurance and Unlimited mitigation plans Note ○ ○
	Warning 
	Function plan
	○ ○ Warning
	○ ○ Enable auto-renewal

3.
4.

Billing methods of the MCA mitigation plan

Notice

1.
2.

	Notice
	○ ○ Warning 

3.
4.

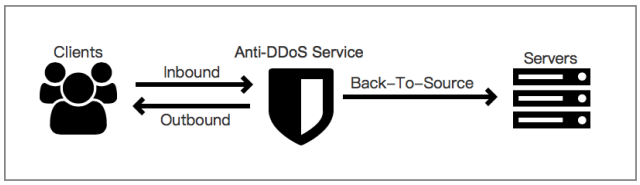
Sec-MCA billing methods

Notice

-
-

1.
2.

	Notice

	Warning 
	Function plan
	Warning
	○ ○ Enable auto-renewal

3.
4.

Related information

- Create an Anti-DDoS Pro or Anti-DDoS Premium instance by calling an API operation

2.Quick Start

2.1. Set up Anti-DDoS Pro using domains

2.1.1. Overview

This topic describes how to configure and use Anti-DDoS Pro or Anti-DDoS Premium to protect website services.

The following table describes the required steps.

Operation	Description
Step 1: Add forwarding rules	In the Anti-DDoS Pro or Anti-DDoS Premium console, add a website service that you want to protect by using a domain name, associate the service with an Anti-DDoS Pro or Anti-DDoS Premium instance, and configure the traffic forwarding rules.
Step 2: Configure service traffic forwarding	Modify the DNS records of your domain name to reroute the traffic directed to your website to an Anti-DDoS Pro or Anti-DDoS Premium instance. The instance scrubs the traffic and then forwards the traffic to the origin server, which protects your website service against DDoS attacks.
Step 3: Configure protection policies	After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your website service, Intelligent Protection is enabled automatically. You can manually adjust anti-DDoS protection policies for your website service, which include Intelligent Protection, Black Lists and White Lists (Domain Names), Blocked Regions (Domain Names), Accurate Access Control, and Frequency Control.
Step 4: View the protection data of your website services	After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your website service, you can use the Security Reports feature and log-related features to view the protection data in the Anti-DDoS Pro or Anti-DDoS Premium console. **Note** Only Anti-DDoS Pro supports the Security Reports and Operation Logs features.

2.1.2. Step 1: Add forwarding rules

To use Anti-DDoS Pro or Anti-DDoS Premium to protect your website service, you must first add the domain name you want to protect and then add a traffic forwarding rule in the Anti-DDoS Pro or Anti-DDoS Premium console.

Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is available. For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

Context

> Note

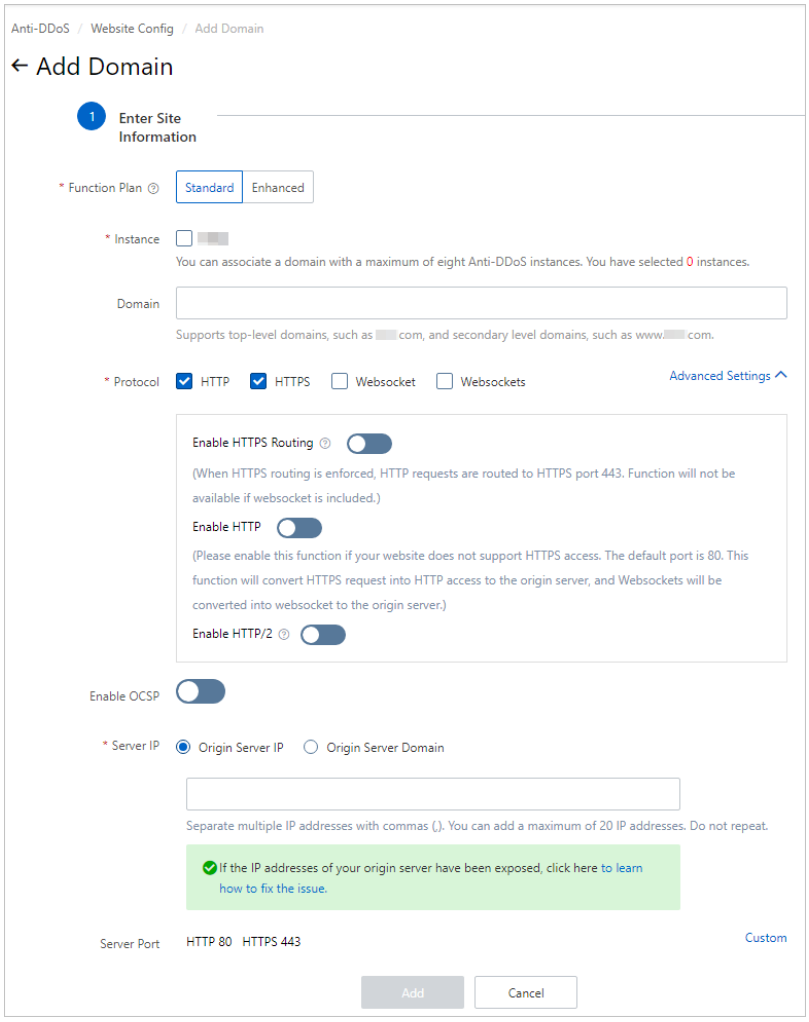
This topic uses Anti-DDoS Pro as an example to describe this specific operation. If you use Anti-DDoS Premium, see Add a website.

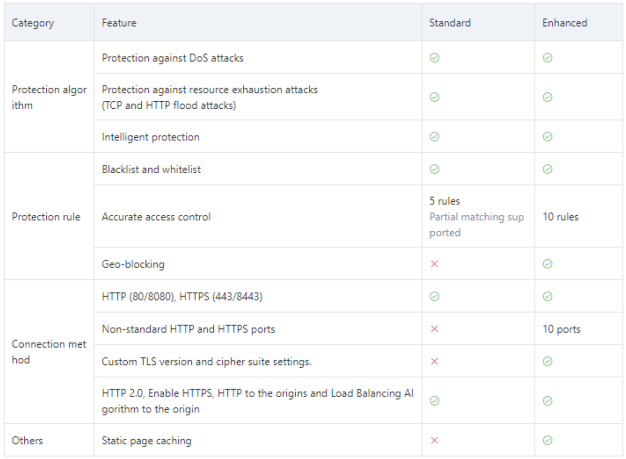
Procedure

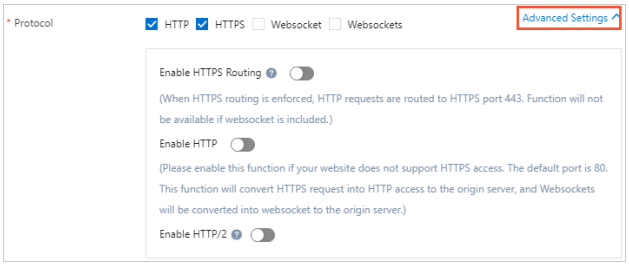
1.
2. In the top navigation bar, select **Mainland China**.
3.
4. On the **Website Config** page, click **Add Domain**.

   > Note You can also import website configurations in batches. For more information, see Import the configurations of more than one website at a time.

5. Complete the **Add Domain** wizard.
   i. In the **Enter Site Information** step, configure the parameters and click Add.



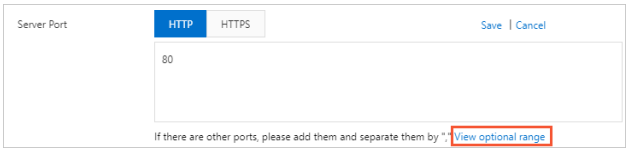
Parameter	Applicable instance	Description
Function Plan	Anti-DDoS Pro and Anti-DDoS Premium instances	The function plan of the Anti-DDoS Pro or Anti-DDoS Premium instance that you want to use. Valid values: **Standard Function** and **Enhanced Function**. You can move the pointer over the ⓘ icon next to **Function Plan** to view the differences between the Standard and Enhanced function plans. The following figure shows the differences. 
Instance	Anti-DDoS Pro and Anti-DDoS Premium instances	The Anti-DDoS Pro or Anti-DDoS Premium instance that you want to use. You can associate a maximum of eight instances with a domain name. The instances associated with the domain name must use the same **function plan**. Available instances are displayed after you configure **Function Plan**. If no instances are displayed, no instances use the function plan that you select. In this case, you can purchase an instance or upgrade the Standard function plan to the Enhanced function plan. For more information, see Upgrade an instance.

Parameter	Applicable instance	Description
Domain	Anti-DDoS Pro and Anti-DDoS Premium instances	The domain name of the website that you want to protect. The domain name must meet the following requirements: ■ The domain name can contain letters, digits, and hyphens (-). The domain name must start with a letter or a digit. ■ The domain name can be a wildcard domain name, such as `*.aliyundoc.com`. If you enter a wildcard domain name, Anti-DDoS Pro or Anti-DDoS Premium automatically matches all subdomains of the wildcard domain name. ■ If you configure a wildcard domain name and an exact-match domain name, the forwarding rules and mitigation policies of the exact-match domain name take precedence. For example, if you configure `*.aliyundoc.com` and `www.aliyundoc.com`, the forwarding rules and mitigation policies of `www.aliyundoc.com` take precedence.
		The type of the protocol that the website uses. Valid values: ■ **HTTP** ■ **HTTPS**: If the website uses HTTPS, select **HTTPS** and upload an SSL certificate file after you save the website configurations. For more information, see Upload an HTTPS certificate. ■ **Websocket**: If you select Websocket, **HTTP** is automatically selected. You cannot select only **Websocket** for the Protocol parameter. ■ **Websockets**: If you select Websockets, **HTTPS** is automatically selected. You cannot select only **Websockets** for the Protocol parameter. If you select **HTTPS**, you can click Advanced Settings to configure the following options. 

Parameter	Applicable instance	Description
Protocol	Anti-DDoS Pro and Anti-DDoS Premium instances	■ **Enable HTTPS Routing**: If the website supports both HTTP and HTTPS, this feature is available. If you enable this feature, all HTTP requests to access the website are redirected to HTTPS requests on the standard port 443. **Notice** ■ This feature is available only when both **HTTP** and **HTTPS** are selected and **Websocket** is cleared. ■ If you access the website over HTTP on a non-standard port and enable this feature, all HTTP requests are redirected to HTTPS requests on the standard port 443. ■ **Enable HTTP**: If the website does not support HTTPS, this feature is available. If this feature is enabled, all HTTPS requests are redirected to HTTP requests and forwarded to origin servers, and all WebSockets requests are redirected to WebSocket requests and forwarded to origin servers. By default, the requests are redirected over the standard port 80. **Notice** ■ If the website does not support HTTPS, turn on Enable HTTP. ■ If you access the website over HTTPS on a non-standard port and enable this feature, all HTTPS requests are redirected to HTTP requests on the standard port 80. ■ **Enable HTTP2**: After you turn on Enable HTTP/2, HTTP/2 is used.

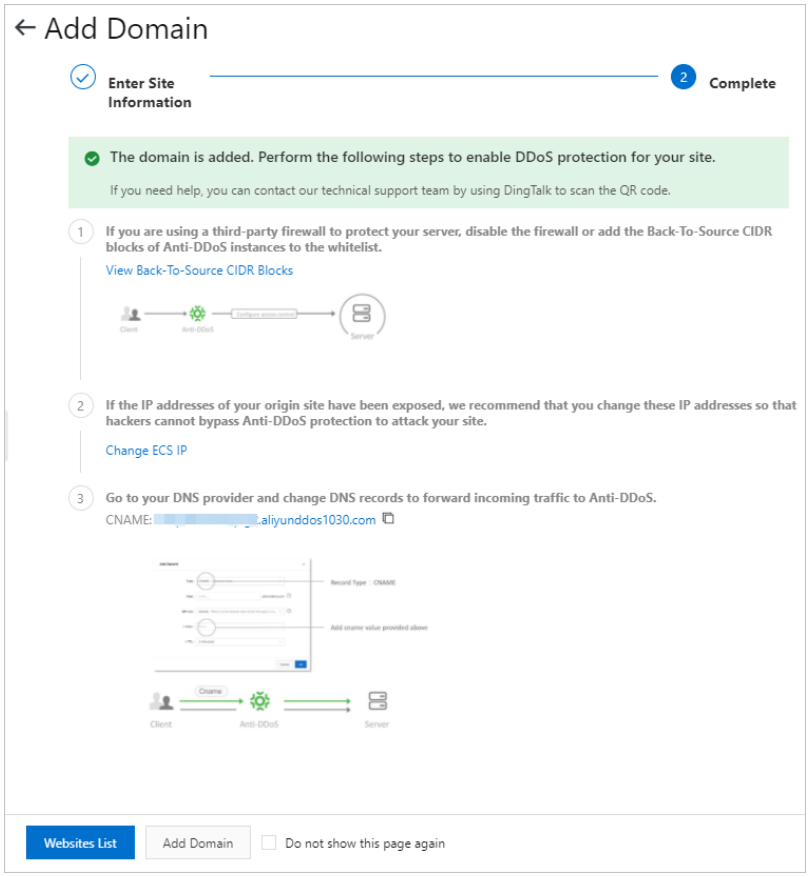
Parameter	Applicable instance	Description
Enable OCSP	Anti-DDoS Pro and Anti-DDoS Premium instances	Specifies whether to enable the Online Certificate Status Protocol (OCSP) feature. **Notice** This feature is available only for a website that supports HTTPS. If **HTTPS** is selected for **Protocol**, we recommend that you enable this feature. OCSP is an Internet protocol that is used by a Certificate Authority (CA) to check the revocation status of a certificate. When a client initiates a Transport Layer Security (TLS) handshake with a server, the client must obtain the certificate and an OCSP response. The OCSP feature is disabled by default. In this case, OCSP queries are sent from a browser that the client uses to a CA. Before the client obtains an OCSP response, subsequent events are blocked. If transient connections or network disconnections occur, a blank page is displayed for a long period of time, and the performance of the website that supports HTTPS is compromised. If the OCSP feature is enabled, Anti-DDoS Pro or Anti-DDoS Premium executes OCSP queries and caches the query results for 300 seconds. When a client initiates a TLS handshake with the server, Anti-DDoS Pro or Anti-DDoS Premium returns the OCSP details and the certificate chain to the client. This prevents blocking issues caused by OCSP queries from the client. OCSP does not cause security risks because OCSP responses cannot be forged.

Parameter	Applicable instance	Description
Server IP	Anti-DDoS Pro and Anti-DDoS Premium instances	The address type of the origin server. You must enter the address of the origin server. Valid values: ■ **Origin Server IP**: the IP address of the origin server. You can enter a maximum of 20 IP addresses. If you enter more than one IP address, separate them with commas (,). ■ If the origin server is hosted on an Elastic Compute Service (ECS) instance, enter the public IP address of the ECS instance. If the ECS instance is associated with a Server Load Balancer (SLB) instance, enter the public IP address of the SLB instance. ■ If the origin server is deployed in data centers or on other clouds, you can run the `ping` *Domain name* command to query the public IP address to which the domain name is resolved and enter the public IP address. ■ **Origin Server Domain**: the domain name of the origin server. Select this option when you deploy a proxy service, such as Web Application Firewall (WAF), between the origin server and Anti-DDoS Pro or Anti-DDoS Premium. You must also enter the address of the proxy, such as a CNAME. You can enter a maximum of 10 domain names. If you enter more than one domain name, separate them with line breaks. If you want to use Anti-DDoS Pro or Anti-DDoS Premium together with WAF, select **Origin Server Domain** and enter the CNAME that WAF assigns. This provides enhanced protection for the website. For more information, see Add a website to both Anti-DDoS Pro or Anti-DDoS Premium and WAF. **Notice** If you enter the default public endpoint of an Object Storage Service (OSS) bucket for **Origin Server Domain**, a custom domain name must be mapped to the bucket. For more information, see Regions and endpoints and Map custom domain names. If you enter more than one IP address or domain name, Anti-DDoS Pro or Anti-DDoS Premium uses IP hash to forward website traffic to the origin servers. After you save the website configurations, you can change the load balancing algorithm. For more information, see Modify the back-to-origin settings for a website.
		The server port that you specify based on the value of **Protocol**.

Parameter	Applicable instance	Description
Server Port	Anti-DDoS Pro and Anti-DDoS Premium instances	If you select **HTTP**, the default port 80 is used. If you select **HTTPS**, the default port 443 is used. **Notice** ■ The port for **Websocket** is the same as the port for **HTTP**. ■ The port for **Websockets** and HTTP/2 is the same as the port for **HTTPS**. You can click **Custom** to the right of the Server Port parameter to specify one or more custom ports. You can specify multiple custom **HTTP** or **HTTPS** ports. If you specify multiple custom ports, separate the ports with commas (,).  Take note of the following limits when you specify custom ports: ■ The custom ports that you want to specify must be supported by Anti-DDoS Pro or Anti-DDoS Premium. You can click **View optional range** to view the HTTP and HTTPS ports that are supported. The ports that are supported vary based on the **function plan** of your Anti-DDoS Pro or Anti-DDoS Premium instance. ■ Anti-DDoS Pro or Anti-DDoS Premium instance of the **Standard function plan**: ■ HTTP ports: ports 80 and 8080 ■ HTTPS ports: ports 443 and 8443 ■ Anti-DDoS Pro or Anti-DDoS Premium instance of the **Enhanced function plan**: ■ HTTP ports: ports that range from 80 to 65535 ■ HTTPS ports: ports that range from 80 to 65535 ■ You can specify up to 10 custom ports for all websites that are added to your Anti-DDoS Pro or Anti-DDoS Premium instance. The custom ports include HTTP ports and HTTPS ports. For example, you want to add Website A and Website B to your Anti-DDoS Pro or Anti-DDoS Premium instance, Website A provides services over HTTP ports, and Website B provides services over HTTPS ports. If you specify HTTP ports 80 and 8080 for Website A, you can specify up to eight HTTPS ports for Website B.

Parameter	Applicable instance	Description
Cname Reuse	Anti-DDoS Premium	Specifies whether to enable CNAME reuse. If more than one website is hosted on the same server, this feature is available. After CNAME reuse is enabled, you need only to map the domain names hosted on the same server to the CNAME that is assigned by Anti-DDoS Premium. For more information, see Use the CNAME reuse feature.

ii. In the **Complete** step, perform the subsequent operations as instructed.



a. Allow back-to-origin IP addresses to access the origin server:

If security software, such as a firewall, is installed on the origin server, you must add the back-to-origin IP addresses of the Anti-DDoS Pro or Anti-DDoS Premium instance to the whitelist of the origin server. This ensures that the traffic from Anti-DDoS Pro or Anti-DDoS Premium is not blocked by the security software on your origin server.

If no security software is installed, skip this step.

b. Change the public IP address of an ECS origin server:

If your origin server is an ECS instance and the origin IP address is exposed, you must change the public IP address of the ECS instance. This prevents attackers from bypassing Anti-DDoS Pro or Anti-DDoS Premium to attack your origin server.

If your origin server is not an ECS instance and the origin IP address is not exposed, skip this step.

c. Upload an HTTPS certificate:

If a website that provides HTTPS services is added to Anti-DDoS Pro or Anti-DDoS Premium, you must upload the SSL certificate file that is associated with the domain name of the website. This way, HTTPS requests can be redirected to Anti-DDoS Pro or Anti-DDoS Premium for protection.

> **Note** If a website is associated with an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the Enhanced function plan, you can create a custom TLS policy for the website after you upload an SSL certificate file. For more information, see Customize a TLS policy.

If the website provides only HTTP services, skip this step.

d. (Optional)Verify the forwarding configurations on your local computer:

Verify that the website configurations that you added to Anti-DDoS Pro or Anti-DDoS Premium take effect on your computer. If you change the DNS record before the configurations for the website take effect, services may be interrupted.

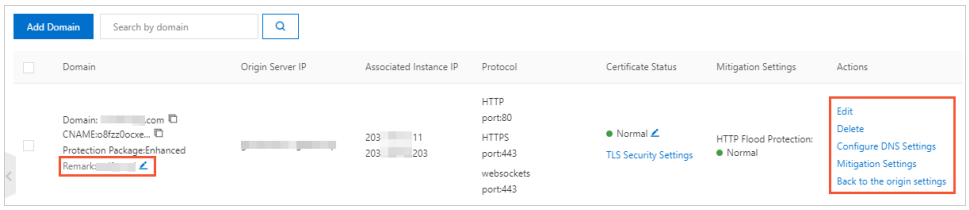
e. Change the DNS record:

Anti-DDoS Pro or Anti-DDoS Premium assigns a CNAME to the website that you added. You must change the DNS record to map the domain name to the CNAME. This way, service traffic can be switched to Anti-DDoS Pro or Anti-DDoS Premium for protection. You can manually change the DNS record or use the NS Access Mode feature to enable the system to automatically change the DNS record.

For more information, see Change DNS records to protect website services and Enable NS Mode Access to protect a website.

iii. Click **Websites List** to view the domain name that you added and the CNAME that is assigned by Anti-DDoS Pro or Anti-DDoS Premium in the website list.

After you complete the **Add Domain** wizard, you can perform the following operations on the newly added domain name:



- Add remarks: You can click the

  icon next to **Remark** to add remarks that help you identify the website configurations.
- Modify or delete the domain name: You can click **Edit** or **Delete** to manage the website configurations that you added.

> **Notice** After you click Edit in the Actions column, you can turn on Getting source port from the real customer on the page that appears. After you turn on Getting source port from the real customer, you can obtain the actual ports of clients or mark the back-to-origin requests that Anti-DDoS Pro or Anti-DDoS Premium forwards to the origin server by using custom HTTP headers. For more information, see Mark back-to-origin requests.

- **Configure DNS settings**: If you purchase a paid edition of Alibaba Cloud DNS, you can enable NS Access Mode. This way, the system automatically changes the DNS record of the domain name and redirects traffic to Anti-DDoS Pro or Anti-DDoS Premium.

  For more information, see Enable NS Mode Access to protect a website.

- Configure mitigation settings: You can click **Mitigation Settings** in the Actions column to go to the **Protection for Website Services** tab and modify the mitigation settings.

  After you add the website, **Intelligent Protection** and **Frequency Control** are enabled by default. You can enable more features and modify protection rules for the website on the **Protection for Website Services** tab.

  For more information, see Use the intelligent protection feature.

- Configure back-to-origin settings: If the website that you add to Anti-DDoS Pro or Anti-DDoS Premium resides on more than one origin server, you can click **Back to the origin settings** to change the **load balancing algorithm** for back-to-origin traffic.

  For more information, see Modify the back-to-origin settings for a website.

Result

Anti-DDoS Pro assigns a CNAME record to the domain name. You only need to map the DNS record of the domain name to the CNAME record of the Anti-DDoS Pro instance to reroute inbound traffic to the instance for traffic scrubbing.

What's next

- Configure service traffic forwarding. For more information, see Step 2: Configure service traffic forwarding.
- (Optional)Upload an HTTPS certificate. If your website supports the HTTPS protocol, you must upload your SSL certificate to enable the Anti-DDoS Pro instance to filter HTTPS requests.

2.1.3. Step 2: Configure service traffic forwarding

After you add a website to an Anti-DDoS Pro or Anti-DDoS Premium instance, you must modify the DNS records of the domain name for the website to reroute the traffic directed to your website to the instance. The instance scrubs the traffic and forwards normal traffic to the origin server. This topic describes how to modify the CNAME record of a domain name. In this example, the DNS resolution service is provided by Alibaba Cloud DNS.

Prerequisites

- A domain name is added to an Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see Step 1: Add forwarding rules.
- The back-to-origin IP addresses of the Anti-DDoS Pro or Anti-DDoS Premium instance are added to the whitelist of the origin server. If you deploy third-party security software, such as a firewall, on your origin server, add the back-to-origin IP addresses to the whitelist of the security software. For

more information, see Allow back-to-origin IP addresses to access the origin server.

- The traffic forwarding settings are in effect. Before you switch service traffic to the Anti-DDoS Pro or Anti-DDoS Premium instance, we recommend that you use your local computer to verify that the instance can forward traffic to the origin server. For more information, see Verify the forwarding configurations on your local computer.

> **Warning** If you switch your service traffic to the Anti-DDoS Pro or Anti-DDoS Premium instance before the forwarding settings take effect, your service may be interrupted.

Context

In the following example, your domain name is hosted on Alibaba Cloud DNS.

> **Note** Alibaba Cloud DNS provides basic DNS services free of charge. It also offers other value-added services in the paid editions. If you activated a paid edition of Alibaba Cloud DNS for your website, we recommend that you enable NS Mode Access to redirect traffic to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Enable NS Mode Access to protect a website.

If you use a third-party DNS service, log on to the system of the DNS provider to change the DNS records. The following example is only for reference.

Assume that you add the domain name `example.aliyundoc.com` to Anti-DDoS Pro or Anti-DDoS Premium. The following procedure describes how to change and add DNS records in the Alibaba Cloud DNS console.

Procedure

1. Log on to the Alibaba Cloud DNS console.
2. On the **Manage DNS** page, find the domain name `aliyundoc.com` and click **Configure** in the Actions column.
3. On the **DNS Settings** page, find the A or CNAME record whose Host is **bgp** and click **Edit** in the Actions column.

   > **Note** If you cannot find the DNS record that you want to manage in the list, you can click **Add Record** to add the record.

4. In the **Edit Record** or **Add Record** dialog box, set **Type** to **CNAME** and change **Value** to the CNAME assigned by Anti-DDoS Pro or Anti-DDoS Premium.
5. Click **Confirm** and wait for the settings to take effect.

What's next

Step 3: Configure protection policies

2.1.4. Step 3: Configure protection policies

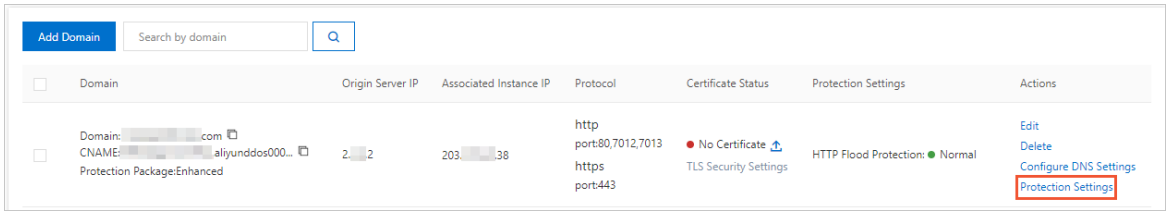
After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your website service, Intelligent Protection is enabled automatically. You can manually adjust anti-DDoS protection policies for your website service, which include Intelligent Protection, Black Lists and White Lists (Domain Names), Blocked Regions (Domain Names), Accurate Access Control, and Frequency Control.

Prerequisites

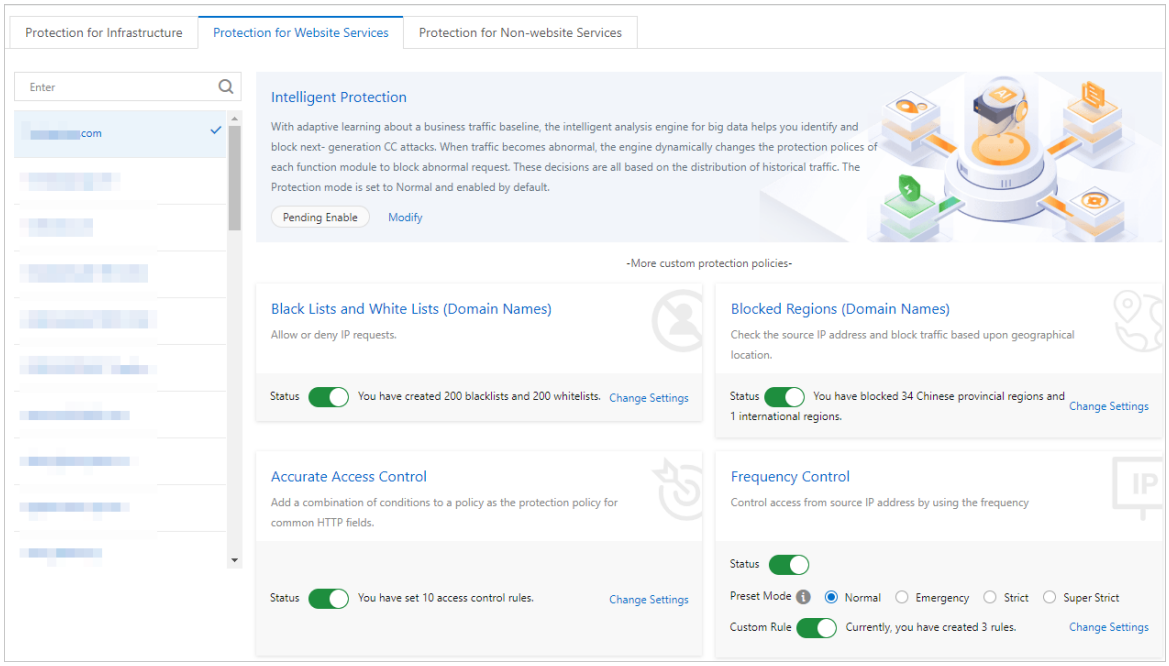
An Anti-DDoS Pro or Anti-DDoS Premium instance is set up by using a domain name. For more information, see Step 1: Add forwarding rules.

Procedure

1.
2.
3.
4. On the **Website Config** page, find the target domain name and click **Mitigation Settings** in the Actions column.



5. On the **Protection for Website Services** tab, configure protection policies for the domain name. Supported protection policies include Intelligent Protection, Black Lists and White Lists (Domain Names), Blocked Regions (Domain Names), Accurate Access Control, and Frequency Control.



   - **Intelligent Protection**: It is enabled by default. Intelligent Protection enables the intelligent and big data-based analysis engine to learn the traffic patterns of workloads, detect and block new types of HTTP flood attacks, and dynamically adjust policies to block malicious requests. You can manually change the protection mode and level. For more information, see Use the intelligent protection feature.
   - **Black Lists and White Lists (Domain Names)**: After this policy is enabled, access requests from the IP addresses or CIDR blocks in the blacklist are blocked, while access requests from the IP addresses or CIDR blocks in the whitelist are allowed. For more information, see Configure blacklists and whitelists for domain names.

- **Blocked Regions (Domain Names)**: You can specify both the regions inside and outside China that you want to block. Requests from IP addresses in the blocked regions are blocked. For more information, see Configure a location blacklist for a domain name.
- **Accurate Access Control**: allows you to customize access control rules. You can filter access requests based on a combination of criteria of commonly used HTTP fields, such as IP, URI, Referer, User-Agent, and Params. For requests that meet these criteria, you can allow, block, or verify them. For more information, see Configure accurate access control rules.
- **Frequency Control**: allows you to restrict the frequency of access from a source IP address to your website. Frequency Control takes effect immediately after it is enabled. By default, the normal mode is used to protect website services against common HTTP flood attacks. You can manually change the protection mode and create custom rules to reinforce protection. For more information, see Configure frequency control.

2.1.5. Step 4: View the protection data of your website services

After you configure an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your website services, you can use the security overview feature and log-related features to view the protection data in the Anti-DDoS Pro or Anti-DDoS Premium console.

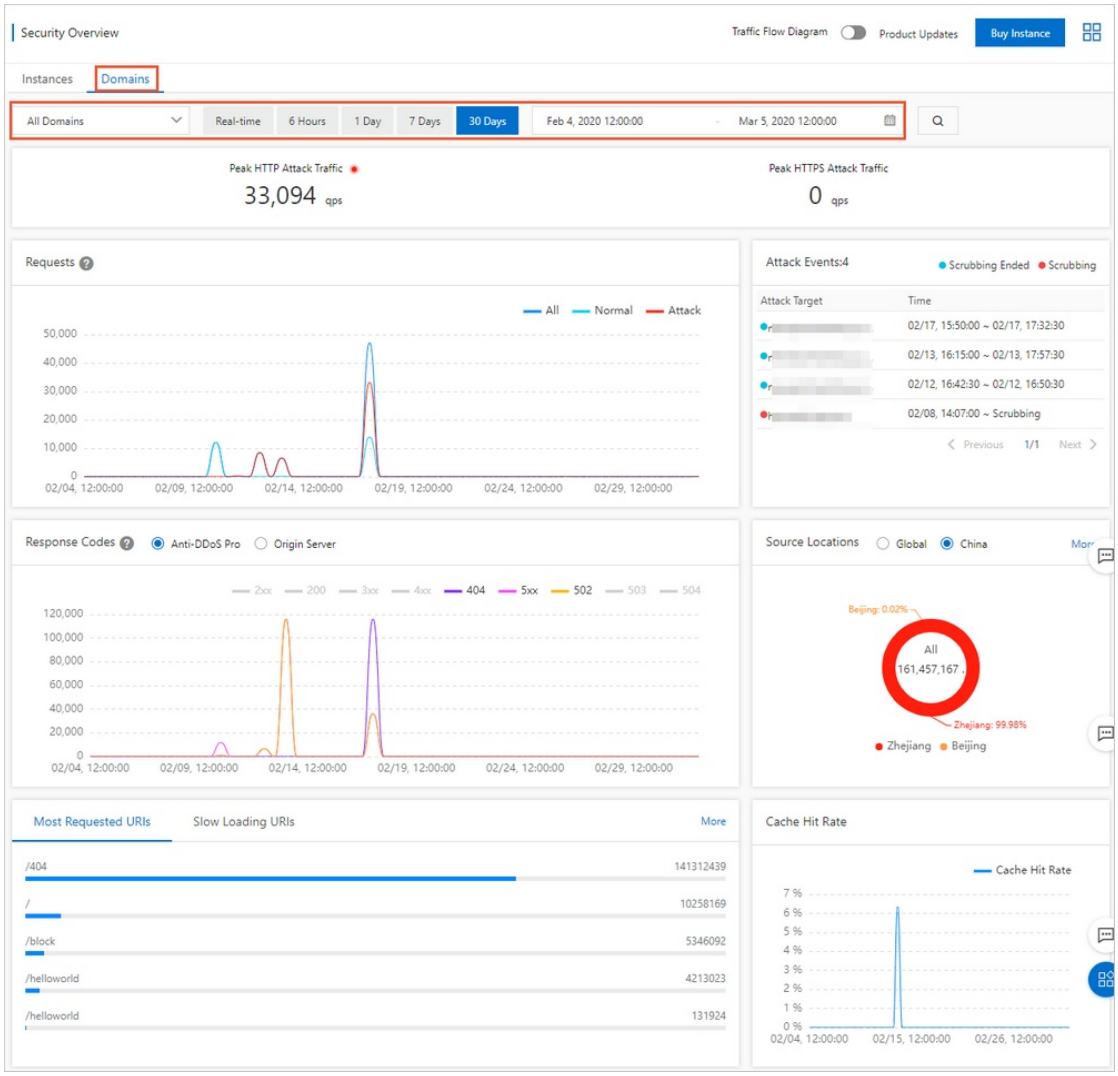
Prerequisites

- A domain name is added to an Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see Step 1: Add forwarding rules.
- The traffic forwarding configuration for your website service is complete. For more information, see Step 2: Configure service traffic forwarding.

Procedure

1.
2.
3. Check the protection data on the Security Overview page.
    i. In the left-side navigation pane, click **Security Overview**.

ii. Click the **Domains** tab, and select the domain name and time range to view the protection data.



For more information, see Check the security overview.

4. Query and analyze log data.
   - Query operations logs.

> **Note** Only Anti-DDoS Pro supports the operations log feature. If you use Anti-DDoS Premium, we recommend that you enable the log analysis feature.

An operations log records the important operations in the last 30 days. For example, this log records the operations performed on IP addresses of protected assets and ECS instances.

a. In the left-side navigation pane, choose **Investigation > Operation Logs**.

b. On the **Operation Logs** page, select the operation object and time range to view the operations log record.

For more information, see View operations logs.

- Query log analysis.

  If you need to analyze log data in real time and display results by using graphs, we recommend that you activate the Log Analysis feature. After the Log Analysis feature is activated, the logs of access to your website and HTTP flood attack logs are collected and maintained by Alibaba Cloud Log Service. You can search and analyze log data in real time, and view search results on dashboards. For more information, see What is Log Service?.

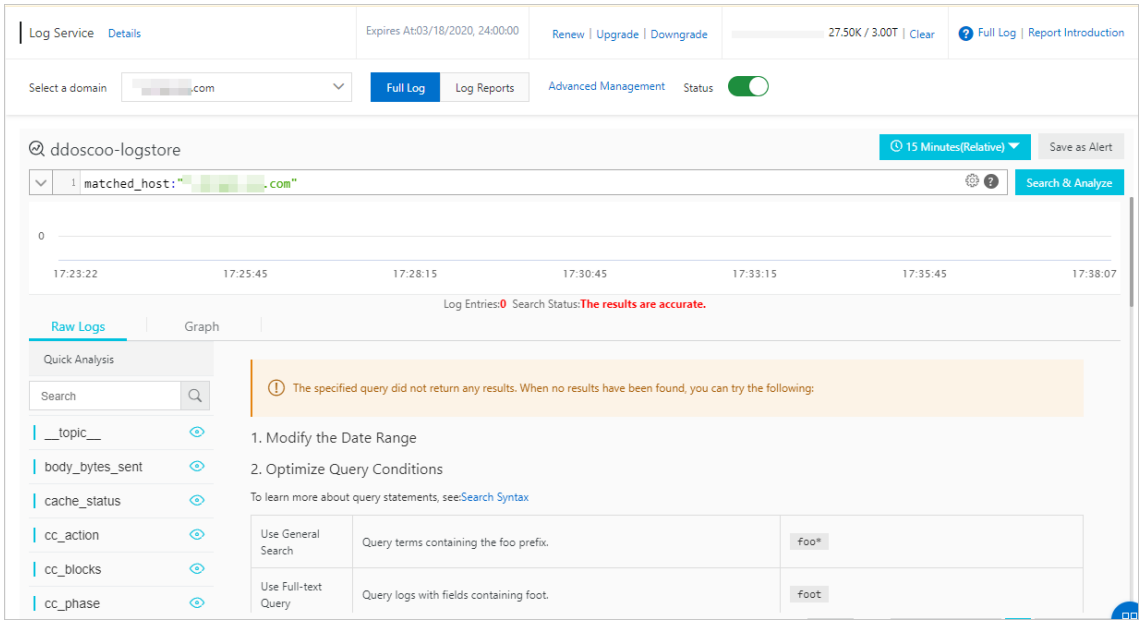
  The Log Analysis feature is a value-added service. To use this service, you must both activate and enable it. To use the log analysis feature, you must perform the following operations:

  a. Activate the feature. For more information, see Activate the Log Analysis feature.

  b. Enable the feature. For more information, see Enable the Log Analysis feature for a website.

  After the Log Analysis feature is activated and enabled, you can navigate to the **Investigation > Log Analysis** page to search and analyze log data in real time. You can also view and edit dashboards, and configure monitoring and alerts on this page.

  > **Note** For more information about the fields supported by the Log Analysis feature, see Fields supported by the Log Analysis feature.



For more information, see Overview.

2.2. Set up Anti-DDoS Pro using IPs and ports

2.2.1. Overview

This topic describes how to configure and use Anti-DDoS Pro or Anti-DDoS Premium to protect non-website services, such as client-based games, mobile games, or apps.

The following table describes the required steps.

Step	Description
Step 1: Create a port forwarding rule	Add a non-website service that you want to protect by using a port in the Anti-DDoS Pro or Anti-DDoS Premium console. Use the IP address of your Anti-DDoS Pro or Anti-DDoS Premium instance as your service IP address to reroute inbound traffic to your instance. After you change the IP address, the instance scrubs the inbound traffic and then forwards the traffic to the origin server.
Step 2: Configure port forwarding and DDoS mitigation policies	Configure port forwarding policies as required, such as session persistence and health checks for multiple origin IP addresses. You can also configure anti-DDoS protection policies for non-website services, such as False Source, Speed Limit for Destination, Packet Length Limit, and Speed Limit for Source.
Step 3: View the protection data of a port	View the traffic that goes through a port on the Security Overview page of the Anti-DDoS Pro or Anti-DDoS Premium console after you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your non-website service.

2.2.2. Step 1: Create a port forwarding rule

To use Anti-DDoS Pro or Anti-DDoS Premium to protect non-website services, such as client-based games, mobile games, or apps, you must create port forwarding rules. You must also use the IP address of your Anti-DDoS Pro or Anti-DDoS Premium instance as the service IP address. This topic describes how to create a port forwarding rule in the Anti-DDoS Pro or Anti-DDoS Premium console.

Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased. For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

Context

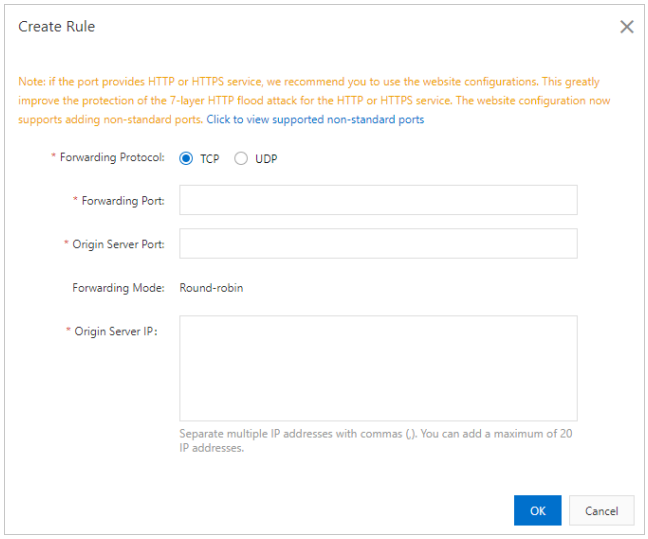
If you configure your Anti-DDoS Pro or Anti-DDoS Premium instance to protect non-website services, your instance supports only Layer 4 forwarding. Both Anti-DDoS Pro and Anti-DDoS Premium provide protection only against Layer 4 attacks, such as SYN and UDP flood attacks. They do not parse Layer 7 packets or mitigate Layer 7 attacks, such as HTTP flood attacks and web attacks. To create an instance to protect non-website services, you need only to create port forwarding rules. Then, you can use the IP address of your instance as the service IP address.

Procedure

1.
2.
3.
4. On the **Port Config** page, select the instance you want to use and click **Create Rule**.

   > **Note** You can also create more than one rule at a time. For more information, see Create multiple forwarding rules at a time.

5. In the **Create Rule** dialog box, configure the following parameters.



Parameter	Description
Forwarding Protocol	The protocol that you want to use to forward traffic. Valid values: **TCP** and **UDP**.
Forwarding Port	The port that you want to use to forward traffic. ◦ We recommend that you specify the same value for both **Forwarding Port** and **Origin Server Port**. ◦ To prevent domain owners from creating their own DNS servers, Anti-DDoS Pro and Anti-DDoS Premium do not protect services that use port 53. ◦ You cannot specify a port that is used as the forwarding port for another rule. In an instance, forwarding rules that use the same protocol must use different forwarding ports. If you attempt to create a rule with a protocol and forwarding port that are used by another rule, an error message appears. The error message indicates that these rules overlap. Do not create a rule that overlaps with forwarding rules that are automatically generated. For more information, see Automatically generate forwarding rules when you add website configurations.
Origin Server Port	The port of the origin server.
Origin Server IP	The IP address of the origin server. **Note** You can specify a maximum of 20 origin IP addresses to implement load balancing. Separate multiple IP addresses with commas (,).

6. Click **OK**.

What's next

After a port forwarding rule is created, you must change the IP address of your service to the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance to redirect service traffic to the instance. After you change the IP address, the instance scrubs inbound traffic and then forwards normal traffic to the origin server.

Notice Before you change the IP address to redirect inbound traffic to your instance, we recommend that you verify that the forwarding rule is in effect. For more information, see Verify the forwarding configurations on your local computer. If you change the IP address of the service before the forwarding rule is applied, your service may be interrupted.

The Anti-DDoS Pro or Anti-DDoS Premium instance uses default policies to scrub and forward traffic. You can customize DDoS mitigation policies and enable the session persistence and health check features based on your business requirements. For more information, see Step 2: Configure port forwarding and DDoS mitigation policies.

2.2.3. Step 2: Configure port forwarding and DDoS mitigation policies

This topic describes how to configure port forwarding policies, such as session persistence and health checks for multiple origin server IP addresses. The topic also describes how to configure DDoS mitigation policies for non-website services. The DDoS mitigation policies include False Source, Speed Limit for Destination, Packet Length Limit, and Speed Limit for Source.

Prerequisites

A port forwarding rule is created. For more information, see Step 1: Create a port forwarding rule.

Context

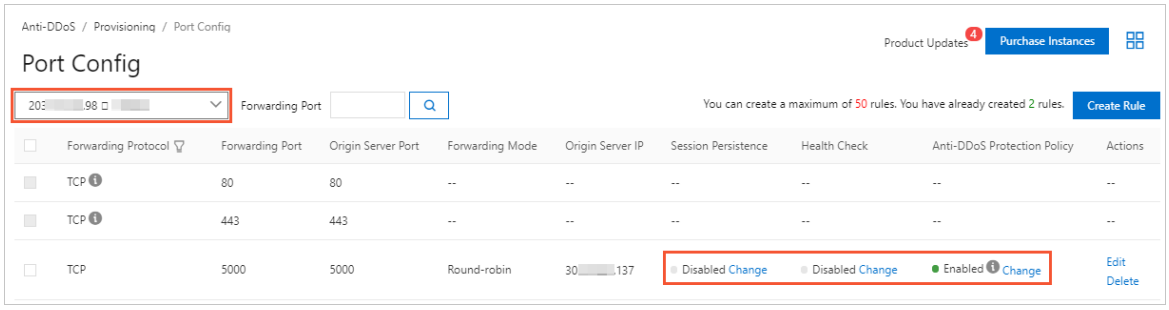
You can configure port forwarding policies and DDoS mitigation policies for non-website services based on your business requirements to improve the forwarding capability of Anti-DDoS Pro or Anti-DDoS Premium.

Anti-DDoS Pro or Anti-DDoS Premium supports the following features:

- You can configure a session persistence policy to forward requests from a specific IP address to the same backend server.
- You can enable the health check feature to check the availability of backend servers. This ensures that requests from clients are forwarded to healthy servers.
- You can configure DDoS mitigation policies to limit the connection speeds and packet lengths of non-website services that are protected by Anti-DDoS Pro or Anti-DDoS Premium. This protects your non-website services against connection-oriented DDoS attacks that consume low bandwidth.

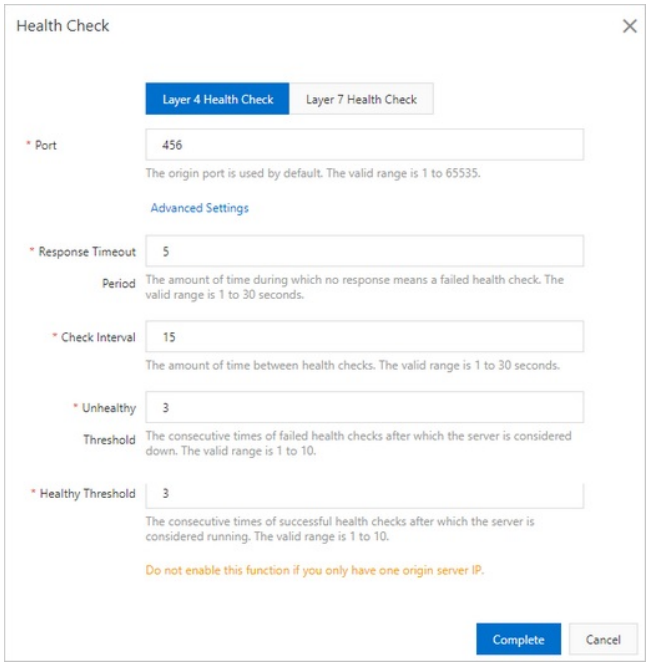
Procedure

1.
2.
3.
4. On the **Port Config** page, select an instance, find the forwarding rule that you want to manage, and then configure the session persistence, health check, and DDoS mitigation policies for non-website services based on your business requirements.



   - **Session Persistence**
     a. Click **Change** in the **Session Persistence** column.
     b. In the **Session Persistence** dialog box, enable or disable session persistence based on your business requirements.
        - To enable session persistence, set the **Timeout Period** parameter and click **Complete**.
        - To disable session persistence, click **Disable Session Persistence**.
   - **Health Check**
     a. Click **Change** in the **Health Check** column.

b. In the **Health Check** dialog box, configure the parameters. For more information about the parameters, see Configure a health check.



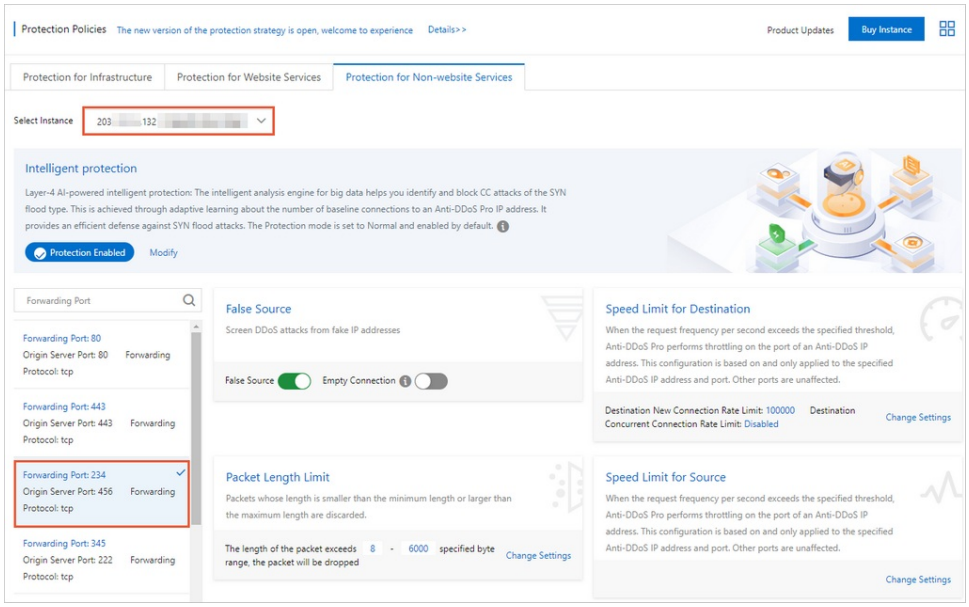
c. Click **Complete**.

To disable a health check, click **Change** in the Health Check column. In the **Health Check** dialog box, click **Disable Health Check**.

- Protection for non-website services

  a. Click **Change** in the **Anti-DDoS Protection Policy** column.

b. On the **Protection for Non-website Services** tab, configure DDoS mitigation policies based on your business requirements. You can configure the following policies:



- **False Source**: verifies and filters DDoS attacks that are initiated from forged IP addresses.
- **Speed Limit for Destination**: The data transfer rate of the port used by the instance that exceeds the maximum visit frequency is limited based on the IP address and port of an Anti-DDoS Pro or Anti-DDoS Premium instance. The data transfer rates of other ports are not limited.
- **Packet Length Limit**: specifies the minimum and maximum lengths of packets that are allowed to pass through. Packets with invalid lengths are discarded.
- **Speed Limit for Source**: The data transfer rate of a source IP address from which access requests exceed the maximum visit frequency is limited based on the IP address and port of an Anti-DDoS Pro or Anti-DDoS Premium instance. The data transfer rates of source IP addresses from which access requests do not exceed the maximum visit frequency are not limited. This policy also supports the blacklist policy. This is when an IP address is added to the blacklist. It applies to IP addresses from which access requests exceed the maximum visit frequency five times within 60 seconds. You can also specify the blocking period.

For more information, see Create an anti-DDoS protection policy.

What's next

Step 3: View the protection data of a port

2.2.4. Step 3: View the protection data of a port

After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your non-website services, you can view the traffic that goes through the port on the Security Overview page of the Anti-DDoS Pro or Anti-DDoS Premium console.

Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is set up by using a port. For more information, see Step 1: Create a port forwarding rule.

Procedure

1.
2.
3.
4. Click the **Instances** tab, select one or more instances, and then specify a time range to view the relevant metrics.

   You can view the following instance information:

   - **Peak Attack Bandwidth** (unit: bit/s) and **Peak Attack Packet Rate** (unit: pps)
   - Traffic trends
     - Anti-DDoS Pro provides the **Bandwidth** trend chart to show traffic information by **bps** or **pps**. You can view the trends of inbound, outbound, and attack traffic of an instance for a specific time range.
     - Anti-DDoS Premium provides the **Overview** tab to show bandwidth trends and the **Inbound Distribution** tab to show the distribution of inbound traffic. Anti-DDoS Premium also provides the **Outbound Distribution** tab to show the distribution of outbound traffic.
   - **Attack Events** of the Blackhole and Mitigation types

     You can move the pointer over an IP address or a port to view the details of an attack, such as Attack Target, Attack Type, Peak Attack Traffic, and Protection Effect.
   - **Connections** on a port
     - **Concurrent Connections**: the total number of concurrent TCP connections established between clients and the instance
     - **New Connections**: the number of new TCP connections established between clients and the instance per second
     - **Active**: the number of TCP connections in the **Established** state
     - **Inactive**: the number of TCP connections in all states except the **Established** state

     > **Note** If you select an instance, the Connections trend chart shows the numbers of connections on different ports. If you select more than one instance, the Connections trend chart shows the total number of connections on all ports.
   - **Source Locations** and **Source Service Providers**
     - **Source Locations**: the distribution of source locations from which normal traffic is sent. Source locations are classified by **Global** and **Mainland China**.
     - **Source Service Providers**: the distribution of Internet service providers (ISPs) from which normal traffic is sent.

3.Check the security overview

After you switch traffic of your service to an Anti-DDoS Pro or Anti-DDoS Premium instance, you can view the metrics and DDoS attack events in real time on the Security Overview page in the Anti-DDoS Pro or Anti-DDoS Premium console.

Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased, and your service is protected by the instance. For more information, see the following topics:

- Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance
- Add a website for website services
- Create forwarding rules for non-website services

Background information

The Security Overview page provides an overview of the following metrics and DDoS attack events:

- Service metrics: clean bandwidth, queries per second (QPS), connections per second (CPS), protected domain names, and protected ports
- Attack events: volumetric DDoS attacks, connection flood attacks, and resource exhaustion attacks

Procedure

1.
2.
3.
4. (Optional)Turn on **Traffic Flow Diagram** to view the background information and concepts.

   Traffic Flow Diagram shows the relationship between origin servers and Anti-DDoS Pro or Anti-DDoS Premium instances, terms, and commonly used units.
5. Click the **Instances** tab, select one or more instances, and then specify a time range to view the relevant metrics.

   You can view the following instance information:

   - **Peak Attack Bandwidth** (unit: bit/s) and **Peak Attack Packet Rate** (unit: pps)
   - Traffic trends
     - Anti-DDoS Pro provides the **Bandwidth** trend chart to show traffic information by **bps** or **pps**. You can view the trends of inbound, outbound, and attack traffic of an instance for a specific time range.
     - Anti-DDoS Premium provides the **Overview** tab to show bandwidth trends and the **Inbound Distribution** tab to show the distribution of inbound traffic. Anti-DDoS Premium also provides the **Outbound Distribution** tab to show the distribution of outbound traffic.
   - **Attack Events** of the Blackhole and Mitigation types

     You can move the pointer over an IP address or a port to view the details of an attack, such as Attack Target, Attack Type, Peak Attack Traffic, and Protection Effect.
   - **Connections** on a port

- **Concurrent Connections**: the total number of concurrent TCP connections established between clients and the instance
- **New Connections**: the number of new TCP connections established between clients and the instance per second
- **Active**: the number of TCP connections in the **Established** state
- **Inactive**: the number of TCP connections in all states except the **Established** state

> **Note** If you select an instance, the Connections trend chart shows the numbers of connections on different ports. If you select more than one instance, the Connections trend chart shows the total number of connections on all ports.

- **Source Locations** and **Source Service Providers**
  - **Source Locations**: the distribution of source locations from which normal traffic is sent. Source locations are classified by **Global** and **Mainland China**.
  - **Source Service Providers**: the distribution of Internet service providers (ISPs) from which normal traffic is sent.

6. Click the **Domains** tab, select one or more domains, and then specify a time range to view the relevant metrics.

   You can view the following domain information:

   - **Peak HTTP Mitigation Traffic** (unit: QPS) and **Peak HTTPS Mitigation Traffic** (unit: QPS)
   - **Requests** trend chart

     The trend of requests is displayed based on the peak values in a specific time range. The displayed time granularity is based on the specific time range:

     - If the time range is less than 1 hour, the granularity is 1 minute.
     - If the time range is from 1 to less than 6 hours, the granularity is 10 minutes.
     - If the time range is from 6 to less than 24 hours, the granularity is 30 minutes.
     - If the time range is from 1 to less than 7 days, the granularity is 1 hour.
     - If the time range is from 7 to less than 15 days, the granularity is 4 hours.
     - For larger time ranges, the granularity is 12 hours.

   - **Mitigation Events**

     You can move the pointer over a domain to view the details of an attack, such as Domains, Peak Attack Traffic, and Attack Type.

   - **Response Codes** trend chart

     The trend chart of response codes shows the accumulated numbers of response codes within a specific time range. The time range and time granularity in this trend chart have definitions similar to the definitions in the **Requests** trend chart. Description of response codes:

     - 2xx: The request is successfully received, understood, and accepted by the server.

       > **Note** Statistics on 2xx response codes include the statistics on the 200 response code.

     - 200: The request succeeded.

- 3xx: The client must perform further operations to complete the request. In most cases, a 3xx response code indicates redirection.
- 4xx: The client may be faulty, which interrupts server processing.
- 5xx: An error or an exception occurred when the server processed the request.
- 502: Anti-DDoS Pro or Anti-DDoS Premium attempts to process the request as a proxy server, but it receives invalid responses from the upstream server.
- 503: The server may be overloaded or in temporary maintenance and cannot process the request.
- 504: Anti-DDoS Pro or Anti-DDoS Premium attempts to process the request as a proxy server, but it does not receive responses from the upstream server in a timely manner.

- **Source Locations**: the distribution of source locations from which requests are sent. Source locations are classified by **Global** and **Mainland China**.
- **Most Requested URIs** and **Slow Loading URIs**
  - **Most Requested URIs**: the top five most requested URIs. The URIs are displayed in descending order. You can click **More** to view the total number of requests for each URI.
  - **Slow Loading URIs**: the top five URIs based on the response time, in milliseconds. The URIs are displayed in descending order. You can click **More** to view the response time of each URI.
- **Cache Hit Rate** trend chart

  You can view the trend chart of cache hit rates only after you enable the static page caching feature. For more information, see Configure static page caching.

4.Provisioning
4.1. Use domains
4.1.1. Add a website

Anti-DDoS Pro and Anti-DDoS Premium protect your website only after you add the website to Anti-DDoS Pro or Anti-DDoS Premium and complete forwarding settings. You can add more than one website at a time. This topic describes how to add your website. This topic also describes how to import the configurations of more than one website to Anti-DDoS Pro or Anti-DDoS Premium at a time.

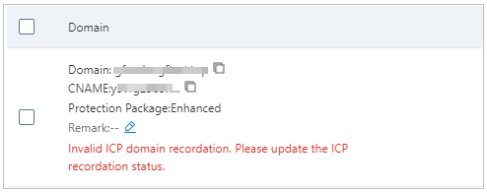
Prerequisites

- An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased.

  For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.
- If you want to add your website to Anti-DDoS Pro, make sure that Internet Content Provider (ICP) filing is complete for the domain name of your website. If you want to add your website to Anti-DDoS Premium, ICP filing is not required.

  For more information, see ICP filing application overview.

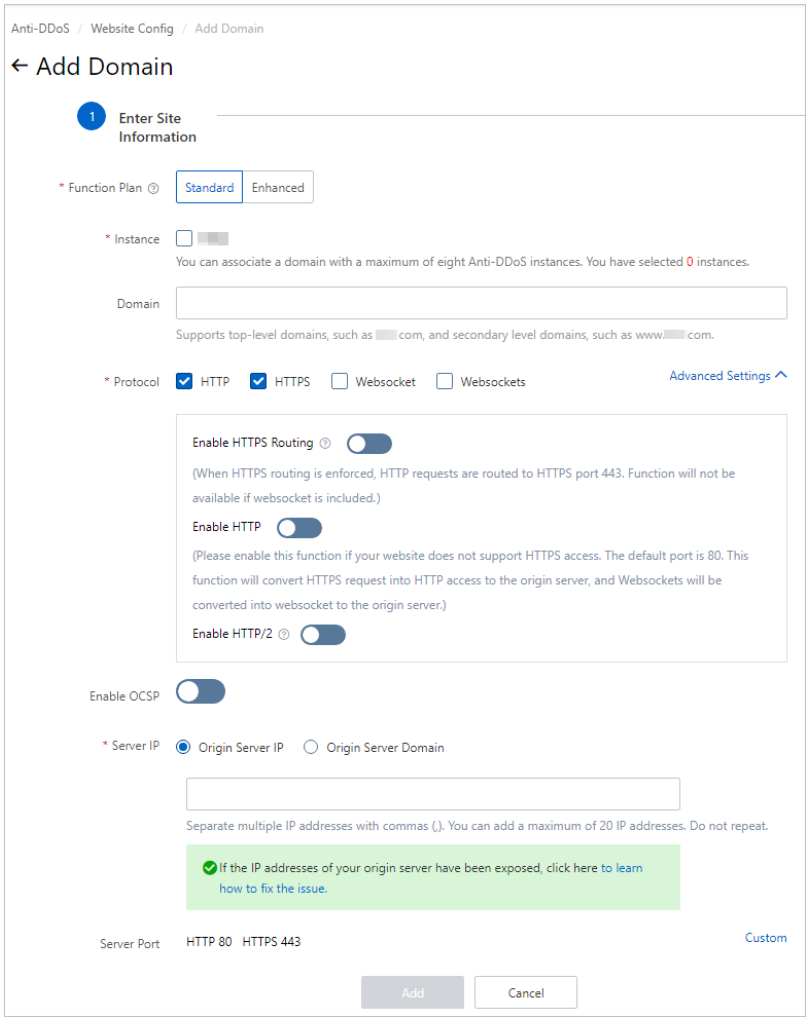
  > **Notice** The information that you use to complete the ICP filing of your domain name must be consistent with the actual information about your domain name. This ensures the validity of the ICP filing. After you add your website to Anti-DDoS Pro, we recommend that you keep the ICP filing information up-to-date. Anti-DDoS Pro checks the status of ICP filing for protected domain names on a regular basis. If the ICP filing of a domain name becomes invalid, Anti-DDoS Pro no longer forwards the traffic of the domain name and displays a message on the **Website Config** page. The following figure shows the message. If you want to resume traffic forwarding, you must update the ICP filing information for the domain name at the earliest opportunity and submit a .



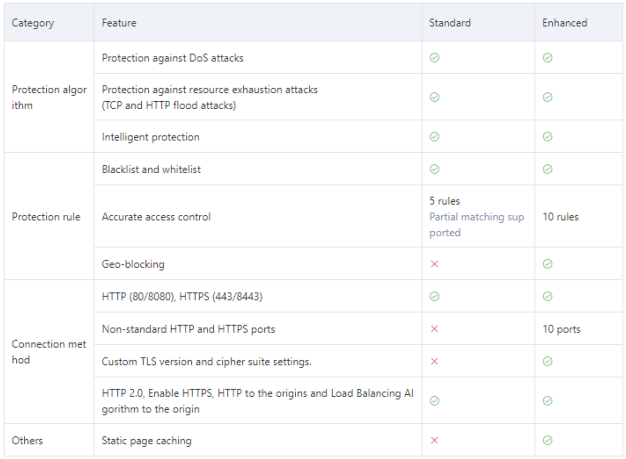
Add a website

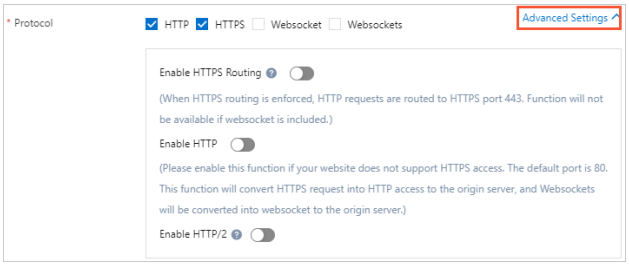
1.
2.
3.
4. On the **Website Config** page, click **Add Domain**.

   You can import the configurations of more than one website at a time. For more information, see Import the configurations of more than one website at a time.
5. Complete the **Add Domain** wizard.
   i. In the **Enter Site Information** step, configure the parameters and click Add.



Parameter	Applicable instance	Description

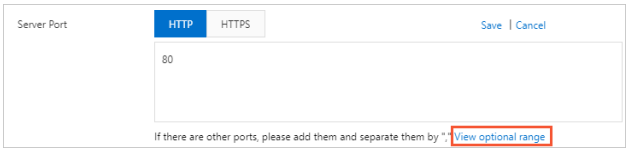
Parameter	Applicable instance	Description
Function Plan	Anti-DDoS Pro and Anti-DDoS Premium instances	The function plan of the Anti-DDoS Pro or Anti-DDoS Premium instance that you want to use. Valid values: **Standard Function** and **Enhanced Function**. You can move the pointer over the icon next to **Function Plan** to view the differences between the Standard and Enhanced function plans. The following figure shows the differences. 
Instance	Anti-DDoS Pro and Anti-DDoS Premium instances	The Anti-DDoS Pro or Anti-DDoS Premium instance that you want to use. You can associate a maximum of eight instances with a domain name. The instances associated with the domain name must use the same **function plan**. Available instances are displayed after you configure **Function Plan**. If no instances are displayed, no instances use the function plan that you select. In this case, you can purchase an instance or upgrade the Standard function plan to the Enhanced function plan. For more information, see Upgrade an instance.

Parameter	Applicable instance	Description
Domain	Anti-DDoS Pro and Anti-DDoS Premium instances	The domain name of the website that you want to protect. The domain name must meet the following requirements: ■ The domain name can contain letters, digits, and hyphens (-). The domain name must start with a letter or a digit. ■ The domain name can be a wildcard domain name, such as `*.aliyundoc.com`. If you enter a wildcard domain name, Anti-DDoS Pro or Anti-DDoS Premium automatically matches all subdomains of the wildcard domain name. ■ If you configure a wildcard domain name and an exact-match domain name, the forwarding rules and mitigation policies of the exact-match domain name take precedence. For example, if you configure `*.aliyundoc.com` and `www.aliyundoc.com`, the forwarding rules and mitigation policies of `www.aliyundoc.com` take precedence.
		The type of the protocol that the website uses. Valid values: ■ **HTTP** ■ **HTTPS**: If the website uses HTTPS, select **HTTPS** and upload an SSL certificate file after you save the website configurations. For more information, see Upload an HTTPS certificate. ■ **Websocket**: If you select Websocket, **HTTP** is automatically selected. You cannot select only **Websocket** for the Protocol parameter. ■ **Websockets**: If you select Websockets, **HTTPS** is automatically selected. You cannot select only **Websockets** for the Protocol parameter. If you select **HTTPS**, you can click Advanced Settings to configure the following options. 

Parameter	Applicable instance	Description
Protocol	Anti-DDoS Pro and Anti-DDoS Premium instances	■ **Enable HTTPS Routing**: If the website supports both HTTP and HTTPS, this feature is available. If you enable this feature, all HTTP requests to access the website are redirected to HTTPS requests on the standard port 443. **Notice** ■ This feature is available only when both **HTTP** and **HTTPS** are selected and **Websocket** is cleared. ■ If you access the website over HTTP on a non-standard port and enable this feature, all HTTP requests are redirected to HTTPS requests on the standard port 443. ■ **Enable HTTP**: If the website does not support HTTPS, this feature is available. If this feature is enabled, all HTTPS requests are redirected to HTTP requests and forwarded to origin servers, and all WebSockets requests are redirected to WebSocket requests and forwarded to origin servers. By default, the requests are redirected over the standard port 80. **Notice** ■ If the website does not support HTTPS, turn on Enable HTTP. ■ If you access the website over HTTPS on a non-standard port and enable this feature, all HTTPS requests are redirected to HTTP requests on the standard port 80. ■ **Enable HTTP2**: After you turn on Enable HTTP/2, HTTP/2 is used.

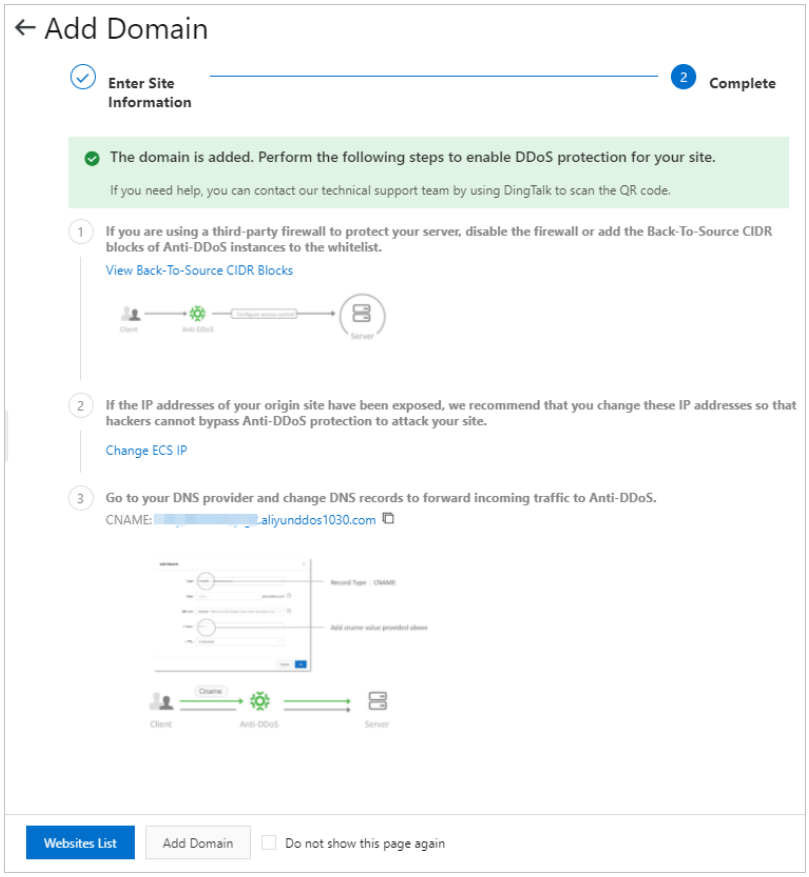
Parameter	Applicable instance	Description
Enable OCSP	Anti-DDoS Pro and Anti-DDoS Premium instances	Specifies whether to enable the Online Certificate Status Protocol (OCSP) feature. **Notice** This feature is available only for a website that supports HTTPS. If **HTTPS** is selected for **Protocol**, we recommend that you enable this feature. OCSP is an Internet protocol that is used by a Certificate Authority (CA) to check the revocation status of a certificate. When a client initiates a Transport Layer Security (TLS) handshake with a server, the client must obtain the certificate and an OCSP response. The OCSP feature is disabled by default. In this case, OCSP queries are sent from a browser that the client uses to a CA. Before the client obtains an OCSP response, subsequent events are blocked. If transient connections or network disconnections occur, a blank page is displayed for a long period of time, and the performance of the website that supports HTTPS is compromised. If the OCSP feature is enabled, Anti-DDoS Pro or Anti-DDoS Premium executes OCSP queries and caches the query results for 300 seconds. When a client initiates a TLS handshake with the server, Anti-DDoS Pro or Anti-DDoS Premium returns the OCSP details and the certificate chain to the client. This prevents blocking issues caused by OCSP queries from the client. OCSP does not cause security risks because OCSP responses cannot be forged.

Parameter	Applicable instance	Description
Server IP	Anti-DDoS Pro and Anti-DDoS Premium instances	The address type of the origin server. You must enter the address of the origin server. Valid values: ■ **Origin Server IP**: the IP address of the origin server. You can enter a maximum of 20 IP addresses. If you enter more than one IP address, separate them with commas (,). ■ If the origin server is hosted on an Elastic Compute Service (ECS) instance, enter the public IP address of the ECS instance. If the ECS instance is associated with a Server Load Balancer (SLB) instance, enter the public IP address of the SLB instance. ■ If the origin server is deployed in data centers or on other clouds, you can run the `ping` *Domain name* command to query the public IP address to which the domain name is resolved and enter the public IP address. ■ **Origin Server Domain**: the domain name of the origin server. Select this option when you deploy a proxy service, such as Web Application Firewall (WAF), between the origin server and Anti-DDoS Pro or Anti-DDoS Premium. You must also enter the address of the proxy, such as a CNAME. You can enter a maximum of 10 domain names. If you enter more than one domain name, separate them with line breaks. If you want to use Anti-DDoS Pro or Anti-DDoS Premium together with WAF, select **Origin Server Domain** and enter the CNAME that WAF assigns. This provides enhanced protection for the website. For more information, see Add a website to both Anti-DDoS Pro or Anti-DDoS Premium and WAF. **Notice** If you enter the default public endpoint of an Object Storage Service (OSS) bucket for **Origin Server Domain**, a custom domain name must be mapped to the bucket. For more information, see Regions and endpoints and Map custom domain names. If you enter more than one IP address or domain name, Anti-DDoS Pro or Anti-DDoS Premium uses IP hash to forward website traffic to the origin servers. After you save the website configurations, you can change the load balancing algorithm. For more information, see Modify the back-to-origin settings for a website.
		The server port that you specify based on the value of **Protocol**.

Parameter	Applicable instance	Description
Server Port	Anti-DDoS Pro and Anti-DDoS Premium instances	If you select **HTTP**, the default port 80 is used. If you select **HTTPS**, the default port 443 is used. **Notice** ■ The port for **Websocket** is the same as the port for **HTTP**. ■ The port for **Websockets** and HTTP/2 is the same as the port for **HTTPS**. You can click **Custom** to the right of the Server Port parameter to specify one or more custom ports. You can specify multiple custom **HTTP** or **HTTPS** ports. If you specify multiple custom ports, separate the ports with commas (,).  Take note of the following limits when you specify custom ports: ■ The custom ports that you want to specify must be supported by Anti-DDoS Pro or Anti-DDoS Premium. You can click **View optional range** to view the HTTP and HTTPS ports that are supported. The ports that are supported vary based on the **function plan** of your Anti-DDoS Pro or Anti-DDoS Premium instance. ■ Anti-DDoS Pro or Anti-DDoS Premium instance of the **Standard function plan**: ■ HTTP ports: ports 80 and 8080 ■ HTTPS ports: ports 443 and 8443 ■ Anti-DDoS Pro or Anti-DDoS Premium instance of the **Enhanced function plan**: ■ HTTP ports: ports that range from 80 to 65535 ■ HTTPS ports: ports that range from 80 to 65535 ■ You can specify up to 10 custom ports for all websites that are added to your Anti-DDoS Pro or Anti-DDoS Premium instance. The custom ports include HTTP ports and HTTPS ports. For example, you want to add Website A and Website B to your Anti-DDoS Pro or Anti-DDoS Premium instance, Website A provides services over HTTP ports, and Website B provides services over HTTPS ports. If you specify HTTP ports 80 and 8080 for Website A, you can specify up to eight HTTPS ports for Website B.

Parameter	Applicable instance	Description
Cname Reuse	Anti-DDoS Premium	Specifies whether to enable CNAME reuse. If more than one website is hosted on the same server, this feature is available. After CNAME reuse is enabled, you need only to map the domain names hosted on the same server to the CNAME that is assigned by Anti-DDoS Premium. For more information, see Use the CNAME reuse feature.

ii. In the **Complete** step, perform the subsequent operations as instructed.



a. Allow back-to-origin IP addresses to access the origin server:

If security software, such as a firewall, is installed on the origin server, you must add the back-to-origin IP addresses of the Anti-DDoS Pro or Anti-DDoS Premium instance to the whitelist of the origin server. This ensures that the traffic from Anti-DDoS Pro or Anti-DDoS Premium is not blocked by the security software on your origin server.

If no security software is installed, skip this step.

b. Change the public IP address of an ECS origin server:

If your origin server is an ECS instance and the origin IP address is exposed, you must change the public IP address of the ECS instance. This prevents attackers from bypassing Anti-DDoS Pro or Anti-DDoS Premium to attack your origin server.

If your origin server is not an ECS instance and the origin IP address is not exposed, skip this step.

c. Upload an HTTPS certificate:

If a website that provides HTTPS services is added to Anti-DDoS Pro or Anti-DDoS Premium, you must upload the SSL certificate file that is associated with the domain name of the website. This way, HTTPS requests can be redirected to Anti-DDoS Pro or Anti-DDoS Premium for protection.

> **Note** If a website is associated with an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the Enhanced function plan, you can create a custom TLS policy for the website after you upload an SSL certificate file. For more information, see Customize a TLS policy.

If the website provides only HTTP services, skip this step.

d. (Optional)Verify the forwarding configurations on your local computer:

Verify that the website configurations that you added to Anti-DDoS Pro or Anti-DDoS Premium take effect on your computer. If you change the DNS record before the configurations for the website take effect, services may be interrupted.

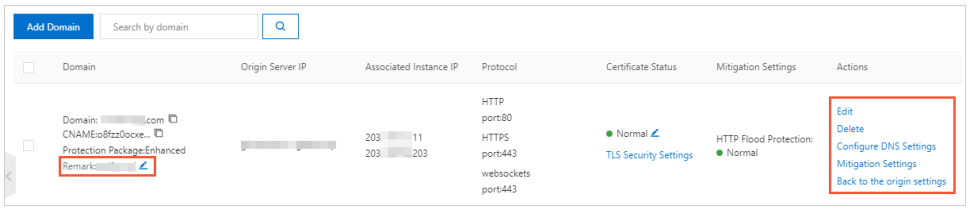
e. Change the DNS record:

Anti-DDoS Pro or Anti-DDoS Premium assigns a CNAME to the website that you added. You must change the DNS record to map the domain name to the CNAME. This way, service traffic can be switched to Anti-DDoS Pro or Anti-DDoS Premium for protection. You can manually change the DNS record or use the NS Access Mode feature to enable the system to automatically change the DNS record.

For more information, see Change DNS records to protect website services and Enable NS Mode Access to protect a website.

iii. Click **Websites List** to view the domain name that you added and the CNAME that is assigned by Anti-DDoS Pro or Anti-DDoS Premium in the website list.

After you complete the **Add Domain** wizard, you can perform the following operations on the newly added domain name:



- Add remarks: You can click the

  icon next to **Remark** to add remarks that help you identify the website configurations.
- Modify or delete the domain name: You can click **Edit** or **Delete** to manage the website configurations that you added.

> **Notice** After you click Edit in the Actions column, you can turn on Getting source port from the real customer on the page that appears. After you turn on Getting source port from the real customer, you can obtain the actual ports of clients or mark the back-to-origin requests that Anti-DDoS Pro or Anti-DDoS Premium forwards to the origin server by using custom HTTP headers. For more information, see Mark back-to-origin requests.

- **Configure DNS settings**: If you purchase a paid edition of Alibaba Cloud DNS, you can enable NS Access Mode. This way, the system automatically changes the DNS record of the domain name and redirects traffic to Anti-DDoS Pro or Anti-DDoS Premium.

  For more information, see Enable NS Mode Access to protect a website.

- Configure mitigation settings: You can click **Mitigation Settings** in the Actions column to go to the **Protection for Website Services** tab and modify the mitigation settings.

  After you add the website, **Intelligent Protection** and **Frequency Control** are enabled by default. You can enable more features and modify protection rules for the website on the **Protection for Website Services** tab.

  For more information, see Use the intelligent protection feature.

- Configure back-to-origin settings: If the website that you add to Anti-DDoS Pro or Anti-DDoS Premium resides on more than one origin server, you can click **Back to the origin settings** to change the **load balancing algorithm** for back-to-origin traffic.

  For more information, see Modify the back-to-origin settings for a website.

What to do next

After you add the website, you must perform the following operations to enable Anti-DDoS Pro or Anti-DDoS Premium to protect the website.

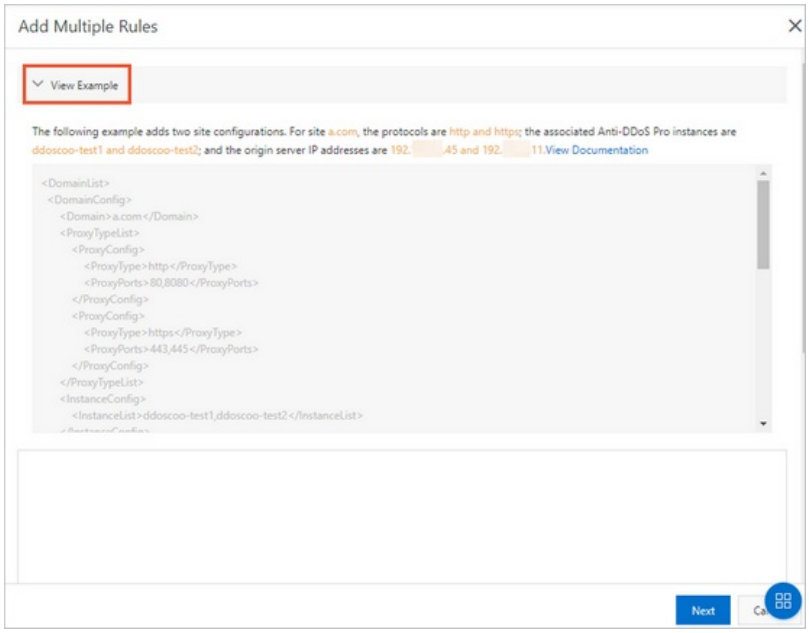
Configuration item	Description	References
Protection for website services	After you add the website, **Global Mitigation Policies**, **Intelligent Protection**, and **Frequency Control** are enabled by default. You can enable more features and modify protection rules for the website on the **Protection for Website Services** tab.	• Configure the global mitigation policy • Use the intelligent protection feature • Configure blacklists and whitelists for domain names • Configure a location blacklist for a domain name • Configure accurate access control rules • Configure frequency control

Configuration item	Description	References
Alert rules in CloudMonitor	CloudMonitor allows you to configure threshold-triggered alert rules for common service metrics and attack events of Anti-DDoS Pro or Anti-DDoS Premium. The common service metrics include the volume of traffic for an Anti-DDoS Pro or Anti-DDoS Premium instance and the number of connections for an Anti-DDoS Pro or Anti-DDoS Premium instance. The traffic and connection metrics can be measured at the IP address level. The attack events include blackhole filtering events and traffic scrubbing events. After you configure a threshold-triggered alert rule, CloudMonitor reports an alert when the rule is triggered. This way, you can handle exceptions and recover your business at the earliest opportunity.	Create threshold-triggered alert rules in the CloudMonitor console
Log Analysis feature	After you enable the Log Analysis feature, Anti-DDoS Pro or Anti-DDoS Premium collects and stores full logs of the website. This way, you can query and analyze the logs that are collected from the website. By default, the Log Analysis feature stores full logs for 180 days. This helps meet the requirements of classified protection.	Quick start

Import the configurations of more than one website at a time

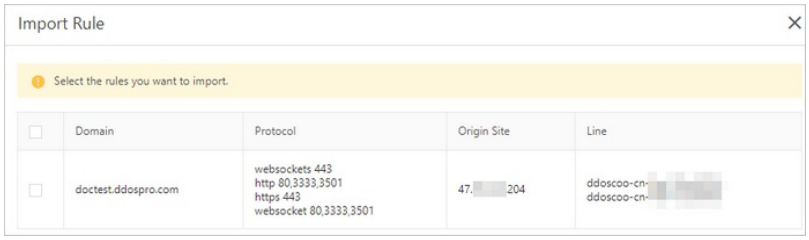
1.
2.
3.
4. On the **Website Config** page, click **Batch Domains Import**.
5. In the **Add Multiple Rules** panel, enter the information about the websites that you want to add and click **Next**.

   If you want to add the configurations of more than one website at a time, save the configurations in an XML file and import the file. For more information about file formats, see Website configurations in an XML file.



If the content of the XML file is valid, the file is parsed into the configurations of the websites that you want to add.

6. In the **Import Rule** panel, select the websites that you want to add and click **OK**.



7. After the configurations are imported, close the **The rules have been created** panel.

4.1.2. Verify the forwarding configurations on your local computer

After you add a domain name or a port to an Anti-DDoS Pro or Anti-DDoS Premium instance, Anti-DDoS Pro or Anti-DDoS Premium forwards the packets received by the port to the port of the origin server. To ensure service stability, we recommend that you verify whether the forwarding configurations take effect on your computer before the inbound traffic is rerouted to Anti-DDoS Pro or Anti-DDoS Premium. This topic describes how to verify the configurations.

Prerequisites

- A website or port is added to an Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see Add a website and Create forwarding rules.
- The back-to-origin CIDR blocks of the Anti-DDoS Pro or Anti-DDoS Premium instance are added to the whitelist of the origin server. For more information, see Allow back-to-origin IP addresses to access the origin server.

Context

To protect a service that is accessed by using a domain name instead of an IP address, you must add a website to Anti-DDoS Pro or Anti-DDoS Premium. After you add a website, you can modify the hosts file or use the CNAME of the Anti-DDoS Pro or Anti-DDoS Premium instance to connect to the server and check whether the forwarding configurations take effect.

Requests to access Layer 4 services, such as games, are processed by using IP addresses instead of domain names. You must add port forwarding rules to Anti-DDoS Pro or Anti-DDoS Premium to protect these services. Then, you can verify the forwarding configurations by using the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance to access the server.

Notice If you switch your service traffic to Anti-DDoS Pro or Anti-DDoS Premium before the forwarding configurations take effect, your service may be interrupted.

Modify the local hosts file

1. Modify the hosts file to reroute the inbound traffic of the protected website to Anti-DDoS Pro or Anti-DDoS Premium. The following procedure shows how to modify the hosts file on a Windows server.
   i. Find the hosts file, which is typically stored in *C:\Windows\System32\drivers\etc*.
   ii. Open the hosts file by using a text editor.
   iii. Add both `the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance and the protected domain name` at the end of the file.

   For example, if the IP address of the instance is `180.173.XX.XX` and the domain name is `demo.aliyundoc.com`, you must add `180.173.XX.XX demo.aliyundoc.com` at the end of the file.
   iv. Save the file.
2. Ping the protected domain name from your computer.
   If the command output includes the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance in the hosts file, the modification takes effect as expected. If the command output includes the IP address of the origin server, refresh the local DNS cache by running `ipconfig/flushdns` in Command Prompt.
3. After you verify that the protected domain name is resolved to the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance, try to access the service by using the domain name. If you can access the service, the configurations take effect.

Use the CNAME assigned by Anti-DDoS Pro or Anti-DDoS Premium to access the origin server

If the client allows you to enter the domain name of the origin server, replace the domain name with the CNAME assigned by Anti-DDoS Pro or Anti-DDoS Premium and check whether the origin server is accessible.

Note After you add a domain name for protection, Anti-DDoS Pro or Anti-DDoS Premium assigns a CNAME to the domain name. You can view the CNAME on the Website Config page.

If the origin server is unaccessible, check whether the prerequisites are met. If the error persists, contact Alibaba Cloud technical support.

Use the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance to access the origin server

Assume that the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance is 99.99.XX.XX, the forwarding port is 1234, the IP address of the origin server is 11.11.XX.XX, and the port of the origin server is 1234.

You can use telnet commands to access the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance over port 1234. If the IP address is accessible, the forwarding rule takes effect.

If the client allows you to enter the IP address of the origin server, you can enter the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance for verification.

4.1.3. Modify the back-to-origin settings for a website

You can configure back-to-origin settings to specify the load balancing algorithm for the back-to-origin requests of a website that is added to Anti-DDoS Pro or Anti-DDoS Premium.

Prerequisites

A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.

Context

If you configure multiple server addresses when you add the website, your Anti-DDoS Pro or Anti-DDoS Premium instance automatically uses the round-robin algorithm to schedule requests destined for your origin servers. This enables load balancing among the origin servers. The server addresses can be origin IP addresses or origin domain names. You can change the load balancing algorithm for back-to-origin requests or specify weights for the server addresses.

The following table describes the load balancing algorithms that are supported.

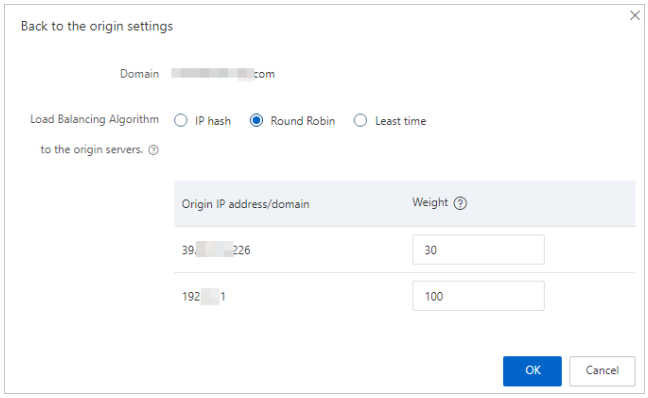
Algorithm	Description
IP hash	This algorithm is used to forward the requests from the same IP address to the same server address.
Round-robin	This algorithm is used to forward requests to all server addresses in sequence. This is the default algorithm. By default, all server addresses have the same weight. You can change the weights of server addresses. The higher the weight of the server address, the higher the possibility that back-to-origin requests are forwarded to the server address.
Least time	The intelligent DNS resolution feature and the least-time algorithm are used to minimize the latency when service traffic is forwarded from your Anti-DDoS Pro or Anti-DDoS Premium instance to origin servers.

Procedure

1.

2.
3.
4. Find the forwarding rule for which you want to modify the back-to-origin settings and click **Back to the origin settings** in the **Actions** column.
5. In the **Back to the origin settings** dialog box, configure **Load Balancing Algorithm to the origin servers**.

   Valid values: **IP hash**, **Round Robin**, and **Least time**. For more information about algorithm differences, see Algorithm descriptions.



6. If you set Load Balancing Algorithm to the origin servers to **Round Robin**, specify weights for server addresses. If you select another algorithm, skip this step.

   A weight must be an integer that ranges from 1 to 100. The higher the weight of the server address, the higher the possibility that back-to-origin requests are forwarded to the server address.
7. Click **OK**.
   After you configure the back-to-origin settings, the instance schedules requests among multiple server addresses based on the load balancing algorithm that you specified.

4.1.4. Modify website configurations

You can modify the existing configuration of your website to add the website to another Anti-DDoS Pro or Anti-DDoS Premium instance or change the origin IP address. For example, you can upgrade the instance from the Standard function plan to the Enhanced function plan. You can modify the configurations of multiple websites at a time. This topic describes how to modify the configurations of one or more websites.

Prerequisites

A website is added to an Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see Add a website.

Modify the configuration of a website

1.
2.
3.
4. Find the website whose configuration you want to modify and click **Edit** in the Actions column.

> **Note** You can also modify the configurations of multiple websites at a time. For more information, see Modify the configurations of multiple websites at a time.

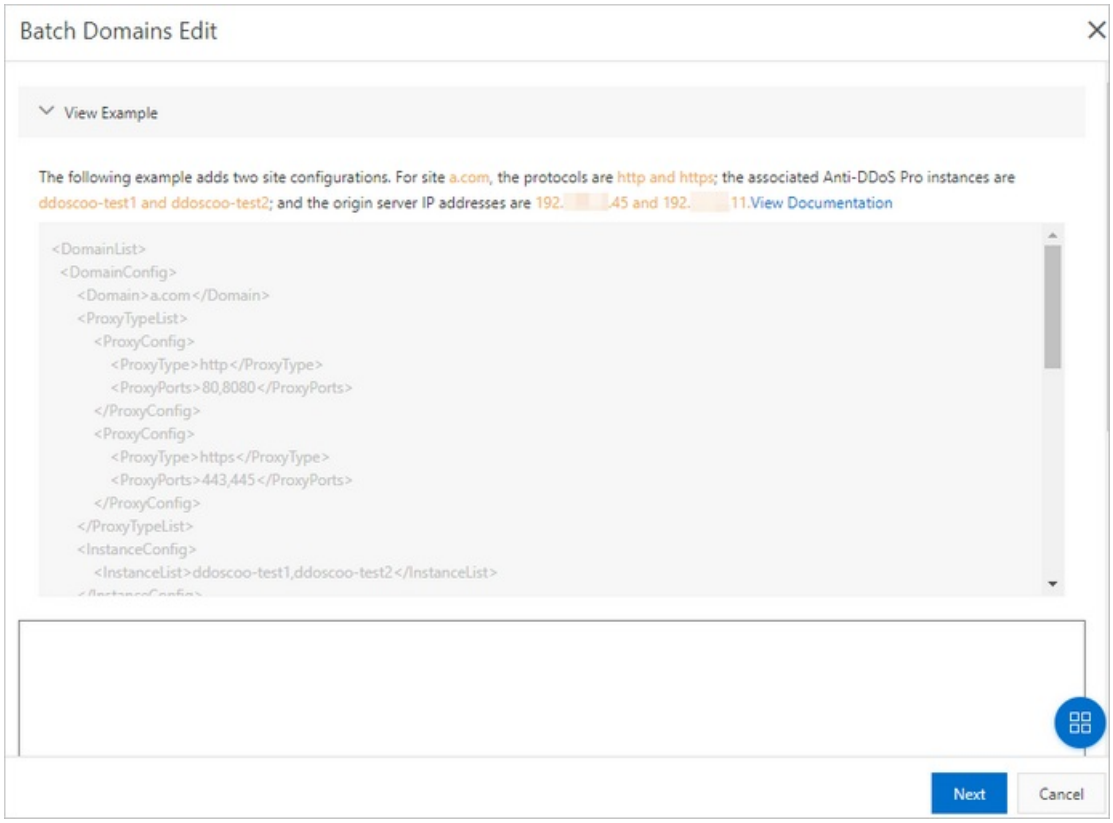
5. On the website details page, modify the configuration of the website and click **OK**.

   You can modify all parameters except for the domain name. For example, if you want to change the instance to which the website is added, change the values of the **Function Plan** and **Instance** parameters. If you want to change the origin IP address, change the value of the **Server IP** parameter. For more information about the configuration of a website , see Website configurations.

Modify the configurations of multiple websites at a time

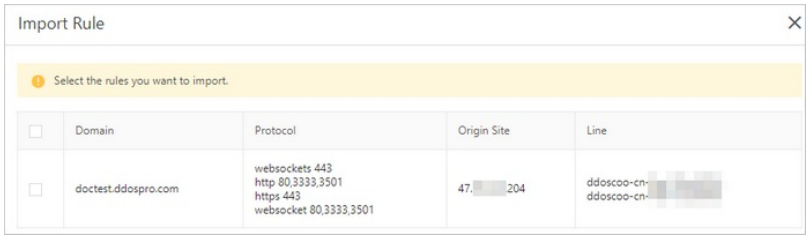
1.
2.
3.
4. On the **Website Config** page, click **Batch Domains Edit**.
5. In the **Batch Domains Edit** panel, enter new configurations and click **Next**.

   You can import an XML file to modify the configurations of multiple website at a time. For more information about the XML file, see Website configurations in an XML file.



   If the values of the parameters in the XML file are valid, the file is parsed into the website configurations that you want to import.

6. In the **Import Rule** panel, select the websites that you want to add and click **OK**.



7. After the configurations are imported, close the **The rules have been created** panel.

4.1.5. Delete a website configuration

If a website no longer requires anti-DDoS protection, you can delete the website configuration. Before you perform this operation, you must update the DNS record. Make sure that the DNS record does not use the IP address of an Anti-DDoS Pro or Anti-DDoS Premium instance or the CNAME record. The CNAME record refers to that assigned by Anti-DDoS Pro or Anti-DDoS Premium, or that assigned by Sec-Traffic Manager. If you delete a website configuration without updating its DNS record, your service may be interrupted.

Prerequisites

The DNS record of the website is updated.

Procedure

1.
2.
3.
4. Find the website configuration that you want to delete and click **Delete** in the Actions column.

   > **Note** Anti-DDoS Pro allows you to delete multiple website configurations at a time. You can select multiple website configurations that you want to delete and click **Batch Delete** below the list.

5. In the message that appears, click **OK**.

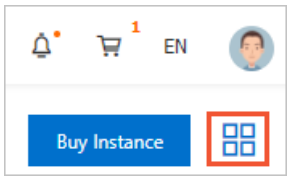
4.1.6. Export multiple website configurations at a time

Anti-DDoS Pro and Anti-DDoS Premium allow you to export multiple website configurations at a time. You can export all website configurations as an XML file and download the file to your computer. The exported files use the same format as the file that you use to import or modify website configurations at a time.

Procedure

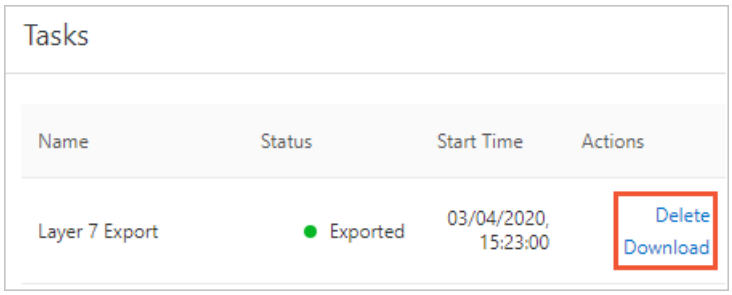
1.
2.
3.
4. Click **Batch Domains Export** below the list to start the export task.

5. After the export task starts, click the Tasks icon in the upper-right corner of the page.



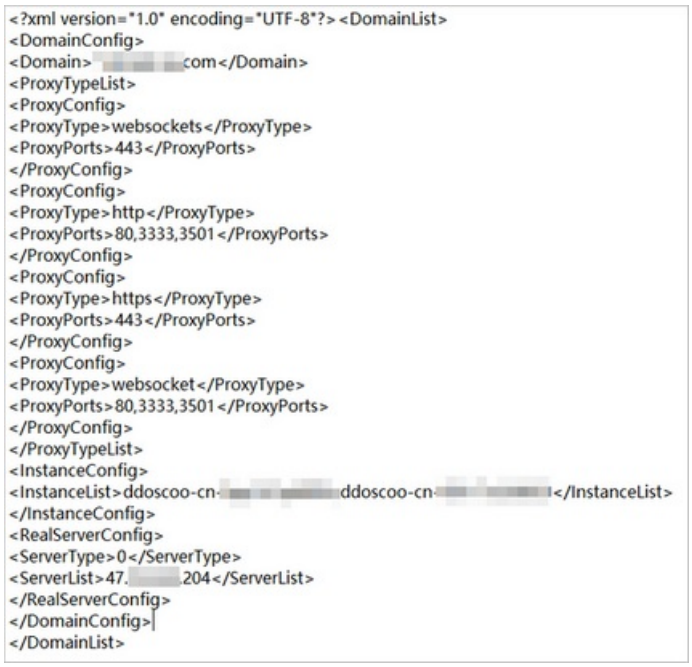
6. In the **Tasks** panel, wait until the export task is complete and click **Download** in the Actions column.

> **Note** If the task is in the **Pending Export** state, wait until the task is complete.



You can use a text editor to view the website configuration in the downloaded *XML* file. For more information, see Website configurations in an XML file.

> **Note** If you use Anti-DDoS Pro, the name of the exported file starts with *DDoSCoo_*. If you use Anti-DDoS Premium, the name of the exported file starts with *DDoSDip_*. The formats of the files exported from the Anti-DDoS Pro and Anti-DDoS Premium consoles are the same.



7. (Optional)In the **Tasks** panel, find the task that you want to delete and click **Delete** in the Actions column.

4.1.7. Specify custom ports

By default, Anti-DDoS Pro and Anti-DDoS Premium protect websites that provide services over HTTP port 80 and HTTPS port 443. If your website provides services over ports other than ports 80 and 443, you must specify the custom ports when you add your website to Anti-DDoS Pro or Anti-DDoS Premium.

Limits on custom ports

Take note of the following limits when you specify custom ports:

- The custom ports that you want to specify must be supported by Anti-DDoS Pro and Anti-DDoS Premium. The ports that are supported vary based on the **function plan** of your Anti-DDoS Pro or Anti-DDoS Premium instance.
  - Anti-DDoS Pro or Anti-DDoS Premium instance of the **Standard function plan**:
    - HTTP ports: ports 80 and 8080
    - HTTPS ports: ports 443 and 8443
  - Anti-DDoS Pro or Anti-DDoS Premium instance of the **Enhanced function plan**:
    - HTTP ports: ports that range from 80 to 65535
    - HTTPS ports: ports that range from 80 to 65535
- You can specify up to 10 custom ports for all websites that are added to your Anti-DDoS Pro or Anti-DDoS Premium instance. The custom ports include HTTP ports and HTTPS ports.

  For example, you want to add Website A and Website B to your Anti-DDoS Pro or Anti-DDoS Premium instance, Website A provides services over HTTP ports, and Website B provides services over HTTPS ports.

  If you specify HTTP ports 80 and 8080 for Website A, you can specify up to eight HTTPS ports for Website B.

Procedure

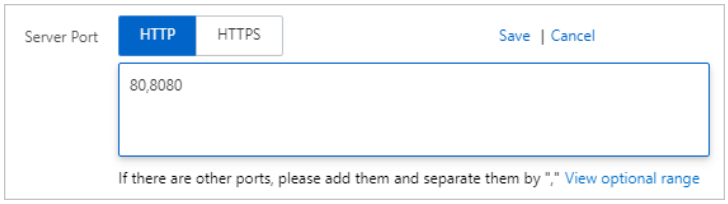
The following procedure shows how to change one or more ports for a website that is added to your Anti-DDoS Pro or Anti-DDoS Premium instance. You can also specify one or more custom ports when you add a website to your Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see Add a website.

1.
2.
3.
4. Find the website whose ports you want to change and click **Edit** in the **Actions** column.
5. On the page that appears, click **Custom** to the right of **Server Port**.

6. Click **HTTP** and enter custom HTTP ports. Click **HTTPS** and enter custom HTTPS ports. Then, click **Save**.

   Separate multiple ports with commas (,). You can click **View optional range** to view the HTTP and HTTPS ports that are supported.



7. Click **OK**. In the **Confirm** message, view the custom ports that you specify.

4.1.8. Upload an HTTPS certificate

To use Anti-DDoS Pro or Anti-DDoS Premium to scrub HTTPS traffic, you must select HTTPS and upload an HTTPS certificate when you add the domain name of a website. If the uploaded HTTPS certificate changes, you must update the certificate in the Anti-DDoS Pro or Anti-DDoS Premium console.

Prerequisites

- A website that supports HTTPS is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.
- The certificate file of the website is prepared.

  If you have uploaded the certificate file to the SSL Certificates Service console, you can select the certificate. Otherwise, you must upload your own certificate and private key files. The following files are required:

  - The public key file in the CRT format or the certificate file in the PEM format
  - The private key file in the KEY format

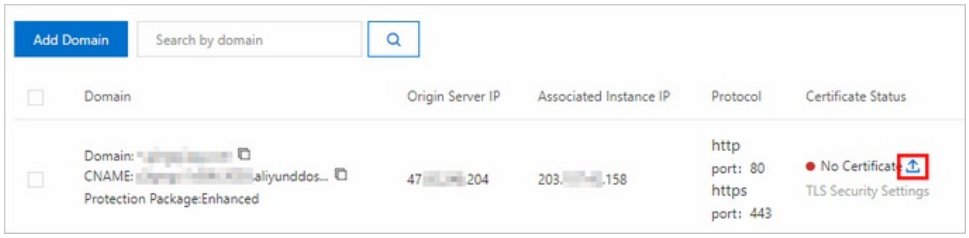
Scenarios

You must upload the HTTPS certificate in the following scenarios:

- You select HTTPS when you add a domain name to Anti-DDoS Pro or Anti-DDoS Premium.
- You select HTTPS when you add a domain name to Anti-DDoS Pro or Anti-DDoS Premium and upload a certificate. You need to replace the uploaded certificate or update the certificate when it expires.

Procedure

1.
2.
3.
4. On the **Website Config** page, find the domain name for which you want to upload a certificate, and click the upload icon in the **Certificate Status** column.

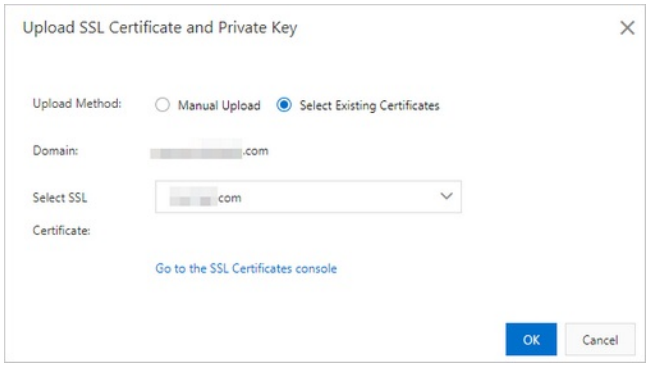


5. In the **Upload SSL Certificate and Private Key** dialog box, set **Upload Method** and configure other parameters.

   You can use one of the following methods to upload your certificate:

- **Select Existing Certificates** (recommended)

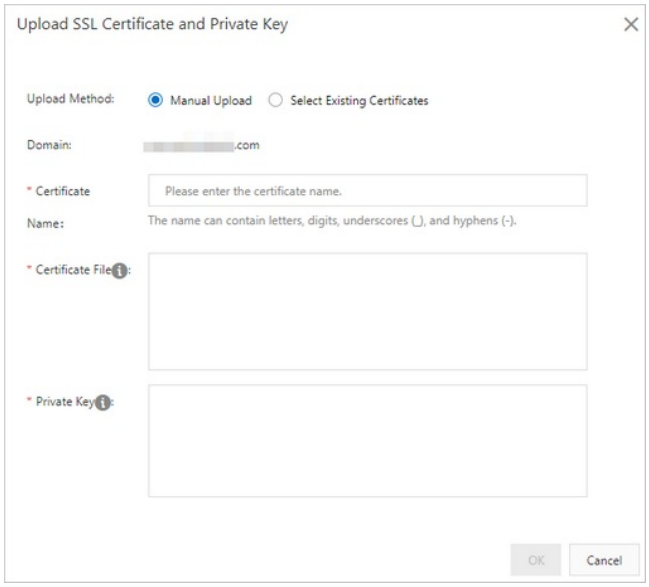
  If you have uploaded the certificate to SSL Certificates Service, you can select the certificate and upload it to Anti-DDoS Pro or Anti-DDoS Premium.



  If you have not uploaded the certificate to SSL Certificates Service, you can click **Go to the SSL Certificates console** to upload your certificate. For more information about how to upload certificates to SSL Certificates Service, see Upload a certificate.

- **Manual Upload**

  Specify **Certificate Name**, copy and paste the content of the certificate file to the **Certificate File** field, and then copy and paste the content of the private key file to the **Private Key** field.



> **Note**
>
> - If the certificate file is in the PEM, CER, or CRT format, you can use a text editor to open the certificate file and copy the file content. If the certificate file is in other formats, such as PFX and P7B, you must convert the file into the PEM format and use a text editor to open the file and copy the file content. For information about how to convert the format of a certificate file, see How do I convert an HTTPS certificate to the PEM format?.
> - If the certificate file has multiple certificates, such as a certificate chain, you must concatenate the content of these certificates and copy the concatenated content to the **Certificate File** field.

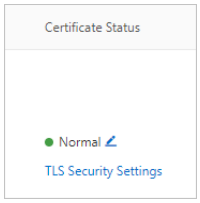
Certificate file example

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxvs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+1M+j2kcubVpsE2cgHdj4v8H6j
Uz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNdyTS5NIL5ir+g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW
/MojmlgfUekC2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv4TMxFhWRiNY7yZ
Io2ZUhl02SIDNggIEeg==
-----END CERTIFICATE-----
```

Private key file example

```
-----BEGIN RSA PRIVATE KEY-----
xxxxxxxxxxxxtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDGM9sTMThLyvsmLQKBgQCr+ujntC1kN
6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f
6ujSoHh2e+D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04RtKadOw==
-----END RSA PRIVATE KEY-----
```

6. Click **OK**.
   After the certificate is uploaded, the **Certificate Status** becomes **Normal**.



If the certificate is updated, you must upload the updated certificate. To upload the certificate, log on to the Anti-DDoS Pro console, click **Website Config**, and then click the icon next to the certificate to upload the updated certificate.

> **Warning** If the certificate is updated but is not uploaded in the Anti-DDoS Pro or Anti-DDoS Premium console, HTTPS traffic cannot be forwarded to the origin server.

FAQ

How do I handle the mismatch between a certificate and its private key?

4.1.9. Customize a TLS policy

Anti-DDoS Pro and Anti-DDoS Premium allow you to customize Transport Layer Security (TLS) policies. After you add your website to Anti-DDoS Pro or Anti-DDoS Premium, you can select TLS protocol versions and cipher suites for the website based on your business requirements. This topic describes how to customize a TLS policy.

Prerequisites

- A website is added to an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the **Enhanced** function plan. For more information, see Add a website.

  You can customize a TLS policy only in an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the Enhanced function plan. If you use an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the Standard function plan, upgrade the function plan of your instance to Enhanced before you can customize a TLS policy. For more information about how to upgrade an Anti-DDoS Pro or Anti-DDoS Premium instance, see Upgrade an instance.

- Your website supports **HTTPS**, and the required SSL certificate is uploaded. For more information, see Upload an HTTPS certificate.

Context

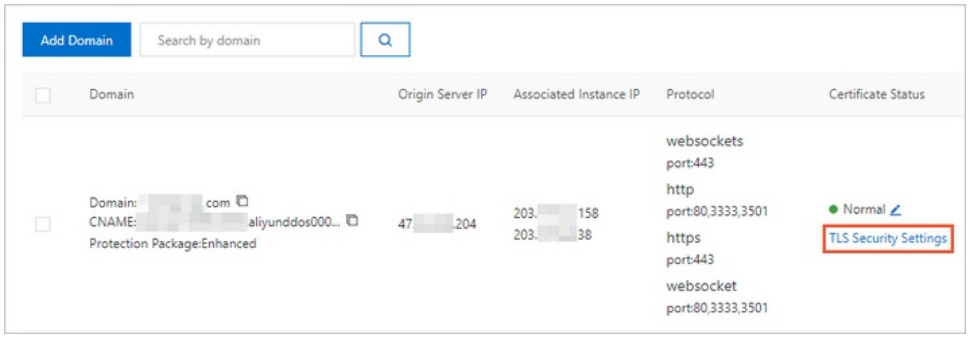
Anti-DDoS Pro and Anti-DDoS Premium support TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. By default, websites that are added to an Anti-DDoS Pro instance support TLS 1.0, TLS 1.1, and TLS 1.2 and websites that are added to an Anti-DDoS Premium instance support TLS 1.1 and TLS 1.2. If the default settings do not meet your business requirements, you can customize a TLS policy.

If one of your services must comply with PCI DSS 3.2, you must disable TLS 1.0 for the service. However, the terminals that access other services support only TLS 1.0, you can customize the TLS policy for each service.

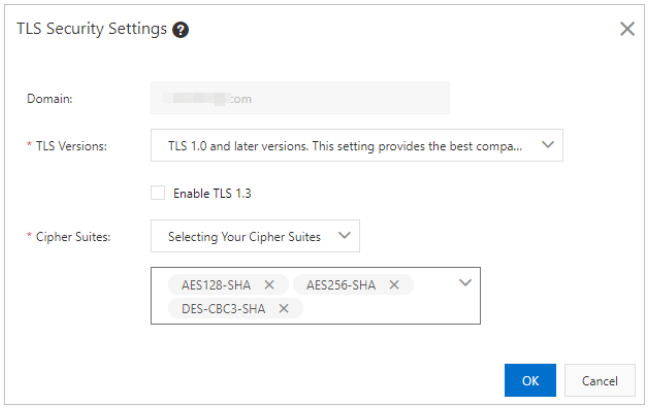
Procedure

1.
2.
3.
4. Find the domain name that you want to configure and click **TLS Security Settings** in the **Certificate Status** column.

   > **Notice** You can customize a TLS policy only if the following conditions are met: The domain name of your website is added to an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the **Enhanced** function plan. Your website supports **HTTPS**. The **Certificate Status** is **Normal**.

5. In the **TLS Security Settings** dialog box, configure **TLS Versions** and **Cipher Suites**.

Parameter	Description
TLS Versions	Select TLS protocol versions that are supported by HTTPS. Valid values: ◦ **TLS 1.0 and later versions. This setting provides the best compatibility but a low security level.**: TLS 1.0, TLS 1.1, and TLS 1.2 are supported. This is the default value. ◦ **TLS1.1 and later versions. This setting provides a good compatibility and a medium security level.**: TLS 1.1 and TLS 1.2 are supported. ◦ **TLS1.2 and later versions. This setting provides a good compatibility and a high security level.**: TLS 1.2 is supported. You can also select **Enable TLS 1.3** based on your business requirements.
Cipher Suites	Select cipher suites that are supported by HTTPS. The following options are available: **Note** To view the cipher suites contained in an option, you can move your pointer over the icon of an option. ◦ **All cipher suites. This setting provides a low security level but a high compatibility.** This is the default value. This option includes the following cipher suites: ■ ECDHE-ECDSA-AES128-GCM-SHA256 ■ ECDHE-ECDSA-AES256-GCM-SHA384 ■ ECDHE-ECDSA-AES128-SHA256 ■ ECDHE-ECDSA-AES256-SHA384 ■ ECDHE-RSA-AES128-GCM-SHA256 ■ ECDHE-RSA-AES256-GCM-SHA384 ■ ECDHE-RSA-AES128-SHA256 ■ ECDHE-RSA-AES256-SHA384 ■ AES128-GCM-SHA256 ■ AES256-GCM-SHA384 ■ AES128-SHA256 AES256-SHA256 ■ ECDHE-ECDSA-AES128-SHA ■ ECDHE-ECDSA-AES256-SHA ■ ECDHE-RSA-AES128-SHA ■ ECDHE-RSA-AES256-SHA ■ AES128-SHA AES256-SHA ■ DES-CBC3-SHA ◦ **Strong cipher suites. This setting provides a high security level but a low compatibility.**: This option is available only when **TLS Versions** is set to **TLS1.2 and later versions. This setting provides**

Parameter	Description
	a good compatibility and a high security level. This option includes the following cipher suites: ■ ECDHE-ECDSA-AES128-GCM-SHA256 ■ ECDHE-ECDSA-AES256-GCM-SHA384 ■ ECDHE-ECDSA-AES128-SHA256 ■ ECDHE-ECDSA-AES256-SHA384 ■ ECDHE-RSA-AES128-GCM-SHA256 ■ ECDHE-RSA-AES256-GCM-SHA384 ■ ECDHE-RSA-AES128-SHA256 ■ ECDHE-RSA-AES256-SHA384 ■ ECDHE-ECDSA-AES128-SHA ■ ECDHE-ECDSA-AES256-SHA ○ **Selecting Your Cipher Suites**: If you select this option, you must select one or more cipher suites from all cipher suites.

6. Click **OK**.

Result

After you customize the TLS policy for your website, Anti-DDoS Pro or Anti-DDoS Premium forwards access requests that are destined for your website based on the TLS policy. If a client uses a TLS protocol version that is not specified in the TLS policy, the access requests that are sent from the client are discarded.

4.1.10. Mark back-to-origin requests

After you add your website to Anti-DDoS Pro or Anti-DDoS Premium, you can turn on the Getting source port from the real customer switch to obtain your actual source ports of clients. You can also mark the back-to-origin requests that Anti-DDoS Pro or Anti-DDoS Premium forwards to the origin server by using custom HTTP headers. This allows the backend servers to perform statistical analysis on the back-to-origin requests in a more convenient manner. This topic describes how to mark the back-to origin requests that Anti-DDoS Pro or Anti-DDoS Premium forwards to your origin server.

Prerequisites

Your website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.

Procedure

1.
2.
3.
4. Find the website whose configurations you want to edit and click **Edit** in the **Actions** column.
5. On the page that appears, find the **Traffic mark** section and configure the following parameters.

Parameter	Description
Getting source port from the real customer	If you want to obtain the actual source port of a client, turn on this switch. After you turn on the switch, Anti-DDoS Pro or Anti-DDoS Premium records the actual source port of the client in the `X-Forwarded-ClientSrcPort` field when Anti-DDoS Pro or Anti-DDoS Premium forwards the back-to origin requests to the origin server. To obtain the actual source port of the client, you can parse the `X-Forwarded-ClientSrcPort` field in the back-to-origin requests. The specific procedures to obtain the actual source ports of clients are similar to how the actual source IP addresses of clients are obtained. For more information, see Obtain the actual source IP addresses of requests.
Custom Header	If you want to create custom HTTP headers, you must specify field names and values. After you create custom HTTP headers, Anti-DDoS Pro or Anti-DDoS Premium adds the custom HTTP headers to the back-to-origin requests. This way, the backend servers can perform statistical analysis on the back-to-origin requests. When you create a custom HTTP header, take note of the following points: ○ Do not use the following default HTTP headers as custom HTTP headers: ■ `X-Forwarded-ClientSrcPort`: This field is used to obtain the actual source ports of clients that access Anti-DDoS Pro or Anti-DDoS Premium (a Layer 7 proxy). ■ `X-Forwarded-ProxyPort`: This field is used to obtain the ports of listeners that access Anti-DDoS Pro or Anti-DDoS Premium (a Layer 7 proxy). ○ Do not use standard HTTP headers such as User-Agent. If you use standard HTTP headers, the original header fields may be overwritten. ○ You can create up to five custom HTTP headers.

6. Click **OK**.

References

Obtain the actual source IP addresses of requests

4.1.11. Website configurations in an XML file

You can export, modify, or import multiple website configurations at a time by using an XML file. This topic describes how to configure a website in an XML file.

Parameters

The website configurations in an XML file start with the `<DomainList>` tag, end with the `</DomainList>` tag, and include the parameters for multiple websites between the <DomainList> tag pair. The configurations for each website start with the `<DomainConfig>` tag, ends with the `</DomainConfig>` tag, and include parameters for each website between the <DomainConfig> tag pair.

Note An extra tag pair `<DomainConfig>..... </DomainConfig>` is required for each additional website configuration.

Parameter	Description
`<Domain>example.aliyundoc.com</Domain>`	The domain name that you want to associate with an Anti-DDoS Pro or Anti-DDoS Premium instance. You can enter only one domain name in a tag pair.
`<ProtocolConfig> <ProtocolList>http,https</ProtocolList> </ProtocolConfig>`	The protocol type of the domain name. You can separate multiple protocol types with commas (,). In this example, the protocol types of the domain name are HTTP and HTTPS.
`<InstanceConfig> <InstanceList>ddoscoo-cn-xxxxxxxxx001</InstanceList> </InstanceConfig>`	The instances that you want to associate with the domain name. **Note** Each instance has a unique ID. Enter the instance IDs between the <InstanceList> tag pair. Separate multiple instance IDs with commas (,).
`<RealServerConfig> <ServerType>0</ServerType> <ServerList>192.0.XX.XX</ServerList> </RealServerConfig>`	The information of the origin server. The configurations include the following parameters: • `<ServerType>0</ServerType>`: identifies origin servers by using IP addresses. • `<ServerType>1</ServerType>`: identifies origin servers by using domain names. `<ServerList>192.0.XX.XX</ServerList>`: the addresses of the origin server. Separate multiple addresses with commas (,) **Note** To associate the domain name of an origin server with an instance, you can use either the IP address or the domain name of an origin server.

Example

```
<DomainList>
 <DomainConfig>
 <Domain>example.aliyundoc.com</Domain>
 <ProtocolConfig>
 <ProtocolList>http,https</ProtocolList>
 </ProtocolConfig>
 <InstanceConfig>
 <InstanceList>ddoscoo-cn-xxxxxxxxx001</InstanceList>
 </InstanceConfig>
 <RealServerConfig>
 <ServerType>0</ServerType>
 <ServerList>192.0.XX.XX</ServerList>
 </RealServerConfig>
 </DomainConfig>
 <DomainConfig>
 <Domain>demo.aliyundoc.com</Domain>
 <ProtocolConfig>
 <ProtocolList>http,websocket,websockets</ProtocolList>
 </ProtocolConfig>
 <InstanceConfig>
 <InstanceList>ddoscoo-cn-xxxxxxxxx002,ddoscoo-cn-xxxxxxxxx00d</InstanceList>
 </InstanceConfig>
 <RealServerConfig>
 <ServerType>1</ServerType>
 <ServerList>learn.aliyundoc.com</ServerList>
 </RealServerConfig>
 </DomainConfig>
 </DomainList>
```

In this example, the following website configurations are added:

- The domain name is example.aliyundoc.com. The protocols are HTTP and HTTPS. The associated instance is ddoscoo-cn-xxxxxxxxx001. The IP address of the origin server is 192.0.XX.XX.
- The domain name is demo.aliyundoc.com. The protocols are HTTP, WebSocket, and WebSockets. The associated instances are ddoscoo-cn-xxxxxxxxx002 and ddoscoo-cn-xxxxxxxxx00dddoscoo-cn-xxxxxxxxx001. The domain name of the origin server is learn.aliyundoc.com.

4.1.12. Use the CNAME reuse feature

If you want to add multiple domain names that are hosted by the same server to an Anti-DDoS Premium instance, we recommend that you apply for the CNAME reuse feature. This feature allows you to configure the instance only once and map multiple domain names hosted by the same server to the CNAME that is assigned by Anti-DDoS Premium.

After CNAME reuse is enabled, you can modify the CNAME to map the domain names hosted by the same server to the CNAME assigned by Anti-DDoS Premium. This way, all the domain names are added to Anti-DDoS Premium.

Prerequisites

A is submitted to apply for CNAME reuse. In this topic, CNAME reuse is enabled.

> **Note** Only Anti-DDoS Premium supports CNAME reuse. Anti-DDoS Pro does not support CNAME reuse.

Scenarios

CNAME reuse is suitable for the following scenarios:

- Customers, such as agents, independent software vendors (ISVs), or distributors, want to add a large number of domain names to an Anti-DDoS Premium instance. Most of the domain names are hosted by the same server, and the number of domain names frequently changes.
- Multiple second-level domain names are required for the promotion and search engine optimization (SEO) of the same service.
- Multiple alternative domain names are required for a service.

Limits

The following table describes the limits of CNAME reuse.

Item	Description
Protocol	HTTP and HTTPS are supported. **Note** If you add domain names by using HTTPS, all the domain names that are mapped to the same CNAME share an SSL certificate after CNAME reuse is enabled.
Origin server	Domain names that are mapped to the same CNAME must be hosted by the same origin server.

Enable CNAME reuse

You can use CNAME reuse along with Sec-Traffic Manager. When you enable CNAME reuse, you can determine whether to use Sec-Traffic Manager. For more information about Sec-Traffic Manager, see Overview.

- If you use Sec-Traffic Manager, you must select a general interaction rule. Then, the CNAME configured in the rule is reused to resolve a domain name.
- If you do not use Sec-Traffic Manager, the CNAME assigned by Anti-DDoS Premium is reused to resolve a domain name.

The configuration descriptions in this topic are based on the following assumptions:

- The origin server has two IP addresses: 192.XX.XX.1 and 192.XX.XX.2.
- IP address 192.XX.XX.1 hosts three domain names: a.example, b.example, and c.example.

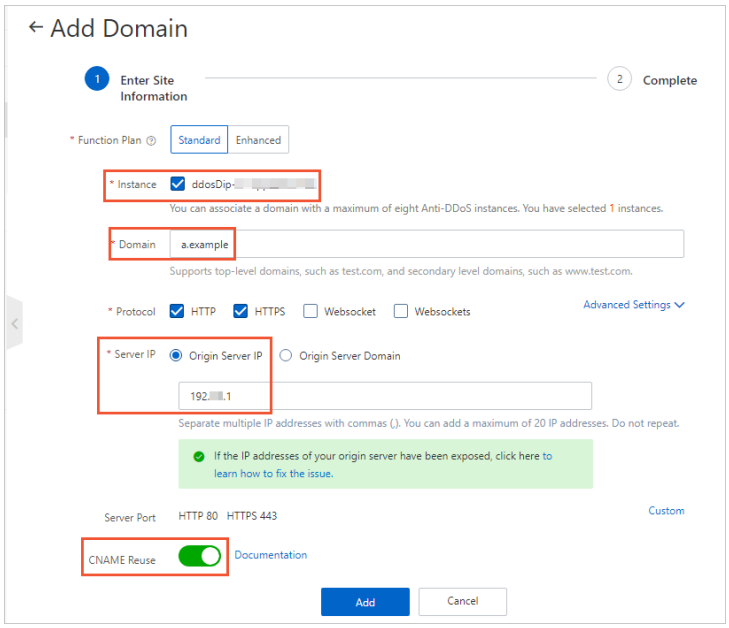
The following procedure describes how to use CNAME reuse to add multiple domain names, such as a.example, b.example, and c.example that are hosted on the IP address 192.XX.XX.1, to an Anti-DDoS Premium instance.

1. Enable CNAME reuse when you configure a website.
   i. Log on to the Anti-DDoS Pro console.
   ii. In the top navigation bar, select **Outside Mainland China**.

iii. In the left-side navigation pane, choose **Provisioning > Website Config**.

iv. Add a domain name and enable CNAME reuse, or enable this feature for an existing domain name. For more information about how to add a domain name, see Add a website.

In the example, the IP address of the origin server is 192.XX.XX.1, and the domain name is a.example.

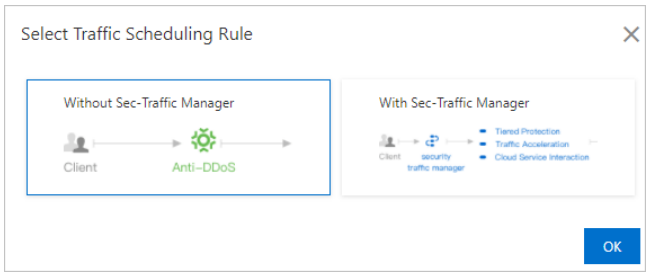


2. Specify whether to use Sec-Traffic Manager. Update the CNAME of the protected domain name.

When you enable CNAME reuse, you must determine whether to use Sec-Traffic Manager.

- Enable CNAME reuse without Sec-Traffic Manager

a. In the **Select Traffic Scheduling Rule** dialog box, click **Without Sec-Traffic Manager** and then **OK**.

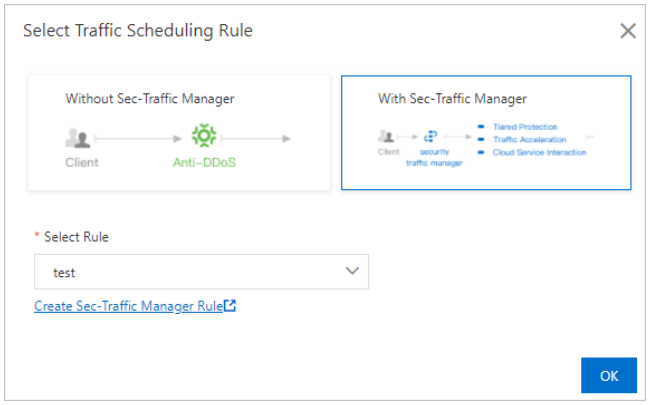


b. After a domain name is added, record the CNAME assigned for the domain name.

c. In the console of the DNS provider, update the DNS records for all the domain names that are hosted on the IP address 192.XX.XX.1. The domain names are a.example, b.example, and c.example. Then, create a CNAME and set the record value of the CNAME to that recorded in the previous step.

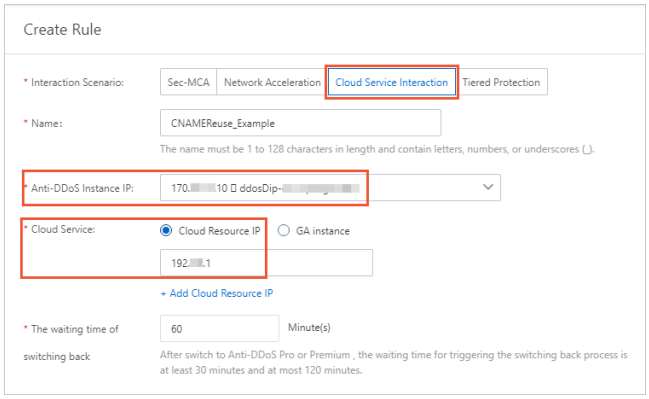
- Enable CNAME reuse with Sec-Traffic Manager

a. In the **Select Traffic Scheduling Rule** dialog box, click **With Sec-Traffic Manager**, select a Sec-Traffic Manager rule, and then click **OK**.



If you enable CNAME reuse with Sec-Traffic Manager, the Sec-Traffic Manager rule must be associated with the IP address of the origin server and the IP address of the Anti-DDoS Premium instance used in the website configuration. In the example, the IP address of the origin server is 192.XX.XX.1. If no rules are available, click **Create Sec-Traffic Manager Rule** to create a rule. Then, apply the rule.

> **Notice** The IP address of the Anti-DDoS Premium instance in the Sec-Traffic Manager rule must be the same as that used in the website configuration.



b. After you select a Sec-Traffic Manager rule, record the CNAME of the rule.

c. In the console of the DNS provider, update the DNS records for all the domain names that are hosted on the IP address 192.XX.XX.1. The domain names are a.example, b.example, and c.example. Then, create a CNAME and set the record value of the CNAME to that recorded in the previous step.

3. (Optional)To add domain names that are hosted on another IP address of the origin server (192.XX.XX.2), repeat Step 1 and Step 2.

Disable CNAME reuse

You can disable CNAME reuse on the Website Config page.

Warning Before you disable this feature, make sure that the service traffic of all the domain names mapped to the CNAME is no longer rerouted to your Anti-DDoS Premium instance. Otherwise, the inbound traffic cannot be forwarded to the origin server.

1.
2. In the top navigation bar, select **Outside Mainland China**.
3.
4. Find the required domain, click **Edit** in the Actions column, and then disable CNAME reuse.
5. Specify whether to retain the website configuration or the Sec-Traffic Manager rule.
   - If you retain the website configuration, the traffic forwarding rules still take effect.
   - If you retain the Sec-Traffic Manager rule, Sec-Traffic Manager still takes effect.

4.2. Use ports

4.2.1. Create forwarding rules

To use Anti-DDoS Pro or Anti-DDoS Premium to protect your non-website services, such as client-based games, mobile games, or apps, you must create forwarding rules on the Port Config page. You can configure DDoS mitigation settings for the forwarding rules that are created for Layer 4 services on the Port Config page. DDoS mitigation settings include session persistence, health check, and DDoS mitigation policies.

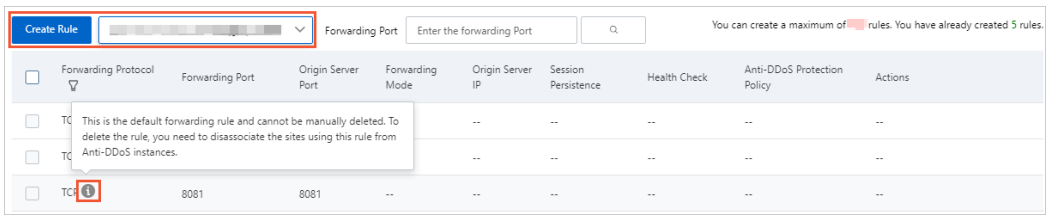
Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased. For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

Create a forwarding rule

1.
2.
3.
4. On the **Port Config** page, select the instance that you want to manage and click **Create Rule**.

Note You can also create more than one forwarding rule at a time. For more information, see Create multiple forwarding rules at a time.



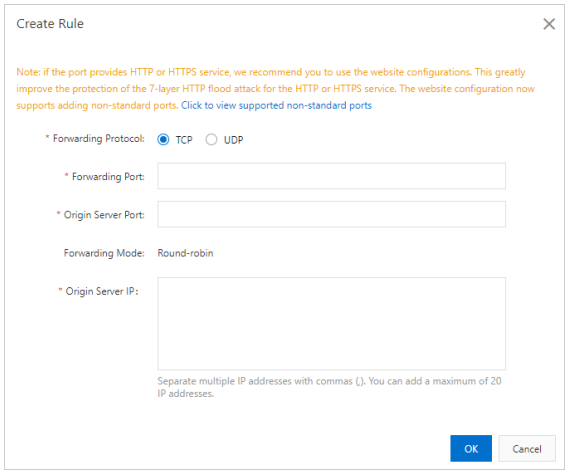
If the icon is displayed next to a protocol in the **Forwarding Protocol** column of a forwarding rule, the forwarding rule was automatically generated when you added a website. This forwarding rule is used to forward the traffic of website services. For more information about how to add a website, see Add a website.

- If you specify port 80 for the origin server when you add a domain name to your instance, Anti-DDoS Pro or Anti-DDoS Premium automatically generates a forwarding rule. This forwarding rule is used to forward TCP traffic to the origin server over port 80.
- If you specify port 443 for the origin server when you add a domain name to your instance, Anti-DDoS Pro or Anti-DDoS Premium automatically generates a forwarding rule. This forwarding rule is used to forward TCP traffic to the origin server over port 443.

If Anti-DDoS Pro and Anti-DDoS Premium automatically generate the preceding forwarding rules when you add another website, Anti-DDoS Pro and Anti-DDoS Premium do not generate the forwarding rules again.

> **Note** You cannot edit or delete rules that are automatically generated. If the websites that use these rules are disassociated from your instance, the rules are automatically deleted.

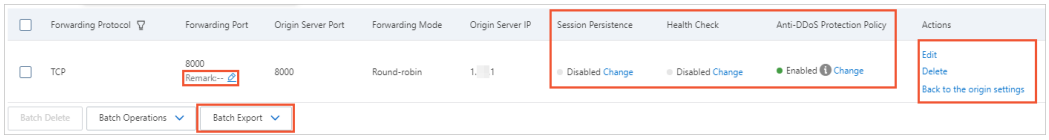
5. In the **Create Rule** dialog box, configure the parameters and click **OK**.



Parameter	Description
Forwarding Protocol	The protocol that you want to use to forward traffic. Valid values: **TCP** and **UDP**.

Parameter	Description
Forwarding Port	The port that you want to use to forward traffic. **Note** ◦ We recommend that you specify the same value for both **Forwarding Port** and **Origin Server Port**. ◦ To prevent domain owners from creating their own DNS servers, Anti-DDoS Pro and Anti-DDoS Premium do not protect services that use port 53. ◦ You cannot specify a port that is in use. For an instance, forwarding rules that use the same protocol must use different forwarding ports. If you attempt to create a rule with a protocol and forwarding port that are configured for another rule, an error message indicating that these rules overlap appears. Make sure that the rule you want to create does not conflict with the forwarding rules automatically generated when you add a website to your instance. For more information, see Website forwarding rules.
Origin Server Port	The port of the origin server.
Origin Server IP	The IP address of the origin server. **Note** You can specify a maximum of 20 origin IP addresses to implement load balancing. Separate multiple IP addresses with commas (,).

After a forwarding rule is created, you can view the rule in the forwarding rule list and perform the following operations on the rule:



- Add **remarks**: Click the

  icon in the **Forwarding Port** column to add remarks for the forwarding rule. You can identify the use scenarios and functionality of different forwarding rules based on the remarks.
- Enable **session persistence** and **health check** or configure **DDoS mitigation policies**.

  For more information, see Configure port forwarding and DDoS mitigation policies.
- Edit or delete rules.

  For more information, see Edit forwarding rules and Delete forwarding rules.
- Modify **back-to-origin settings** to enable the origin redundancy feature for a port forwarding rule. This feature enables Anti-DDoS Pro and Anti-DDoS Premium to deliver higher disaster

recovery (DR) capabilities of back-to-origin links.

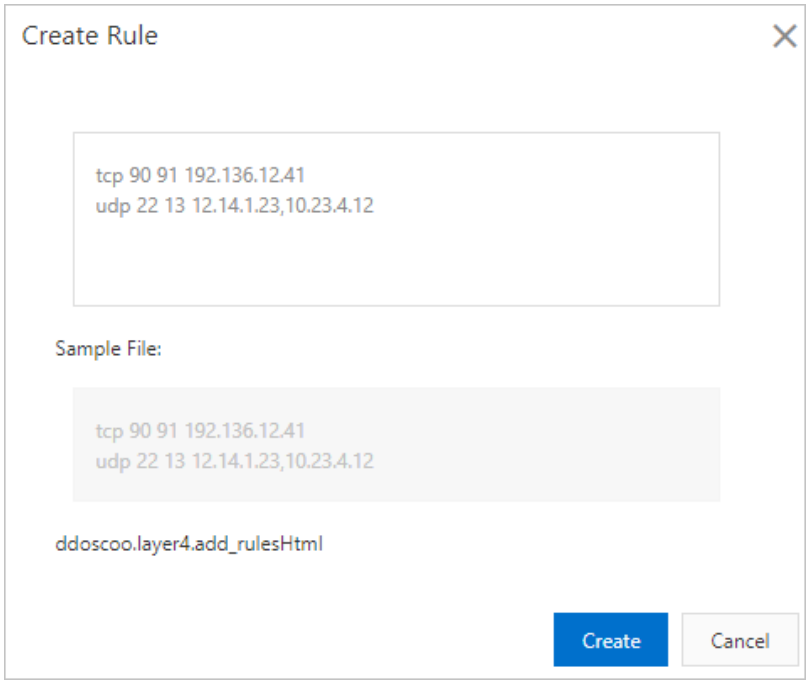
For more information, see Modify the back-to-origin settings for a port.

- Export multiple forwarding rules and mitigation settings at a time.

  For more information, see Export multiple port configurations.

Create multiple forwarding rules at a time

1.
2.
3.
4. On the **Port Config** page, select the instance that you want to manage and choose **Batch Operations > Create Rule**.
5. In the **Create Rule** dialog box, enter the required information as shown in the sample file and click **OK**.

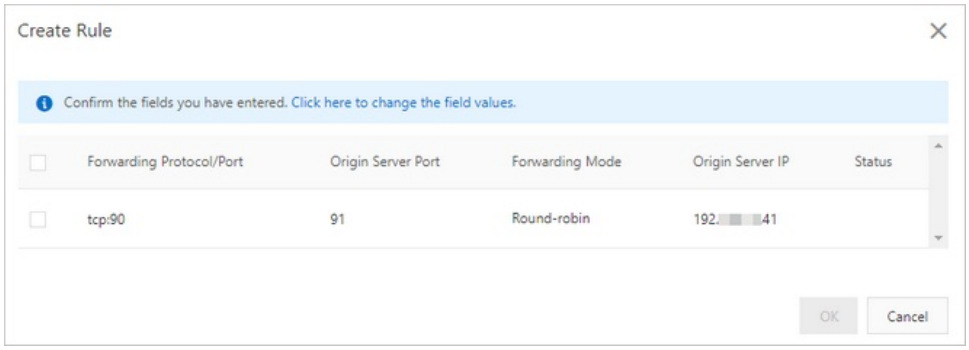


Take note of the following items when you enter the information:

- Each line represents a rule.
- From left to right, the fields in each rule indicate the following information: traffic protocol, forwarding port, origin server port, and origin IP address. Fields are separated by spaces.

  For more information about the fields, see Rule parameters.

6. Check the information that you entered, select the rules that you want to create, and then click **OK**.



7. After the rules are uploaded, close the **Create Rule** dialog box.

What to do next

After you create forwarding rules, you must perform the following operations to enable your instance to protect your non-website services.

1. Allow the back-to-origin IP address of your instance on the origin server. This way, the traffic from your instance is allowed by the security software on your origin server.

   For more information, see Allow back-to-origin IP addresses to access the origin server.

2. Verify that the forwarding rules are in effect on your computer to prevent service exceptions caused by invalid forwarding rule configurations.

   For more information, see Verify the forwarding configurations on your local computer.

   > **Warning** If you switch your service traffic to your instance before the forwarding rules take effect, your services may be interrupted.

3. Switch the traffic of your non-website services to your instance by using one of the following methods:
   - If your service is reachable over an IP address, replace the service IP address with the exclusive IP address of your instance.

     > **Note** The method to replace the IP address varies based on your platform.

   - If your service is also reachable over a domain name, such as example.com, that functions as the server address or is added to a client program, change the A record at the DNS provider of the domain name to redirect the traffic to the exclusive IP address of your instance.

     For more information, see Change the DNS record.

4.2.2. Verify the forwarding configurations on your local computer

After you add a domain name or a port to an Anti-DDoS Pro or Anti-DDoS Premium instance, Anti-DDoS Pro or Anti-DDoS Premium forwards the packets received by the port to the port of the origin server. To ensure service stability, we recommend that you verify whether the forwarding configurations take effect on your computer before the inbound traffic is rerouted to Anti-DDoS Pro or Anti-DDoS Premium. This topic describes how to verify the configurations.

Prerequisites

- A website or port is added to an Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see Add a website and Create forwarding rules.
- The back-to-origin CIDR blocks of the Anti-DDoS Pro or Anti-DDoS Premium instance are added to the whitelist of the origin server. For more information, see Allow back-to-origin IP addresses to access the origin server.

Context

To protect a service that is accessed by using a domain name instead of an IP address, you must add a website to Anti-DDoS Pro or Anti-DDoS Premium. After you add a website, you can modify the hosts file or use the CNAME of the Anti-DDoS Pro or Anti-DDoS Premium instance to connect to the server and check whether the forwarding configurations take effect.

Requests to access Layer 4 services, such as games, are processed by using IP addresses instead of domain names. You must add port forwarding rules to Anti-DDoS Pro or Anti-DDoS Premium to protect these services. Then, you can verify the forwarding configurations by using the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance to access the server.

Notice If you switch your service traffic to Anti-DDoS Pro or Anti-DDoS Premium before the forwarding configurations take effect, your service may be interrupted.

Modify the local hosts file

1. Modify the hosts file to reroute the inbound traffic of the protected website to Anti-DDoS Pro or Anti-DDoS Premium. The following procedure shows how to modify the hosts file on a Windows server.
   i. Find the hosts file, which is typically stored in *C:\Windows\System32\drivers\etc*.
   ii. Open the hosts file by using a text editor.
   iii. Add both `the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance and the protected domain name` at the end of the file.
   For example, if the IP address of the instance is `180.173.XX.XX` and the domain name is `demo.aliyundoc.com`, you must add `180.173.XX.XX demo.aliyundoc.com` at the end of the file.
   iv. Save the file.
2. Ping the protected domain name from your computer.
   If the command output includes the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance in the hosts file, the modification takes effect as expected. If the command output includes the IP address of the origin server, refresh the local DNS cache by running `ipconfig/flushdns` in Command Prompt.
3. After you verify that the protected domain name is resolved to the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance, try to access the service by using the domain name. If you can access the service, the configurations take effect.

Use the CNAME assigned by Anti-DDoS Pro or Anti-DDoS Premium to access the origin server

If the client allows you to enter the domain name of the origin server, replace the domain name with the CNAME assigned by Anti-DDoS Pro or Anti-DDoS Premium and check whether the origin server is accessible.

> **Note** After you add a domain name for protection, Anti-DDoS Pro or Anti-DDoS Premium assigns a CNAME to the domain name. You can view the CNAME on the Website Config page.

If the origin server is unaccessible, check whether the prerequisites are met. If the error persists, contact Alibaba Cloud technical support.

Use the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance to access the origin server

Assume that the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance is 99.99.XX.XX, the forwarding port is 1234, the IP address of the origin server is 11.11.XX.XX, and the port of the origin server is 1234.

You can use telnet commands to access the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance over port 1234. If the IP address is accessible, the forwarding rule takes effect.

If the client allows you to enter the IP address of the origin server, you can enter the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance for verification.

4.2.3. Modify the back-to-origin settings for a port

You can configure back-to-origin settings to enable the origin redundancy feature for a port forwarding rule. This feature improves the disaster recovery (DR) capabilities of back-to-origin links for Anti-DDoS Pro and Anti-DDoS Premium.

Prerequisites

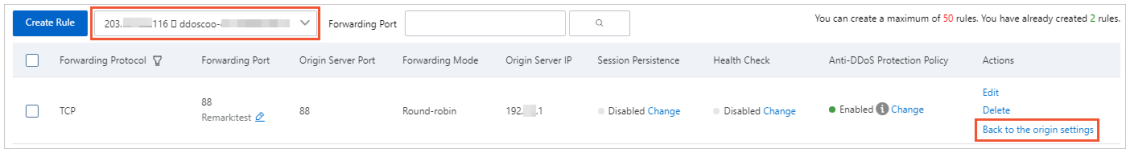
A port forwarding rule is created. For more information, see Create forwarding rules.

Context

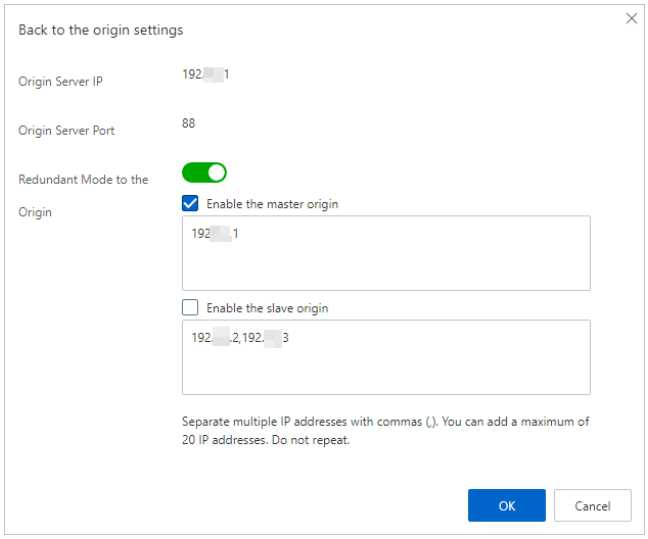
Origin redundancy allows you to configure the IP addresses of both the primary and secondary origin servers. You can specify whether to forward back-to-origin requests to the primary origin server or secondary origin server at any time. This way, your Anti-DDoS Pro or Anti-DDoS Premium instance forwards service traffic to the origin server that you specified. If a back-to-origin link fails, you can quickly switch service traffic to the backup link to ensure normal service access.

Enable origin redundancy

1.
2.
3.
4. On the page that appears, select the instance that you want to manage.
5. Find the forwarding rule for which you want to enable origin redundancy and click **Back to the origin settings** in the **Actions** column.



6. In the **Back to the origin settings** dialog box, turn on **Redundant Mode to the Origin**.



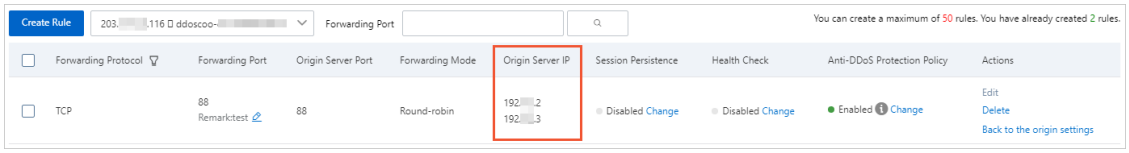
   i. In the **Note** message, click **OK**.
   When you enable origin redundancy, the current origin IP address of the forwarding rule is automatically used as the IP address of the primary origin server, and service traffic is forwarded to the primary origin server.

   ii. Configure the IP addresses for the primary and secondary origin servers and select the origin server that you want to enable.

   You can configure a maximum of 20 IP addresses for each origin server. Separate multiple IP addresses with commas (,).

   iii. Click **OK**.

After you enable origin redundancy, the value of **Origin Server IP** that you specified for the forwarding rule is changed to the IP address of the origin server that you enabled. When the origin IP address of the forwarding rule is changed to the IP address of the origin server that you enabled, you can no longer modify the forwarding rule to change the origin IP address.



If you want to switch between the origin servers, you need only to modify the back-to-origin settings of the forwarding rule to select the origin server that you want to enable.

Disable origin redundancy

If you no longer need origin redundancy, you can turn off **Redundant Mode to the Origin** in the **Back to the origin settings** dialog box. For more information, see Enable origin redundancy.

> **Note** After you disable origin redundancy, the IP address of the origin server that you enabled is automatically used as the origin IP address of the forwarding rule. For example, if the secondary origin server is enabled and you disable origin redundancy, the IP address of the secondary origin server is automatically used as the origin IP address of the forwarding rule to forward service traffic.

After you disable origin redundancy, you can modify the forwarding rule to change the origin IP address of the forwarding rule. For more information, see Edit forwarding rules.

4.2.4. Edit forwarding rules

You can edit forwarding rules and change the origin server IP addresses in the rules. This topic describes how to edit one or more forwarding rules.

Prerequisites

Forwarding rules are created for your Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see Create forwarding rules.

Limits

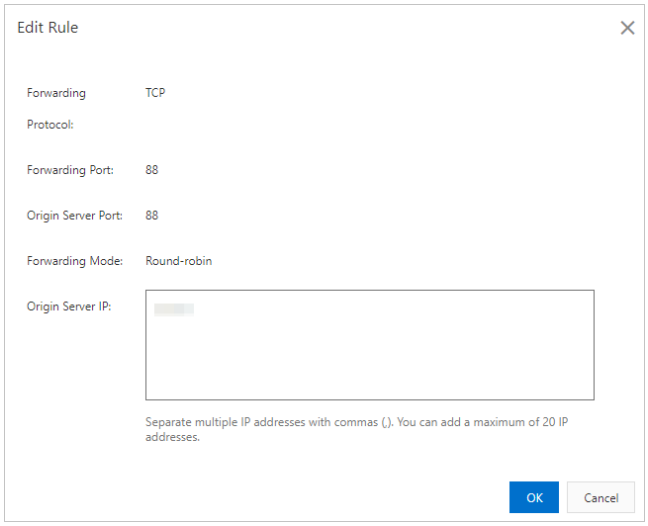
- You can change the IP addresses of origin servers only for forwarding rules that are manually created. Automatically generated rules do not support this operation.
- If the forwarding protocol and port of a rule are changed, we recommend that you create a forwarding rule.

Edit a forwarding rule

1.
2.
3.
4. On the **Port Config** page, select the instance that you want to manage.
5. Find the rule that you want to edit, and click **Edit** in the Actions column.

   > **Note** If you use an Anti-DDoS Pro instance, you can edit more than one rule at a time. For more information, see Edit more than one forwarding rule at a time.

6. In the **Edit Rule** dialog box, change the value of **Origin Server IP** and click **OK**.

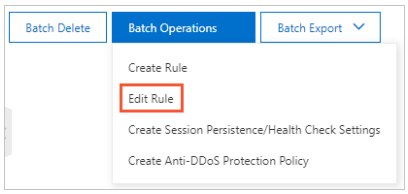


After you change the IP addresses of the origin servers, Anti-DDoS Pro or Anti-DDoS Premium forwards traffic based on the new rule.

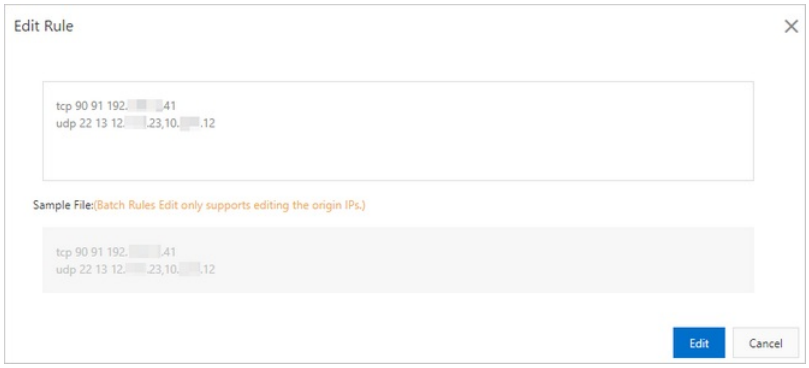
Edit more than one forwarding rule at a time

Note Only Anti-DDoS Pro allows you to edit more than one forwarding rule at a time. When you modify more than one rule, you can change only the IP addresses of the origin servers.

1.
2.
3.
4. On the **Port Config** page, select the instance that you want to manage and choose **Batch Operations > Edit Rule**.



5. In the **Edit Rule** dialog box, enter the information as shown in the sample file and click **OK**.



You can create a rule based on the following requirements.

- Each line represents a rule.
- From left to right, the fields in each rule indicate the following parameters: forwarding protocol,

forwarding port, origin server port, and IP address of the origin server. Fields are separated by spaces. For more information about the parameters, see Rule parameters.

6. Confirm the entered information, select the rules that you want to apply, and then click **OK**.
7. Close the **Edit Rule** dialog box.

4.2.5. Delete forwarding rules

You can delete manually created forwarding rules that are no longer required. Before this operation, ensure that inbound traffic is no longer rerouted to Anti-DDoS Pro or Anti-DDoS Premium instances. If you delete a forwarding rule before you restore the IP address of your service from that of your Anti-DDoS Pro or Anti-DDoS Premium instance to the actual IP address, your service may be interrupted.

Prerequisites

The IP address of your service is restored from that of your Anti-DDoS Pro or Anti-DDoS Premium instance to the actual IP address.

Procedure

1.
2.
3.
4. On the **Port Config** page, select the instance that you want to manage.
5. Find the rule that you want to delete and click **Delete** in the Actions column.

> **Note** To delete multiple rules at a time, select the rules and click **Batch Delete** below the rule list.

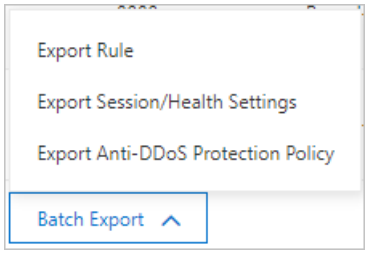
6. In the message that appears, click **OK**.

4.2.6. Export multiple port configurations

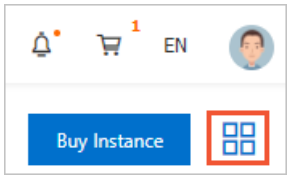
Anti-DDoS Pro and Anti-DDoS Premium allow you to export multiple port configurations at a time. You can export manually created forwarding rules, session and health check settings, and anti-DDoS protection policies under an Anti-DDoS Pro or Anti-DDoS Premium instance as a TXT file. You can also download the file to your local machine. The exported file has the same format as the file used to manage multiple rules, session and health check settings, and anti-DDoS protection policies.

Procedure

1.
2.
3.
4. On the **Port Config** page, select the target instance.
5. Below the rule list, click **Batch Export** and select **Export Rule**, **Export Session/Health Settings**, or **Export Anti-DDoS Protection Policy** as required.

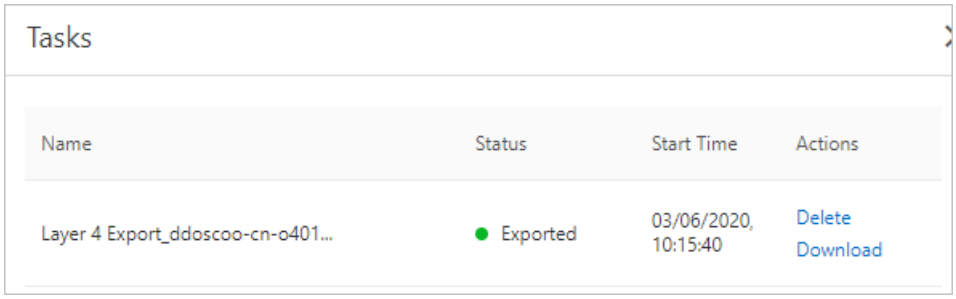


6. After the export task starts, click the Tasks icon in the upper-right corner of the page.



7. In the **Tasks** pane, click **Download** in the Actions column that corresponds to the export record after the export task is completed.

> **Note** If the task is in the **Pending Export** state, wait until the task is completed.



After the exported file is downloaded to your local machine, you can open the TXT file to view the rules or settings. For more information about the format in the TXT file, see The format of content in the files.

8. (Optional)In the **Tasks** pane, find the task that you want to delete and click **Delete** in the Actions column.

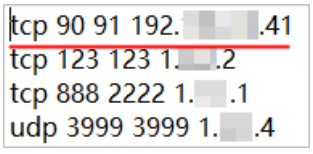
The format of content in the files

All exported files are in TXT format. The format in the files varies with the exported content.

> **Note** If you use Anti-DDoS Pro, the name of the exported file starts with *DDoSCoo_*. If you use Anti-DDoS Premium, the name of the exported file starts with *DDoSDip_*. The formats of the files exported from the Anti-DDoS Pro and Anti-DDoS Premium consoles are the same.

- Rule files

  Each row represents a rule that contains four values. From left to right, the fields in each rule indicate the following parameters: forwarding protocol, forwarding port, origin server port, and origin server IP address.



For more information, see Create forwarding rules.

- Files of session and health check settings

  Each row represents a rule. From left to right, the fields in each rule indicate the following parameters: forwarding port, forwarding protocol, session persistence timeout, health check type, port, response timeout period, check interval, unhealthy threshold, healthy threshold, path, and domain. If the value of session persistence timeout is 0, session persistence is disabled. If no value is specified for the health check type, the health check is disabled, and the values that follow the parameter are left blank. The values of path and domain are only provided for HTTP-based health checks.

  ```
  90 tcp 0
  123 tcp 0
  888 tcp 0
  8080 tcp 400 http 22 5 5 3 3 /search.php example.com
  ```

  For more information, see Configure session persistence.

- Files of anti-DDoS protection policies

  Each row represents a rule. From left to right, the fields in each rule indicate the following parameters: forwarding port, forwarding protocol, source new connection rate limit, source concurrent connection rate limit, destination new connection rate limit, destination concurrent connection rate limit, minimum packet length, maximum packet length, and false source and empty connection. The value of the last field applies only when TCP is used. You must turn on False Source before you turn on Empty Connection.

  ```
  90 tcp 20000 50000 0 0 1 6000 on off
  123 tcp 0 0 100000 0 0 6000 on on
  888 tcp 20000 0 0 0 0 6000 on off
  8080 tcp 1 1 100 1000 0 6000 on off
  ```

  For more information, see Create anti-DDoS protection policies for multiple port forwarding rules at a time.

4.2.7. Configure a health check

Anti-DDoS Pro and Anti-DDoS Premium provide Layer 4 and Layer 7 health checks for protected non-website services. The health check feature is suitable for services that have more than one origin server IP address. This feature is used to check the availability of the backend servers. After you add a port forwarding rule to Anti-DDoS Pro or Anti-DDoS Premium, you can enable the health check feature for the forwarding rule.

Prerequisites

- A port forwarding rule for a non-website service is configured on the Port Config page.

  For more information, see Create forwarding rules.

- The IP addresses of origin servers are configured in the port forwarding rule.

  > **Notice** If you configure only one IP address of the origin server in a port forwarding rule, we recommend that you do not enable the health check feature.

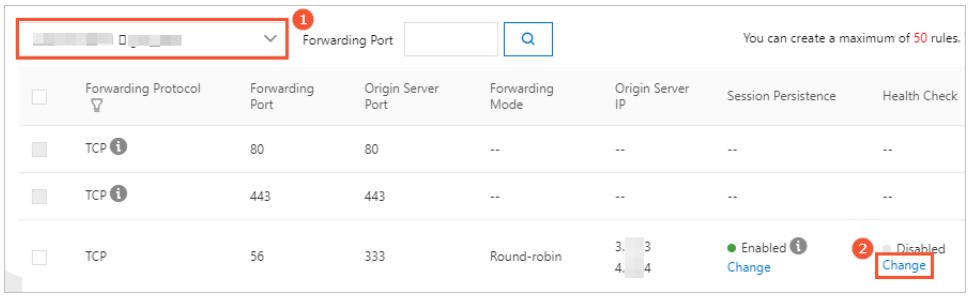
Context

The health check feature is suitable for services that have more than one origin server IP address. When Anti-DDoS Pro or Anti-DDoS Premium forwards traffic to backend servers, this feature verifies the availability of the backend servers. Therefore, traffic is forwarded to healthy backend servers to ensure that the services properly run. For more information, see Health check overview.

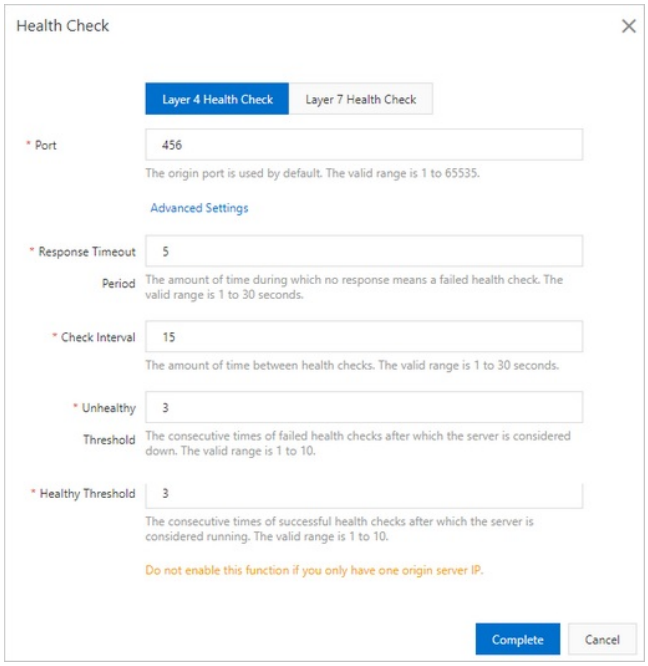
Enable the health check feature

1.
2.
3.
4. On the **Port Config** page, select the instance, find the forwarding rule that you want to manage, and then click **Change** in the **Health Check** column.

> **Note** To configure the health check feature for more than one forwarding rule at a time, you can select the rules and choose Batch Operations > Create Session Persistence/Health Check Settings. For more information, see Configure session persistence and health checks for more than one forwarding rule.



5. In the **Health Check** dialog box, configure the parameters and click **Complete**.



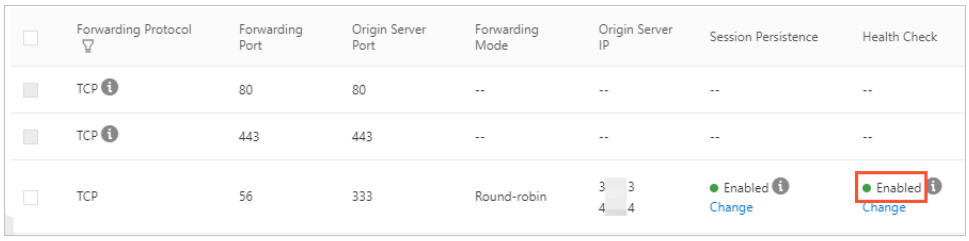
Anti-DDoS Pro or Anti-DDoS Premium allows you to configure Layer 4 and Layer 7 health checks. The following table describes the parameters.

> **Note** You can configure advanced options for Layer 4 and Layer 7 health checks. You must click **Advanced Settings** to show advanced options. We recommend that you do not modify the advanced options.

Type	Parameter	Description
Layer 4 Health Check	**Port**	The port that the health check feature uses to communicate with the backend server. Valid values: 1 to 65535. By default, the backend port configured for a listener is used. **Note** The Layer 4 health check is suitable for TCP and UDP forwarding rules.
Layer 7 Health Check	**Domain** and **Path**	During a Layer 7 health check, Anti-DDoS Pro or Anti-DDoS Premium sends an HTTP HEAD request to the default homepage of the origin server. **Note** The Layer 7 health check is suitable only for TCP forwarding rules. If you do not want to use the default homepage of the origin server for health checks, you must specify a domain name and a path of the page that you want to check. If you have limited the host field for the HTTP HEAD request, you need only to specify a URI for health checks. The Domain parameter is optional. The default value is the IP address of the backend server.
	Port	The port that the health check feature uses to communicate with the backend server. Valid values: 1 to 65535. By default, the backend port configured for a listener is used.
Advanced Settings	**Response Timeout Period**	The timeout period of a health check. Valid values: 1 to 30. Unit: seconds. If the backend server does not respond within the specified timeout period, the backend server is unhealthy.
	Check Interval	The interval between two consecutive health checks. Valid values: 1 to 30. Unit: seconds. **Note** Each scrubbing node in the Anti-DDoS Pro or Anti-DDoS Premium cluster performs health checks on backend servers at the specified interval independently and concurrently. The scrubbing nodes may perform health checks on the same backend server at different points in time. Therefore, the health check records on the backend server do not indicate the time interval specified for the health check.
	Unhealthy Threshold	The number of consecutive failed health checks performed on a backend server by the same scrubbing node before the backend server is declared as unhealthy. Valid values: 1 to 10.

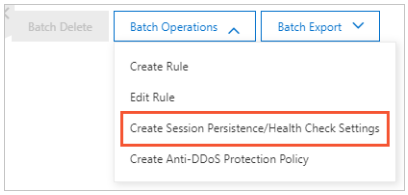
Type	Parameter	Description
	Healthy Threshold	The number of consecutive successful health checks performed on a backend server by the same scrubbing node before the backend server is declared as healthy. Valid values: 1 to 10.

After the health check feature is enabled, **Enabled** appears in the **Health Check** column for the forwarding rule.

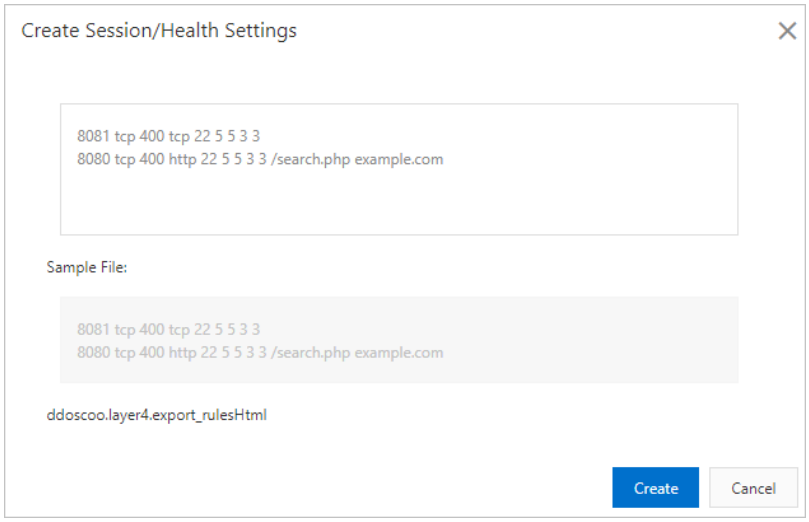


Configure session persistence and health checks for more than one forwarding rule

1.
2.
3.
4. On the **Port Config** page, select the instance that you want to manage and choose **Batch Operations > Create Session Persistence/Health Check Settings**.



5. In the **Create Session Persistence/Health Check Settings** dialog box, enter the required information as shown in the sample file and click **OK**.



> **Note** You can export health check settings to a TXT file, modify the settings in the TXT file, and then copy and paste the settings to the Create Session Persistence/Health Check Settings dialog box. For more information, see Export multiple port configurations.

The formats of session persistence and health check settings must meet the following requirements:

- Each line represents a forwarding rule.
- From left to right, the fields in each forwarding rule indicate the following parameters: forwarding port, forwarding protocol, session persistence timeout period, health check type, port, response timeout period, check interval, unhealthy threshold, healthy threshold, path, and domain name. The supported forwarding protocols are TCP, HTTP, and UDP. The session persistence timeout period is measured in seconds, and the valid value ranges from 30 to 3600. Fields are separated by spaces.
- Forwarding ports must be the ports that are specified in forwarding rules.
- If a forwarding rule uses UDP, we recommend that you configure a UDP health check. If a forwarding rule uses TCP, we recommend that you configure a TCP health check (Layer 4 health check) or HTTP health check (Layer 7 health check).
- If you configure an HTTP health check, the Path parameter is required, but the Domain parameter is optional.

4.2.8. Configure session persistence

After you add non-website services to Anti-DDoS Pro or Anti-DDoS Premium, issues such as logon timeout or disconnections may occur. In this case, you can enable the session persistence feature. This feature forwards requests from the same client to the same backend server within a specified period. This topic describes how to configure session persistence for a port forwarding rule.

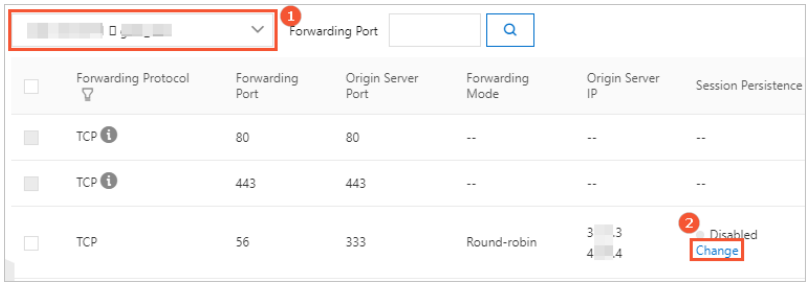
Prerequisites

A port forwarding rule for a non-website service is configured on the Port Config page. For more information, see Create forwarding rules.

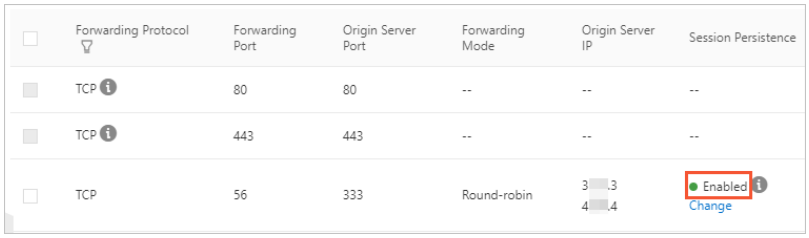
Enable session persistence

1.
2.
3.
4. On the **Port Config** page, select the instance, find the forwarding rule that you want to manage, and then click **Change** in the **Session Persistence** column.

> **Note** You can also enable session persistence for more than one forwarding rule of an instance at a time. For more information, see Configure session persistence and health checks for more than one rule at a time.

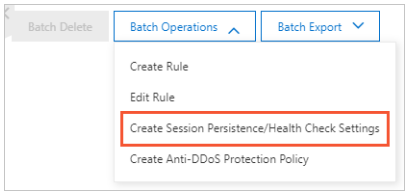


5. In the **Session Persistence** dialog box, set **Timeout Period** and click **Complete**. The timeout period is measured in seconds, and the valid value ranges from 30 to 3600.
   After the session persistence feature is enabled, the status of **Session Persistence** changes to **Enabled**.

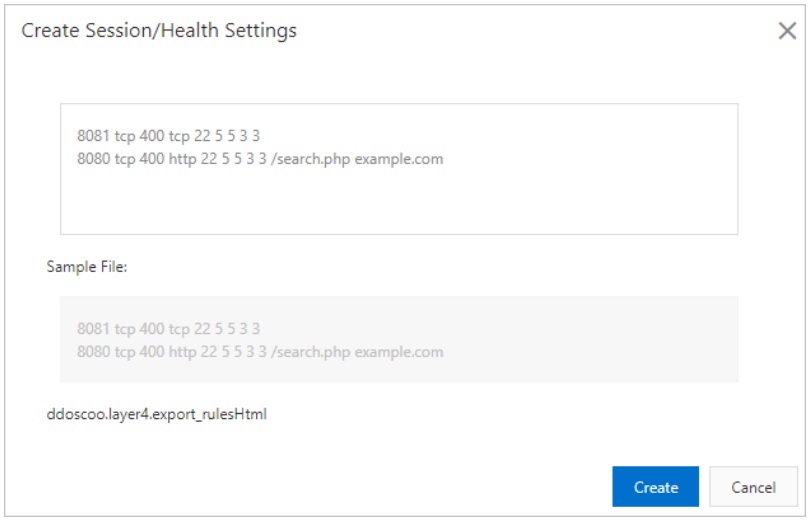


Configure session persistence and health checks for more than one forwarding rule

1.
2.
3.
4. On the **Port Config** page, select the instance that you want to manage and choose **Batch Operations > Create Session Persistence/Health Check Settings**.



5. In the **Create Session Persistence/Health Check Settings** dialog box, enter the required information as shown in the sample file and click **OK**.



Note You can export health check settings to a TXT file, modify the settings in the TXT file, and then copy and paste the settings to the Create Session Persistence/Health Check Settings dialog box. For more information, see Export multiple port configurations.

The formats of session persistence and health check settings must meet the following requirements:

- Each line represents a forwarding rule.
- From left to right, the fields in each forwarding rule indicate the following parameters: forwarding port, forwarding protocol, session persistence timeout period, health check type, port, response timeout period, check interval, unhealthy threshold, healthy threshold, path, and domain name. The supported forwarding protocols are TCP, HTTP, and UDP. The session persistence timeout period is measured in seconds, and the valid value ranges from 30 to 3600. Fields are separated by spaces.
- Forwarding ports must be the ports that are specified in forwarding rules.
- If a forwarding rule uses UDP, we recommend that you configure a UDP health check. If a forwarding rule uses TCP, we recommend that you configure a TCP health check (Layer 4 health check) or HTTP health check (Layer 7 health check).
- If you configure an HTTP health check, the Path parameter is required, but the Domain parameter is optional.

4.3. Provisioning settings

4.3.1. Change DNS records to protect website services

After you add a website to Anti-DDoS Pro or Anti-DDoS Premium, you must change the DNS records to map the domain name of the website to a CNAME that is assigned by Anti-DDoS Pro or Anti-DDoS Premium or to the IP address of an Anti-DDoS Pro or Anti-DDoS Premium instance. This way, the traffic that is destined for the website is redirected to Anti-DDoS Pro or Anti-DDoS Premium for protection. This topic describes how to change the DNS records of a website. DNS records can be CNAME or A records. In this example, the DNS resolution service is provided by the free edition of Alibaba Cloud DNS.

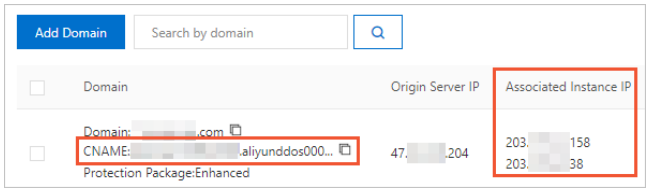
Prerequisites

- A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.
- The back-to-origin IP addresses of the Anti-DDoS Pro or Anti-DDoS Premium instance are added to the whitelist of the origin server. If you deploy third-party security software, such as a firewall, on your origin server, add the back-to-origin IP addresses to the whitelist of the security software. For more information, see Allow back-to-origin IP addresses to access the origin server.
- The traffic forwarding settings are in effect. Before you switch service traffic to the Anti-DDoS Pro or Anti-DDoS Premium instance, we recommend that you use your local computer to verify that the instance can forward traffic to the origin server. For more information, see Verify the forwarding configurations on your local computer.

> **Warning** If you switch your service traffic to the Anti-DDoS Pro or Anti-DDoS Premium instance before the forwarding settings take effect, your service may be interrupted.

Access methods

When you change the DNS records, you can map the domain name of the website to a CNAME that is assigned by Anti-DDoS Pro or Anti-DDoS Premium or to the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance. To obtain the two addresses, you can log on to the Anti-DDoS Pro console and choose **Provisioning > Website Config**.



The following list describes the differences between the access methods that use the CNAME record and the A record:

- If you use the CNAME record, you need to change DNS records only once. If the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance changes, the instance automatically redirects traffic based on the CNAME record. If your website is associated with multiple instances, Anti-DDoS Pro or Anti-DDoS Premium automatically schedules traffic to these instances.
- If you use the A record, you must change DNS records each time the IP address of the instance changes. If your website is associated with multiple instances, you must manually schedule traffic to these instances.

We recommend that you use the CNAME record. You can use the A record only if the CNAME record is unavailable or conflicts with other DNS records.

Procedure

In the following example, your domain name is hosted on Alibaba Cloud DNS.

> **Note** Alibaba Cloud DNS provides basic DNS services free of charge. It also offers other value-added services in the paid editions. If you activated a paid edition of Alibaba Cloud DNS for your website, we recommend that you enable NS Mode Access to redirect traffic to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Enable NS Mode Access to protect a website.

If you use a third-party DNS service, log on to the system of the DNS provider to change the DNS records. The following example is only for reference.

Assume that you add the domain name `example.aliyundoc.com` to Anti-DDoS Pro or Anti-DDoS Premium. The following procedure describes how to change and add DNS records in the Alibaba Cloud DNS console.

1. Log on to the Alibaba Cloud DNS console.
2. On the **Manage DNS** page, find the domain name `aliyundoc.com` and click **Configure** in the Actions column.
3. On the **DNS Settings** page, find the A or CNAME record whose Host is **bgp** and click **Edit** in the Actions column.

   > **Note** If you cannot find the DNS record that you want to manage in the list, you can click **Add Record** to add the record.

4. In the **Add Record** or **Edit Record** panel, select a record type and change the record.
   - CNAME record: Set the **Type** parameter to **CNAME** and the **Value** parameter to the CNAME that is assigned by Anti-DDoS Pro or Anti-DDoS Premium for the domain name. This record type is recommended.

     > **Note** To obtain the CNAME, log on to the Anti-DDoS Pro console and choose **Provisioning > Website Config**.

   - A record: Set the **Type** parameter to **A** and the **Value** parameter to the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance with which the domain name is associated.

     > **Note** To obtain the IP address, log on to the Anti-DDoS Pro console and choose **Provisioning > Website Config**.

5. Click **Confirm** and wait for the settings to take effect.
6. Check whether the website is accessible.

   If an exception occurs during website access, see How do I handle the issues of slow response, high latency, and access failure on websites that are protected by an Anti-DDoS Pro or Anti-DDoS Premium instance?.

References

After you add your website to Anti-DDoS Pro or Anti-DDoS Premium, you can perform the following operations:

- Enable Sec-Traffic Manager and configure scheduling rules between Anti-DDoS Pro or Anti-DDoS Premium and protected cloud resources. These rules trigger Anti-DDoS Pro or Anti-DDoS Premium only in specific scenarios. For more information, see Overview.
- Change the public IP address of the Elastic Compute Service (ECS) instance where your origin server resides. If the IP address of your origin server is exposed, attackers may bypass Anti-DDoS Pro or Anti-DDoS Premium to attack the origin server. To protect against this type of attack, you can change the IP address of the ECS origin server in the Anti-DDoS Pro or Anti-DDoS Premium console. For more information, see Change the public IP address of an ECS origin server.

4.3.2. Enable NS Mode Access to protect a website

After you add a website to Anti-DDoS Pro, you must modify the DNS records of your website to reroute inbound traffic to the Anti-DDoS Pro instance. If you have purchased the paid edition of Alibaba Cloud DNS service for domain name resolution, you can enable NS Mode Access to automatically modify DNS records. This topic describes how to enable NS Mode Access in the Anti-DDoS Pro console.

Prerequisites

- An Anti-DDoS Pro instance is purchased.

  > **Note** Only Anti-DDoS Pro supports NS Mode Access. If you use Anti-DDoS Premium, we recommend that you modify the DNS records of websites. For more information, see Change DNS records to protect website services.

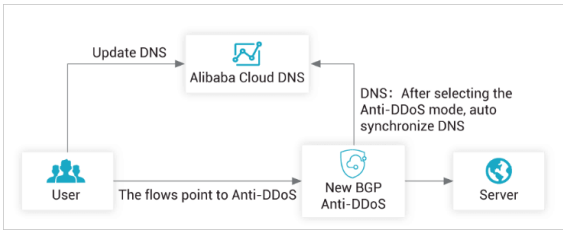
- The domain name of your website is managed by the paid edition of Alibaba Cloud DNS.
- A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.
- The back-to-origin IP addresses of the Anti-DDoS Pro or Anti-DDoS Premium instance are added to the whitelist of the origin server. If you deploy third-party security software, such as a firewall, on your origin server, add the back-to-origin IP addresses to the whitelist of the security software. For more information, see Allow back-to-origin IP addresses to access the origin server.
- The traffic forwarding settings are in effect. Before you switch service traffic to the Anti-DDoS Pro or Anti-DDoS Premium instance, we recommend that you use your local computer to verify that the instance can forward traffic to the origin server. For more information, see Verify the forwarding configurations on your local computer.

  > **Warning** If you switch your service traffic to the Anti-DDoS Pro or Anti-DDoS Premium instance before the forwarding settings take effect, your service may be interrupted.

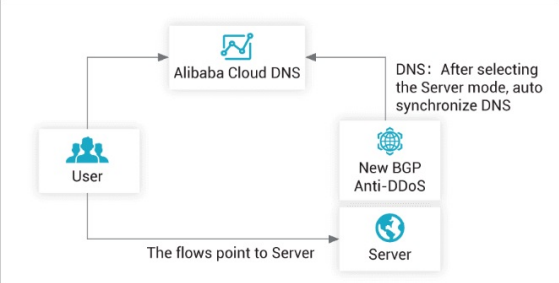
Context

After you enable NS Mode Access, Anti-DDoS Pro automatically modifies the DNS records based on the forwarding rules in the website configuration. NS Mode Access supports the following two modes:

- Anti-DDoS: enables Anti-DDoS Pro and automatically modifies DNS records to reroute inbound traffic to the Anti-DDoS Pro instance.

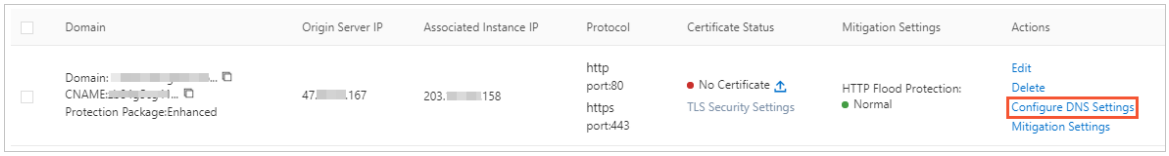
- Back-To-Source: disables Anti-DDoS Pro and forwards the traffic to the origin server.



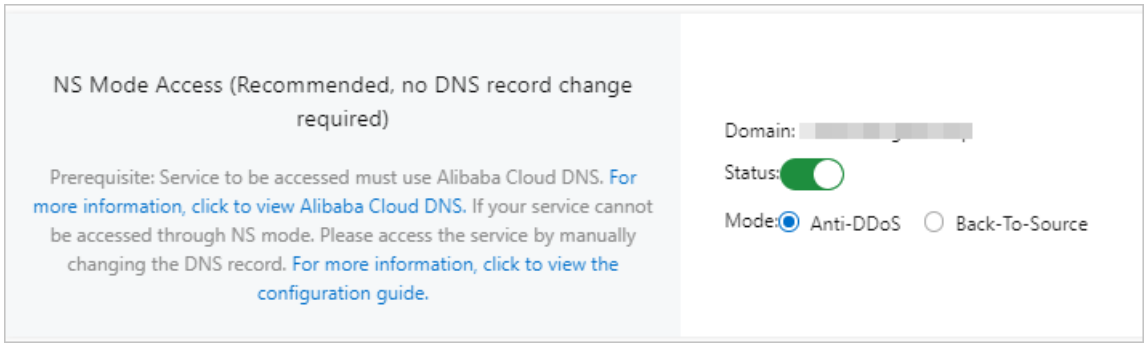
We recommend that you use the following steps to configure NS Mode Access. If the domain name of your website is managed by a third-party DNS service and cannot be migrated to Alibaba Cloud DNS, NS Mode Access is unavailable. In this case, you must manually modify the DNS records of your website. For more information, see Change DNS records to protect website services.

Procedure

1.
2. In the top navigation bar, select **Mainland China**.
3.
4. On the **Website Config** page, find the domain name whose DNS records you want to modify and click **Configure DNS Settings** in the Actions column.



5. On the **Configure DNS Settings** page, find the **NS Mode Access** section, turn on **Status**, and select **Anti-DDoS** or **Back-To-Source** as the access mode.
   - If you select the Anti-DDoS mode, Anti-DDoS Pro automatically modifies the DNS records and reroutes inbound traffic to the Anti-DDoS Pro instance.
   - If you select the Back-to-Origin mode, Anti-DDoS Pro automatically modifies the DNS records and forwards inbound traffic to the origin server.



   If you have purchased the paid edition of Alibaba Cloud DNS, you can enable this feature. If you did not purchase the paid edition of Alibaba Cloud DNS, an error message appears.
6. Wait for the settings to take effect. You can use a third-party DNS testing platform to check whether a domain name is resolved as expected.

4.3.3. Modify the CNAME record to protect a non-website service

To add a non-website service to Anti-DDoS Pro or Anti-DDoS Premium, you must create port forwarding rules and change the IP address of the service to the IP address of an Anti-DDoS Pro or Anti-DDoS Premium instance. In specific scenarios, you may need to use domain names to set up multiple Anti-DDoS Pro instances for Layer 4 services and set up an automatic mechanism to switch service traffic among these instances. In this is the case, we recommend that you add the domain names to Anti-DDoS Pro or Anti-DDoS Premium instances and then modify the CNAME records of the domain names.

Context

This example shows how to set up Anti-DDoS Pro for a gaming service whose domain is demo.aliyundoc.com, TCP ports are 1234 and 5678, and the origin server IP address is 1.1.XX.XX.

Procedure

1. Add the website that you want to protect and obtain the CNAME record assigned to the website.
   i. Log on to the Anti-DDoS Pro console.
   ii. In the top navigation bar, select the region where your server is deployed.
      - **Mainland China**: Anti-DDoS Pro
      - **Outside Mainland China**: Anti-DDoS Premium
   iii. In the left-side navigation pane, choose **Provisioning > Website Config**.
   iv. On the **Website Config** page, click **Add Domain**.
   v. On the **Add Domain** wizard, set the parameters in the **Enter Site Information** step and click **Add**.

      The parameters are described as follows:

      - **Function Plan** and **Instance**: Select the instances with which you want to associate the domain name. In this example, the domain name is associated with two instances that use the enhanced function plan.
      - **Domain**: Enter the domain name that you want to protect. In this example, the domain name is demo.aliyundoc.com.
      - **Protocol** and **Server Port**: Use the default values.
      - **Server IP**: Select **Origin Server IP** and enter the IP address of the origin server.
        - If the domain name provides website services, you must specify the actual protocol and IP address of the origin server.
        - If the domain name does not provide website services, you can enter any IP address. The user traffic is rerouted by using the port forwarding rules created in step 2.

      For more information, see Add a website.

   After you add a domain name, Anti-DDoS Pro or Anti-DDoS Premium assigns a CNAME record to the domain name.
2. Create a port forwarding rule.
   i. In the left-side navigation pane, choose **Provisioning > Port Config**.

ii. On the **Port Config** page, select the instance for which you want to create a port forwarding rule and click **Create Rule**.

> **Note** Select one of the associated instances from step 1.

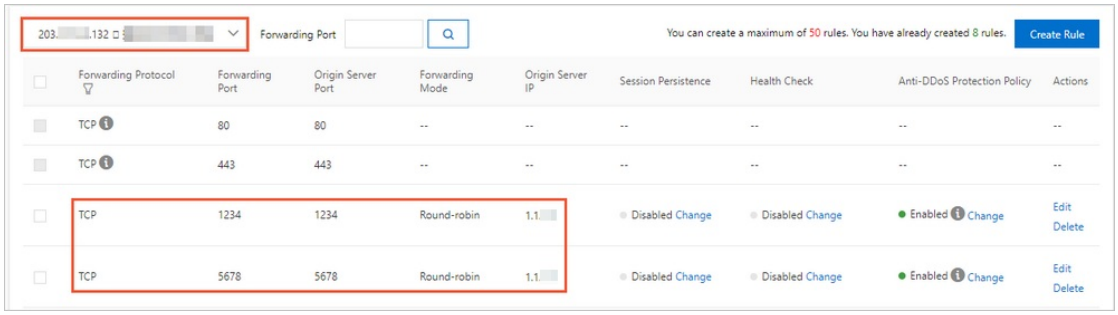
iii. In the **Create Rule** dialog box, specify the required parameters and click **Complete**.

The parameter configurations in this example are described as follows:

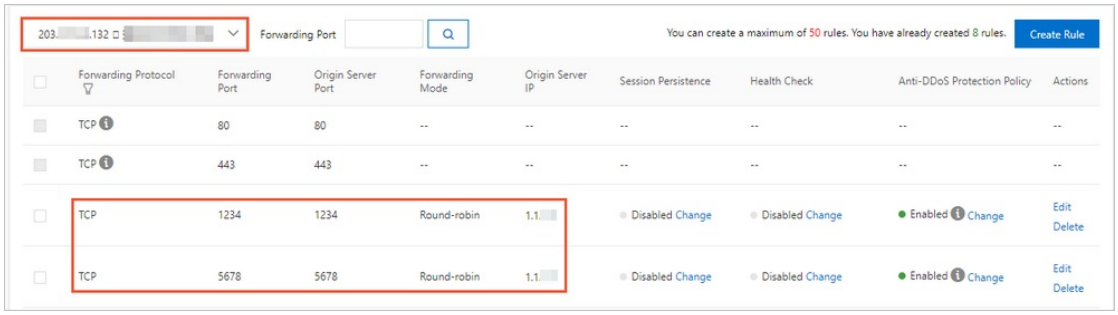
- **Forwarding Protocol**: Select TCP.
- **Forwarding Port**: Enter 1234.
- **Origin Server Port**: Enter 1234.
- **Origin Server IP**: Enter 1.1.XX.XX. This parameter specifies the IP address of the origin server.

For more information, see Create forwarding rules.

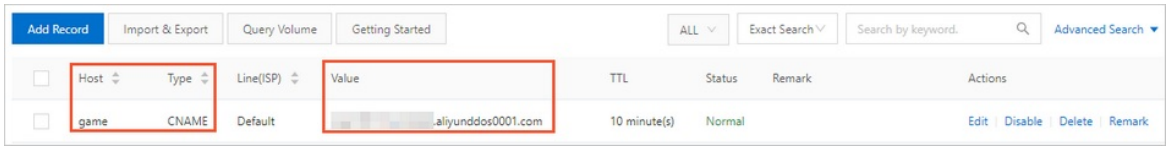
iv. Repeat the preceding two steps to create another port forwarding rule for the instance. In this rule, set both the forwarding port and origin server port to 5678.



v. Repeat the preceding three steps to create port forwarding rules for other instances.



3. Go to the DNS provider that has the domain name demo.aliyundoc.com to modify the DNS record. Use the CNAME record to map the domain name to the CNAME record obtained in step 1.



For more information, see Change DNS records to protect website services.

4.3.4. Change the CNAME record to redirect traffic to Sec-Traffic Manager

After you use Sec-Traffic Manager to create a scheduling rule for a domain name, you must change the CNAME record of the domain name to redirect traffic to Sec-Traffic Manager. The rule takes effect only after you change the CNAME record. This topic describes how to change the CNAME record of a domain name to redirect traffic to Sec-Traffic Manager. In this example, the DNS resolution service is provided by Alibaba Cloud DNS.

Prerequisites

A scheduling rule is added by using Sec-Traffic Manager. For more information, see Overview.

Context

After you add a scheduling rule by using Sec-Traffic Manager, Sec-Traffic Manager generates a CNAME. To redirect inbound traffic to Sec-Traffic Manager, you must change the CNAME record of the domain name of the website to map the domain name to the CNAME that is assigned by Sec-Traffic Manager.

In the following example, your domain name is hosted on Alibaba Cloud DNS.

If you use a third-party DNS service, log on to the system of the DNS provider to change the DNS records. The following example is only for reference.

Assume that the domain name that is specified in the scheduling rule is `aliyundoc.com`. The following procedure describes how to change and add DNS records in the Alibaba Cloud DNS console.

Procedure

1. Log on to the Alibaba Cloud DNS console.
2. On the **Manage DNS** page, find the domain name `aliyundoc.com` and click **Configure** in the Actions column.
3. On the **DNS Settings** page, find the A or CNAME record whose Host is **bgp** and click **Edit** in the Actions column.

   > **Note** If you cannot find the DNS record that you want to manage in the list, you can click **Add Record** to add the record.

4. In the **Edit Record** or **Add Record** panel, set the **Type** parameter to **CNAME** and the **Value** parameter to the CNAME that is assigned by Sec-Traffic Manager.

   To query the CNAME, log on to the Anti-DDoS Pro console and choose **Provisioning > Sec-Traffic Manager**.
5. Click **Confirm** and wait for the settings to take effect.
6. Check whether the website is accessible.

   If an exception occurs during website access, see How do I handle the issues of slow response, high latency, and access failure on websites that are protected by an Anti-DDoS Pro or Anti-DDoS Premium instance?.

4.4. Sec-Traffic Manager

4.4.1. Overview

Anti-DDoS Pro and Anti-DDoS Premium both provide Sec-Traffic Manager for you to configure rules on the interaction between them and the protected cloud services. You can configure rules for Anti-DDoS Pro or Anti-DDoS Premium. These rules take effect only in specific scenarios. This feature ensures service continuity and provides protection against distributed denial-of-service (DDoS) attacks. Sec-Traffic Manager provides features such as cloud service interaction, tiered protection, Content Delivery Network (CDN) interaction, Dynamic Route for CDN (DCDN) interaction, network acceleration, and Sec-MCA.

Scenarios

If you add your websites to Anti-DDoS Pro or Anti-DDoS Premium, you only need to add the domain names of your websites. For more information, see Add a website. If you add your non-website services to Anti-DDoS Pro or Anti-DDoS Premium, you only need to add the ports of your services. For more information, see Create forwarding rules.

After your services are added to Anti-DDoS Pro or Anti-DDoS Premium, all service traffic, including normal and malicious traffic, is forwarded to Anti-DDoS Pro or Anti-DDoS Premium. Malicious traffic is filtered out, and only normal traffic is forwarded to the origin server. During normal service access, normal traffic is also forwarded by Anti-DDoS Pro or Anti-DDoS Premium. This may cause a low latency to the service.

To resolve this issue, you can enable the cloud service interaction feature of Sec-Traffic Manager. If no attacks occur, normal traffic is directly forwarded to the origin server without increasing latency. If attacks occur, traffic is switched to Anti-DDoS Pro or Anti-DDoS Premium for scrubbing and forwarding.

In addition to the preceding scenarios, Sec-Traffic Manager enables interactions between Anti-DDoS Pro or Anti-DDoS Premium and Anti-DDoS Origin, CDN, DCDN, Mainland China Acceleration (MCA), and Sec-MCA. For more information, see Benefits.

> **Note** Anti-DDoS Pro and Anti-DDoS Premium provides Sec-Traffic Manager for you to configure rules for your service access. Whether to use Sec-Traffic Manager does not affect the billing of Anti-DDoS Pro and Anti-DDoS Premium. For more information about the billing methods of Anti-DDoS Pro and Anti-DDoS Premium, see Billing methods of Anti-DDoS Pro and Billing methods of the Insurance and Unlimited mitigation plans.

Benefits

The following table describes the interaction scenarios of Sec-Traffic Manager and related topics.

× indicates that Anti-DDoS Pro does not support this interaction scenario.

Interaction scenario	Description	Anti-DDoS Pro	Anti-DDoS Premium

Interaction scenario	Description	Anti-DDoS Pro	Anti-DDoS Premium
Cloud Service Interaction	Your services use **Alibaba Cloud public IP addresses** and are protected by **Anti-DDoS Pro or Anti-DDoS Premium** to achieve the following effects: • If no DDoS attacks occur, service traffic is directly forwarded to the origin server. Anti-DDoS Pro or Anti-DDoS Premium is dormant to avoid a high latency. • If DDoS attacks occur, Anti-DDoS Pro or Anti-DDoS Premium automatically takes effect. Anti-DDoS Pro or Anti-DDoS Premium scrubs service traffic and forwards normal traffic to the origin server. **Note** Anti-DDoS Pro or Anti-DDoS Premium can interact with Alibaba Cloud Global Accelerator (GA). For more information, see 什么是全球加速.	Create a cloud service interaction rule	
Tiered Protection	Your services are protected by **Anti-DDoS Origin Enterprise** and **Anti-DDoS Pro or Anti-DDoS Premium** to achieve the following effects: • Anti-DDoS Origin Enterprise protects your services from low-volume DDoS attacks. Service traffic is directly forwarded to the origin server without increasing latency. • If volumetric DDoS attacks are detected, Anti-DDoS Pro or Anti-DDoS Premium takes effect. Anti-DDoS Pro or Anti-DDoS Premium scrubs service traffic and forwards normal traffic to the origin server.	Create a tiered protection rule	
CDN/DCDN Interaction	Your websites use **Alibaba Cloud CDN or DCDN** and are protected by **Anti-DDoS Pro or Anti-DDoS Premium** to achieve the following effects: • If no DDoS attacks occur, the nearest CDN or DCDN node is used for acceleration. • If DDoS attacks occur, Anti-DDoS Pro or Anti-DDoS Premium automatically takes effect.	Create a CDN or DCDN interaction rule	

Interaction scenario	Description	Anti-DDoS Pro	Anti-DDoS Premium
Network Acceleration	Your services are protected by **Anti-DDoS Premium Insurance or Unlimited plan** and **MCA** to achieve the following effects: • If no DDoS attacks occur, the IP address that network acceleration provides is used to speed up service access. • If DDoS attacks occur, Anti-DDoS Premium automatically takes effect. **Note** Network acceleration is suitable for the scenarios in which services are deployed outside mainland China and users of services come from mainland China. For more information, see Configure Anti-DDoS Premium MCA.	×	Create a network acceleration rule
Sec-MCA	Your services are protected by **Anti-DDoS Premium Insurance or Unlimited plan** and **Sec-MCA** to achieve the following effects: • The traffic from Internet service providers (ISPs) in mainland China, excluding China Mobile, is redirected to the IP address of the Anti-DDoS Premium Sec-MCA instance. • The traffic from China Mobile and ISPs outside mainland China is redirected to the IP address of the Anti-DDoS Premium instance. **Note** Sec-MCA accelerates access of users in mainland China to services in regions outside mainland China. It also mitigates volumetric DDoS attacks on the networks of ISPs in mainland China, excluding China Mobile. For more information, see Configure Anti-DDoS Premium Sec-MCA.	×	Create a Sec-MCA rule

4.4.2. Create a cloud service interaction rule

You can create cloud service interaction rules to enable Anti-DDoS Pro or Anti-DDoS Premium to work together with the Alibaba Cloud resources that have public IP addresses. The cloud service interaction feature prevents additional service access latency after your website is added to your Anti-DDoS Pro or Anti-DDoS Premium instance.

Prerequisites

- Your services use the Alibaba Cloud resources that have public IP addresses, such as an elastic IP address (EIP) or a Web Application Firewall (WAF), Elastic Compute Service (ECS), or Server Load Balancer (SLB) instance that has a public IP address.
- An Anti-DDoS Pro instance of the Profession mitigation plan or an Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan is purchased.

> **Notice** The clean bandwidth and queries per second (QPS) of the instance must meet the protection requirements of your services.

For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

- Your website is added to the Anti-DDoS Pro or Anti-DDoS Premium instance.

  For more information, see Add a website.

- The Anti-DDoS Pro or Anti-DDoS Premium instance forwards service traffic as expected.

  For more information, see Verify the forwarding configurations on your local computer.

Context

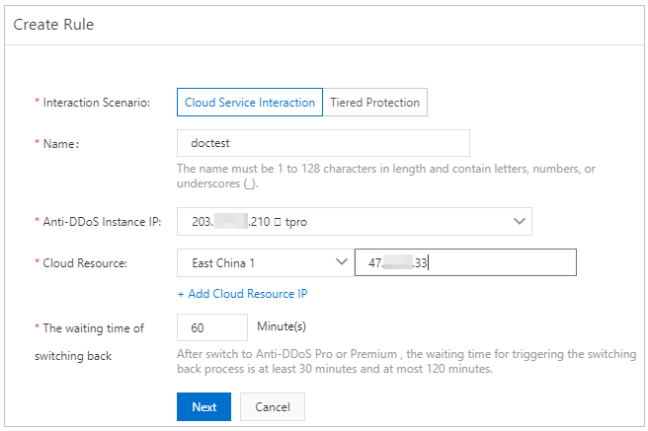
After you add your service to the Anti-DDoS Pro or Anti-DDoS Premium instance, service traffic is automatically scrubbed by the instance. Then, only normal traffic is forwarded to the origin server. Even if no attacks occur, service traffic is forwarded by the instance, which increases service access latency.

If you want to avoid additional latency, you can create a cloud service interaction rule for Sec-Traffic Manager. This rule allows service traffic to be switched to the instance for scrubbing and then to the origin server only if an attack occurs. If no attacks occur, service traffic is directly forwarded to the origin server.

Create an interaction rule

1.
2.
3.
4. On the **General** tab, click **Create Rule**.
5. In the **Create Rule** panel, configure a **cloud service interaction** rule and click **Next**.

   Sample configuration of a cloud service interaction rule in the Anti-DDoS Pro console



Parameter	Description
Interaction Scenario	Select **Cloud Service Interaction**.

Parameter	Description
Name	Enter a name for the rule. The name can be up to 128 characters in length and can contain letters, digits, and underscores (_).
Anti-DDoS Instance IP	Select an Anti-DDoS Pro or Anti-DDoS Premium instance.
Cloud Service	Enter the IP address of the **cloud resource**. You can enter an EIP or enter the IP address of an ECS instance, SLB instance, or WAF instance. You can click **Add Cloud Resource IP** to add more IP addresses. You can add a maximum of 20 IP addresses. **Note** After you add multiple IP addresses, these IP addresses are associated with the specified Anti-DDoS Pro or Anti-DDoS Premium instance. If one of the IP addresses is attacked, service traffic is forwarded to other IP addresses. Service traffic is forwarded to the Anti-DDoS Pro or Anti-DDoS Premium instance only if all IP addresses are attacked. For more information about how to forward service traffic to Anti-DDoS Pro or Anti-DDoS Premium when one of the IP addresses is attacked, see Share one Anti-DDoS Pro or Anti-DDoS Premium instance among multiple cloud resources.
The waiting time of switching back	Specify the waiting time before the service traffic is switched from your Anti-DDoS Pro or Anti-DDoS Premium instance back to the IP address of a cloud resource. When the attack stops and the waiting time that you specify elapses, the service traffic is automatically switched back to the IP address of the cloud resource. You can specify a value that ranges from 30 to 120. Unit: minutes. We recommend that you set the value to 60.

6. Change the DNS records of the domain name as prompted and click **Complete**.

   For the cloud service interaction rule to take effect, you must change the DNS records of your domain name on the website of the DNS service provider to map the domain name to the CNAME provided by Sec-Traffic Manager. If your DNS service is provided by Alibaba Cloud DNS, you need only to change the DNS records in the Alibaba Cloud DNS console.

   Notice After you change the DNS records of your domain name, the cloud service interaction rule takes effect. Before you change the DNS records, we recommend that you modify the *hosts* file on your computer to verify the cloud service interaction rule. This helps avoid incompatibility issues caused by inconsistent back-to-origin policies. Alibaba Cloud CDN (CDN) allows you to change the origin host for back-to-origin requests. However, you cannot use Anti-DDoS Pro or Anti-DDoS Premium to change the origin host for back-to-origin requests. If you use CDN together with Anti-DDoS Pro or Anti-DDoS Premium to retrieve data from an Object Storage Service (OSS) object, the normal traffic that is forwarded by Anti-DDoS Pro or Anti-DDoS Premium cannot be identified by OSS. As a result, your services are interrupted. For more information about origin hosts, see Origin hosts.

For more information about how to verify traffic forwarding rules, see Verify the forwarding configurations on your local computer.

For more information about how to change the DNS records of a domain name, see Change the CNAME record to redirect traffic to Sec-Traffic Manager.

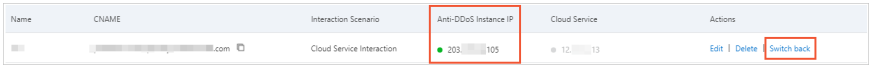
If no DDoS attacks occur on your cloud resource after you enable the cloud service interaction rule, service traffic is not scrubbed by your Anti-DDoS Pro or Anti-DDoS Premium instance and is directly forwarded from the client to the cloud resource. If DDoS attacks occur on your cloud resource after you enable the cloud service interaction rule, service traffic is automatically switched to your Anti-DDoS Pro or Anti-DDoS Premium instance for scrubbing, and only normal traffic is forwarded to the cloud resource. After service traffic is automatically switched to your Anti-DDoS Pro or Anti-DDoS Premium instance, the instance switches the service traffic back to the cloud resource when the attacks stop and the **waiting time** that you specify elapses.

In addition to automatic switchback, you can also manually switch the service traffic to your Anti-DDoS Pro or Anti-DDoS Premium instance for scrubbing and then to the cloud resource based on the protection requirements of your services. For more information, see What to do next.

What to do next

After a cloud service interaction rule is created, you can perform the following operations on the rule.

Operation	Description
Switch to DDoS	If traffic scrubbing by your Anti-DDoS Pro or Anti-DDoS Premium instance is not automatically triggered, the icon is displayed in the **Cloud Service** column. In this case, you can manually switch service traffic to the instance for scrubbing. You can manually switch service traffic before blackhole filtering is triggered. This reduces adverse impacts on your services.  Service traffic can be switched to your Anti-DDoS Pro or Anti-DDoS Premium instance only if blackhole filtering is not triggered for the IP address of the instance. **Notice** After you manually switch service traffic to your Anti-DDoS Pro or Anti-DDoS Premium instance, the service traffic cannot be automatically switched back to the associated cloud resources. To switch the service traffic back to the associated cloud resources, you must click **Switch back** to manually switch the service traffic.

Operation	Description
Switch back	If service traffic is scrubbed by your Anti-DDoS Pro or Anti-DDoS Premium instance, the icon is displayed in the **Anti-DDoS Instance IP** column. In this case, you can manually switch the service traffic back to the associated cloud resources.  **Notice** • Before you manually switch the service traffic, make sure that the attacks stop and the associated cloud resources also work as expected. This prevents the associated cloud resources from being added to sandboxes and prevents service interruptions. • If you click **Switch to DDoS** to switch service traffic to your Anti-DDoS Pro or Anti-DDoS Premium instance, you can switch the service traffic back to the associated cloud resource only by clicking **Switch back**. If blackhole filtering is triggered for the IP addresses of all associated cloud resources, the switchback fails. If blackhole filtering is deactivated for some cloud resources, service traffic is first switched back to these cloud resources. After blackhole filtering is deactivated for the remaining cloud resources, service traffic is also switched back to these cloud resources.
Edit	You can modify the cloud service interaction rule. However, you cannot change the values of **Interaction Scenario** and **Name** for the rule.
Delete	You can delete the cloud service interaction rule. **Warning** Before you delete a rule, make sure that the domain name of your website is not mapped to the CNAME provided by Sec-Traffic Manager. Otherwise, access to the website may fail after you delete the rule.

4.4.3. Create a tiered protection rule

You can create tiered protection rules to enable Anti-DDoS Pro or Anti-DDoS Premium to work together with Anti-DDoS Origin Enterprise. The tiered protection feature helps resolve the issue that the access latency of normal traffic is increased after you add your website to your Anti-DDoS Pro or Anti-DDoS Premium instance. If you enable tiered protection, Anti-DDoS Origin protects your services, which does not increase access latency. If volumetric attacks occur, Anti-DDoS Pro or Anti-DDoS Premium starts to protect your services instead.

Prerequisites

- Your services use the Alibaba Cloud resources that have public IP addresses, such as an elastic IP address (EIP) or a Web Application Firewall (WAF), Elastic Compute Service (ECS), or Server Load Balancer (SLB) instance that has a public IP address.
- An Anti-DDoS Origin Enterprise instance is purchased. The IP address of your cloud resource or an elastic IP address (EIP) is added to the instance for protection. The cloud resource can be an Elastic Compute Service (ECS) instance, Server Load Balancer (SLB) instance, or Web Application Firewall (WAF) instance.

  > **Notice** The Anti-DDoS Origin Enterprise instance must reside in the same region as your cloud resource.

  For more information, see Purchase an Anti-DDoS Origin Enterprise instance and Add a cloud service to Anti-DDoS Origin Enterprise for protection.
- An Anti-DDoS Pro instance of the Profession mitigation plan or an Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan is purchased.

  > **Notice** The clean bandwidth and queries per second (QPS) of the instance must meet the protection requirements of your services.

  For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.
- Your website is added to the Anti-DDoS Pro or Anti-DDoS Premium instance.

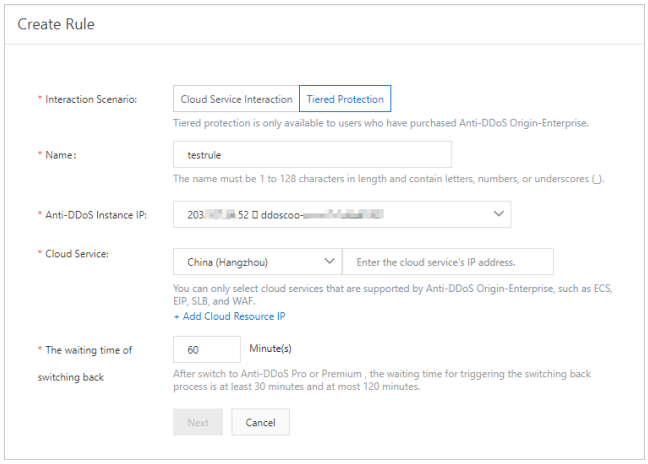
  For more information, see Add a website.
- The Anti-DDoS Pro or Anti-DDoS Premium instance forwards service traffic as expected.

  For more information, see Verify the forwarding configurations on your local computer.

Create a tiered protection rule

1.
2.
3.
4. On the **General** tab, click **Create Rule**.
5. In the **Create Rule** panel, configure a **tiered protection** rule and click **Next**.

   Sample configuration of a tiered protection rule in the Anti-DDoS Pro console



Parameter	Description
Interaction Scenario	Select **Tiered Protection**.
Name	Enter a name for the rule. The name can be up to 128 characters in length and can contain letters, digits, and underscores (_).
Anti-DDoS Instance IP	Select an Anti-DDoS Pro or Anti-DDoS Premium instance.

Parameter	Description
Cloud Service	Cloud Resource IP: Select the region where the cloud resource resides and enter the IP address of the cloud resource. **Notice** You must enter an EIP or enter the IP address of a cloud resource that is added to the Anti-DDoS Origin Enterprise instance. The cloud resource can be an ECS instance, SLB instance, or WAF instance. For more information, see Add a cloud service to Anti-DDoS Origin Enterprise for protection. You can click **Add Cloud Resource IP** to add more IP addresses. You can add a maximum of 20 IP addresses. **Note** After you add multiple IP addresses, these IP addresses are associated with the specified Anti-DDoS Pro or Anti-DDoS Premium instance. If one of the IP addresses is attacked, service traffic is forwarded to other IP addresses. Service traffic is forwarded to the Anti-DDoS Pro or Anti-DDoS Premium instance only if all IP addresses are attacked. For more information about how to forward service traffic to Anti-DDoS Pro or Anti-DDoS Premium when one of the IP addresses is attacked, see Share one Anti-DDoS Pro or Anti-DDoS Premium instance among multiple cloud resources.
The waiting time of switching back	Specify the waiting time before the service traffic is switched from your Anti-DDoS Pro or Anti-DDoS Premium instance back to the IP address of a cloud resource. When the attack stops and the waiting time that you specify elapses, the service traffic is automatically switched back to the IP address of the cloud resource. You can specify a value that ranges from 30 to 120. Unit: minutes. We recommend that you set the value to 60.

6. Change the DNS records of the domain name as prompted and click **Complete**.

   For the cloud service interaction rule to take effect, you must change the DNS records of your domain name on the website of the DNS service provider to map the domain name to the CNAME provided by Sec-Traffic Manager. If your DNS service is provided by Alibaba Cloud DNS, you need only to change the DNS records in the Alibaba Cloud DNS console.

> **Notice** After you change the DNS records of your domain name, the cloud service interaction rule takes effect. Before you change the DNS records, we recommend that you modify the *hosts* file on your computer to verify the cloud service interaction rule. This helps avoid incompatibility issues caused by inconsistent back-to-origin policies. Alibaba Cloud CDN (CDN) allows you to change the origin host for back-to-origin requests. However, you cannot use Anti-DDoS Pro or Anti-DDoS Premium to change the origin host for back-to-origin requests. If you use CDN together with Anti-DDoS Pro or Anti-DDoS Premium to retrieve data from an Object Storage Service (OSS) object, the normal traffic that is forwarded by Anti-DDoS Pro or Anti-DDoS Premium cannot be identified by OSS. As a result, your services are interrupted. For more information about origin hosts, see Origin hosts.

For more information about how to verify traffic forwarding rules, see Verify the forwarding configurations on your local computer.

For more information about how to change the DNS records of a domain name, see Change the CNAME record to redirect traffic to Sec-Traffic Manager.

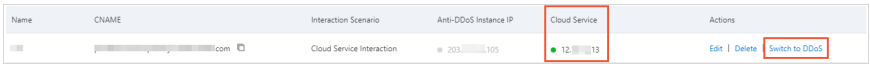
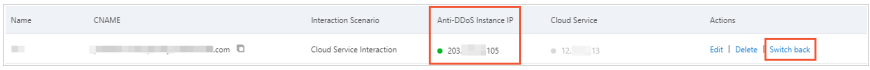
After the tiered protection rule is created, Anti-DDoS Origin Enterprise automatically protects the service traffic that is destined for the IP address. The service traffic is automatically switched to your Anti-DDoS Pro or Anti-DDoS Premium instance for scrubbing only if volumetric DDoS attacks occur on the IP address. This way, only normal traffic is forwarded to the cloud resource. After the service traffic is automatically switched to your Anti-DDoS Pro or Anti-DDoS Premium instance, the instance switches the service traffic back to the cloud resource when the attacks stop and the **waiting time** that you specify elapses. This way, Anti-DDoS Origin Enterprise continues to protect your services.

In addition to automatic switchover, you can also manually switch the service traffic to your Anti-DDoS Pro or Anti-DDoS Premium instance and then manually switch the service traffic back to the cloud resource based on the protection requirements of your services. For more information, see What to do next.

What to do next

After a cloud service interaction rule is created, you can perform the following operations on the rule.

Operation	Description

Operation	Description
Switch to DDoS	If traffic scrubbing by your Anti-DDoS Pro or Anti-DDoS Premium instance is not automatically triggered, the ● icon is displayed in the **Cloud Service** column. In this case, you can manually switch service traffic to the instance for scrubbing. You can manually switch service traffic before blackhole filtering is triggered. This reduces adverse impacts on your services.  Service traffic can be switched to your Anti-DDoS Pro or Anti-DDoS Premium instance only if blackhole filtering is not triggered for the IP address of the instance. **Notice** After you manually switch service traffic to your Anti-DDoS Pro or Anti-DDoS Premium instance, the service traffic cannot be automatically switched back to the associated cloud resources. To switch the service traffic back to the associated cloud resources, you must click **Switch back** to manually switch the service traffic.
Switch back	If service traffic is scrubbed by your Anti-DDoS Pro or Anti-DDoS Premium instance, the ● icon is displayed in the **Anti-DDoS Instance IP** column. In this case, you can manually switch the service traffic back to the associated cloud resources.  **Notice** • Before you manually switch the service traffic, make sure that the attacks stop and the associated cloud resources also work as expected. This prevents the associated cloud resources from being added to sandboxes and prevents service interruptions. • If you click **Switch to DDoS** to switch service traffic to your Anti-DDoS Pro or Anti-DDoS Premium instance, you can switch the service traffic back to the associated cloud resource only by clicking **Switch back**. If blackhole filtering is triggered for the IP addresses of all associated cloud resources, the switchback fails. If blackhole filtering is deactivated for some cloud resources, service traffic is first switched back to these cloud resources. After blackhole filtering is deactivated for the remaining cloud resources, service traffic is also switched back to these cloud resources.
Edit	You can modify the cloud service interaction rule. However, you cannot change the values of **Interaction Scenario** and **Name** for the rule.

Operation	Description
Delete	You can delete the cloud service interaction rule. **Warning** Before you delete a rule, make sure that the domain name of your website is not mapped to the CNAME provided by Sec-Traffic Manager. Otherwise, access to the website may fail after you delete the rule.

4.4.4. Create a CDN or DCDN interaction rule

You can create Alibaba Cloud CDN (CDN) or Dynamic Route for CDN (DCDN) interaction rules to enable Anti-DDoS Pro or Anti-DDoS Premium to work together with CDN or DCDN. If no DDoS attacks occur after you enable CDN or DCDN interaction, the nearest CDN or DCDN node is used to accelerate service access. Service traffic is switched to your Anti-DDoS Pro or Anti-DDoS Premium instance for scrubbing only if DDoS attacks occur.

Prerequisites

- The domain name is added to CDN or DCDN.

  For more information, see Add a domain name for CDN interaction or Add a domain name for DCDN interaction.

- An Anti-DDoS Pro instance of the **Enhanced** function plan and Profession mitigation plan or an Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan is purchased.

  Notice The clean bandwidth and queries per second (QPS) of the instance must meet the protection requirements of your services.

  For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

- Your website is added to the Anti-DDoS Pro or Anti-DDoS Premium instance for protection.

  For more information, see Add a website.

- The Anti-DDoS Pro or Anti-DDoS Premium instance forwards service traffic as expected.

  For more information, see Verify the forwarding configurations on your local computer.

Usage notes

The following table describes the requirements that must be met before you can use CDN or DCDN interaction.

Item	Description
Service type	You can enable CDN or DCDN interaction only for HTTP and HTTPS services. You cannot enable this feature for live video streaming.

Item	Description
Service scenario	You can enable CDN or DCDN interaction in the following service scenarios: • Your service is attacked more than three times per week. • Your service requires DDoS mitigation settings to immediately take effect. **Note** After service traffic is switched to your Anti-DDoS Pro or Anti-DDoS Premium instance, the settings take effect based on the time to live (TTL) values of your domain name system (DNS) records. • Your service bandwidth and QPS exceed the upper limits. **Note** If your service bandwidth exceeds 3 Gbit/s and the QPS exceeds 10,000, submit a to contact technical support.
Status of CDN- or DCDN-accelerated domain names	A CDN- or DCDN-accelerated domain name cannot be added to a sandbox. **Note** If CDN or DCDN adds your domain name to a sandbox, we recommend that you use only Anti-DDoS Pro or Anti-DDoS Premium and do not enable CDN or DCDN interaction.

Conditions for automatic switchover

When you create a CDN or DCDN interaction rule, you must configure a QPS threshold to trigger automatic traffic switchover between CDN or DCDN and Anti-DDoS Pro or Anti-DDoS Premium.

The following conditions must be met before an automatic switchover can be triggered:

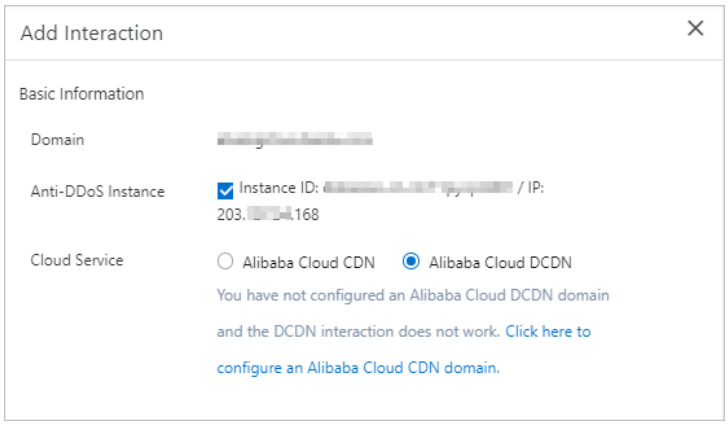
- Conditions for the switchover from CDN or DCDN to Anti-DDoS Pro or Anti-DDoS Premium
  - The QPS exceeds the threshold for 3 consecutive times within 3 minutes or for more than 6 times within 10 minutes, and the traffic on the CDN or DCDN node does not exceed 10 Gbit/s.
  - A domain name is added to a sandbox, and the traffic on the CDN or DCDN node does not exceed 10 Gbit/s.
- Conditions for the switchover from Anti-DDoS Pro or Anti-DDoS Premium to CDN or DCDN
  - The QPS remains less than 80% of the threshold, and the success rate of protection against HTTP flood attacks remains less than 10% for more than 12 consecutive hours.
  - The IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance cannot be in blackhole filtering or traffic scrubbing in the last 60 minutes. Your domain name is not added to a sandbox.
  - Service traffic can be switched back to CDN or DCDN only in the time range from 08:00 to 23:00.

Create a CDN or DCDN interaction rule

The following procedure describes how to create a CDN or DCDN interaction rule in the Anti-DDoS Pro console. You can also configure CDN interaction in the CDN console. For more information, see Integrate Alibaba Cloud CDN with Anti-DDoS.

1.
2.

3.
4. Click the **CDN/DCDN Interaction** tab.
5. Find the domain name for which you want to create a CDN or DCDN interaction rule and click **Add Interaction** in the **Actions** column.
6. In the **Add Interaction** panel, configure the parameters and click **Next**.



Parameter	Description
Anti-DDoS Instance	The Anti-DDoS Pro or Anti-DDoS Premium instance to which the domain name is added. Make sure that the Anti-DDoS Pro or Anti-DDoS Premium instance uses the **Enhanced** function plan. If the system returns the message **To use the CDN interaction feature, you must purchase the Enhanced Function plan for this instance.**, upgrade the instance as prompted. If the system returns the message **You have not selected any Anti-DDoS instances.**, add your domain name to the Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see Add a website.
Cloud Service	If your domain name is added to **CDN** or **DCDN**, the cloud service is automatically selected. No manual operations are required. If your domain name is not added to **CDN** or **DCDN**, select **Alibaba Cloud CDN** or **Alibaba Cloud DCDN** and add the domain name as prompted.
Request per Second	The minimum QPS threshold. If the QPS reaches this threshold, traffic switchover to Anti-DDoS Pro or Anti-DDoS Premium is triggered. For more information, see Conditions for automatic switchover. **Note** We recommend that you set the value to more than two to three times the historical peak QPS of your website to handle traffic spikes. Do not specify a value that is less than 500 even if the QPS of your website is low.

7. Change the DNS records of the domain name as prompted and click **Complete**.

   For the cloud service interaction rule to take effect, you must change the DNS records of your domain name on the website of the DNS service provider to map the domain name to the CNAME provided by Sec-Traffic Manager. If your DNS service is provided by Alibaba Cloud DNS, you need

only to change the DNS records in the Alibaba Cloud DNS console.

> **Notice** After you change the DNS records of your domain name, the cloud service interaction rule takes effect. Before you change the DNS records, we recommend that you modify the *hosts* file on your computer to verify the cloud service interaction rule. This helps avoid incompatibility issues caused by inconsistent back-to-origin policies. Alibaba Cloud CDN (CDN) allows you to change the origin host for back-to-origin requests. However, you cannot use Anti-DDoS Pro or Anti-DDoS Premium to change the origin host for back-to-origin requests. If you use CDN together with Anti-DDoS Pro or Anti-DDoS Premium to retrieve data from an Object Storage Service (OSS) object, the normal traffic that is forwarded by Anti-DDoS Pro or Anti-DDoS Premium cannot be identified by OSS. As a result, your services are interrupted. For more information about origin hosts, see Origin hosts.

For more information about how to verify traffic forwarding rules, see Verify the forwarding configurations on your local computer.

For more information about how to change the DNS records of a domain name, see Change the CNAME record to redirect traffic to Sec-Traffic Manager.

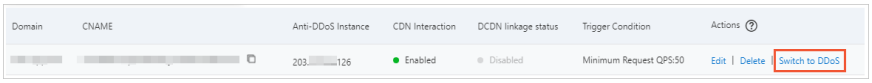
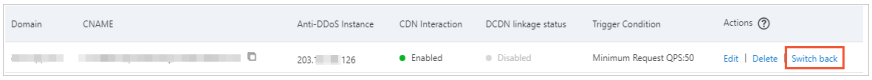
After a CDN or DCDN interaction rule is created, if the QPS of the domain name does not meet the conditions for the switchover from CDN or DCDN to Anti-DDoS Pro or Anti-DDoS Premium, service traffic is routed to the nearest CDN or DCDN node to accelerate service access. In this case, service traffic is not scrubbed by your Anti-DDoS Pro or Anti-DDoS Premium instance. Service traffic is switched to your Anti-DDoS Pro or Anti-DDoS Premium instance for scrubbing only if the QPS of the domain name meets the conditions for the switchover from CDN or DCDN to Anti-DDoS Pro or Anti-DDoS Premium. This way, only normal service traffic is forwarded to the origin server. After service traffic is automatically switched to your Anti-DDoS Pro or Anti-DDoS Premium instance, the instance switches the service traffic back to the CDN or DCDN node if the conditions for the switchover from Anti-DDoS Pro or Anti-DDoS Premium to CDN or DCDN are met.

In addition to automatic switchover, you can also manually switch the service traffic to your Anti-DDoS Pro or Anti-DDoS Premium instance and then manually switch the service traffic back to the CDN or DCDN node based on the protection requirements of your services. For more information, see What to do next.

What to do next

After a CDN or DCDN interaction rule is created, you can perform the following operations on the rule.

Operation	Description

Operation	Description
Switch to DDoS	If traffic scrubbing by your Anti-DDoS Pro or Anti-DDoS Premium instance is not automatically triggered, you can manually switch the service traffic to the instance for scrubbing. You can manually switch service traffic before blackhole filtering is triggered. This reduces adverse impacts on your services.  Service traffic can be switched to your Anti-DDoS Pro or Anti-DDoS Premium instance only if blackhole filtering is not triggered for the IP address of the instance. **Notice** After you manually switch the service traffic to your Anti-DDoS Pro or Anti-DDoS Premium instance, the service traffic cannot be automatically switched back to the CDN or DCDN node. To switch the service traffic back to the CDN or DCDN node, you must click **Switch back** to manually switch the service traffic.
Switch back	If service traffic is scrubbed by your Anti-DDoS Pro or Anti-DDoS Premium instance, you can manually switch the service traffic back to the CDN or DCDN node.  **Notice** • Before you switch the service traffic back to the CDN or DCDN node, make sure that the attacks stop and CDN or DCDN acceleration also works as expected. This prevents the CDN- or DCDN-accelerated domain name from being added to a sandbox and prevents service interruptions. • If you click **Switch to DDoS** to switch the service traffic to your Anti-DDoS Pro or Anti-DDoS Premium instance, you must click **Switch back** to switch the service traffic back to the CDN or DCDN node.
Edit	You can modify the CDN or DCDN interaction rule and change the value of **QPS** to modify the conditions for the switchover to Anti-DDoS Pro or Anti-DDoS Premium.

Operation	Description
Delete	You can delete the CDN or DCDN interaction rule. **Warning** Before you delete an interaction rule, make sure that the domain name of your website is not mapped to the CNAME provided by Sec-Traffic Manager. Otherwise, access to the website may fail after you delete the rule.

4.4.5. Create a network acceleration rule

You can create network acceleration rules to enable an Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan to work together with an Anti-DDoS Premium instance of the MCA mitigation plan. If no attacks occur after you enable the network acceleration feature, service access is accelerated by the Anti-DDoS Premium instance of the MCA mitigation plan. If attacks occur, service traffic is switched to the Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan for scrubbing. This way, only normal service traffic is forwarded to the origin server.

Prerequisites

- An Anti-DDoS Premium instance of the MCA mitigation plan is purchased.

  For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.
- An Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan is purchased.

  Notice The clean bandwidth and queries per second (QPS) of the instance must meet the protection requirements of your services.

  For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.
- Your website is added to an Anti-DDoS Premium instance. The website is associated with both the Anti-DDoS Premium instance of the MCA mitigation plan and the Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan.

  For more information, see Add a website.
- Both the Anti-DDoS Premium instance of the MCA mitigation plan and the Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan forward service traffic as expected.

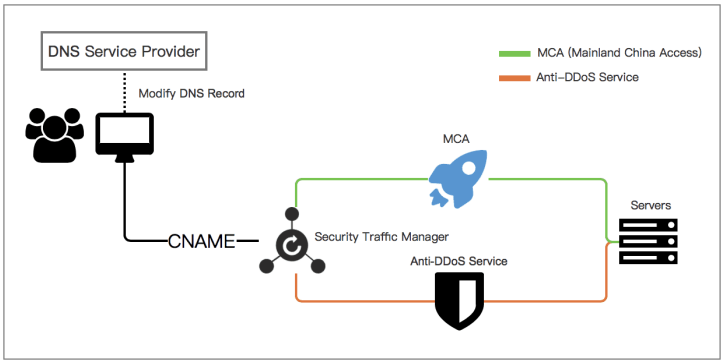
  For more information, see Verify the forwarding configurations on your local computer.

Context

Network acceleration is suitable for scenarios in which services are deployed outside mainland China but most users of the services are located in mainland China. In these scenarios, if you use only the Anti-DDoS Premium instance of the Insurance or Ultimate mitigation plan to protect your services, the access latency is increased for the users in mainland China.

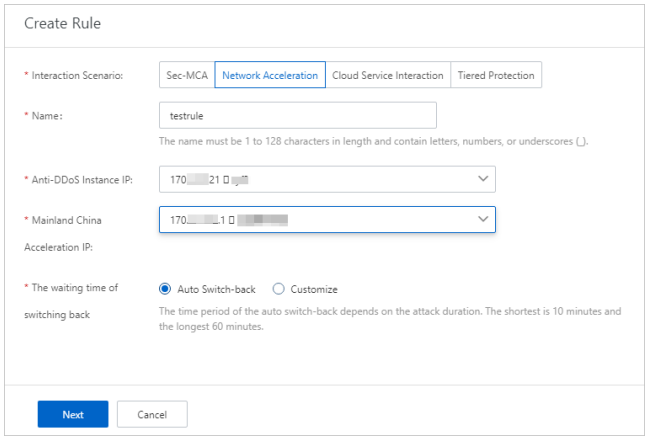
You can purchase an Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan and an Anti-DDoS Premium instance of the MCA mitigation plan. This way, if no attacks occur, service access is accelerated by the Anti-DDoS Premium instance of the MCA mitigation plan. If attacks occur, service traffic is switched to the Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan for scrubbing.

The following figure shows how network acceleration works. For more information, see Configure Anti-DDoS Premium MCA.



Create a network acceleration rule

1.
2.
3.
4. On the **General** tab, click **Create Rule**.
5. In the **Create Rule** panel, configure a **network acceleration** rule and click **Next**.



Parameter	Description
Interaction Scenario	Select **Network Acceleration**.
Name	Enter a name for the rule. The name can be up to 128 characters in length and can contain letters, digits, and underscores (_).
Anti-DDoS Instance IP	Select an Anti-DDoS Pro or Anti-DDoS Premium instance.
Mainland China Acceleration IP	Select the IP address of the Anti-DDoS Premium instance of the MCA mitigation plan.

Parameter	Description
The waiting time of switching back	Specify the waiting time before the service traffic is switched back. Valid values: ○ **Auto Switch-back**: the waiting time before the service traffic is automatically switched back based on the duration of attacks. Valid values: 10 to 60. Unit: minutes. ○ **Customize**: the custom waiting time that is required before the service traffic is switched back. Valid values: 30 to 120. Unit: minutes. To avoid frequent switchover operations, we recommend that you specify a waiting time of 60 minutes.

6. Change the DNS records of the domain name as prompted and click **Complete**.

   For the cloud service interaction rule to take effect, you must change the DNS records of your domain name on the website of the DNS service provider to map the domain name to the CNAME provided by Sec-Traffic Manager. If your DNS service is provided by Alibaba Cloud DNS, you need only to change the DNS records in the Alibaba Cloud DNS console.

   > **Notice** After you change the DNS records of your domain name, the cloud service interaction rule takes effect. Before you change the DNS records, we recommend that you modify the *hosts* file on your computer to verify the cloud service interaction rule. This helps avoid incompatibility issues caused by inconsistent back-to-origin policies. Alibaba Cloud CDN (CDN) allows you to change the origin host for back-to-origin requests. However, you cannot use Anti-DDoS Pro or Anti-DDoS Premium to change the origin host for back-to-origin requests. If you use CDN together with Anti-DDoS Pro or Anti-DDoS Premium to retrieve data from an Object Storage Service (OSS) object, the normal traffic that is forwarded by Anti-DDoS Pro or Anti-DDoS Premium cannot be identified by OSS. As a result, your services are interrupted. For more information about origin hosts, see Origin hosts.

   For more information about how to verify traffic forwarding rules, see Verify the forwarding configurations on your local computer.

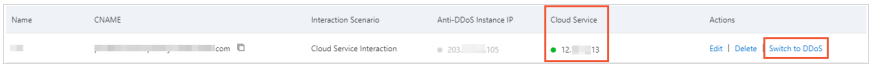
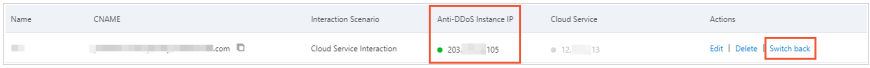
   For more information about how to change the DNS records of a domain name, see Change the CNAME record to redirect traffic to Sec-Traffic Manager.

If no attacks occur after a network acceleration rule is created, service access of users in mainland China is accelerated by using the Anti-DDoS Premium instance of the MCA mitigation plan. If attacks occur, the service traffic is switched to the Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan for scrubbing. This way, only normal service traffic is forwarded to the origin server. If service traffic is automatically switched to the Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan, the instance switches the service traffic back to the Anti-DDoS Premium of the MCA mitigation plan when the attacks stop and the **waiting time** that you specify elapses.

In addition to automatic switchover, you can also manually switch the service traffic to the Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan and then manually switch the service traffic back to the Anti-DDoS Premium instance of the MCA mitigation plan based on the protection requirements of your services. For more information, see What to do next.

What to do next

After a cloud service interaction rule is created, you can perform the following operations on the rule.

Operation	Description
Switch to DDoS	If traffic scrubbing by your Anti-DDoS Pro or Anti-DDoS Premium instance is not automatically triggered, the ● icon is displayed in the **Cloud Service** column. In this case, you can manually switch service traffic to the instance for scrubbing. You can manually switch service traffic before blackhole filtering is triggered. This reduces adverse impacts on your services.  Service traffic can be switched to your Anti-DDoS Pro or Anti-DDoS Premium instance only if blackhole filtering is not triggered for the IP address of the instance. **Notice** After you manually switch service traffic to your Anti-DDoS Pro or Anti-DDoS Premium instance, the service traffic cannot be automatically switched back to the associated cloud resources. To switch the service traffic back to the associated cloud resources, you must click **Switch back** to manually switch the service traffic.
Switch back	If service traffic is scrubbed by your Anti-DDoS Pro or Anti-DDoS Premium instance, the ● icon is displayed in the **Anti-DDoS Instance IP** column. In this case, you can manually switch the service traffic back to the associated cloud resources.  **Notice** • Before you manually switch the service traffic, make sure that the attacks stop and the associated cloud resources also work as expected. This prevents the associated cloud resources from being added to sandboxes and prevents service interruptions. • If you click **Switch to DDoS** to switch service traffic to your Anti-DDoS Pro or Anti-DDoS Premium instance, you can switch the service traffic back to the associated cloud resource only by clicking **Switch back**. If blackhole filtering is triggered for the IP addresses of all associated cloud resources, the switchback fails. If blackhole filtering is deactivated for some cloud resources, service traffic is first switched back to these cloud resources. After blackhole filtering is deactivated for the remaining cloud resources, service traffic is also switched back to these cloud resources.
Edit	You can modify the cloud service interaction rule. However, you cannot change the values of **Interaction Scenario** and **Name** for the rule.

Operation	Description
Delete	You can delete the cloud service interaction rule. **Warning** Before you delete a rule, make sure that the domain name of your website is not mapped to the CNAME provided by Sec-Traffic Manager. Otherwise, access to the website may fail after you delete the rule.

4.4.6. Create a Sec-MCA rule

To add a Sec-MCA rule, you must purchase an Anti-DDoS Premium Insurance or Unlimited instance and an Anti-DDoS Premium Sec-MCA instance. You can direct traffic from all ISPs in mainland China (excluding China Mobile) to the IP address of the Sec-MCA instance and direct traffic from China Mobile and regions outside mainland China to the IP address of the Anti-DDoS Premium instance.

Prerequisites

- A **Sec-MCA** instance is purchased, and your service is added to the instance. For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance and Configure Anti-DDoS Premium Sec-MCA.

  Note You only need to add your service to the Sec-MCA instance and do not need to modify DNS records of the domain name.

-
- Both the Anti-DDoS Premium instance of the MCA mitigation plan and the Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan forward service traffic as expected.

  For more information, see Verify the forwarding configurations on your local computer.

Context

Sec-MCA accelerates service access in scenarios where your service is deployed outside mainland China but your users reside in mainland China. It also mitigates volumetric DDoS attacks on the networks of ISPs in mainland China, excluding China Mobile.

If you want to provide quick and stable access for all users, including users in and outside mainland China and users from various ISPs, such as China Unicom and China Mobile, you can use the Sec-MCA instance together with the Anti-DDoS Premium Insurance or Unlimited instance.

For more information, see Configure Anti-DDoS Premium Sec-MCA.

Procedure

1.
2.
3.
4. On the **General** tab, click **Create Rule**.
5. In the **Create Rule** pane, configure a **Sec-MCA** rule and click **Next**.

Parameter	Description
Interaction Scenario	Select **Sec-MCA**.
Name	Specify the name of the rule. The rule name can be up to 128 characters in length and can contain letters, digits, and underscores (_).
Sec-MCA	Select the IP address of the Sec-MCA instance.
Anti-DDoS Premium	Select an Anti-DDoS Pro or Anti-DDoS Premium instance.

After the rule is created, Sec-Traffic Manager assigns a CNAME address for the rule. You can view the created rule and **CNAME** address in the rule list.

6. Modify the DNS records.

   Modify the DNS records of your domain name on the website of the DNS service provider to point the domain name to the CNAME address provided by Sec-Traffic Manager. For more information, see Change the CNAME record to redirect traffic to Sec-Traffic Manager.

What to do next

- Edit an interaction rule: On the **General** tab, find the rule that you want to edit and click **Edit** in the Actions column. You can modify parameters except **Interaction Scenario** and **Name**.
- Delete an interaction rule: On the **General** tab, find the rule that you want to delete and click **Delete** in the Actions column.

> **Warning** Before you delete an interaction rule, make sure that the service traffic is no longer directed to the CNAME address assigned by Sec-Traffic Manager. Otherwise, your service becomes unavailable after you delete the rule.

4.4.7. Share one Anti-DDoS Pro or Anti-DDoS Premium instance among multiple cloud resources

This topic describes how to associate IP addresses of multiple cloud resources to one Anti-DDoS Pro or Anti-DDoS Premium instance in cloud service interaction and tiered protection scenarios. If one of the cloud resources is attacked, service traffic of this cloud resource is switched to Anti-DDoS Pro or Anti-DDoS Premium.

Cloud service interaction

1. Configure Sec-Traffic Manager.

   For example, you have three cloud resources. Add an interaction rule for the IP address of each resource and associate the three rules with the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see Create a cloud service interaction rule.

2. Modify the DNS records.

Add three CNAME records for your domain name and set the record values to the CNAME addresses in the three rules created in Step 1. For more information, see Change the CNAME record to redirect traffic to Sec-Traffic Manager.

3. Verify the DNS records. Open a DNS test website to verify that the CNAME records added in Step 2 take effect.

Tiered protection

1. Purchase an Anti-DDoS Origin Enterprise instance.

   Add the three cloud resources to Anti-DDoS Origin Enterprise for protection. For more information, see Add a cloud service to Anti-DDoS Origin Enterprise for protection.

2. Configure Sec-Traffic Manager.

   Create a tiered protection rule for the IP address of each cloud resource and associate the three rules with the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see Create a tiered protection rule.

3. Modify the DNS records.

   Add three CNAME records for your domain name and set the record values to the CNAME addresses in the three rules created in Step 2. For more information, see Change the CNAME record to redirect traffic to Sec-Traffic Manager.

4. Verify the DNS records. Open a DNS test website to verify that the CNAME records added in Step 3 take effect.

4.5. Allow back-to-origin IP addresses to access the origin server

To use Anti-DDoS Pro or Anti-DDoS Premium to protect your website, we recommend that you add the back-to-origin IP addresses to the whitelist of the origin server. This ensures that the traffic from Anti-DDoS Pro or Anti-DDoS Premium is not blocked by security software on your origin server.

Context

If you deploy third-party security software on your origin server, such as a firewall, add the back-to-origin IP addresses of Anti-DDoS Pro or Anti-DDoS Premium to the whitelist of the security software.

> **Notice** After you switch service traffic to Anti-DDoS Pro or Anti-DDoS Premium, the instance scrubs the traffic and uses back-to-origin IP addresses to forward the traffic to the origin server. If the back-to-origin IP addresses are not in the whitelist on your firewall, the traffic from Anti-DDoS Pro or Anti-DDoS Premium may be blocked. This results in a failure to access your website.

If you use Anti-DDoS Pro or Anti-DDoS Premium to protect your website, the inbound traffic is rerouted to Anti-DDoS Pro or Anti-DDoS Premium for scrubbing. Then, Anti-DDoS Pro or Anti-DDoS Premium forwards the normal traffic to the origin server. In the back-to-origin process, network traffic is forwarded to the origin server by an Anti-DDoS Pro or Anti-DDoS Premium instance.

Anti-DDoS Pro and Anti-DDoS Premium function as reverse proxies and support the Full NAT mode.

Before Anti-DDoS Pro or Anti-DDoS Premium is used, the origin server receives requests from the distributed IP addresses of clients. If no attacks are launched against your services, each source IP address sends a small number of requests.

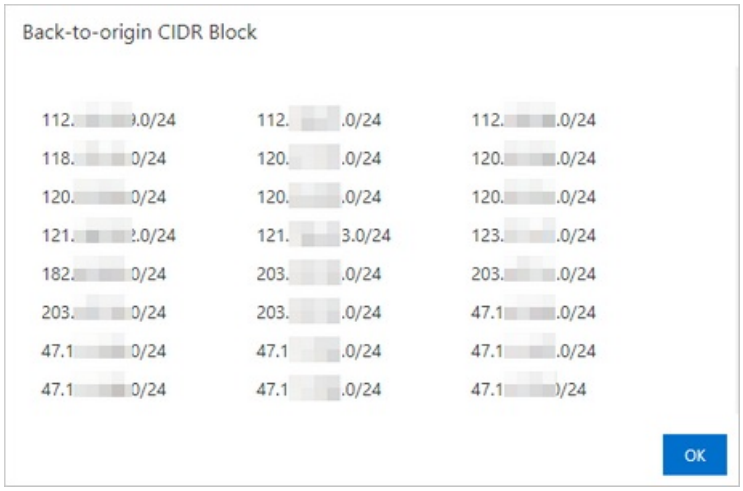
After Anti-DDoS Pro or Anti-DDoS Premium is used, the origin server receives all requests from a limited number of back-to-origin IP addresses. Each IP address forwards a larger number of requests than the client. As a result, the back-to-origin IP addresses may be regarded as malicious. If other DDoS protection policies are configured on the origin server, these back-to-origin IP addresses may be blocked or subject to bandwidth limits.

For example, the most common 502 error indicates that the origin server does not respond to the requests forwarded from back-to-origin IP addresses, and the back-to-origin IP addresses may be blocked by the firewall on the origin server.

Therefore, we recommend that you disable the firewall and other security software on the origin server after you set up forwarding rules. This ensures that the back-to-origin IP addresses of Anti-DDoS Pro or Anti-DDoS Premium are not affected by the protection policies on the origin server. Alternatively, you can perform the following steps to find the back-to-origin IP addresses of Anti-DDoS Pro and Anti-DDoS Premium and add them to the whitelist of the security software on the origin server.

Procedure

1.
2.
3.
4. On the **Website Config** page, click **View Back-To-Source CIDR Blocks** in the upper-right corner.
5. In the **Back-To-Source CIDR Block** dialog box, copy the back-to-origin IP addresses used by Anti-DDoS Pro or Anti-DDoS Premium.



6. Add the back-to-origin IP addresses to the whitelist of the security software on your origin server.

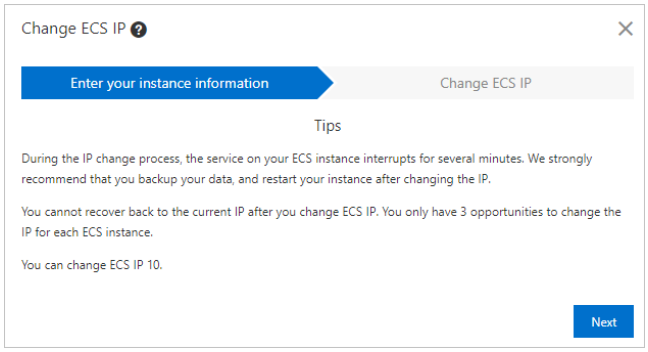
4.6. Change the public IP address of an ECS origin server

If the IP address of your origin server is exposed, we recommend that you change the public IP address of your Elastic Compute Service (ECS) instance to prevent attackers from bypassing Anti-DDoS Pro or Anti-DDoS Premium to attack the origin server. You can change the public IP address of an ECS instance in the Anti-DDoS Pro or Anti-DDoS Premium console up to 10 times.

Procedure

1.
2.
3.
4. In the upper-right corner of the **Website Config** page, click **Change ECS IP**.
5. In the **Change ECS IP** dialog box, read the tips and click **Next**.

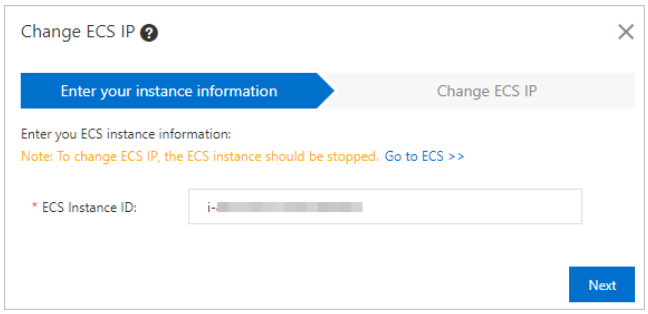
   Notice If you change the public IP address of an ECS instance, your service is interrupted for a few minutes. We recommend that you back up your data before you perform this operation.



6. (Optional)Stop your ECS instance.

   To change the IP address of your ECS instance, you must stop the instance. If you have stopped your ECS instance, go to the next step.

   If you do not stop your ECS instance, click **Go to ECS** in the **Change ECS IP** dialog box. Then, stop your ECS instance in the ECS console. For more information about how to stop an ECS instance, see Stop an instance.



7. Return to the **Change ECS IP** dialog box, specify **ECS Instance ID**, and then click **Next**.
8. After the IP address is released, click **Next**. Anti-DDoS Pro or Anti-DDoS Premium automatically assigns a new IP address to the ECS instance.
9. Click **OK**.

   Note After you change the IP address of an ECS origin server, set up Anti-DDoS Pro or Anti-DDoS Premium and do not expose the new IP address.

4.7. Configure Anti-DDoS Premium MCA

An Anti-DDoS Premium Mainland China Acceleration (MCA) instance can be used with an Anti-DDoS Premium Insurance Plan or Unlimited Plan instance to accelerate access to your services that are deployed outside mainland China.

Prerequisites

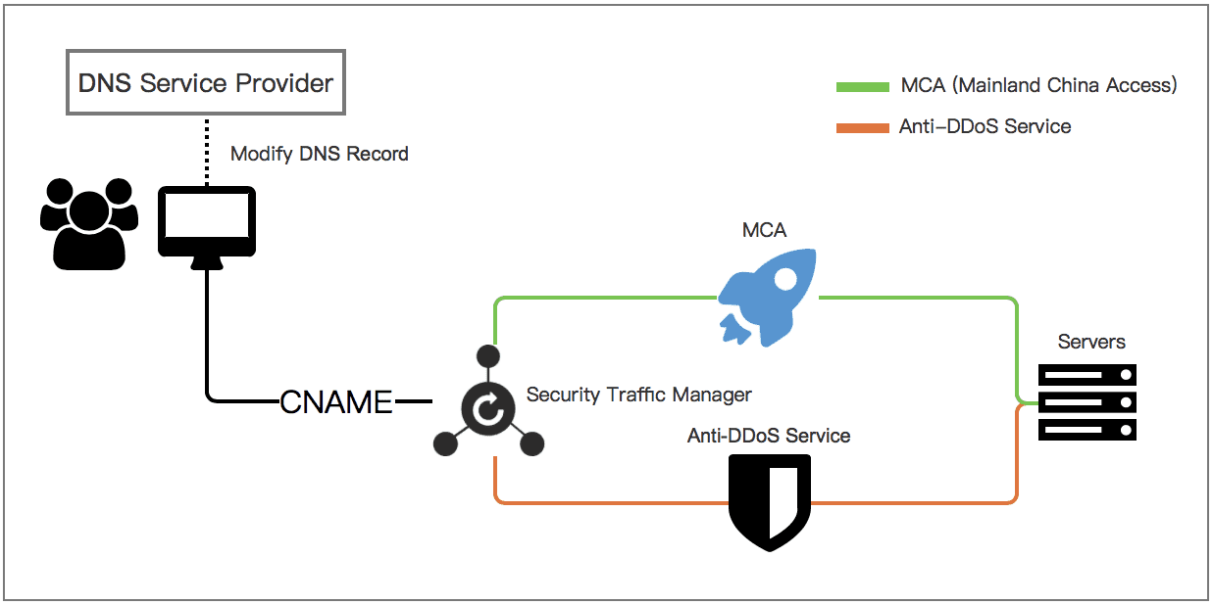
An Anti-DDoS Premium instance is created.

> **Note** Only Anti-DDoS Premium supports MCA. Anti-DDoS Pro does not support MCA.

Context

After you configure an Anti-DDoS Premium MCA instance that is used with an Anti-DDoS Premium Insurance Plan or Unlimited Plan instance, the instance protects your services. If no DDoS attacks are launched, the Anti-DDoS Premium MCA instance accelerates web access to your services. Otherwise, the Anti-DDoS Premium Insurance Plan or Unlimited Plan instance automatically takes over to mitigate DDoS attacks against your services.

For more information about the scenarios to which MCA applies, see Scenarios of Anti-DDoS Premium.



You can configure an Anti-DDoS Premium MCA instance for a domain name (Layer 7) or service port (Layer 4).

After you purchase Anti-DDoS Premium MCA and Insurance Plan or Unlimited Plan instances, add your domain name or service port to the instances in the Anti-DDoS Premium console. Then, configure a Sec-Traffic Manager rule to enable the auto-switching between an Anti-DDoS Premium MCA instance and an Anti-DDoS Premium Insurance Plan or Unlimited Plan instance. This rule forwards non-attack traffic to the origin server of your web service.

Procedure

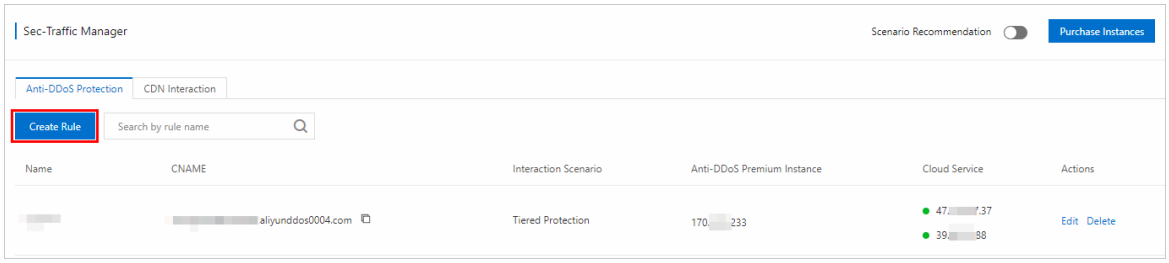
1.
2. In the top navigation bar, select **Outside Mainland China**.
3. Add your website or non-website services to both the Anti-DDoS Premium Insurance Plan or Unlimited Plan instance and the Anti-DDoS Premium MCA instance.

   > **Note** In this step, you do not need to change the DNS record.

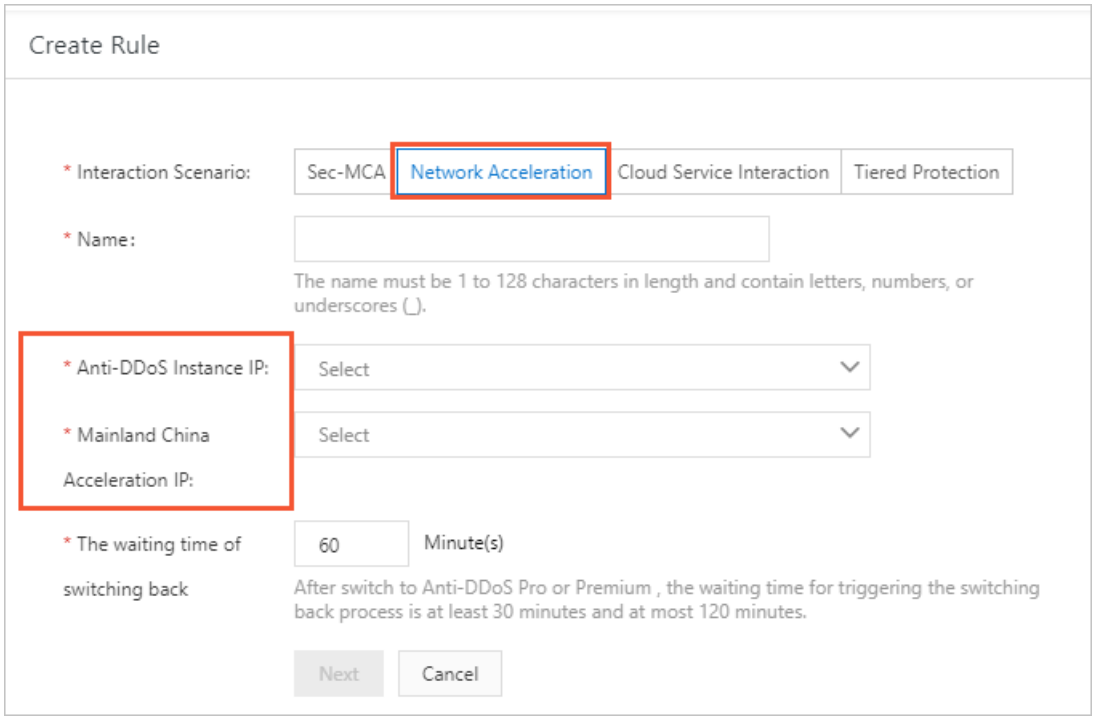
   - For information about how to add a website service to an Anti-DDoS Premium instance, see Add a website. When you add the website service and select dedicated IP addresses of Anti-DDoS Premium, select the dedicated IP addresses of both your Insurance Plan or Unlimited Plan and MCA instances.
   - For information about how to add a service port to an Anti-DDoS Premium instance, see Create forwarding rules. Create forwarding rules for the Anti-DDoS Premium MCA instance and the Anti-DDoS Premium Insurance Plan or Unlimited Plan instance for your non-website services.

     > **Note** Before you add your non-website services to the Anti-DDoS Premium MCA instance, make sure that the services can be accessed by using domain names. This ensures that traffic can be automatically redirected to the Anti-DDoS Premium MCA instance. If your services are accessed by using IP addresses, traffic cannot be automatically redirected.

4. Navigate to the **Sec-Traffic Manager** page, click the **General** tab, and click **Create Rule**.



5. On the **Create Rule** page, configure the required parameters and click **Next**.
   - **Interaction Scenario**: Select **Network Acceleration**.
   - **Name**: Enter the name of the rule.
   - **Anti-DDoS Instance IP**: Select the dedicated IP address of the Anti-DDoS Premium Insurance Plan or Unlimited Plan instance.
   - **Acceleration IP**: Select the dedicated IP address of the Anti-DDoS Premium MCA instance.



After the rule is created, the system uses the Anti-DDoS Premium MCA instance to accelerate web access if no DDoS attacks are launched. If DDoS attacks are launched, Sec-Traffic Manager automatically redirects traffic to the Anti-DDoS Premium Insurance Plan or Unlimited Plan instance for traffic scrubbing.

After you create a port forwarding rule, the system generates a CNAME address. You only need to change the DNS record to map the domain name to the CNAME address.

> **Note** When you add your services, make sure that you have selected the dedicated IP addresses of both the Anti-DDoS Premium Insurance Plan or Unlimited Plan instance and the Anti-DDoS Premium MCA instance.

6. Change the DNS record for the domain name at your DNS service provider.

   After you map your domain name to the CNAME address generated in Sec-Traffic Manager, the traffic is automatically redirected to Sec-Traffic Manager.

   > **Note** Automatic traffic redirection is achieved based on the CNAME address. Therefore, you must use the CNAME record.

4.8. Configure Anti-DDoS Premium Sec-MCA

Anti-DDoS Premium supports Secure Mainland China Acceleration (Sec-MCA). This allows you to accelerate access from mainland China to services in regions outside mainland China. Sec-MCA provides traffic scrubbing capabilities of more than 2 Tbit/s. This improves the access speed and stability of your business.

Prerequisites

An Anti-DDoS Premium Sec-MCA instance is purchased. For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

Context

Sec-MCA provides DDoS scrubbing capabilities and speeds up user access. Furthermore, you do not need to switch to an Anti-DDoS Premium instance to protect your services.

> **Note** **MCA** does not provide DDoS scrubbing capabilities. If your services are under attack, you must switch to an Anti-DDoS Premium instance. If DDoS attacks occur frequently, you must continually switch to an Anti-DDoS Premium instance.

The following table lists the differences between MCA and Sec-MCA.

Protect traffic from mainland China ISPs, excluding China Mobile

To provide quick and stable access for users who use mainland China Internet Service Providers (ISPs), excluding China Mobile, you can use only Anti-DDoS Premium Sec-MCA.

> **Note** Users of China Mobile or outside mainland China cannot access your services by using the IP addresses of Sec-MCA. For information about how to accelerate access for these users, see Protect traffic from all ISPs.

1.
2.
3. Add your website or non-website services to your Anti-DDoS Premium Sec-MCA instance.
   - Website configuration: Select the dedicated IP address of your Anti-DDoS Premium Sec-MCA instance. For more information, see Add a website.
   - Port configuration for non-website services: Configure a port forwarding rule in an Anti-DDoS Premium Sec-MCA instance. For more information, see Create forwarding rules.
4. Redirect the traffic to the Anti-DDoS Premium Sec-MCA instance and protect your services.
   - Website configuration: Change the CNAME record to point the website to the CNAME address assigned by Anti-DDoS Premium. For more information, see Change DNS records to protect website services.
   - Port configuration for non-website services: After you create a port forwarding rule, set the IP address to be protected to the IP address of the Anti-DDoS Premium instance.

Protect traffic from all ISPs

If you want to provide quick and stable access for users in and outside mainland China irrespective of ISPs, you can use Anti-DDoS Premium Insurance Plan or Unlimited Plan and Sec-MCA. You must create a Sec-MCA rule in **Sec-Traffic Manager**.

1.
2.
3. Add your website or non-website services to the Sec-MCA instance of Anti-DDoS Premium Insurance Plan or Unlimited Plan.

> **Note** In this step, you do not need to change the DNS record.

- Website configuration: When you select the dedicated IP address of your Anti-DDoS Premium instance, you must select the dedicated IP addresses of both the Anti-DDoS Premium Insurance Plan or Unlimited Plan instance and the Anti-DDoS Premium Sec-MCA instance. For more information, see Add a website.
- Port configuration for non-website services: You must configure a port forwarding rule in both the Anti-DDoS Premium Insurance Plan or Unlimited Plan instance and the Anti-DDoS Premium Sec-MCA instance. For more information, see Create forwarding rules.

> **Note** Before you add your non-website services to an Anti-DDoS Premium Sec-MCA instance, make sure that the services can be accessed by using domain names. This ensures that traffic can be automatically redirected to the Anti-DDoS Premium Sec-MCA instance. If your services are accessed by using IP addresses, traffic cannot be automatically redirected.

4. Choose **Provisioning > Sec-Traffic Manager**. On the page that appears, click the **General** tab.
5. Click **Create Rule**. In the dialog box that appears, configure the following parameters and click **Next**.
   - **Interaction Scenario**: Select **Sec-MCA**.
   - **Name**: Enter the name of the rule.
   - **Sec-MCA**: Select an Anti-DDoS Premium Sec-MCA instance.
   - **Anti-DDoS Premium**: Select an Anti-DDoS Premium Insurance Plan or Unlimited Plan instance.

   After you create a port forwarding rule, the system generates a CNAME address. You only need to change the DNS record to map the domain name to the CNAME address.
   - The traffic from mainland China ISPs, excluding China Mobile, is redirected to the IP address of the Anti-DDoS Premium Sec-MCA instance.
   - The traffic from China Mobile and regions outside mainland China is redirected to the IP address of Anti-DDoS Premium.

   > **Note** When you add your services, make sure that you have selected the dedicated IP addresses of both the Anti-DDoS Premium Insurance Plan or Unlimited Plan instance and the Anti-DDoS Premium Sec-MCA instance.
6. Change the DNS record for the domain name at your DNS service provider.

   After you map your domain name to the CNAME address generated in Sec-Traffic Manager, the traffic is automatically redirected to Sec-Traffic Manager.

   > **Note** Automatic traffic redirection is achieved based on the CNAME address. Therefore, you must use the CNAME record.

5.Resource management

5.1. Overview

Asset management is used to manage the assets of Anti-DDoS Pro or Anti-DDoS Premium. The assets include Anti-DDoS Pro or Anti-DDoS Premium instances, Anti-DDoS plans, and advanced global protection sessions. For example, you can purchase instances, renew instances, and modify instance specifications. This topic describes the asset types and asset management operations that are supported by Anti-DDoS Pro and Anti-DDoS Premium.

Asset management in Anti-DDoS Pro

The following table describes the asset types and asset management operations that are supported by Anti-DDoS Pro.

Asset type	Purchase method	Description	Supported operation
Anti-DDoS Pro instance of the Professional plan	You can purchase a subscription instance.	BGP networks in mainland China are used to intelligently defend against Tbit/s-level DDoS attacks.	• Purchase mitigation plans for Anti-DDoS Pro and Anti-DDoS Premium • Modify the burstable protection bandwidth of an instance • Upgrade an instance • Renew an instance • Manage tags of instance
Anti-DDoS plan	You cannot purchase an Anti-DDoS plan. However, if specific requirements are met, you can submit a ticket to apply for an Anti-DDoS plan.	An Anti-DDoS plan is used to pay for the fees that are generated for burstable protection provided by an Anti-DDoS Pro instance.	Apply for and use Anti-DDoS plans

Asset management in Anti-DDoS Premium

The following table describes the asset types and asset management operations that are supported by Anti-DDoS Premium.

Asset type	Purchase method	Description	Supported operation
Anti-DDoS Premium instance of the Insurance or Unlimited plan	You can purchase a subscription instance.	The global anycast network is used to defend against the DDoS attacks from locations that are close to the attack source.	• Purchase mitigation plans for Anti-DDoS Pro and Anti-DDoS Premium • Upgrade an instance • Renew an instance
Anti-DDoS Premium instance of the MCA plan	You can purchase a subscription instance.	An Anti-DDoS Premium instance of the MCA plan serves as an access acceleration component to accelerate access in mainland China when no attacks occur. The instance cannot mitigate DDoS attacks. **Notice** This instance must be used together with an Anti-DDoS Premium instance of the Insurance or Unlimited plan.	
Anti-DDoS Premium instance of the Sec-MCA plan	You can purchase a subscription instance.	An Anti-DDoS Premium instance of the Sec-MCA plan is used to accelerate access in mainland China. The instance can mitigate DDoS attacks for lines that are not provided by China Mobile, such as China Telecom and China Unicom. **Notice** If you want to mitigate DDoS attacks for lines that are provided by China Mobile and accelerate access in regions outside mainland China, you must use an Anti-DDoS Premium instance of the Sec-MCA plan together with an Anti-DDoS Premium instance of the Insurance or Unlimited plan.	

Asset type	Purchase method	Description	Supported operation
Global advanced mitigation session	You can purchase global advanced mitigation by session. A global advanced mitigation session is valid for one year.	If the two global advanced mitigation sessions that are provided free of charge each month are exhausted, you can purchase more global advanced mitigation sessions. **Notice** Global advanced mitigation sessions must be used together with an Anti-DDoS Premium instance of the Insurance plan.	Purchase global advanced mitigation sessions

5.2. Modify the burstable protection bandwidth of an instance

After you purchase an Anti-DDoS Pro instance, you can modify the burstable protection bandwidth of the instance based on your business requirements. The burstable protection bandwidth determines the maximum capability of the instance to defend against DDoS attacks, which indicates the peak traffic of the DDoS attacks that the instance can mitigate.

Prerequisites

An Anti-DDoS Pro instance is purchased. For more information, see Purchase mitigation plans for Anti-DDoS Pro and Anti-DDoS Premium.

Notice The burstable protection bandwidth is available only for Anti-DDoS Pro instances. By default, an Anti-DDoS Premium instance provides unlimited advanced protection, and no burstable protection bandwidth is required for the instance.

Context

An Anti-DDoS Pro instance has both basic protection bandwidth and burstable protection bandwidth. The burstable protection bandwidth must be no less than the basic protection bandwidth. The methods to modify the basic protection bandwidth and burstable protection bandwidth of an Anti-DDoS Pro instance vary based on the billing methods. To modify the basic protection bandwidth, you must upgrade your instance. To modify the burstable protection bandwidth, you can change the bandwidth value in the Anti-DDoS Pro console or upgrade your instance at any time. For more information about the billing methods, see Anti-DDoS Pro billing methods.

A high burstable protection bandwidth indicates the high peak traffic of DDoS attacks that the instance can mitigate. Burstable protection is triggered only when DDoS attacks occur and the peak attack traffic is between the basic protection bandwidth and burstable protection bandwidth. On the day after the attacks stop, a bill is generated for the pay-as-you-go resources that are used by your Anti-DDoS Pro instance to provide burstable protection. No costs are generated for the resources that are used for burstable protection in the following scenarios:

- No DDoS attacks occur, or DDoS attacks occur but the attack traffic does not exceed the basic protection bandwidth.

  In this scenario, basic protection can cope with the attacks.

- DDoS attacks occur, and the attack traffic exceeds the burstable protection bandwidth.

  In this scenario, the IP address of the attacked asset enters the blackhole filtering state. The asset becomes accessible over the Internet only after the attacks stop and blackhole filtering is deactivated. For more information, see Blackhole filtering policy of Alibaba Cloud.

You can specify the burstable protection bandwidth for your Anti-DDoS Pro instance based on multiple factors. The factors include the traffic volume of the DDoS attacks that your services may encounter and your budget for service protection. You can set the burstable protection bandwidth to the minimum value that is equal to the basic protection bandwidth. In this case, burstable protection is disabled for your Anti-DDoS Pro instance, and no bills are generated for pay-as-you-go resources. The maximum burstable protection bandwidth that you can set varies based on the basic protection bandwidth of an Anti-DDoS Pro instance. For example, if the basic protection bandwidth of an Anti-DDoS Pro instance is 30 Gbit/s, the maximum burstable protection bandwidth of the instance can be set to 300 Gbit/s. If the basic protection bandwidth of an Anti-DDoS Pro instance is greater than or equal to 300 Gbit/s, the maximum burstable protection bandwidth is unlimited.

Procedure

1.
2.
3.
4. Find the required instance and click the

   icon next to **Protection Bandwidth** in the **Status** column.
5. In the **Change Burstable Bandwidth** dialog box, select a value and click **OK**.
   You can view the new protection bandwidth of the instance in the **Status** column. **Burstable ***G** indicates that the current burstable protection bandwidth of the instance is *** Gbit/s.

References

FAQ about the billing of burstable protection

5.3. Configure burstable clean bandwidth

If your business traffic may spike, we recommend that you enable the burstable clean bandwidth feature for your Anti-DDoS Pro or Anti-DDoS Premium instance. This avoids packet loss when the peak business traffic exceeds the clean bandwidth of your instance.

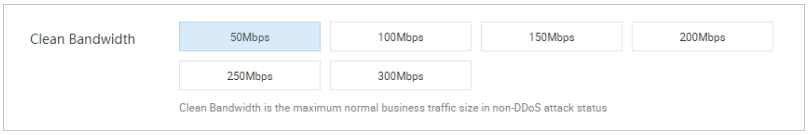
Prerequisites

An Anti-DDoS Pro instance is purchased.

For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

Context

By default, the burstable clean bandwidth feature is disabled for your instance. After you add services to your instance, the peak business traffic may exceed the **clean bandwidth** that you select when you purchase the instance. If this situation happens, random packet loss occurs during traffic forwarding. If this situation lasts for a long period of time, throttling occurs, and the access to your services is affected.



The following list describes the scenarios in which the peak business traffic exceeds the clean bandwidth and the solutions specific to the scenarios:

- If the clean bandwidth of your instance cannot meet your business requirements, you must upgrade your instance to increase the clean bandwidth. For more information, see Upgrade an instance.
- If the clean bandwidth of your instance can meet your daily business requirements but cannot meet the requirements to handle traffic spikes, we recommend that you enable the burstable clean bandwidth feature.

  After you enable the burstable clean bandwidth feature, you can specify a burstable clean bandwidth to increase the upper limit of the total bandwidth that is supported by the instance. You are charged for the burstable clean bandwidth based on the pay-as-you-go billing method. For more information about the billing for the burstable clean bandwidth, see Billing of the burstable clean bandwidth feature.

Scenarios

We recommend that you enable the burstable clean bandwidth feature for your instance in the following scenarios:

- Holiday promotions, such as Black Friday
- Release of services, such as launch of a new gaming server or new product
- Sharp increase in the number of access requests to websites, such as access requests to online course selection systems and government lottery systems within a specific period of time

Limits

After you enable the burstable clean bandwidth feature, the total bandwidth of the Anti-DDoS Pro instance can be up to 5 Gbit/s. The total bandwidth is equal to the clean bandwidth plus the burstable clean bandwidth that you specify. The burstable clean bandwidth cannot exceed nine times the clean bandwidth.

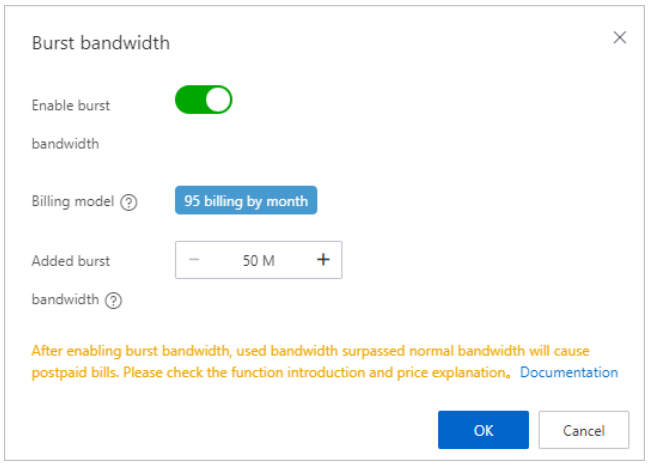
Examples:

- If the clean bandwidth is 100 Mbit/s, the maximum burstable clean bandwidth that you can specify is 900 Mbit/s. If you specify a burstable clean bandwidth of 900 Mbit/s, the Anti-DDoS Pro instance supports the maximum business traffic of 1 Gbit/s.
- If the clean bandwidth is 1 Gbit/s, the maximum burstable clean bandwidth that you can specify is 4 Gbit/s. If you specify a burstable clean bandwidth of 4 Gbit/s, the Anti-DDoS Pro instance supports the maximum business traffic of 5 Gbit/s.
- If the clean bandwidth is 5 Gbit/s, you cannot enable the burstable clean bandwidth feature. In this case, if you need a higher bandwidth, submit a or contact customer service.

Enable the burstable clean bandwidth feature

1.
2.
3.
4. In the instance list, find the instance that you want to enable the feature and click the

   icon to the right of **Added burst bandwidth** in the **Instance Type** column.
5. In the **Burst bandwidth** dialog box, turn on **Enable burst bandwidth** and specify a burstable clean bandwidth based on your business requirements.

   The minimum burstable clean bandwidth is 50 Mbit/s. The maximum burstable clean bandwidth can be nine times the clean bandwidth of the instance. For example, if the clean bandwidth is 100 Mbit/s, the maximum burstable clean bandwidth that you can specify is 900 Mbit/s.

   > **Notice** The sum of the clean bandwidth and the burstable clean bandwidth that you specify cannot exceed 5 Gbit/s. To prevent throttling, make sure that the sum is greater than your peak business traffic. For more information, see Billing examples.

6. Click **OK**.
   After you complete the preceding settings, you can view the value of **Added burst bandwidth** in the **Instance Type** column.

After you enable the burstable clean bandwidth feature, you can refer to the preceding steps to specify a greater value for the **Added burst bandwidth** parameter. If you want to disable the burstable clean bandwidth feature, turn off **Enable burst bandwidth**.

> **Notice**
>
> - You can disable the burstable clean bandwidth feature for each instance only once within one calendar month. If you disable the burstable clean bandwidth feature in a month, you are charged for the burstable clean bandwidth that you use when the feature is enabled in this month.
> - The burstable clean bandwidth feature is automatically disabled in the following scenarios:
>   - Your instance expires. Expired instances do not provide services.
>   - Your Alibaba Cloud account has an overdue payment. In this case, all services that are charged based on the pay-as-you-go billing method are unavailable.
>
> To continue using the feature, you must renew your instance or settle the overdue payment and enable the feature.

To view the logs of the burstable clean bandwidth, navigate to the **Investigation > Operation Logs** page. You can view the logs that are generated when you enable and disable the burstable clean bandwidth feature and modify the burstable clean bandwidth. For more information, see View operations logs.

Query bills for the burstable clean bandwidth

After you enable the burstable clean bandwidth feature, you can query the bill for the burstable clean bandwidth for each calendar month. To query the bills, log on to the and navigate to the **Investigation > System logs** page.

The billing cycle is one calendar month. You are billed based on the following rules:

- At 10:00 on the first day of each calendar month, the bill for the burstable clean bandwidth of the previous month is displayed on the **System logs** page, and Alibaba Cloud sends notifications to the contacts of your Alibaba Cloud account by email.

  The bill is in the **To be billed** state. The bill covers only the burstable clean bandwidth that you used within the previous month. You can view the bill details to check the usage of the burstable clean bandwidth within the previous month. For more information, see Query system logs.

  If you have any concerns about the usage of the burstable clean bandwidth, submit a . If the amount of the burstable clean bandwidth in the bill is different from your actual usage, the bill is **terminated**, and you are not required to make a payment.

- If you do not have concerns about the bill, the bill of the previous month is displayed on the **System logs** page at 10:00 on the tenth day of the current month.

  The bill is in the **Already billed** state, and the fees are automatically deducted from the balance of your Alibaba Cloud account. Make sure that the balance of your Alibaba Cloud account is sufficient. If your account has an overdue payment, all services that are charged based on the pay-as-you-go billing method become unavailable. The burstable clean bandwidth feature also becomes unavailable.

5.4. Upgrade an instance

If the specifications of your Anti-DDoS Pro or Anti-DDoS Premium instance cannot meet your business requirements, you can upgrade the specifications of the instance in the Anti-DDoS Pro console. The specifications include the function plan, clean bandwidth, and the numbers of protected domain names and ports. This topic describes how to upgrade an Anti-DDoS Pro or Anti-DDoS Premium instance.

Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased. For more information, see Purchase mitigation plans for Anti-DDoS Pro and Anti-DDoS Premium.

Context

An instance upgrade indicates the upgrade of instance specifications. After you upgrade your instance, you must pay the price difference for the validity period that remains. You cannot downgrade your instance after the upgrade.

> **Notice** You can only upgrade your instance.

Supported asset types and specifications

The following table describes the asset types and specifications that can be upgraded.

Asset type	Supported specification
Anti-DDoS Pro instance of the Professional plan	Basic protection bandwidth, burstable protection bandwidth, clean bandwidth, function plan, business QPS, and numbers of protected ports and domain names.
Anti-DDoS Premium instance of the Insurance or Unlimited plan	Mitigation plan, clean bandwidth, function plan, business QPS, and numbers of protected ports and domain names. You can upgrade the mitigation plan from Insurance to Mitigation only for an Anti-DDoS Premium instance of the Insurance plan.
Anti-DDoS Premium instance of the MCA plan	Clean bandwidth.
Anti-DDoS Premium instance of the Sec-MCA plan	Clean bandwidth, function plan, business QPS, and numbers of protected ports and domain names.

Procedure

1.
2.
3.
4. Find the instance that you want to upgrade and click **Upgrade** in the **Actions** column.
5. On the **Upgrade/Downgrade** page, configure the parameters based on your business requirements. Read and select **Terms of Service**. Then, click **Buy Now**.
6. Complete the payment.

You can view the new instance specifications on the **Instances** page.

5.5. Renew an instance

Before your Anti-DDoS Pro or Anti-DDoS Premium instance is released, you can manually renew the instance to extend the subscription period. To prevent your services from being adversely affected by instance expiration, you can also enable auto-renewal before your instance expires. This way, Alibaba Cloud automatically renews the instance when the instance is about to expire. This topic describes how to manually renew an Anti-DDoS Pro or Anti-DDoS Premium instance. This topic also describes how to enable auto-renewal for the instance.

Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased. For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

Supported asset types

You can renew the following types of Anti-DDoS Pro or Anti-DDoS Premium instances:

- Anti-DDoS Pro instance of the Profession mitigation plan
- Anti-DDoS Premium instance of the Insurance or Unlimited mitigation plan
- Anti-DDoS Premium instance of the MCA mitigation plan
- Anti-DDoS Premium instance of the Sec-MCA mitigation plan

Impacts of instance expiration

If you do not renew your Anti-DDoS Pro instance in time after the instance expires, your services are adversely affected. The following table describes the impacts.

Time period	Protection capability	Traffic forwarding	Instance configuration
From the expiration date to 7 calendar days (excluded) after the expiration date	The instance provides only the basic protection against attacks of 5 Gbit/s. If you renew your instance within this time period, the instance continues to provide the protection capabilities based on the plan that you purchased.	The instance still forwards service traffic.	Instance configurations are retained.

Time period	Protection capability	Traffic forwarding	Instance configuration
7 calendar days (included) after the expiration date to 15 calendar days (excluded) after the expiration date	The instance provides only the basic protection against attacks of 5 Gbit/s.	The instance no longer forwards service traffic. **Warning** If you no longer need Anti-DDoS Pro, you must switch service traffic from the Anti-DDoS Pro instance to the origin server seven calendar days before the expiration date. Otherwise, access to your services may be adversely affected. If you want to switch service traffic, make sure that the domain name of your website does not map to the CNAME assigned by Anti-DDoS Pro. You must also make sure that your non-website service does not use an exclusive IP address provided by the instance. If you renew your instance within this time period, the instance continues to forward service traffic, and you do not need to configure the instance again.	Instance configurations are retained.

Time period	Protection capability	Traffic forwarding	Instance configuration
15 calendar days (included) after the expiration date to later points in time	The instance provides only the basic protection against attacks of 5 Gbit/s.	The instance no longer forwards service traffic.	The Anti-DDoS Pro instance is released. **Warning** After all Anti-DDoS Pro instances that are created by using your Alibaba Cloud account are released, the configurations that are added to Anti-DDoS Pro, such as website access configurations, port access configurations, mitigation settings, and reports, are deleted and cannot be restored. If you want to use Anti-DDoS Pro again, you must purchase and configure another Anti-DDoS Pro instance.

If you do not renew your Anti-DDoS Premium instance in time after the instance expires, your services are adversely affected. The following table describes the impacts.

Time period	Protection capability	Traffic forwarding	Instance configuration
From the expiration date to 30 (excluded) calendar days after the expiration date	The instance provides only the basic protection against attacks of 5 Gbit/s. If you renew your instance within this time period, the instance continues to provide the protection capabilities based on the plan that you purchased.	The instance still forwards service traffic.	Instance configurations are retained.

Time period	Protection capability	Traffic forwarding	Instance configuration
30 (included) calendar days after the expiration date to later points in time	The instance provides only the basic protection against attacks of 5 Gbit/s.	The instance no longer forwards service traffic. **Warning** If you no longer need Anti-DDoS Premium, you must switch service traffic from the Anti-DDoS Premium instance to the origin server 30 calendar days before the expiration date. Otherwise, access to your services may be adversely affected. If you want to switch service traffic, make sure that the domain name of your website does not map to the CNAME assigned by Anti-DDoS Premium. You must also make sure that your non-website service does not use an exclusive IP address provided by the instance.	The Anti-DDoS Premium instance is released. **Warning** After all Anti-DDoS Premium instances that are created by using your Alibaba Cloud account are released, the configurations that are added to Anti-DDoS Premium, such as website access configurations, port access configurations, mitigation settings, and reports, are deleted and cannot be restored. If you want to use Anti-DDoS Premium again, you must purchase and configure another Anti-DDoS Premium instance.

Manually renew an instance

Before your Anti-DDoS Pro or Anti-DDoS Premium instance is released, you can manually renew the instance and retain the original configurations of the instance.

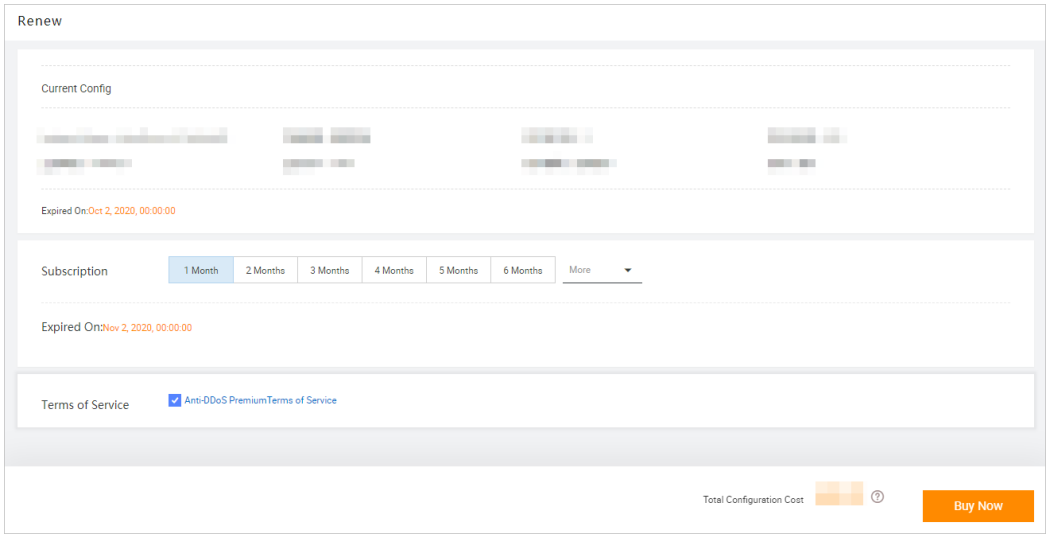
Notice If the instance is released, you cannot manually renew the instance. For more information, see Impacts of instance expiration.

We recommend that you manually renew your instance based on the following suggestions:

- Anti-DDoS Pro instance: Renew your Anti-DDoS Pro instance any time before the expiration date or within seven calendar days after the expiration date. This way, the forwarding of service traffic is not adversely affected.
- Anti-DDoS Premium instance: Renew your Anti-DDoS Premium instance any time before the expiration date or within 30 calendar days after the expiration date. This way, the forwarding of service traffic is not adversely affected.

You can perform the following steps to manually renew your instance:

1.
2.
3.
4. Find the instance that you want to renew and click **Renew** in the **Actions** column.
5. On the **Renew** page, set **Plan**, which specifies the renewal duration. Read and select **Terms of Service**. Then, click **Buy Now**.



6. Complete the payment.

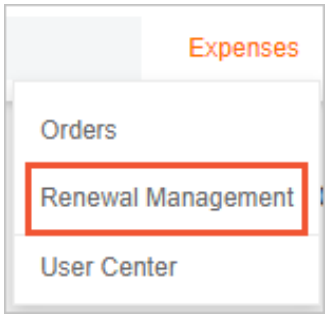
You can check the new expiration date of your instance on the **Instances** page. The subscription period is extended based on the specified renewal duration.

Enable auto-renewal

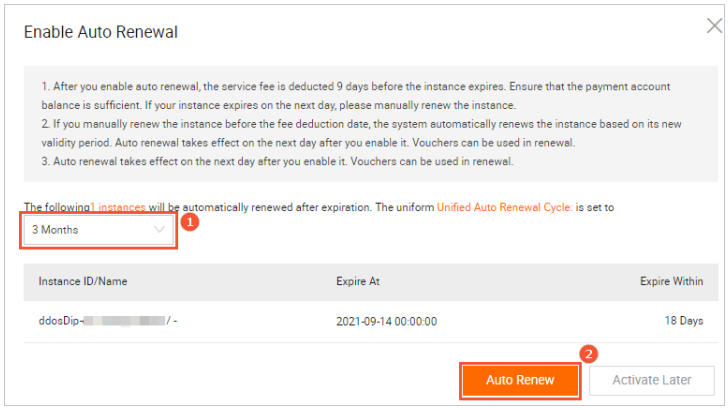
You can enable auto-renewal only within two or more calendar days before the instance expires. If your instance is about to expire the following day, you must manually renew the instance.

You can perform the following steps to enable auto-renewal for your instance.

1.
2. In the top navigation bar, choose **Expenses > Renewal Management**.



3. On the **Manual** tab of the Renewal page, find the instance that you want to renew and click **Enable Auto Renewal** in the **Actions** column.
4. In the **Enable Auto Renewal** dialog box, select an **auto-renewal period** and click **Auto Renew**.



After you enable auto-renewal for the instance, you can view the auto-renewal settings of the instance on the **Auto** tab. Alibaba Cloud automatically deducts fees from your account balance to renew your instance nine calendar days before the expiration date. Then, the subscription period of the instance is extended based on the renewal duration that you specified.

If you no longer need auto-renewal for your instance, you can enable **manual renewal** for your instance on the **Auto** tab.

5.6. Manage tags of instance

Anti-DDoS Pro allows you to classify and query instances by using custom tags. After you create a custom tag, you can add the tag to Anti-DDoS Pro instances that have the same purpose or attribute. This allows you to classify instances and query multiple instances at a time. This topic describes how to create and manage custom tags and also query instances based on the tags.

Context

Each tag is a key-value pair. Anti-DDoS Pro poses the following limits on tags:

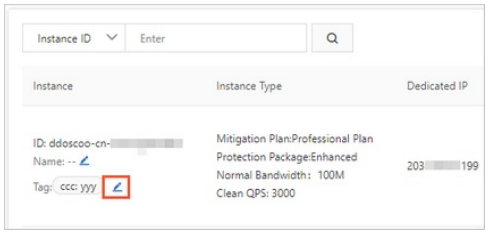
- You can add tags to only Anti-DDoS Pro instances, which are deployed in **mainland China**.
- You can add up to 20 tags to an instance.
- The key of each tag that is added to an instance must be unique. If you add a tag that has the same key as an existing tag, the value of the new tag overwrites that of the existing tag.
- Each tag must be added to at least one instance.

Add a tag

1.

2.
3.
4. On the **Instances** page, find the instance to which you want to add a tag and click the

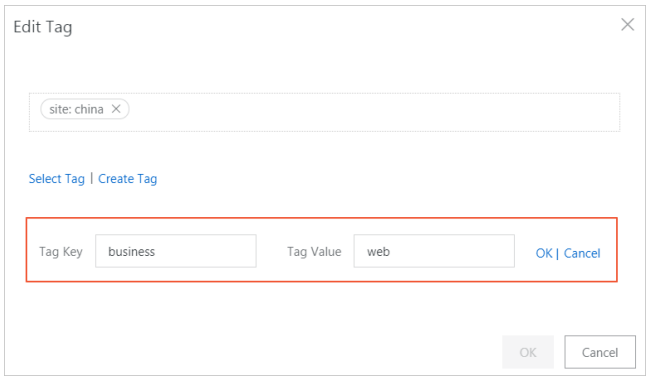
   icon next to a **tag** in the **Instance** column.



5. In the **Edit Tag** dialog box, add a tag to the instance.

   You can use one of the following methods to add a tag to the instance:

   - To add an existing tag, you can click **Select Tag** and select a tag key and a tag value from the tag list.
   - To create a tag, you can click **Create Tag**, specify **Tag Key** and **Tag Value**, and then click **OK**.

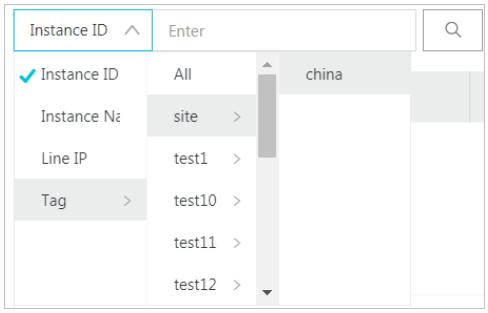


   You can add more than one tag to the instance.

6. Click **OK**.
   After the tag is added, you can view the tag in the **Instance** column.

Query instances based on tags

1.
2.
3.
4. On the **Instances** page, select **Tag** from the drop-down list next to the search box and select the tag key and value.



Instances that have the specified tag are displayed in the instance list.

Remove a tag

You can remove tags from only one instance at a time.

1.
2.
3.
4. On the **Instances** page, find the instance from which you want to remove a tag and click the

   icon next to a **tag** in the **Instance** column.
5. In the **Edit Tag** dialog box, click the

   icon next to the tag that you want to remove and click **OK**.

> **Note** After a tag is removed from an instance, the tag is deleted if it is not added to other instances.

5.7. Apply for and use Anti-DDoS plans

Anti-DDoS plans are a value-added feature that is provided by Anti-DDoS Pro. The plans can be used to offset the bandwidth fees that are charged for protecting your workloads against volumetric DDoS attacks after the basic protection bandwidth is exhausted.

What are Anti-DDoS plans

In most cases, if the peak throughput of DDoS attacks exceeds the basic protection bandwidth, you can use burstable protection to protect your workloads or deactivate blackhole filtering.

- If you use burstable protection, you can adjust the bandwidth based on the peak throughput. Fees are charged based on the difference between the basic protection bandwidth and the bandwidth used to protect your workloads against DDoS attacks. For more information, see Anti-DDoS Pro billing methods. If you adopt this protection approach, additional fees are charged
- If you do not use burstable protection, the bandwidth of burstable protection equals the basic protection bandwidth. In this case, if the attack throughput exceeds the basic protection bandwidth, blackhole filtering is triggered. After the attacks stop, you must deactivate blackhole filtering to recover your workloads. This protection approach has negative impacts on your workloads. However,

no additional fees are charged.

If the attack throughput exceeds the basic protection bandwidth, you can use an Anti-DDoS plan to protect your workloads without paying additional fees.

> **Note** Only Anti-DDoS Pro supports Anti-DDoS plans. If you use Anti-DDoS Premium, you cannot use Anti-DDoS plans.

An Anti-DDoS plan consists of the protection bandwidth and the mitigation sessions. In this example, you have an Anti-DDoS plan that provides up to three mitigation sessions and can be used to offset the fees that are charged for up to 300 Gbit/s of protection bandwidth.

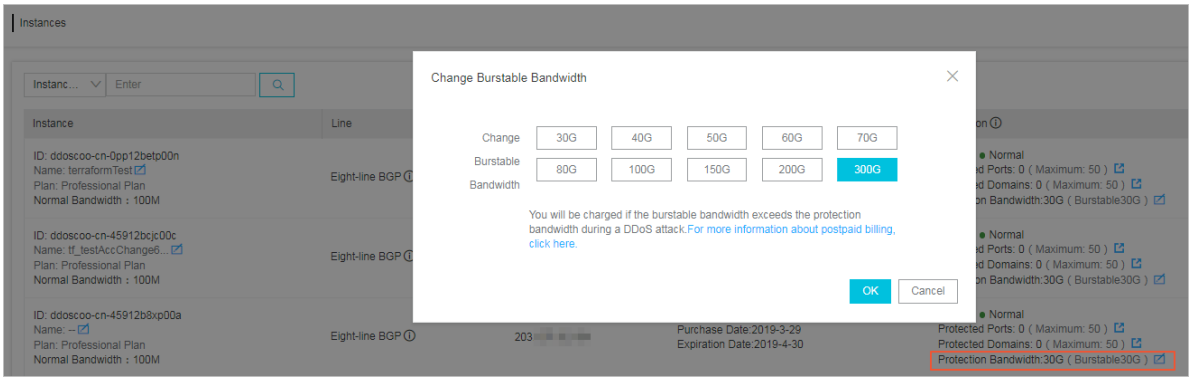
- 300 Gbit/s: If the basic protection bandwidth is exhausted, the plan can be used to offset the fees that are charged for up to 300 Gbit/s of protection bandwidth. If the attack throughput is greater than the basic protection bandwidth plus 300 Gbit/s, you cannot use the plan to offset the protection fees. In this case, fees are charged based on the actual usage. For more information, see Anti-DDoS Pro billing methods.
- Three mitigation sessions: The plan can be used three times. No matter how many attacks occur within one day, only one mitigation session is consumed.

If you use Anti-DDoS plans, take note of the following items:

- Anti-DDoS plans do not improve protection capacity. You can use a plan to offset only the fees that are charged for burstable protection within the protection bandwidth of the plan. The protection capacity is based on the basic protection bandwidth and burstable protection bandwidth.

  We recommend that you adjust the burstable protection bandwidth to use a plan in a more efficient manner. You can change the maximum bandwidth of burstable protection to the total amount of the basic protection bandwidth plus the protection bandwidth of the plan.

  For example, if the basic protection bandwidth is 30 Gbit/s and the protection bandwidth of the plan is 300 Gbit/s, you can set the burstable protection bandwidth to 330 Gbit/s. The actual bandwidth must be within the supported bandwidth range.



- If the difference between the peak attack throughput and the basic protection bandwidth equals to or is smaller than the protection bandwidth of a plan, you can use the plan to offset burstable protection fees.
- If you consume all the mitigation sessions of the plan, we recommend that you set the burstable protection bandwidth to the basic protection bandwidth at the first opportunity to avoid unexpected burstable protection fees.
- You can use the plan to offset fees that are charged for burstable protection bandwidth only on or after the day you obtain the plan. However, if the bills for burstable protection bandwidth are generated, you cannot use the plan.

Differences of Anti-DDoS plans between Anti-DDoS Pro and Anti-DDoS Pro of the previous version

Item	Anti-DDoS Pro of the previous version	Anti-DDoS Pro
Prerequisites	You must associate a plan with the IP address of an Anti-DDoS Pro instance.	You do not need to associate a plan with the IP address of an Anti-DDoS Pro instance. Anti-DDoS Pro instances automatically select the plan that has the earliest expiration time.
Deductible fees	Offsets pay-as-you-go bills generated upon burstable protection within the protection bandwidth of the plan.	Offsets pay-as-you-go bills generated by the amount calculated based on the following formula: Peak attack throughput - Basic protection bandwidth.

Apply for Anti-DDoS plans

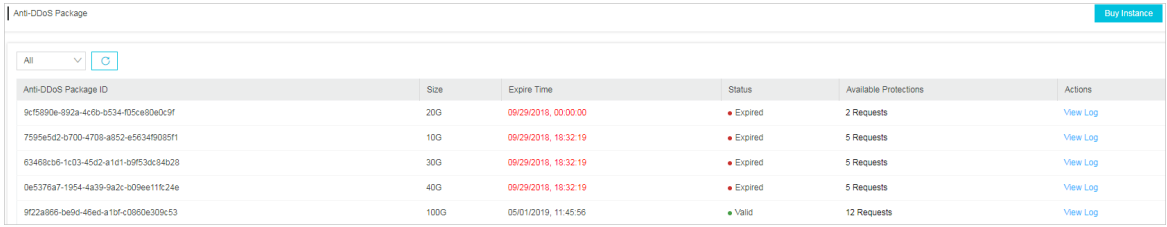
Anti-DDoS plans are a free value-added feature. If you meet one of the following requirements, contact the sales manager or customer service in the DingTalk service group or submit a to apply for this feature.

- You have purchased an Anti-DDoS Pro instance for the first time.
- You have been using Anti-DDoS Pro for more than three months.
- You have purchased an Anti-DDoS Pro instance on an annual subscription basis.

Use Anti-DDoS plans

After you obtain an Anti-DDoS plan, the plan is automatically applied if DDoS attacks occur and the conditions of applying the plan are met. You can check the details of the plan and usage records in the Anti-DDoS Pro console. A plan is effective only within its validity period and if the plan still has remaining mitigation sessions.

1.
2. In the top navigation bar, select **Mainland China**.
3.
4. On the **Anti-DDoS Package** page, view details of all plans.
   - **Anti-DDoS Package ID**: the unique identifier of a plan.
   - **Size**: the size of a plan.
   - **Expire Time**: the time when a plan expires.
   - **Status**: the status of a plan. Valid values: Valid, Exhausted, and Expired.
   - **Available Protections**: the number of remaining mitigation sessions.



5. Click **View Log** in the Actions column to view the records of operations.

5.8. Purchase global advanced mitigation sessions

An Anti-DDoS Premium instance of the Insurance mitigation plan or of the Secure Mainland China Acceleration (Sec-MCA) mitigation plan provides two advanced mitigation sessions free of charge per month. If the two advanced mitigation sessions that are provided each month cannot meet your business requirements, we recommend that you purchase global advanced mitigation sessions to improve mitigation capabilities.

Types of global advanced mitigation sessions

Global advanced mitigation sessions are categorized into the following types:

- Global advanced mitigation session for the Insurance mitigation plan: This type is available only for Anti-DDoS Premium instances of the Insurance mitigation plan.
- Global advanced mitigation session for the Sec-MCA mitigation plan: This type is available only for Anti-DDoS Premium instances of the Sec-MCA mitigation plan.

Method to use global advanced mitigation sessions

If the two advanced mitigation sessions that are provided free of charge are exhausted within a month and a volumetric attack whose traffic exceeds the clean bandwidth of your Anti-DDoS Premium instance occurs, Anti-DDoS Premium starts to consume the global advanced mitigation sessions that you purchase to protect your service.

The global advanced mitigation sessions are shared by all valid Anti-DDoS Premium instances of the Insurance mitigation plan and of the Sec-MCA mitigation plan within your Alibaba Cloud account. You are not required to bind the global advanced mitigation sessions to the instances.

The validity period of global advanced mitigation sessions is one year. After you purchase global advanced mitigation sessions, you must use the global advanced mitigation sessions within one year. If you do not use the global advanced mitigation sessions within one year, the global advanced mitigation sessions expire and cannot be used.

> **Notice** After you purchase global advanced mitigation sessions, you cannot request a refund of the fees that you paid.

For more information about the billing methods of global advanced mitigation sessions, see Billing methods of global advanced mitigation sessions.

Limits on the use of advanced mitigation sessions

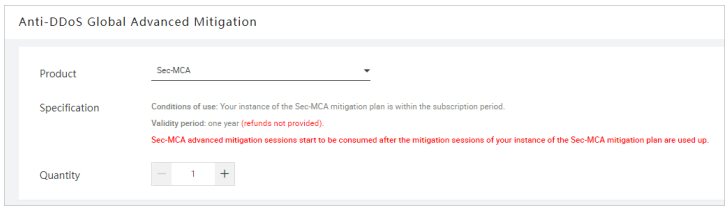
Each Alibaba Cloud account can use advanced mitigation sessions up to 20 times per calendar month. The advanced mitigation sessions include the advanced mitigation sessions that are provided free of charge and the global advanced mitigation sessions that you purchase. After your Alibaba Cloud account uses advanced mitigation sessions for 20 times within a calendar month, the advanced mitigation feature is disabled.

In this case, you cannot use the advanced mitigation feature for the current calendar month. You can only continue to use the feature in the following calendar month.

Note If your business frequently experiences volumetric DDoS attacks, we recommend that you purchase an Anti-DDoS Premium instance of the Ultimate mitigation plan. The instance provides unlimited advanced mitigation sessions.

Procedure

1.
2.
3.
4. In the upper-right corner of the **Instances** page, click **Purchase**.
5. On the **Global Advanced Mitigation** page, select **Insurance** or **Sec-MCA** for **Product**, and set **Quantity** to the number of global advanced mitigation sessions that you want to purchase.



6. Click **Buy Now** and complete the payment.
   After you purchase global advanced mitigation sessions, you can view the numbers of available advanced mitigation sessions for the Anti-DDoS Premium instances of the Insurance mitigation plan and of the Sec-MCA mitigation plan above the instance list.

   To view the global advanced mitigation sessions that you purchase and the validity period of the global advanced mitigation sessions, log on to the Billing Management console and choose **Resource Packages > Overview**.

6.Query and analysis

6.1. View information on the Attack Analysis page

After you add your service to Anti-DDoS Pro or Anti-DDoS Premium, you can view the events and details of attacks on the Attack Analysis page. This way, you can view the protection status of your service. You can also provide feedback on the protection effect. This topic describes how to view information on the Attack Analysis page.

Prerequisites

- An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased.

  For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

- Your service is added to Anti-DDoS Pro or Anti-DDoS Premium.

  For more information about how to add website services, see Add a website.

  For more information about how to add non-website services, such as client gaming, mobile gaming, and app services, see Create forwarding rules.

Context

The **Attack Analysis** page displays DDoS attack events and the event details. On the **Attack Analysis** page, you can view the information about an attack event, such as the attack target, start time and end time of the attack, and peak attack traffic. You can also provide feedback on the protection effect.

DDoS attack events are classified into the following types:

- **Volumetric** attack events: Attackers send a multitude of service requests from a large number of zombie servers to the IP address of an Anti-DDoS Pro or Anti-DDoS Premium instance at the same time. As a result, the network devices and servers are overloaded, and network congestion and service failures may occur.

  If attackers send service requests to multiple IP addresses of your Anti-DDoS Pro instances or Anti-DDoS Premium instances at the same time, multiple volumetric attack events are recorded.

- Events of **web resource exhaustion** attacks: Attackers simulate normal users to send service requests to a web service whose domain name is added to an Anti-DDoS Pro or Anti-DDoS Premium instance. The attackers frequently access pages that consume large amounts of resources in the web service. As a result, the resources of the servers are exhausted, and the web service cannot respond to normal service requests. For more information about how to add a domain name to an Anti-DDoS Pro or Anti-DDoS Premium instance, see Add a website.

  If attackers send service requests to multiple domain names that are protected by an Anti-DDoS Pro or Anti-DDoS Premium instance at the same time, multiple events of web resource exhaustion attacks are recorded.

- Events of **connection flood** attacks: Attackers establish TCP or UDP connections to a service port that is added to an Anti-DDoS Pro or Anti-DDoS Premium instance. As a result, the servers of the service are overloaded and cannot process new connection requests, and service failures may occur. For more information about how to add a service port to an Anti-DDoS Pro or Anti-DDoS Premium

instance by using ports, see Create forwarding rules.

If attackers send connection requests to multiple service ports that are added to an Anti-DDoS Pro or Anti-DDoS Premium instance at the same time, multiple events of connection flood attacks are recorded.

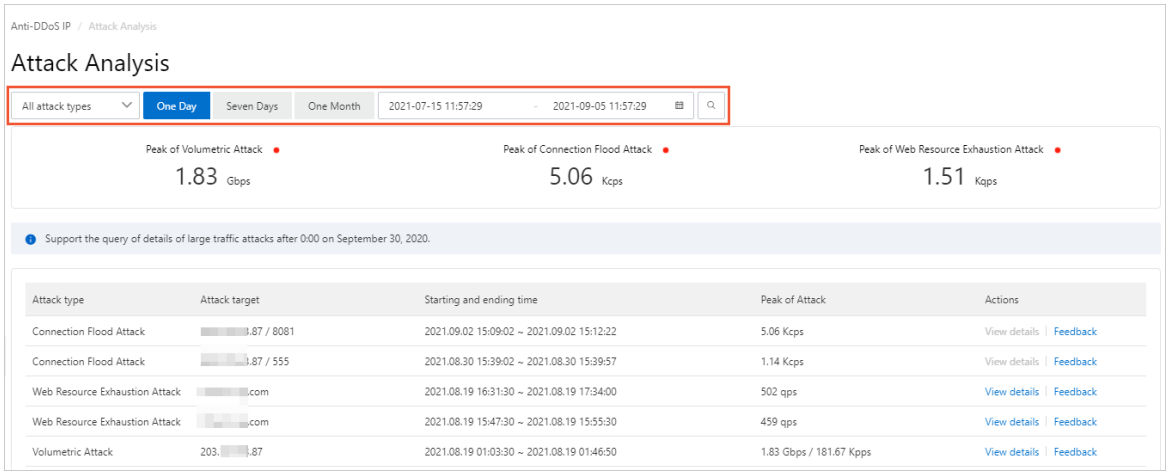
You can also view the event details on the **Attack Analysis** page. The details include the source IP addresses, attack types, and source locations. This allows you to view the attack mitigation process in a visualized manner. This also improves user experience.

Query attack events

1.
2.
3.
4. On the **Attack Analysis** page, select an attack type and a time range to query attack events.

   The following attack types and time ranges are supported:

   - Attack type: **Web Resource Exhaustion Attack**, **Connection Flood Attack**, **Volumetric Attack**, or **All attack types**.
   - Time range: **One Day**, **Seven Days**, or **One Month**. You can also specify a custom time range. A custom time range must be within the last 180 days.



   The **Attack Analysis** page displays the following information:

   - In the upper part of the page, **Peak of Volumetric Attack (bps)**, **Peak of Connection Flood Attack (cps)**, and **Peak of Web Resource Exhaustion Attack (qps)** are displayed.
   - In the lower part of the page, attack events are displayed. The information about each attack event includes **Attack type**, **Attack target**, **Starting and ending time**, and **Peak of Attack**.

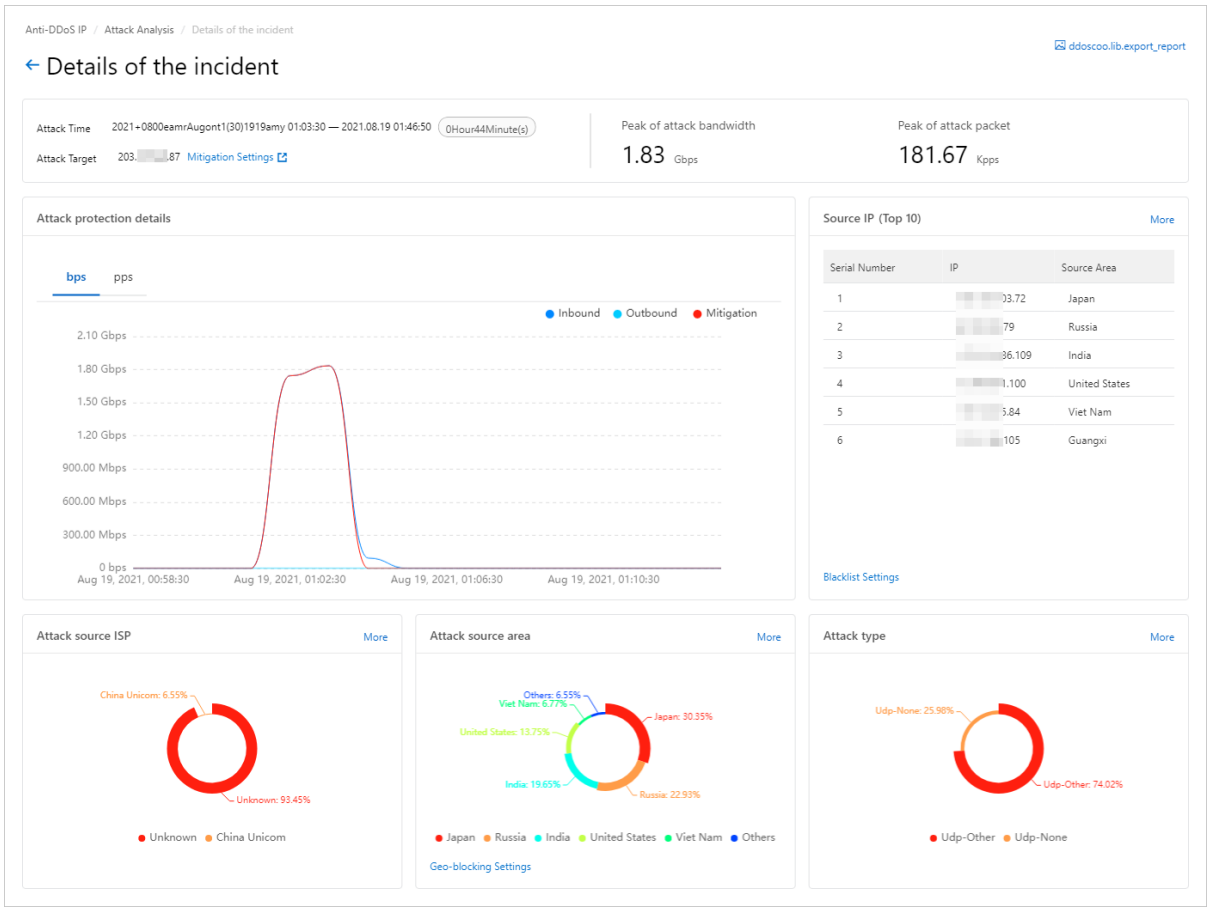
   If you have suggestions or questions about the protection effect on an attack event, click **Feedback** in the **Actions** column to submit your feedback. All your suggestions are appreciated.

   You can view the details about an attack event. You can click **View details** in the **Actions** column of an attack event to view the event details. For more information, see View event details of volumetric attacks, View event details of web resource exhaustion attacks, and View event details of connection flood attacks.

View event details of volumetric attacks

On the **Attack Analysis** page, find a **Volumetric Attack** event and click **View details** in the Actions column. The **Details of the incident** page appears. You can view the event details and configure protection settings.

> **Notice** You can query the event details of volumetric attacks that occur after 00:00 on September 30, 2020.



The **Details of the incident** page displays the following information:

- In the upper part of the page, **Attack Time**, **Attack Target**, **Peak of attack bandwidth (bps)**, and **Peak of attack packet (pps)** are displayed. The Attack Target parameter indicates the IP address of an Anti-DDoS Pro or Anti-DDoS Premium instance.

  You can click **Mitigation Settings** next to **Attack Target**. On the **Protection for Infrastructure** tab of the page that appears, you can configure mitigation policies for the Anti-DDoS Pro or Anti-DDoS Premium instance that is attacked. For more information, see Configure the IP address blacklist and whitelist for an Anti-DDoS Pro or Anti-DDoS Premium instance.

- **Attack protection details**: displays the trends of inbound and outbound traffic, the traffic scrubbing bandwidth, and the packets during the attack. The **bps** tab displays the trends of inbound and outbound traffic and the traffic scrubbing bandwidth. The **pps** tab displays the trends of packets.
- **Attack source IP**: displays the top 10 IP addresses from which the most attacks are launched and the locations to which the IP addresses belong. You can click **More** to view information about the top 100 source IP addresses.

> **Note** The top source 100 IP addresses include the source IP addresses of attacks and the source IP addresses of normal requests.

If you want to block traffic from specific IP addresses, click **Blacklist Settings** in the lower-left corner of the Attack source IP section. On the **Protection for Infrastructure** tab of the page that appears, configure **Blacklist and Whitelist (Instance IP)**. For more information, see Configure the IP address blacklist and whitelist for an Anti-DDoS Pro or Anti-DDoS Premium instance.

- **Attack source ISP**: displays the distribution of Internet service providers (ISPs) from which attack traffic originates. You can click **More** to view the distribution of requests by ISP.

  > **Notice** The Attack source ISP section is available only in the Anti-DDoS Pro console.

- **Attack source area**: displays the distribution of locations from which attack traffic originates. You can click **More** to view the distribution of requests by location.

  If you want to block traffic from specific locations, click **Geo-blocking Settings** in the lower-left corner of the Attack source area section. On the **Protection for Infrastructure** tab of the page that appears, configure **Blocked Regions**. For more information, see Configure blocked regions.

- **Attack type**: displays the distribution of protocols that are used to launch attacks. You can click **More** to view the distribution of attack types by protocol.

In the upper-right corner of the **Details of the incident** page, you can click **Export Report**, and then click **Export as PNG** or **Export as PDF** to save the current event details page to your computer in the PNG or PDF format.

View event details of web resource exhaustion attacks

On the **Attack Analysis** page, find a **Web Resource Exhaustion Attack** event and click **View details** in the Actions column. The **Details of the incident** page appears.You can view the event details and configure protection settings.

> **Notice** You can query the event details of web resource exhaustion attacks that occur after 00:00 on July 15, 2021.

The **Details of the incident** page displays the following information:

- In the upper part of the page, **Attack Time**, **Attack Target**, **Peak Requests (QPS)**, **Total Received Requests**, and **Total Blocked Requests** are displayed. The Attack Target parameter indicates the domain name that is added to an Anti-DDoS Pro or Anti-DDoS Premium instance.

  You can click **Mitigation Settings** next to **Attack Target**. On the **Protection for Website Services** tab of the page that appears, you can configure mitigation policies for the attacked domain name. For more information, see Use the intelligent protection feature.

- **Attack protection details**: displays the total inbound queries per second (QPS), the trends of the QPS that trigger the policies of different protection modules during the attack, and **Effective Time of Policies** and **Blocked Requests** of the triggered policies.

  The protection modules include **Blacklist**, **Blocked Regions**, **Frequency Control**, **Accurate Access Control**, and **Others**. The Others protection module blocks requests such as the requests that fail CAPTCHA verification. For more information about how to configure different protection modules, see Use the intelligent protection feature.

In the upper-right corner of the Attack protection details section, you can specify a time range to query.

- **Source Areas of Attacks**: displays the distribution of locations from which attack requests originate. You can switch between **Global** and **Mainland China** to view locations by country or by administrative region in China. You can click **More** to view the distribution of requests by location.

  If you want to block requests from specific locations, click **Mitigation Settings** in the lower-left corner of the Source Areas of Attacks section. On the **Protection for Website Services** tab of the page that appears, configure **Blocked Regions (Domain Names)**. For more information, see Configure a location blacklist for a domain name.

- **URL**: displays the top five URLs that receive the most requests. The URLs are displayed in descending order of the number of received requests. You can click **More** to view all requested URLs and the distribution of the URLs. After you click More, the requested URIs and the domain names to which the URIs belong are displayed.

  If you want to configure throttling policies for specific URIs, click **Mitigation Settings** in the lower-left corner of the URL section. On the **Protection for Website Services** tab of the page that appears, configure **Frequency Control**. For more information, see Configure frequency control.

- **Requests Blocked by Protection Modules**: displays the distribution of requests that are blocked by different protection modules.

  You can click **Mitigation Settings** in the lower-left corner of the Requests Blocked by Protection Modules section. On the **Protection for Website Services** tab of the page that appears, configure policies for different protection modules. For more information, see Use the intelligent protection feature.

- **Top 10 Policies**: displays the distribution of the top 10 policies that are most frequently triggered. You can click **More** to view the distribution of the top 100 protection policies that are most frequently triggered.

  You can click **Mitigation Settings** in the lower-left corner of the Top 10 Policies section. On the **Protection for Website Services** tab of the page that appears, configure policies for different protection modules. For more information, see Use the intelligent protection feature.

In the upper-right corner of the **Details of the incident** page, you can click **Export Report**, and then click **Export as PNG** or **Export as PDF** to save the current event details page to your computer in the PNG or PDF format.

View event details of connection flood attacks

On the **Attack Analysis** page, find a **Connect Flood Attack** event and click **View details** in the Actions column. The **Details of the incident** page appears.You can view the event details and configure protection settings.

> **Notice** You can query the event details of connection flood attacks that occur after 00:00 on September 20, 2021.

The **Details of the incident** page displays the following information:

- In the upper part of the page, **Attack Time**, **Attack Target**, **Maximum Concurrent Connections**, and **Maximum New Connections** are displayed. The Attack Target parameter indicates the IP address and port number of an Anti-DDoS Pro or Anti-DDoS Premium instance. The value of the Maximum Concurrent Connections parameter indicates the maximum number of concurrent connections. The value of the Maximum New Connections parameter indicates the maximum number

of new connections per second.

You can click **Mitigation Settings** next to **Attack Target**. On the **Protection for Infrastructure** tab of the page that appears, you can configure mitigation policies for the Anti-DDoS Pro or Anti-DDoS Premium instance that is attacked. For more information, see Configure the IP address blacklist and whitelist for an Anti-DDoS Pro or Anti-DDoS Premium instance.

- **Attack protection details**: displays the trends of **new connections** and **concurrent connections**.

  The trend of new connections displays suspicious connections that are blocked by different mitigation policies. The mitigation policies include **Blacklist**, **Blocked Regions**, and **Speed Limit for Source**. The Speed Limit for Source policy includes **Source Concurrent Connection Rate Limit**, **PPS Limit for Source**, and **Bandwidth Limit for Source**. For more information about how to configure the mitigation policies, see Configure the IP address blacklist and whitelist for an Anti-DDoS Pro or Anti-DDoS Premium instance, Configure blocked regions, and Configure the speed limit for source IP addresses.

  The trend of concurrent connections displays **active** and **inactive** connections.

  In the upper-right corner of the Attack protection details section, you can specify a time range to query.

- **Attack source IP**: displays the top five IP addresses from which the most suspicious connections are established and the locations to which the IP addresses belong. You can click **More** to view information about the top 100 source IP addresses of attacks.

  > **Note** You can view only the top 100 source IP addresses of attacks.

  If you want to block traffic from an IP address, you can configure the **Blacklist and Whitelist (Instance IP)** policy for the instance that is attacked. For more information, see Configure the IP address blacklist and whitelist for an Anti-DDoS Pro or Anti-DDoS Premium instance.

- **Attack type**: displays the distribution of protocols that are used to initiate attacks. You can click **More** to view the distribution of attack types by protocol.
- **Attack source area**: displays the distribution of locations from which attack requests originate. You can click **More** to view the distribution of requests by location.

  If you want to block requests from a location, you can configure the **Blocked Regions** policy for the instance that is attacked. For more information, see Configure blocked regions.

In the upper-right corner of the **Details of the incident** page, you can click **Export Report**, and then click **Export as PNG** or **Export as PDF** to save the current event details page to your computer in the PNG or PDF format.

6.2. Log analysis

6.2.1. Overview

Anti-DDoS Pro and Anti-DDoS Premium are integrated with Alibaba Cloud Log Service to collect and analyze full logs of website access. Log Analysis is a value-added feature. You must enable this feature before you can use it. After you enable Log Analysis, Log Service collects the access logs of the website that is protected by Anti-DDoS Pro or Anti-DDoS Premium in real time. Then, you can query and analyze the logs, and view the log reports.

Description of Log Analysis

The Log Analysis feature of Anti-DDoS Pro or Anti-DDoS Premium is provided based on Log Service. You can query and analyze logs in the Anti-DDoS Pro console. This helps you analyze your website services that are protected by Anti-DDoS Pro or Anti-DDoS Premium. After you enable Log Analysis, you can consume and deliver logs by using Log Service. This allows you to manage the website access logs of Anti-DDoS Pro or Anti-DDoS Premium.

For more information about Log Service, see What is Log Service?.

Scenarios

You can use Log Analysis in the following scenarios:

- Troubleshoot website access issues

  After Log Analysis is enabled for your website, you can query and analyze logs that are collected from the website in real time. For example, you can use SQL statements to analyze website access logs and use the analysis results to troubleshoot and analyze access issues, and view information, such as the read and write latencies and the distribution of Internet service providers (ISPs).

- Track HTTP flood attacks

  Website access logs record the sources and distribution of HTTP flood attacks. You can query and analyze access logs in real time to identify the attack sources and track attack events. This helps you choose appropriate protection policies. For example, you can analyze the geographical distribution of HTTP flood attacks and query page views (PVs) of your website.

- Analyze website operations

  Website access logs record information about website traffic in real time. You can use SQL statements to query and analyze logs and obtain real-time information about website operations. For example, you can identify the most visited websites, source IP addresses of the clients, the browsers that initiated the requests, and the distribution of clients to facilitate the analysis of website operations.

Billing

Log Analysis supports only the subscription billing method. For more information, visit the buy page of Log Analysis.

References

Topic	Description
Quick start	This topic describes how to enable and use Log Analysis. **Notice** If this is the first time you use Log Analysis, you must enable and configure the feature based on this topic.
Fields included in full logs	This topic describes the fields that are included in the logs of Anti-DDoS Pro or Anti-DDoS Premium.

Topic	Description
Query and analyze logs	This topic describes how to use query and analysis statements to query and analyze the logs of Anti-DDoS Pro or Anti-DDoS Premium.
Query log reports	This topic describes how to use the DDoS Access Center and DDoS Operation Center dashboards that are preset in Log Analysis.

6.2.2. Billing

The Log Analysis feature uses the subscription billing method. The fees are calculated based on the log storage capacity that you purchase.

Overview

The Log Analysis feature is a value-added capability that is provided by Anti-DDoS Pro and Anti-DDoS Premium. However, you must separately purchase this feature. After you add your websites to your Anti-DDoS Pro or Anti-DDoS Premium instance, the instance does not store the access logs of the websites. If you want to store the access logs and use the access logs for business analysis, you must enable the Log Analysis feature.

To enable the Log Analysis feature, you can go to the buy page of Log Analysis. You are charged for the Log Analysis feature based on the **log storage capacity** and **log storage duration** that you select. For more information about how to enable the Log Analysis feature, see Step 1: Enable Log Analysis.

After you enable the Log Analysis feature, a Log Analysis instance is provided. You can use the Log Analysis feature to collect the access logs of your websites within the validity period of the Log Analysis instance. You can query and analyze the access logs, and configure alerts based on the access logs.

Notice The Log Analysis instance and the Anti-DDoS Pro or Anti-DDoS Premium instance are independent of each other and must be separately managed. For example, you must separately renew the Anti-DDoS Pro or Anti-DDoS Premium instance and the Log Analysis instance.

Log storage specifications

Specification	Impact on billing	Description	Modification supported after the Log Analysis feature is enabled

Specification	Impact on billing	Description	Modification supported after the Log Analysis feature is enabled
Log storage capacity	Yes	When you enable the Log Analysis feature, you must specify the log storage capacity. The log storage capacity is measured in TB. The fees that are displayed on the buy page of Log Analysis shall prevail.	Supported. After you enable the Log Analysis feature, you can perform the following operations to modify the log storage capacity: • Upgrade your Log Analysis instance to increase the log storage capacity. For more information, see Increase the log storage capacity. • Downgrade your Log Analysis instance to decrease the log storage capacity. For more information, see Decrease the log storage capacity. **Warning** If the log storage capacity is exhausted, new logs cannot be stored and are lost. Logs that are stored longer than the log storage duration that you specify are automatically deleted. When the log storage capacity is exhausted, you can upgrade your Log Analysis instance to increase the log storage capacity or delete logs. For more information about how to delete logs, see Delete logs.
Log storage duration	No	By default, logs are stored for 180 days.	Supported. After you enable the Log Analysis feature, you can customize the log storage duration. You can specify a value that ranges from 30 days to 180 days. For more information, see Modify the log storage duration.

Specificati on	Impact on billing	Description	Modification supported after the Log Analysis feature is enabled
Storage object	No	Only the full logs of the websites for which log collection is enabled are stored.	Supported. After you enable the Log Analysis feature, you can enable or disable log collection for the websites that are added to your Anti-DDoS Pro or Anti-DDoS Premium instance. For more information, see Step 2: Enable the log collection feature.
Log field	No	For more information about the log fields that are included in the full logs of Anti-DDoS Pro or Anti-DDoS Premium, see Fields included in full logs.	Not supported.

Method to select a log storage capacity

The following example shows how to select the required log storage capacity based on the daily QPS of your website:

In most cases, each request log occupies approximately 2 KB of storage. If the average QPS of your website is 500, the required storage for the logs that are generated within a day is 86,400,000 KB, which is approximately 82 GB. This value is calculated by using the following formula: 500 × 60 × 60 × 24 × 2 = 86,400,000. If you want to store logs that are generated within 180 days, the required log storage capacity is 15,552,000,000 KB, which is approximately 14.5 TB. This value is calculated by using the following formula: 86,400,000 × 180 = 15,552,000,000.

Expiration

When your Log Analysis instance expires, the following issues occur:

- Anti-DDoS Pro or Anti-DDoS Premium no longer stores new logs.
- The logs that are stored are retained for seven days.

  If you renew your Log Analysis instance within seven days, you can continue to use this instance. Otherwise, all logs are deleted.

  For more information about how to renew your Log Analysis instance, see Renew a Log Analysis instance.

6.2.3. Fields included in full logs

This topic describes the fields that are included in the full logs of Anti-DDoS Pro or Anti-DDoS Premium.

Field	Description	Example
__topic__	The topic of the log. The value is fixed as ddos_access_log, which indicates the logs of Anti-DDoS Pro or Anti-DDoS Premium.	ddos_access_log
body_bytes_sent	The size of the body in the request. Unit: bytes.	2
content_type	The type of the content.	application/x-www-form-urlencoded
host	The requested domain name.	api.aliyundoc.com
http_cookie	The request cookie.	k1=v1;k2=v2
http_referer	The referer of the request. If the referer does not exist, a hyphen (-) is returned.	http://aliyundoc.com
http_user_agent	The user agent of the request.	Dalvik/2.1.0 (Linux; U; Android 10; Android SDK built for x86 Build/QSR1.200715.002)
http_x_forwarded_for	The IP address of the upstream proxy.	192.0.XX.XX
https	Indicates whether the request is an HTTPS request. Valid values: true and false.	true
matched_host	The domain name that is matched, which can be a wildcard domain name. If no domain names are matched, a hyphen - is returned.	*.aliyundoc.com
real_client_ip	The actual IP address of the client. If no actual IP addresses are retrieved, a hyphen - is returned.	192.0.XX.XX
isp_line	The information about the Internet service provider (ISP) line, such as Border Gateway Protocol (BGP), China Telecom, or China Unicom.	China Telecom
remote_addr	The IP address from which the request is initiated.	192.0.XX.XX
remote_port	The ID of the port from which the request is initiated.	23713
request_length	The size of the request. Unit: bytes.	123
request_method	The HTTP method of the request.	GET
request_time_msec	The processing time of the request. Unit: milliseconds.	44

Field	Description	Example
request_uri	The URI of the request.	/answers/377971214/banner
server_name	The name of the origin server that is matched. If no origin servers are matched, `default` is returned.	api.aliyundoc.com
status	The HTTP status code.	200
time	The time of the request.	2018-05-02T16:03:59+08:00
cc_action	The action that is triggered in an HTTP flood mitigation policy. Valid values include none, challenge, pass, close, captcha, wait, and login.	close
cc_blocks	Indicates whether the request is blocked by an HTTP flood mitigation policy. • The value `1` indicates that the request is blocked. • Other values indicate that the request is allowed. **Note** In some cases, a log does not contain this field. If a log does not contain the cc_blocks field, the `last_result` field is used to record whether the request is blocked by an HTTP flood mitigation policy.	1
last_result	The final action on the request. Valid values: • `ok`: The request is allowed. • `failed`: The request is not allowed. For example, the request is blocked, or the verification fails. **Note** In some cases, a log does not contain this field. If a log does not contain the last_result field, the `cc_blocks` field is used to record whether the request is blocked by an HTTP flood mitigation policy.	failed
cc_phase	The HTTP flood mitigation policy. Valid values: seccookie, server_ip_blacklist, static_whitelist, server_header_blacklist, server_cookie_blacklist, server_args_blacklist, and qps_overmax.	server_ip_blacklist
ua_browser	The identifier of the browser. **Note** In some cases, a log does not contain this field.	ie9

Field	Description	Example
ua_browser_family	The series of the browser. Note In some cases, a log does not contain this field.	internet explorer
ua_browser_type	The type of the browser. Note In some cases, a log does not contain this field.	web_browser
ua_browser_version	The version of the browser. Note In some cases, a log does not contain this field.	9.0
ua_device_type	The type of the client. Note In some cases, a log does not contain this field.	computer
ua_os	The identifier of the operating system that runs on the client. Note In some cases, a log does not contain this field.	windows_7
ua_os_family	The series of the operating system that runs on the client. Note In some cases, a log does not contain this field.	windows
upstream_addr	The list of origin addresses that are separated by commas (,). Each address is in the `IP:Port` format.	192.0.XX.XX:443
upstream_ip	The origin IP address.	192.0.XX.XX
upstream_response_time	The response time of the back-to-origin request. Unit: seconds.	0.044
upstream_status	The HTTP status code of the back-to-origin request.	200
user_id	The ID of the Alibaba Cloud account.	166688437215****

Field	Description	Example
querystring	The query string in the request.	token=bbcd&abc=123

6.2.4. Quick start

This topic describes how to enable and use the Log Analysis feature provided by Anti-DDoS Pro or Anti-DDoS Premium.

Prerequisites

- An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased and your website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.

  Before you can use Log Analysis to collect and store the logs of your website, and then query and analyze the collected logs, you must add the website to Anti-DDoS Pro or Anti-DDoS Premium.
- Log Service is activated.

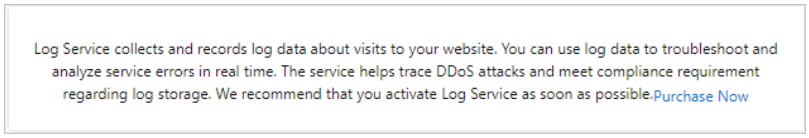
  If this is the first time you log on to the Log Service console, you must activate Log Service as prompted.

Step 1: Enable Log Analysis

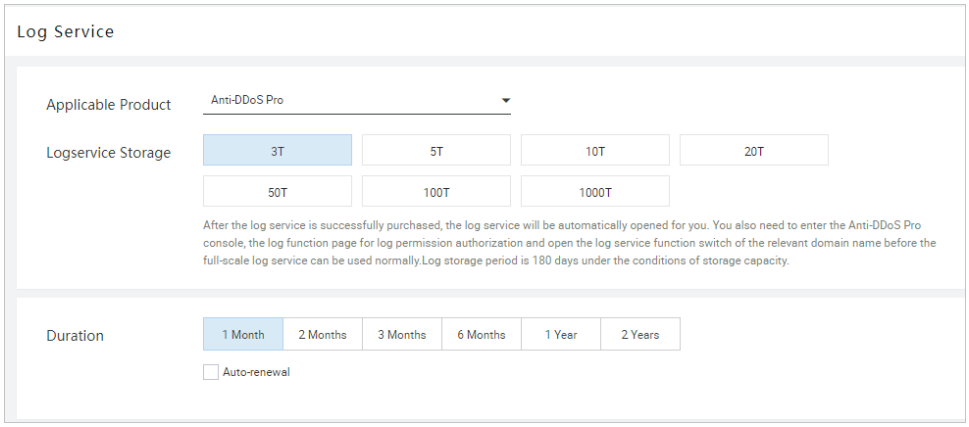
Perform the following steps to enable Log Analysis:

1.
2.
3.
4. On the **Log Analysis** page, click **Purchase Now**.

   If you have enabled Log Analysis, **Purchase Now** does not appear. You can directly use the feature. For more information, see Step 2: Enable the log collection feature.

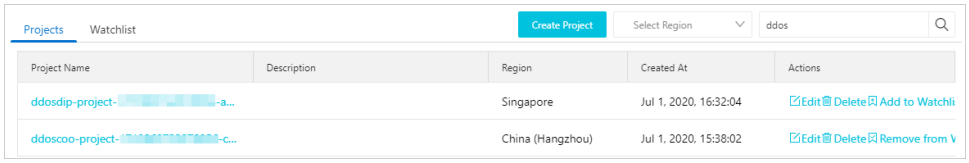
   

5. On the **Log Service** page, configure the following parameters.

Parameter	Description
Applicable Product	Select **Anti-DDoS Pro** or **Anti-DDoS Premium**.
Logservice Storage	Select the capacity to store logs. Unit: TB. Valid values: 3T, 5T, 10T, 20T, 50T, 100T, and 1000T. If log storage is large enough and within the validity period, logs are stored from the first day the feature is used. The logs that are generated within the following 180 consecutive days are stored. Logs from day 181 overwrite logs from day 1, which indicates that the logs generated only within the last 180 days are stored. In most cases, each request log occupies about 2 KB of storage. If the average queries per second (QPS) of your service is 500, the storage required for a day is 86,400,000 KB (about 82 GB). The storage is calculated based on the following formula: 500 x 60 x 60 x 24 x 2 = 86,400,000. If you want to store logs of the last 180 days, the storage required is 14,832 GB (about 14.5 TB), and you need to specify the Logservice Storage parameter based on this value. The default log retention period is 180 days. **Notice** After the log storage is exhausted, new logs cannot be stored.
Duration	Select a validity period for the feature. Valid values: 1 Month, 2 Months, 3 Months, 6 Months, 1 Year, and 2 Years. **Notice** If Log Analysis expires, new logs cannot be stored.

6. Click **Buy Now** and complete the payment.
   After you purchase Log Analysis, Log Service automatically creates a dedicated project for Anti-DDoS Pro or Anti-DDoS Premium. This dedicated project is used to manage the logs of Anti-DDoS Pro or Anti-DDoS Premium. You can view the dedicated project on the homepage of the Log Service console.



   The name of the dedicated project for Anti-DDoS Pro starts with `ddoscoo-project`. The name of the dedicated project for Anti-DDoS Premium starts with `ddosdip-project`.

   A dedicated project for Anti-DDoS Pro or Anti-DDoS Premium contains the following resources:

   - A dedicated Logstore that is used to store the logs of Anti-DDoS Pro or Anti-DDoS Premium. The name of the dedicated Logstore for Anti-DDoS Pro starts with `ddoscoo-logstore`. The name of the dedicated Logstore for Anti-DDoS Premium starts with `ddosdip-logstore`.
   - Two preset log dashboards that are used to display the log analysis results in charts. The dashboards are DDoS Access Center and DDoS Operation Center. The information in the dashboards is the same for both Anti-DDoS Pro and Anti-DDoS Premium.

7. Go to the **Log Analysis** page and authorize Anti-DDoS Pro or Anti-DDoS Premium to store logs to

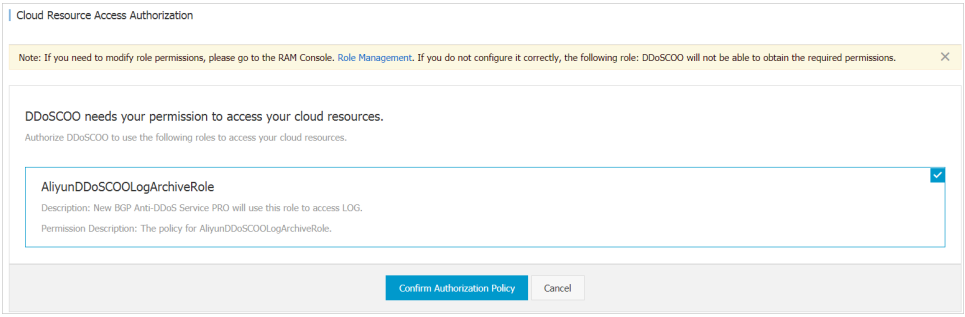
the dedicated Logstore of Log Service.

> **Note** You need to perform the authorization operations only once. If you have completed the authorization, skip this step.

Perform the following steps to authorize Anti-DDoS Pro or Anti-DDoS Premium:

i. Click **Authorize**.

ii. On the **Cloud Resource Access Authorization** page, click **Confirm Authorization Policy**.



After you enable the Log Analysis feature and complete authorization, you can start to use this feature on the **Log Analysis** page. Before you use this feature, you must enable log collection for the domain name of your website. For more information, see Step 2: Enable the log collection feature.

Step 2: Enable the log collection feature

By default, Anti-DDoS Pro and Anti-DDoS Premium do not collect logs of the added websites. Anti-DDoS Pro and Anti-DDoS Premium collect the logs of the websites and store the collected logs to the dedicated Logstores in Log Service only after you enable log collection for the domain names of the websites. Then, you can query and analyze the logs.

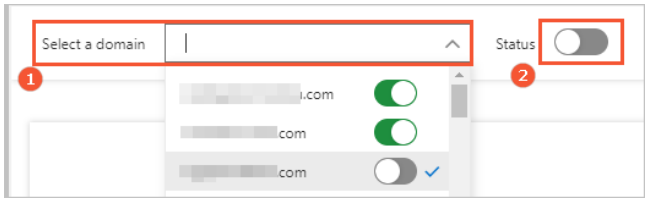
Perform the following steps to enable log collection for the domain name of a website:

1.
2.
3.
4. On the **Log Analysis** page, enable log collection for the domain name of a website.

> **Notice** Before you enable log collection for a domain name, you must add the domain name to Anti-DDoS Pro or Anti-DDoS Premium. The domain name list displays the added domain names.

You can use one of the following methods to enable log collection for domain names:

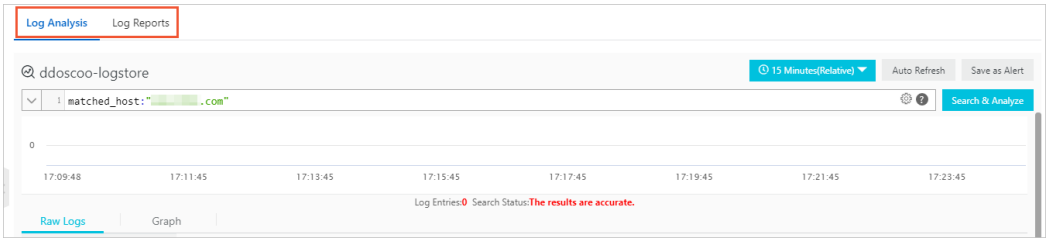
- Enable log collection for a domain name: Select a domain name from the **Select a domain** drop-down list and turn on **Status**.
- Enable log collection for multiple domain names at a time: Click **Batch config** in the upper-right corner of the page. In the **Batch config** panel, select multiple domain names and click **Turn on in a batch**.



After log collection is enabled, Anti-DDoS Pro or Anti-DDoS Premium collects and stores the logs of websites for query and analysis. For more information about how to query and analyze logs, see Step 3: Use Log Analysis.

Step 3: Use Log Analysis

After you enable log collection for a domain name, you can query and analyze the collected logs on the **Log Analysis** tab of the **Log Analysis** page. You can also view the log reports in the dashboards that are preset for Anti-DDoS Pro or Anti-DDoS Premium on the **Log Reports** tab.



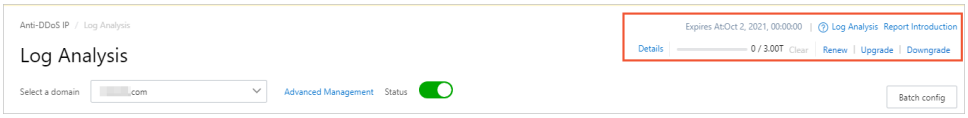
The following table describes the features that are provided on the Log Analysis page. For more information, see Common operations on logs of Alibaba Cloud services.

Tab	Feature	Description	References
Log Analysis	Log query and analysis	You can query and analyze the collected log data in real time. A query and analysis statement consists of a search clause and an analytics clause that are separated by a vertical bar (|). For example, you can use the following statement to query the number of visits to a domain: `* | SELECT COUNT(*) as times, host GROUP by host ORDER by times desc limit 100` For more information about query and analysis statements, see Common query statements.	Query and analyze logs Fields included in full logs
	Analysis results in charts	A query and analysis statement contains the syntax for analytics. After the statement is executed, analysis results are automatically displayed in tables. The analysis results can also be displayed in a variety of charts, such as a line chart, column chart, or pie chart. You can choose a display method based on your business requirements.	Chart overview
	Monitoring and alerting	You can configure alert rules based on the charts in a dashboard to monitor service status in real time.	Alerting overview

Tab	Feature	Description	References
Log Reports	Dashboard	Log Service provides dashboards for you to analyze data in real time. After you query and analyze logs by using query and analysis statements, you can save the charts of analysis results to a dashboard. Log Analysis provides two preset dashboards: **DDoS Access Center** and **DDoS Operation Center**. You can also subscribe to dashboards and send dashboard data to specific recipients by using emails or DingTalk messages.	Query log reports Subscribe to a dashboard

Step 4: Manage the configurations

The specifications of the Log Analysis feature are displayed in the upper-right corner of the **Log Analysis** page. You can perform the following operations in this section:



- Query the validity period of the Log Analysis feature. If Log Analysis is about to expire, you can click **Renew** to extend the validity period of the feature.

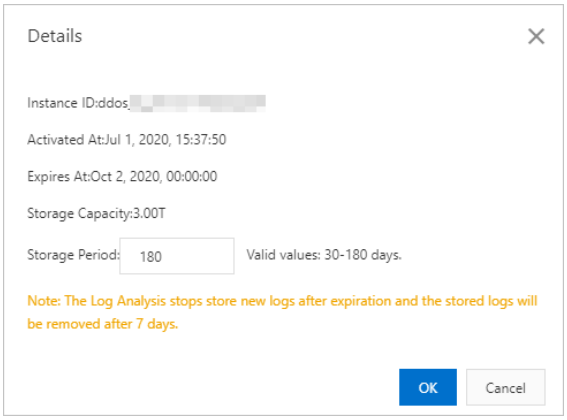
  > **Warning** If Log Analysis expires, new logs cannot be stored. Seven days after Log Analysis expires, all existing logs are cleared.

- Query the usage of log storage. If log storage is to be exhausted, you can click **Upgrade** to expand log storage. Alternatively, you can click **Clear** to delete the logs that are no longer required.

  The usage of log storage displayed in the Anti-DDoS Pro console is not updated in real time. The displayed usage does not include the usage from the last two hours.

  > **Note** We recommend that you check the usage of log storage at regular intervals when you use Log Analysis. When the usage of log storage exceeds 70%, expand the log storage to make sure that new logs can be stored. If a specific amount of log storage remains idle for a long period of time, you can reduce the log storage.

- Change the duration to store logs. Logs are stored for 180 days by default. You can click **Details** and set **Storage Period** to a value that ranges from 30 to 180 in the **Details** dialog box. Unit: days.



Common query statements

- Queries the type of attacks that are blocked.

```
* | select cc_action,cc_phase,count(*) as t group by cc_action,cc_phase order by t desc l
imit 10
```

- Queries the QPS.

```
* | select time_series(__time__,'15m','%H:%i','0') as time,count(*)/900 as QPS group by t
ime order by time
```

- Queries the domain names that are attacked.

```
* and cc_blocks:1 | select cc_action,cc_phase,count(*) as t group by cc_action,cc_phase o
rder by t desc limit 10
```

- Queries the URLs that are attacked.

```
* and cc_blocks:1 | select count(*) as times,host,request_path group by host,request_path
order by times
```

- Queries the details about a request.

```
* | select date_format(date_trunc('second',__time__),'%H:%i:%s') as time,host,request_uri
,request_method,status,upstream_status,querystring limit 10
```

- Queries the details about the 5XX status codes.

```
* and status>499 | select host,status,upstream_status,count(*)as t group by host,status,u
pstream_status order by t desc
```

- Queries the distribution of request latencies.

```
* | SELECT count_if(upstream_response_time<20) as "<20",
count_if(upstream_response_time<50 and upstream_response_time>20) as "<50",
count_if(upstream_response_time<100 and upstream_response_time>50) as "<100",
count_if(upstream_response_time<500 and upstream_response_time>100) as "<500",
count_if(upstream_response_time<1000 and upstream_response_time>500) as "<1000",
count_if(upstream_response_time>1000) as ">1000"
```

6.2.5. Query and analyze logs

After you enable Log Analysis for your domain name in the Anti-DDoS Pro or Anti-DDoS Premium console, you can query and analyze logs on the Log Analysis page in real time. This topic describes how to query and analyze Anti-DDoS Pro or Anti-DDoS Premium logs.

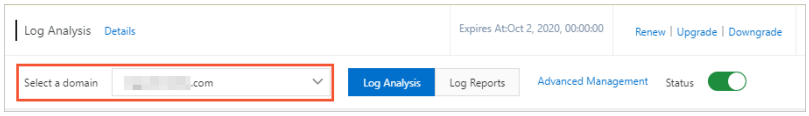
Prerequisites

- The domain name of your website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.
- The Log Analysis feature is enabled for the domain name. For more information, see Overview.

Procedure

1.
2.
3.
4. Select the target domain name.

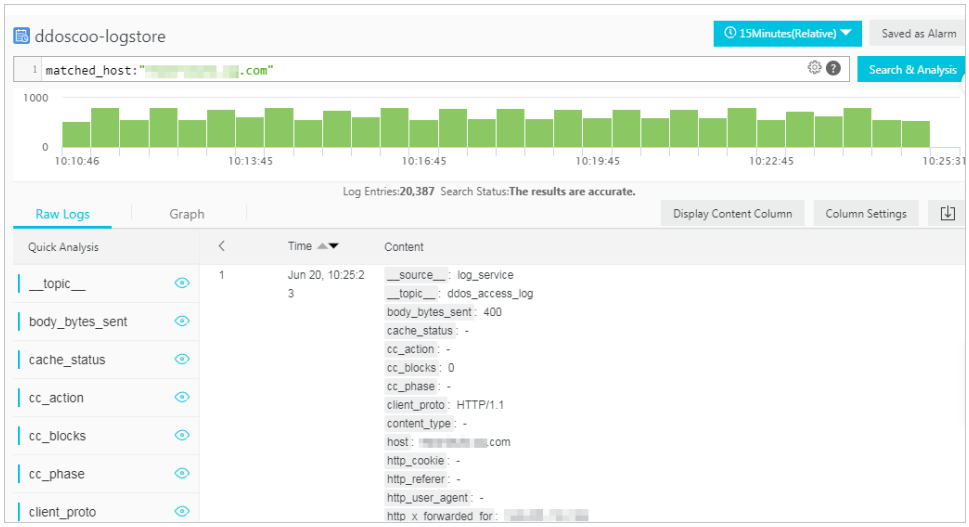
   > **Note** Make sure that the **Status** switch is turned on for the domain name.

5. Click **15 Minutes(Relative)** to specify a time range.

   You can specify a relative time range, time frame, or custom time range.

   > **Note**
   > - Anti-DDoS Pro and Anti-DDoS Premium logs are retained for 180 days. By default, you can query logs only over the last 180 days.
   > - The query results may contain logs that are generated 1 minute earlier or later than the specified time range.

6. Enter a query and analysis statement in the search box.

   A query and analysis statement consists of a search clause and an analytics clause that are

separated by a vertical bar (|). Format: `Search clause|Analytics clause`.

Clause	Required?	Description
Search clause	No	A search clause specifies search conditions, including keywords, wildcard characters, values, ranges, and combined conditions. If you leave the search clause empty or enter an asterisk (*), no conditions are specified. In this case, all logs are returned. For more information, see Search syntax. **Note** For more information about log fields, see Fields included in full logs.
Analytics clause	No	You can use an analytics clause to analyze and aggregate the query results. If you leave the analytics clause empty, the query results are returned but not analyzed. For more information, see Log analysis overview. **Note** ◦ In an analytics clause, the `from log` part is similar to the `from <table name>` part in a standard SQL statement and can be omitted. ◦ By default, the first 100 log entries are returned. You can modify the number of log entries to be returned by using the LIMIT clause.

7. Click **Search & Analyze** to view the query and analysis results.
   You can view the results in a log distribution histogram, on the **Raw Logs** tab, or on the **Graph** tab. You can also configure alerts and saved searches. For more information, see Manage query and analysis results.

6.2.6. Query log reports

Log reports on the Log Analysis page of the Anti-DDoS Pro and Anti-DDoS Premium console support dashboards of Log Service. You can view log reports on the default dashboards: DDoS Access Center and DDoS Operation Center. After you enable Log Analysis for a domain name, you can query log reports on the default dashboards.

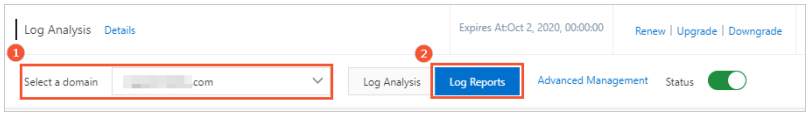
Prerequisites

- The domain name of your website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.
- The Log Analysis feature is enabled for the domain name. For more information, see Overview.

Procedure

1.
2.
3.
4. Select the target domain name and click **Log Reports**.

> **Note** Make sure that the **Status** switch is turned on for the domain name.



You can view log reports on the following dashboards:

- **DDoS Access Center**: shows the basic website metrics, access trends, request source distribution, and other statistics such as access domain names and client types. The website metrics include PVs, UVs, inbound traffic, and peak bandwidth.
- **DDoS Operation Center**: shows the overall operations status of the website, including inbound and outbound traffic trends, requests and interception trends, attackers, and visited websites.

> **Note**
> - The log reports are displayed in different types of charts. For more information, see Chart overview.
> - For more information about the charts provided by the default dashboards, see Charts on the default dashboards.

5. Specify a time range to view the log reports on a dashboard.

   Each chart on the dashboard is generated based on the statistics within a specific time range. For example, the default time range is 1 hour for a website access chart and 1 week for an access trend chart. To specify the same time range for all charts on the dashboard, use the time picker.

   i. In the upper-right corner of the dashboard, click **Please Select**.

   ii. In the **Time** pane, specify a time range.

   You can specify a relative time range, time frame, or custom time range.

   The specified time range applies to all charts on the dashboard.

> **Note** The time range you specify applies to the charts only once and is not saved. The next time you open the dashboard, the charts are still displayed within the default time ranges.

Charts on the default dashboards

DDoS Access Center

Chart name	Type	Default time range	Description	Example value

Chart name	Type	Default time range	Description	Example value
PV	Single value	1 hour (relative)	The total number of PVs.	100000
UV	Single value	1 hour (relative)	The total number of UVs.	100000
Inbound traffic	Single value	1 hour (relative)	The total volume of inbound traffic of the website. Unit: MB.	300 MB
Peak network in	Single value	Today (time frame)	The maximum inbound data transmission rate of the website. Unit: byte/s.	100 Bytes/s
Peak network out	Single value	Today (time frame)	The maximum outbound data transmission rate of the website. Unit: byte/s.	100 Bytes/s
Traffic network trend	Double-line chart	1 week (relative)	The trends of inbound and outbound traffic. Unit: KB/s.	None
PV/UV trends	Double-line chart	1 week (relative)	The trends of PVs and UVs.	None
Access status distribution	Pie chart	1 week (relative)	The distribution of requests with different status codes, such as 400, 304, and 200. Unit: count/minute.	None
Access source	World map	1 hour (relative)	The distribution of PVs from different countries.	None
Traffic in source (world)	World map	1 hour (relative)	The distribution of inbound traffic from different countries. Unit: MB.	None

Chart name	Type	Default time range	Description	Example value
Traffic in source (China)	Map of China	1 hour (relative)	The distribution of inbound traffic from different provinces in China. Unit: MB.	None
Access heat map	Amap	1 hour (relative)	The heat map that shows the geographical locations of visitors.	None
Network provider source	Donut chart	1 hour (relative)	The distribution of the inbound traffic from different Internet service providers (ISPs), such as China Telecom, China Unicom, China Mobile, and CERNET. Unit: MB.	None
Referer	Table	1 hour (relative)	The top 100 most used referer URLs, target hosts, and the number of redirections.	None
Access line distribution	Donut chart	1 hour (relative)	The distribution of Anti-DDoS Pro or Anti-DDoS Premium lines.	None
Client distribution	Donut chart	1 hour (relative)	The top 20 most used user agents, such as iPhone, iPad, Internet Explorer, and Google Chrome.	None
Request content type distribution	Donut chart	1 hour (relative)	The top 20 most requested content types, such as HTML, form, JSON, and streaming data.	None
Access domain name	Donut chart	1 hour (relative)	The top 20 most visited domain names of the website.	None

Chart name	Type	Default time range	Description	Example value
Top clients	Table	1 hour (relative)	Information about the top 100 clients that initiates the most requests. The information includes the IP addresses, PVs, inbound traffic, number of invalid requests, and number of attacks.	None
URL with slowest response	Table	1 hour (relative)	Information about the top 100 URLs with the longest response time. The information includes the websites, URLs, response time, and the number of accesses.	None

DDoS Operation Center

Chart name	Type	Default time range	Description	Example value
Inbound and outbound bandwidth (Kbit/s)	Double-line chart	1 week (relative)	The trends of inbound and outbound bandwidth.	None
Request and interception	Double-line chart	1 week (relative)	The trends of the total numbers of requests and intercepted attack requests.	None

Chart name	Type	Default time range	Description	Example value
Attacker list	Table	1 hour (relative)	Information about the top 100 attackers that initiates the most attack requests. The information includes the attacker IP addresses, source locations, number of attacks, and total attack traffic.	None
Top 10 attacked websites	Table	1 hour (relative)	The top 10 most attacked websites.	None

6.2.7. Modify the log storage duration

By default, the Log Analysis feature stores full logs for 180 days. You can customize the log storage duration based on your business requirements. You can specify a value that ranges from 30 days to 180 days.

Prerequisites

The Log Analysis feature is enabled for your Anti-DDoS Pro or Anti-DDoS Premium instance.

For more information, see Step 1: Enable Log Analysis.

Context

After you enable the Log Analysis feature, Anti-DDoS Pro or Anti-DDoS Premium stores logs for 180 days starting from the day when you enable the feature. If you want to store logs, make sure that the log storage capacity is sufficient and your Log Analysis instance is within its validity period. Anti-DDoS Pro and Anti-DDoS Premium store logs that are generated within the last 180 days. Logs that are generated on the first day after the 180-day log storage duration overwrite the logs generated on the first day of the previous 180-day log storage duration.

You can customize the log storage duration based on your business requirements. You can specify a value that ranges from 30 days to 180 days. The required log storage capacity increases with the log storage duration.

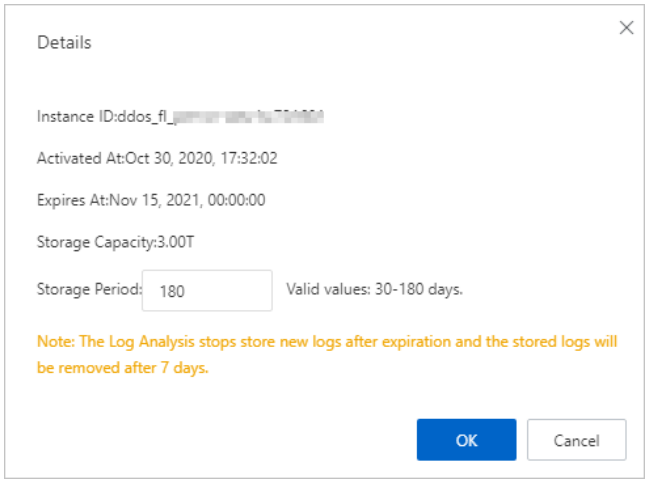
If the log storage capacity is exhausted, new logs cannot be stored and are lost. In this case, we recommend that you increase the log storage capacity. For more information, see Increase the log storage capacity.

Procedure

1.
2.

3.
4. In the upper-right corner of the **Log Analysis** page, click **Details**.
5. In the **Details** dialog box, configure the **Storage Period** parameter. Unit: days.

   You can specify a value that ranges from 30 days to 180 days.



6. Click **OK**.
   After you modify the log storage duration, the Log Analysis feature stores logs within the duration that you specify and automatically deletes expired logs.

6.2.8. Manage log storage capacity

After you enable the Log Analysis feature, you can modify the log storage capacity or delete all stored logs.

Prerequisites

The Log Analysis feature is enabled for your Anti-DDoS Pro or Anti-DDoS Premium instance.

For more information, see Step 1: Enable Log Analysis.

Context

You can increase or decrease the log storage capacity based on your business requirements. For more information, see Increase the log storage capacity and Decrease the log storage capacity. If you enable log collection for a new website, the required log storage capacity increases. If you reduce the log storage duration, the log storage capacity that is required for the same business scale decreases.

Method to calculate the required log storage capacity

The following example shows how to estimate the required log storage capacity based on the daily QPS of your website:

In most cases, each request log occupies approximately 2 KB of storage. If the average QPS of your website is 500, the required storage for the logs that are generated within a day is 86,400,000 KB, which is approximately 82 GB. This value is calculated by using the following formula: 500 × 60 × 60 × 24 × 2 = 86,400,000. If you want to store logs that are generated within 180 days, the required log storage capacity is 15,552,000,000 KB, which is approximately 14.5 TB. This value is calculated by using the following formula: 86,400,000 × 180 = 15,552,000,000.

Method to handle exhausted log storage capacity

If the log storage capacity is exhausted, new logs cannot be stored and are lost. To resolve this issue, you can perform one of the following operations:

- (Recommended) Increase the log storage capacity. For more information, see Increase the log storage capacity.
- Delete stored logs and reduce the log storage duration. For more information, see Delete logs and Modify the log storage duration.

> Notice
> - If you perform this operation, all logs are deleted and cannot be recovered. Before you delete the stored logs, make sure that you no longer need all logs.
> - Each Alibaba Cloud account can delete stored logs twice. If you want to delete stored logs more than twice, submit a . We recommend that you do not frequently delete logs. If the log storage capacity cannot meet your business requirements, we recommend that you increase the log storage capacity at the earliest opportunity.

Increase the log storage capacity

If the log storage capacity cannot meet your business requirements, you can increase the log storage capacity.

1.
2.
3.
4. In the upper-right corner of the **Log Analysis** page, click **Upgrade**.
5. On the **Upgrade/Downgrade** page, select a **log storage capacity** that is greater than the current one, and read and select **Log Service Terms of Service**.

   Example: If the current log storage capacity is 3 TB, you can select 5 TB or higher.
6. Click **Buy Now** and complete the payment.
   After the log storage capacity is increased, you can view the new log storage capacity and usage in the upper-right corner of the **Log Analysis** page.

Decrease the log storage capacity

If the log storage capacity exceeds your business requirements, you can decrease the log storage capacity.

1.
2.
3.
4. In the upper-right corner of the **Log Analysis** page, click **Downgrade**.
5. On the **Upgrade/Downgrade** page, select a **log storage capacity** that is less than the current one, and read and select **Log Service Terms of Service**.

   Example: If the current log storage capacity is 10 TB, you can select 5 TB or lower.
6. Click **Buy Now** and complete the payment.
   After the log storage capacity is decreased, you can view the new log storage capacity and usage

in the upper-right corner of the **Log Analysis** page.

Delete logs

If you do not want stored logs to occupy your log storage, you can delete the logs. After you delete the logs, all logs that are stored are deleted.

1.
2.
3.
4. In the upper-right corner of the **Log Analysis** page, click **Clear**.

   > **Notice** If no logs are stored, the **Clear** operation is not supported.

5. In the **Are you sure to clear all logs?** message, click **OK**.

   Each Alibaba Cloud account can delete stored logs twice. If you want to delete stored logs more than twice, submit a . We recommend that you do not frequently delete logs. If the log storage capacity cannot meet your business requirements, we recommend that you increase the log storage capacity at the earliest opportunity.

   > **Warning** You cannot recover the logs that you delete. Proceed with caution.

   After you delete the logs, you must wait for 2 to 3 hours before you can view the result in the upper-right corner of the **Log Analysis** page.

6.2.9. Renew a Log Analysis instance

When a Log Analysis instance expires, the instance no longer stores new logs. All stored logs are retained for seven days. When the retention period elapses, all logs are deleted and cannot be recovered. To prevent the issues that are related to an expired Log Analysis instance, we recommend that you pay attention to the expiration time of the instance and renew the instance at the earliest opportunity, or enable auto-renewal.

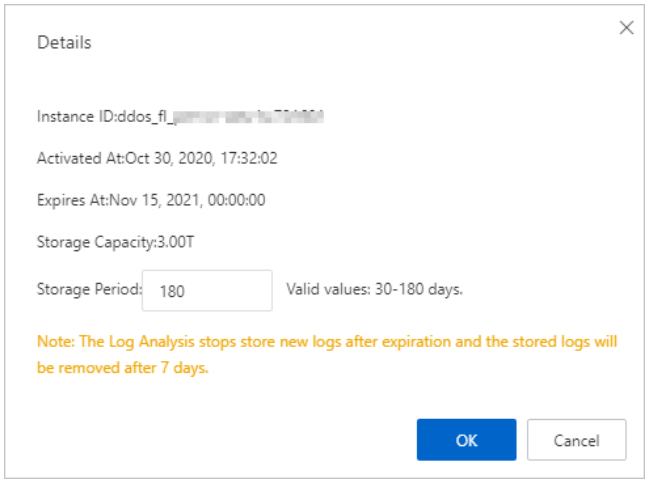
Prerequisites

The Log Analysis feature is enabled for your Anti-DDoS Pro or Anti-DDoS Premium instance.

For more information, see Step 1: Enable Log Analysis.

Query the expiration time of the Log Analysis instance

1.
2.
3.
4. In the upper-right corner of the **Log Analysis** page, click **Details**.
5. In the **Details** dialog box, view the value of the **Expires At** parameter.



Manually renew the Log Analysis instance

1.
2.
3.
4. In the upper-right corner of the **Log Analysis** page, click **Renew**.
5. On the **Renew** page, configure the **Duration** parameter, and read and select **Log Service Terms of Service**.
6. Click **Buy Now** and complete the payment.
   After you renew the Log Analysis instance, you can click **Details** on the **Log Analysis** page to view the new value of the **Expires At** parameter.

Enable auto-renewal

1.
2. In the top navigation bar, choose **Expenses > Renewal Management**.
3. On the **Manual** tab, find the **Full Log** instance that you want to renew and click **Enable Auto Renewal** in the **Actions** column.
4. In the **Enable Auto Renewal** dialog box, select an **auto-renewal period** and click **Auto Renew**.

   Example: If the **auto-renewal period** is set to **three months**, Alibaba Cloud extends the subscription period of the Log Analysis instance for three months and deducts fees from the balance of your Alibaba Cloud account.

   After you enable auto-renewal, you can view the auto-renewal configurations on the **Auto** tab. You can also click **Enable Manual Renewal** to enable manual renewal.

6.3. View operations logs

If you use Anti-DDoS Pro, you can view important operations logs of the last 180 days on the Operation Logs page of the Anti-DDoS Pro console.

Prerequisites

An Anti-DDoS Pro instance is purchased.

> **Note** Only Anti-DDoS Pro supports the operations logs feature. If you use Anti-DDoS Premium, you cannot view operations logs.

Context

Operations logs record only important operations of the last 180 days.

You can view the following types of operations logs:

- IP address changes of ECS instances
- Deactivation of blackhole filtering
- Blocking or unblocking traffic
- Changes of the scrubbing mode for Layer 4 traffic
- Changes of the mitigation mode for HTTP flood attacks
- Changes of the burstable protection bandwidth

Procedure

1.
2. In the top navigation bar, select **Mainland China**.
3.
4. On the **Operation Logs** page, select **IP**, **Global Advanced Mitigation**, or **ECS** and specify a time range to view specific operations logs.

6.4. Query system logs

You can query the bills for the burstable clean bandwidth of your Anti-DDoS Pro or Anti-DDoS Premium instance on the System logs page.

Prerequisites

- An Anti-DDoS Pro instance is purchased.

  For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.
- The burstable clean bandwidth feature is enabled for the instance.

  For more information, see Configure burstable clean bandwidth.

Context

On the **System logs** page, you can query the system events of the instance within the last 180 days. Only the bills for the burstable clean bandwidth are provided.

After you enable the burstable clean bandwidth feature, you can query the bills for the burstable clean bandwidth within the last 180 days on the **System logs** page. For more information about the billing of the burstable clean bandwidth, see Billing of the burstable clean bandwidth feature.

Procedure

1.
2.

3. In the left-side navigation pane, choose **Investigation > System logs**.
4. On the **System logs** page, specify the time range in which you want to query the bills for the burstable clean bandwidth.

   One of the following states is displayed in the **Status** column of a bill:

   - **To be billed**: The bill for the burstable clean bandwidth is not generated.

     In the **Details** dialog box, you can query the traffic of your business within the last 3 hours or the last 1 day with a single click.

     - The blue solid line indicates the peak inbound traffic of your business. The purple solid line indicates the peak outbound traffic of your business.
     - The green dotted line indicates the clean bandwidth of your instance. The red dotted line indicates the actual usage of the burstable clean bandwidth.
     - The gray line indicates the metered bandwidth that is used to meter the burstable clean bandwidth.

   - **Terminated bill**: The billing for the burstable clean bandwidth is terminated, and you are not required to make a payment.
   - **Already billed**: The burstable clean bandwidth is billed based on the actual usage.

6.5. Query advanced mitigation logs

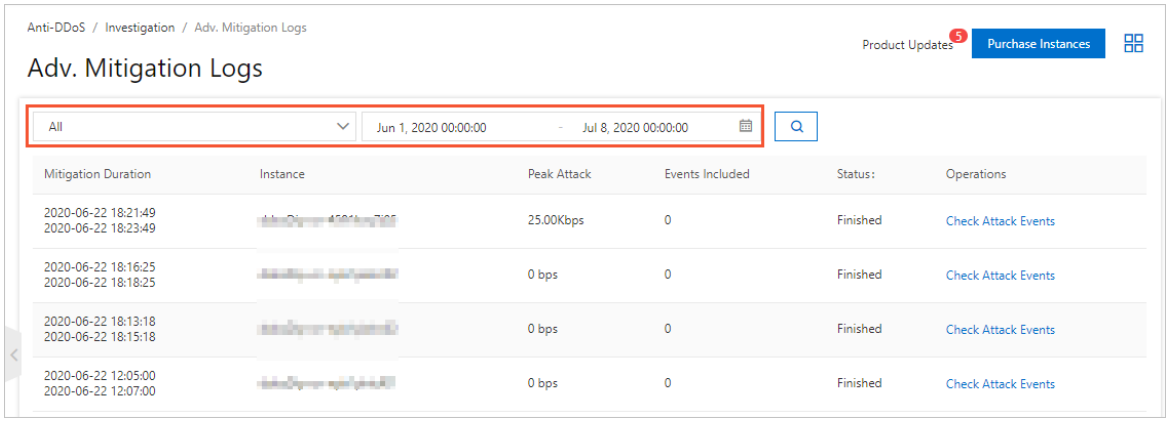
If you use Anti-DDoS Premium, you can query the advanced mitigation logs in the last 30 days on the Adv. Mitigation Logs page of the Anti-DDoS Premium console.

Prerequisites

An Anti-DDoS Premium instance is created.

Procedure

1.
2. In the top navigation bar, select **Outside Mainland China**.
3.
4. On the **Adv. Mitigation Logs** page, select the instance and time range to query the logs.



6.6. CloudMonitor alerts

6.6.1. Create threshold-triggered alert rules in the CloudMonitor console

CloudMonitor allows you to configure threshold-triggered alert rules for common service metrics and attack events of Anti-DDoS Pro or Anti-DDoS Premium. The common service metrics include the volume of traffic for an Anti-DDoS Pro or Anti-DDoS Premium instance and the number of connections for an Anti-DDoS Pro or Anti-DDoS Premium instance. The traffic and connection metrics can be measured at the IP address level. The attack events include blackhole filtering events and traffic scrubbing events. After you configure a threshold-triggered alert rule, CloudMonitor reports an alert when the rule is triggered. This way, you can handle exceptions and recover your business at the earliest opportunity.

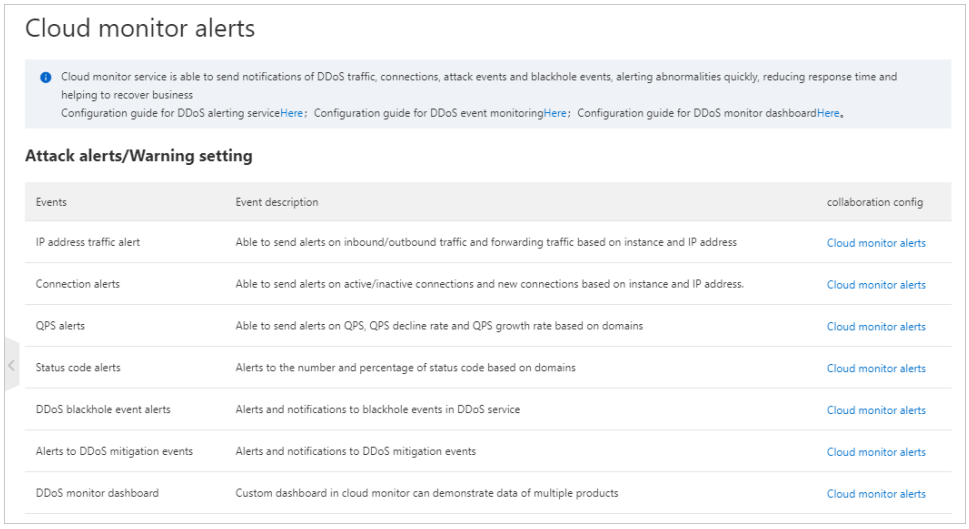
CloudMonitor is a service that monitors Internet applications and Alibaba Cloud resources. For more information, see What is CloudMonitor?.

Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased. For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

Procedure

1.
2.
3.
4. On the **Cloud monitor alerts** page, find the service metric or attack event for which you want to configure a threshold-triggered alert rule and click **Cloud monitor alerts** in the **collaboration config** column.



   - To configure a threshold-triggered alert rule for **IP address traffic alert**, **Connection alerts**, **QPS alerts**, or **Status code alerts**, click **Cloud monitor alerts** in the collaboration config column.

     The **Alert Rules** page of the CloudMonitor console appears. You can create a threshold-triggered alert rule for each service metric of Anti-DDoS Pro or Anti-DDoS Premium on this page. For more information, see Configure an alert rule for Anti-DDoS Pro or Anti-DDoS Premium.

- To configure a threshold-triggered alert rule for **DDoS blackhole event alerts** and **Alerts to DDoS mitigation events**, click **Cloud monitor alerts** in the collaboration config column.

  The **Event Monitoring** page of the CloudMonitor console appears. You can create a threshold-triggered alert rule for each attack event of Anti-DDoS Pro or Anti-DDoS Premium on this page. For more information, see Monitor attack events that occur on Anti-DDoS Pro or Anti-DDoS Premium.

- To configure a threshold-triggered alert rule for **DDoS monitor dashboard**, click **Cloud monitor alerts** in the collaboration config column.

  The **Dashboard** page of the CloudMonitor console appears. You can create a dashboard for Anti-DDoS Pro or Anti-DDoS Premium on this page. Then, you can create widgets on the dashboard. For more information, see Create an Anti-DDoS Pro or Anti-DDoS Premium dashboard.

6.6.2. Configure an alert rule for Anti-DDoS Pro or Anti-DDoS Premium

This topic describes how to configure an alert rule for Anti-DDoS Pro or Anti-DDoS Premium in the CloudMonitor console. After alert rules are configured, CloudMonitor notifies you of exceptions in traffic and connections on the IP addresses of your Anti-DDoS Pro or Anti-DDoS Premium instances. This allows you to handle exceptions and restore workloads at the earliest opportunity.

Context

CloudMonitor is a service that allows you to monitor Internet applications and Alibaba Cloud resources. If alerts are triggered, CloudMonitor sends notifications. You can customize alert rules to specify how the alert system checks monitoring data. If the monitoring data meets the custom alert rules, CloudMonitor sends notifications. After you configure alert rules for important metrics, you are notified if exceptions are detected for these metrics. This allows you to handle exceptions at the earliest opportunity. For more information, see Overview.

The alerting feature provided by CloudMonitor supports Anti-DDoS Pro and Anti-DDoS Premium. You can configure alert rules for Anti-DDoS Pro and Anti-DDoS Premium in the CloudMonitor console.

The following table describes the metrics of Anti-DDoS Pro and Anti-DDoS Premium supported by CloudMonitor.

Metric	Dimension	Unit
Out_Traffic	Instance or IP address	bit/s
In_Traffic	Instance or IP address	bit/s
Back_Traffic (traffic that is scrubbed by Anti-DDoS Pro or Anti-DDoS Premium and is forwarded to the origin server)	Instance or IP address	bit/s
Active_connection	Instance or IP address	Count
Inactive_connection	Instance or IP address	Count
New_connection	Instance or IP address	Count
qps	Domain name	Count/second

Metric	Dimension	Unit
qps_ratio_down	Domain name	%
qps_ratio_up	Domain name	%
resp2xx	Domain name	Count
resp2xx_ratio	Domain name	%
resp3xx	Domain name	Count
resp3xx_ratio	Domain name	%
resp404	Domain name	Count
resp404_ratio	Domain name	%
resp4xx	Domain name	Count
resp4xx_ratio	Domain name	%
resp5xx	Domain name	Count
resp5xx_ratio	Domain name	%
upstream_resp2xx	Domain name	Count
upstream_resp2xx_ratio	Domain name	%
upstream_resp3xx	Domain name	Count
upstream_resp3xx_ratio	Domain name	%
upstream_resp404	Domain name	Count
upstream_resp404_ratio	Domain name	%
upstream_resp4xx	Domain name	Count
upstream_resp4xx_ratio	Domain name	%
upstream_resp5xx	Domain name	Count
upstream_resp5xx_ratio	Domain name	%

Procedure

1. Log on to the CloudMonitor console.
2. (Optional)Create an alert contact. If you have created a contact, skip this step.
   i. In the left-side navigation pane, choose **Alerts > Alert Contacts**.
   ii. On the **Alert Contacts** tab, click **Create Alert Contact**.

iii. In the **Set Alert Contact** panel, configure the parameters, drag the slider to complete verification, and then click **OK**.

3. (Optional)Create an alert group. If you have created an alert group, skip this step.

> **Note** CloudMonitor sends alert notifications only to an alert group. You can add one or more alert contacts to an alert group.

i. In the left-side navigation pane, choose **Alerts > Alert Contacts**.

ii. On the **Alert Contact Group** tab, click **Create Alert Contact Group**.

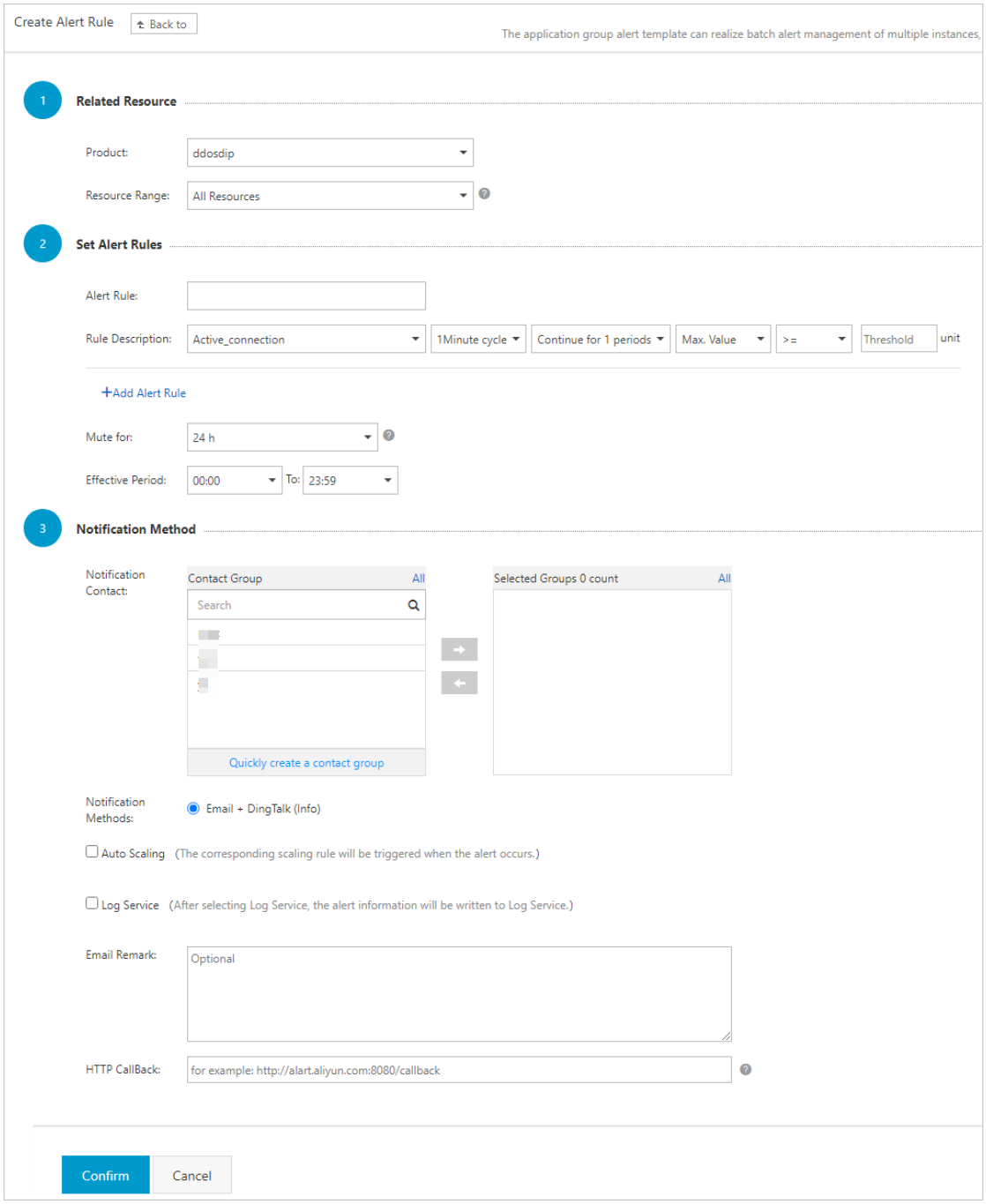
iii. In the **Create Alert Contact Group** panel, enter a group name in the **Group Name** field. Select the alert contact that you create from the **Existing Contacts** section and add the contact to the Selected Contacts section. Then, click **Confirm**.

4. Create an alert rule.

i. In the left-side navigation pane, choose **Alerts > Alert Rules**.

ii. On the **Threshold Value Alert** tab, click **Create Alert Rule**.

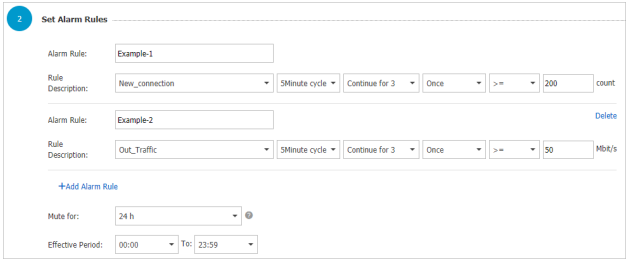
iii. On the **Create Alert Rule** page, configure the parameters and click **Confirm**.



The following table describes the parameters used to create an alert rule.

Section	Parameter	Description
	Product	Select **NewBGPDDoS** (Anti-DDoS Pro) or **ddosdip** (Anti-DDoS Premium).

Section	Parameter	Description
Related Resource	**Resource Range**	Select the resources on which the alert rule takes effect. Valid values: **All Resources** or **Instances**. ■ **All Resources**: The alert rule takes effect on all your Anti-DDoS Pro or Anti-DDoS Premium instances. An alert notification is sent when one of the instances matches the alert rule. ■ **Instances**: The alert rule takes effect on the Anti-DDoS Pro or Anti-DDoS Premium instances that you select. An alert notification is sent only when all the selected instances match the alert rule.
	Alert Rule	Specify the name of the alert rule.

Section	Parameter	Description
Set Alert Rules	Rule Description	Specify the conditions that are used to trigger alerts. **Note** We recommend that you specify the thresholds of metrics based on your business requirements. For more information, see Anti-DDoS Pro and Anti-DDoS Premium metrics. A low threshold may frequently trigger alerts and negatively affect user experience. A high threshold may leave insufficient time for you to handle attacks. Examples: ■ `New_connection | 5Minute cycle | Continue for 3 periods | Once | > | 200` : In this rule, the detection period is 5 minutes, and 1 data point is reported each minute. The data point indicates the number of new connections. CloudMonitor checks the data points generated within three consecutive detection periods, which are 15 data points in total. If a data point exceeds 200, an alert notification is sent. ■ `Out_Traffic | 5Minute cycle | Continue for 3 periods | Once | ≥ | 50 Mbit/s` : In this rule, the detection period is 5 minutes, and 1 data point is reported each minute. The data point indicates the transfer rate of outbound traffic. CloudMonitor checks the data points generated within three consecutive detection periods, which are 15 data points in total. If a data point is greater than or equal to 50 Mbit/s, an alert notification is sent. You can click **Add Alert Rule** to add more alert rules. Then, specify **Alert Rule** and **Rule Description** for each alert rule. 
	Mute for	Specify a mute period. If an alert is not cleared within the mute period, the notification for the alert is sent again after the mute period elapses. The minimum value is 5 minutes, and the maximum value is 24 hours.
	Effective Period	Specify the period during which the alert rule remains effective. CloudMonitor sends alert notifications within the effective period and only records alerts beyond the effective period.

Section	Parameter	Description
Notification Method	Notification Contact	Select the alert group that receives alert notifications.
	Notification Methods	Set the value to **Email + DingTalk (Info)**.
	Auto Scaling	If you select Auto Scaling, a scaling rule is triggered when the alert is triggered.
	Log Service	If you select Log Service, CloudMonitor writes alert information to Log Service.
	Email Remark	Optional. Enter the information that you want to include in alert notification emails.
	HTTP CallBack	Enter a public URL to which CloudMonitor sends alert notifications by using POST requests. You can enter only an HTTP URL.

After the alert rule is created, if the monitoring data of an Anti-DDoS Pro or Anti-DDoS Premium metric matches the alert rule description, an alert notification is sent to the specified alert group by using the specified request method.

6.6.3. Monitor attack events that occur on Anti-DDoS Pro or Anti-DDoS Premium

This topic describes how to configure alert rules for attack events that occur on Anti-DDoS Pro or Anti-DDoS Premium in the CloudMonitor console. The events include blackhole filtering events, traffic scrubbing events, events of flood attacks at Layer 4, and events of HTTP flood attacks at Layer 7. After alert rules are configured, CloudMonitor notifies you of the latest attack events that occur on Anti-DDoS Pro or Anti-DDoS Premium. This allows you to handle exceptions and restore workloads at the earliest opportunity.

Context

CloudMonitor is a service that allows you to monitor Internet applications and Alibaba Cloud resources. CloudMonitor provides the event monitoring feature. This feature allows you to query the system events generated by different services and view event statistics. This helps you stay informed about the usage of your cloud services.

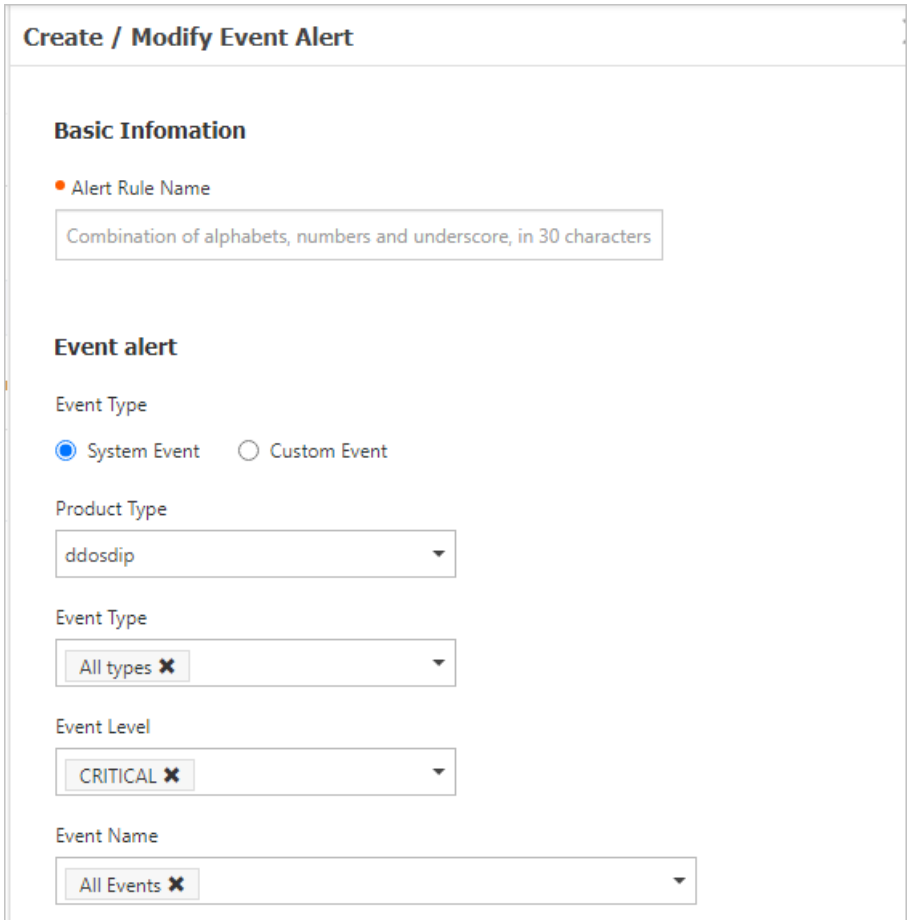
You can query the blackhole filtering events, traffic scrubbing events, events of flood attacks at Layer 4, and events of HTTP flood attacks at Layer 7 that occur on Anti-DDoS Pro or Anti-DDoS Premium. You can also configure alert rules based on the event levels. When you configure alert rules, you can configure notification methods, such as emails, DingTalk, and alert callbacks. This way, you can be notified of critical events immediately after they occur and handle the events at the earliest opportunity. This helps implement automated online O&M. For more information, see Overview of event monitoring.

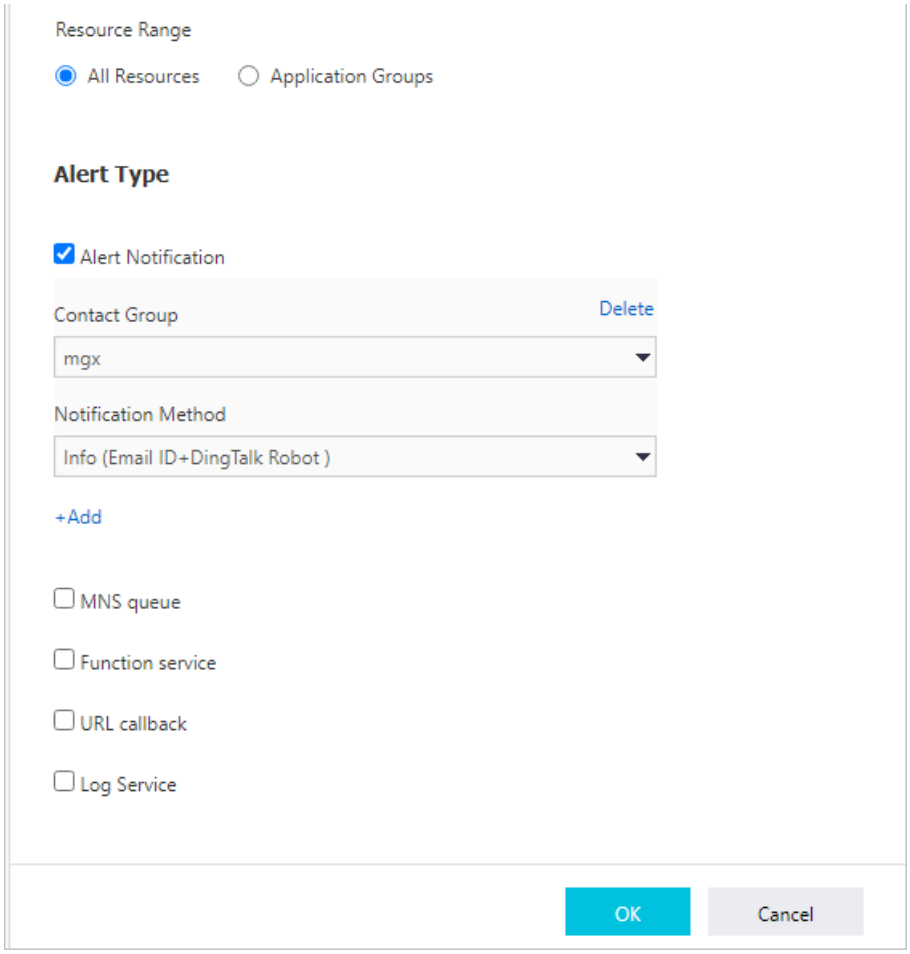
Procedure

1. Log on to the CloudMonitor console.
2. (Optional)Create an alert contact. If you have created a contact, skip this step.
   i. In the left-side navigation pane, choose **Alerts > Alert Contacts**.
   ii. On the **Alert Contacts** tab, click **Create Alert Contact**.
   iii. In the **Set Alert Contact** panel, configure the parameters, drag the slider to complete verification, and then click **OK**.
3. (Optional)Create an alert group. If you have created an alert group, skip this step.

   > **Note** CloudMonitor sends alert notifications only to an alert group. You can add one or more alert contacts to an alert group.

   i. In the left-side navigation pane, choose **Alerts > Alert Contacts**.
   ii. On the **Alert Contact Group** tab, click **Create Alert Contact Group**.
   iii. In the **Create Alert Contact Group** panel, enter a group name in the **Group Name** field. Select the alert contact that you create from the **Existing Contacts** section and add the contact to the Selected Contacts section. Then, click **Confirm**.
4. Create an alert rule for events.
   i. In the left-side navigation pane, click **Event Monitoring**.
   ii. On the **Alert Rules** tab of the page that appears, click **System Event** and then **Create Event Alert**.
   iii. In the **Create/Modify Event Alert** panel, configure the parameters and click **OK**.



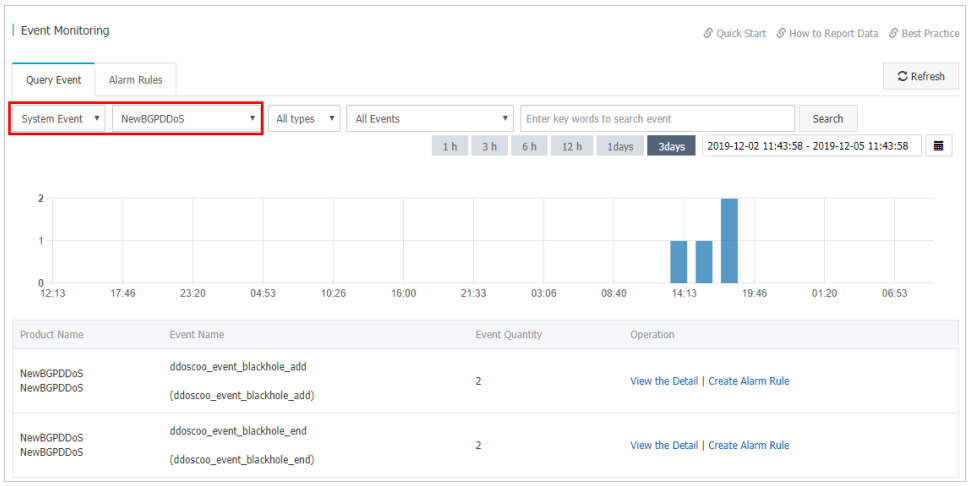


Section	Parameter	Description
Basic Information	**Alert Rule Name**	Enter the name of the alert rule.
	Event Type	Select **System Event**.
	Product Type	Select **NewBGPDDoS** (Anti-DDoS Pro) or **ddosdip** (Anti-DDoS Premium).
	Event Type	Select the type of event for which you want to receive alert notifications. Valid values: ■ **DDoS Blackhole Filtering**: blackhole filtering events ■ **DDoS Traffic Scrubbing**: traffic scrubbing events ■ **Layer 4 Flood Attack**: events of flood attacks at Layer 4 ■ **Layer 7 HTTP Flood Attack**: events of HTTP flood attacks at Layer 7

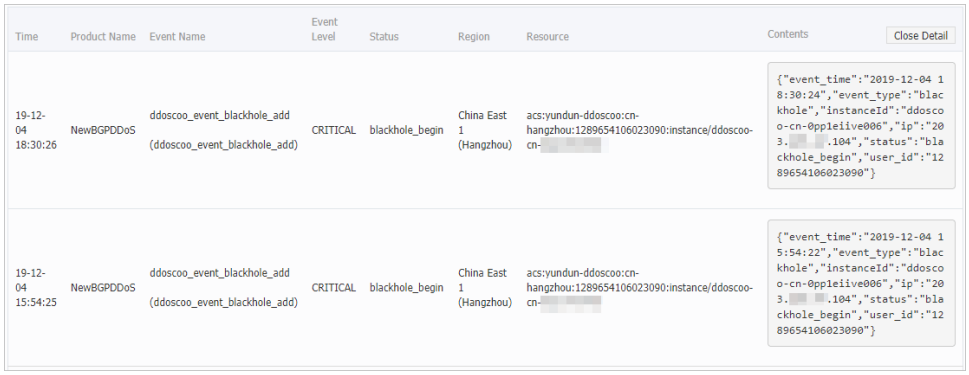
Section	Parameter	Description
Event alert	Event Level	Select the level of event for which you want to receive alert notifications. Valid values: **CRITICAL**, **WARN**, and **INFO**. **Notice** You can select multiple levels. If you select multiple levels, you must select **CRITICAL** for all events.
	Event Name	Select the event for which you want to receive alert notifications. The valid values of this parameter vary based on the value of the Event Type parameter. The following list describes the events of each event type: ■ Blackhole filtering events: **ddosdip_event_blackhole_add** and **ddosdip_event_blackhole_end** ■ Traffic scrubbing events: **ddosdip_event_defense_add** and **ddosdip_event_defense_end** ■ Events of flood attacks at Layer 4: **ddosdip_event_cc4_add** and **ddosdip_event_cc4_end** ■ Events of HTTP flood attacks at Layer 7: **ddosdip_event_cc7_add** and **ddosdip_event_cc7_end**
	Resource Range	Select **All Resources**.
Alert Type	Alert Notification	Select **Alert Notification** and configure **Contact Group** and **Notification Method**. ■ Contact Group: Select an existing alert group. ■ Notification Method: Set the value to **Info (Email ID+DingTalk Robot)**. Only this option is supported. You can click **Add** to add more alert groups and notification methods.
	MNS queue	You do not need to specify this parameter.
	Function service	You do not need to specify this parameter.
	URL callback	You do not need to specify this parameter.
	Log Service	You do not need to specify this parameter.

After the alert rule for events is created, if the specified events occur on Anti-DDoS Pro or Anti-DDoS Premium, an alert notification is sent to the specified alert group.

5. (Optional)Query events. You can query the events that recently occurred on Anti-DDoS Pro or Anti-DDoS Premium in the CloudMonitor console.
   i. On the **Event Monitoring** page, click the **Query Event** tab.
   ii. Select **System Event** and **NewBGPDDoS** (Anti-DDoS Pro) or **ddosdip** (Anti-DDoS Premium). Then, specify the event type and time range to query related events.



   iii. In the event list, click **View the Detail** to view the details of an event.



6.6.4. Create an Anti-DDoS Pro or Anti-DDoS Premium dashboard

This topic describes how to create a custom Anti-DDoS Pro or Anti-DDoS Premium dashboard and add charts to the dashboard in the Cloud Monitor console. Custom dashboards and charts help you monitor workloads of Anti-DDoS Pro or Anti-DDoS Premium.

Context

Cloud Monitor is a service that monitors applications and Alibaba Cloud resources. It allows you to view monitoring data in custom dashboards. You can aggregate monitoring data of different products and instances that run the same type of workload by using one dashboard. For more information, see Overview.

The dashboard feature provided by Cloud Monitor supports Anti-DDoS Pro and Anti-DDoS Premium. You can create and customize dashboards in the Cloud Monitor console.

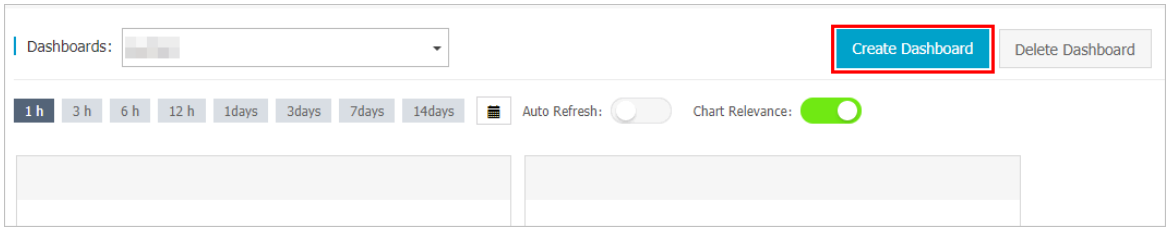
The following table describes the metrics of Anti-DDoS Pro and Anti-DDoS Premium supported by Cloud Monitor.

Metric	Dimension	Unit
Out_Traffic	Instance or IP address	bit/s
In_Traffic	Instance or IP address	bit/s
Back_Traffic (traffic that is scrubbed by Anti-DDoS Pro or Anti-DDoS Premium and is forwarded to the origin server)	Instance or IP address	bit/s
Active_connection	Instance or IP address	Count
Inactive_connection	Instance or IP address	Count
New_connection	Instance or IP address	Count
qps	Domain name	Count/second
qps_ratio_down	Domain name	%
qps_ratio_up	Domain name	%
resp2xx	Domain name	Count
resp2xx_ratio	Domain name	%
resp3xx	Domain name	Count
resp3xx_ratio	Domain name	%
resp404	Domain name	Count
resp404_ratio	Domain name	%
resp4xx	Domain name	Count
resp4xx_ratio	Domain name	%
resp5xx	Domain name	Count
resp5xx_ratio	Domain name	%
upstream_resp2xx	Domain name	Count
upstream_resp2xx_ratio	Domain name	%
upstream_resp3xx	Domain name	Count
upstream_resp3xx_ratio	Domain name	%
upstream_resp404	Domain name	Count

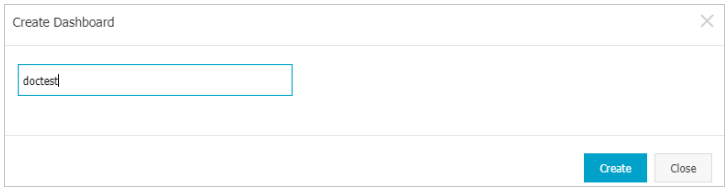
Metric	Dimension	Unit
upstream_resp404_ratio	Domain name	%
upstream_resp4xx	Domain name	Count
upstream_resp4xx_ratio	Domain name	%
upstream_resp5xx	Domain name	Count
upstream_resp5xx_ratio	Domain name	%

Procedure

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, choose **Dashboard > Custom Dashboard**.
3. On the page that appears, click **Create Dashboard**.

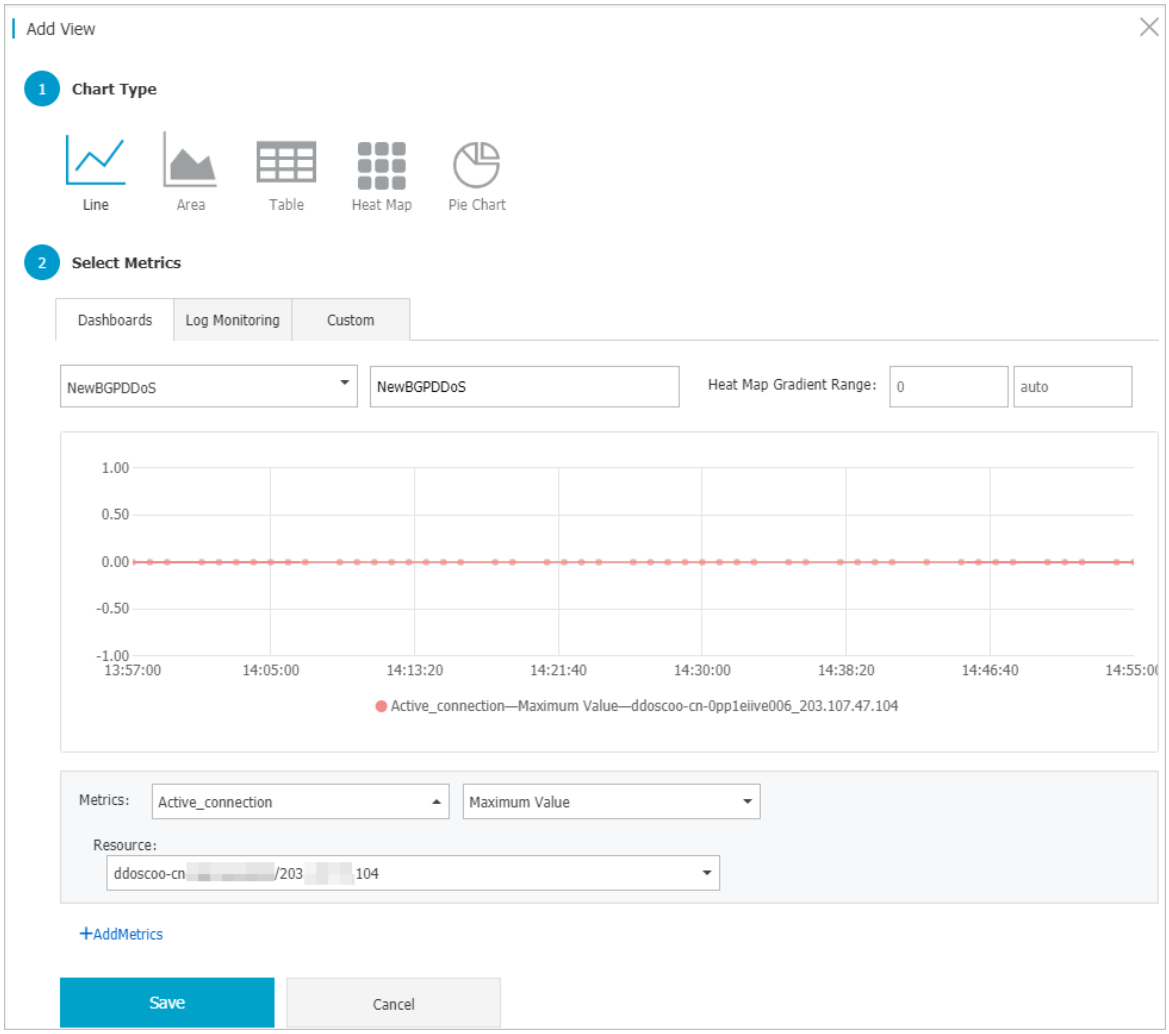


4. In the **Create Dashboard** dialog box, specify a name for the dashboard and click **Create**.



After the dashboard is created, you are redirected to the Dashboards page. You can select a dashboard from the **Dashboards** drop-down list to view or manage the dashboard.

5. Click **Add View**. In the **Add View** panel, configure information of the chart.

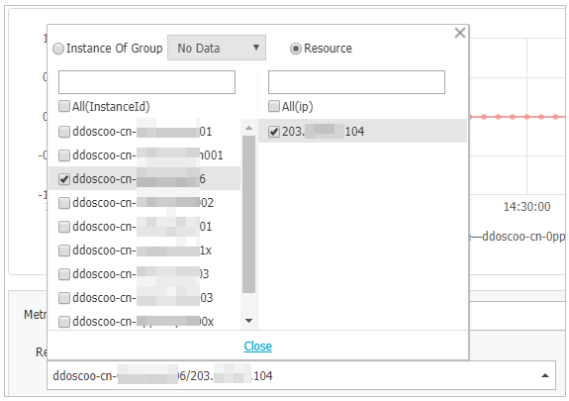


i. **Chart Type**: Supported chart types are Line, Area, Table, Heat Map, and Pie Chart.

For more information, see Manage the monitoring charts of a custom dashboard.

ii. **Select Metrics**: Click the **Dashboards** tab and select **NewBGPDDoS** (AntiDDoS Pro) or **ddosdip** (Anti-DDoS Premium). Then, configure **Metrics** and **Resource**.

- Metrics: Select the metrics that you want to monitor. For more information, see Anti-DDoS Pro and Anti-DDoS Premium metrics.
- Resource: Select the Anti-DDoS Pro or Anti-DDoS Premium instances and IP addresses that you want to monitor.



Click **Add Metrics** if you want to add more metrics.

iii. Click **Save** to create the chart.

You can repeat the preceding step to add more charts to the dashboard.

7.Protection settings

7.1. Protection for infrastructure

7.1.1. Configure the IP address blacklist and whitelist for an Anti-DDoS Pro or Anti-DDoS Premium instance

The IP address blacklist configured for an Anti-DDoS Pro or Anti-DDoS Premium instance is used to deny the requests from specified source IP addresses to the instance, and the IP address whitelist is used to allow the requests from specified source IP addresses. After you configure the blacklist and whitelist, the instance denies requests from the IP addresses that are added to the blacklist and allows the requests from the IP addresses that are added to the whitelist. This topic describes how to configure the blacklist and whitelist.

Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased. For more information, see Purchase mitigation plans for Anti-DDoS Pro and Anti-DDoS Premium.

Context

The blacklist and whitelist configurations take effect only for individual Anti-DDoS Pro or Anti-DDoS Premium instances. You can manually add IP addresses to the blacklist or the whitelist, and search for, delete, or download the IP addresses that are added to the blacklist or whitelist.

Requests from the IP addresses in the blacklist are denied by the Anti-DDoS Pro or Anti-DDoS Premium instance. The following list describes the blocking periods of IP addresses:

- If you manually add IP addresses to the blacklist, you must specify a blocking period. You can specify a blocking period from five minutes to seven days.
- The blacklist contains malicious IP addresses that are marked by the intelligent protection algorithms of Anti-DDoS Pro or Anti-DDoS Premium. The intelligent protection algorithms dynamically calculate the blocking periods of malicious IP addresses. The blocking period can be from 5 minutes to 1 hour. If attacks are frequently launched from a malicious IP address, Anti-DDoS Pro or Anti-DDoS Premium automatically extends the blocking period of the malicious IP address.

Requests from the IP addresses in the whitelist are allowed by the Anti-DDoS Pro or Anti-DDoS Premium instance. The IP addresses in the whitelist remain valid unless you manually remove them.

If an IP address is added to both the whitelist and blacklist, the whitelist takes effect at a higher priority. If you want to add an IP address that is added to the whitelist to the blacklist, you must first remove the IP address from the whitelist.

Procedure

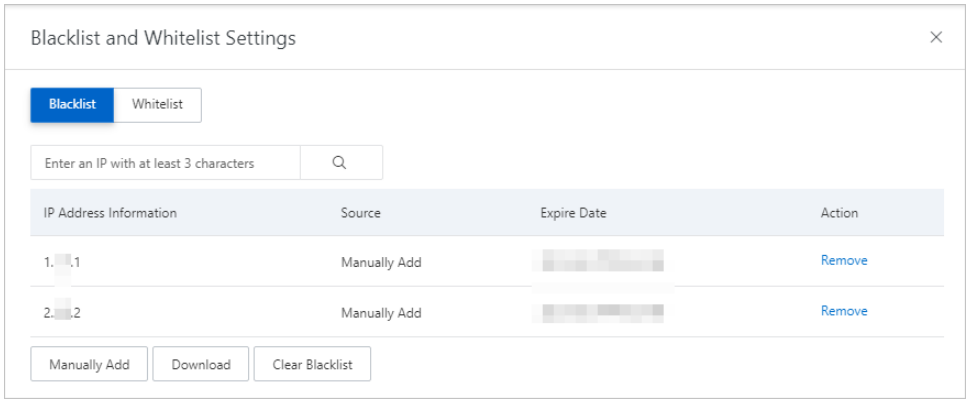
1.
2.
3.
4. On the **Protection for Infrastructure** tab, select the instance for which you want to configure

the whitelist or blacklist.

You can search for an instance by instance ID or description.

5. In the **Blacklist and Whitelist (Instance IP)** section, click **Change Settings**.

6. In the **Blacklist and Whitelist Settings** panel, click **Blacklist** or **Whitelist** to manage the blacklist or whitelist.



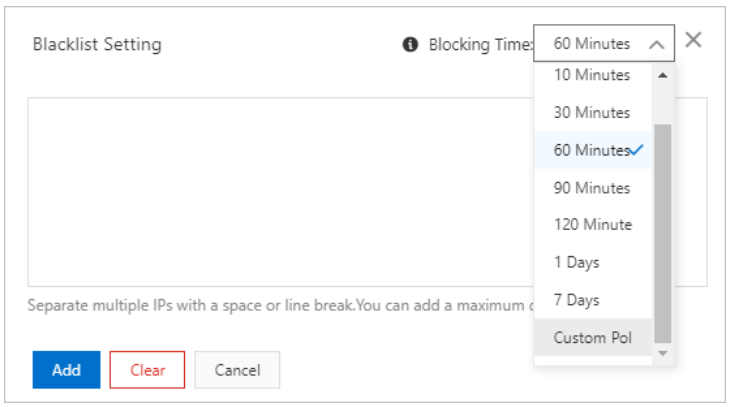
   - For more information about blacklist management, see Step 7.
   - For more information about whitelist management, see Step 8.

7. Manage the blacklist.
   - Add an IP address to the blacklist
     a. Click **Manually Add**.

        You can add up to 2,000 IP addresses to the blacklist. If you enter more than one IP address, separate them with spaces or line breaks.

     b. In the **Blacklist Setting** dialog box, enter the IP address and set **Blocking Time**.

        You can select a blocking period from the **Blocking Time** drop-down list. The blocking period can be from five minutes to seven days. You can also customize a blocking period in seconds.



     c. Click **Add**.

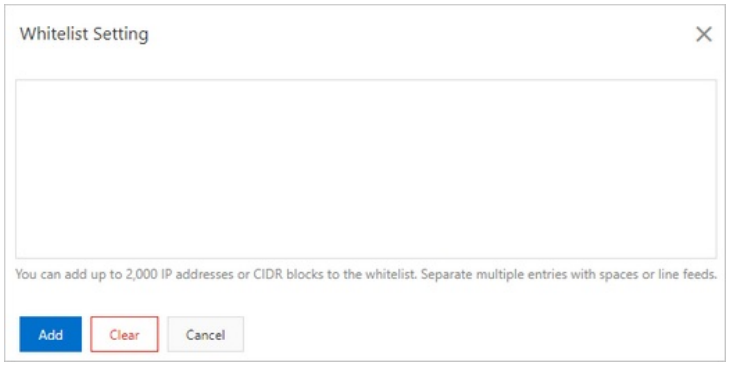
After the IP address is added to the blacklist, requests from this IP address are blocked during the specified blocking period. After the specified blocking period expires, this IP address is removed from the blacklist. If you want to deny the requests from this IP address, add the IP address to the blacklist again.

- Search for IP addresses in the blacklist: Enter a keyword in the search box to search for IP addresses that contain the keyword.
- Clear the blacklist: Click **Clear Blacklist** to remove all IP addresses from the blacklist. You can also click **Delete** next to an IP address to remove it from the blacklist.
- Download the blacklist
  a. Click **Download** to start a download task.
  b. In the message that appears, click **OK**.
  c. Close the **Blacklist and Whitelist Settings** panel.
  d. In the upper-right corner of the page, click the icon to expand the task list.
  e. Find the download task. After the status of the task changes to **Exported**, click **Download** in the Actions column.

  After you download the blacklist and save it as a TXT file to your computer, you can open the TXT file and view details about the blacklist.

8. Manage a whitelist.
   - Add an IP address to the whitelist.
     a. Click **Manually Add**.
     b. In the **Whitelist Setting** dialog box, enter the IP address from which the requests are allowed to the whitelist.

     > **Note** You can add up to 2,000 IP addresses to the whitelist. If you enter more than one IP address, separate them with spaces or line breaks.

     c. Click **Add**.

     After the IP address is added to the whitelist, requests from this IP address are directly forwarded to the origin server. The IP addresses in the whitelist remain valid unless you manually remove them.
   - Search for IP addresses in the whitelist: Enter a keyword in the search box to search for IP addresses that contain the keyword.
   - Clear the whitelist: Click **Clear Whitelist** to remove all IP addresses from the whitelist. You can

also click **Delete** next to an IP address to remove it from the whitelist.

- Download the whitelist.
  a. Click **Download** to start a download task.
  b. In the message that appears, click **OK**.
  c. Close the **Blacklist and Whitelist Settings** panel.
  d. In the upper-right corner of the page, click the icon to expand the task list.
  e. Find the download task. After the status of the task changes to **Exported**, click **Download** in the Actions column.

  After you download the whitelist and save it as a TXT file to your computer, you can open the TXT file and view details about the whitelist.

7.1.2. Use the feature of UDP Reflection Attacks Protection

If you want to use Anti-DDoS Pro or Anti-DDoS Premium to protect your UDP service, we recommend that you use the feature of UDP Reflection Attacks Protection. You can use this feature to configure filtering policies with a few clicks. Then, Anti-DDoS Pro or Anti-DDoS Premium discards the UDP traffic over specific ports based on the policies. This way, UDP reflection attacks are mitigated. This topic describes how to use the feature.

Prerequisites

- An Anti-DDoS Pro or Anti-DDoS Premium instance that uses the **Enhanced** function plan is purchased. For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

  The feature is available only for an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the Enhanced function plan. If you use an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the Standard function plan, you must upgrade your instance before you can use the feature. For more information, see Upgrade an instance.
- A forwarding rule over UDP is created on the **Port Config** page. For more information, see Create forwarding rules.

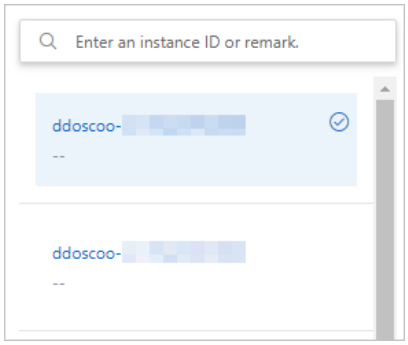
  The feature takes effect only on UDP traffic. Therefore, you can enable the feature only after you add your UDP service to Anti-DDoS Pro or Anti-DDoS Premium.

  If you do not create a forwarding rule or create only forwarding rules over TCP on the **Port Config** page, Anti-DDoS Pro or Anti-DDoS Premium discards all UDP traffic by default. In this situation, you do not need to configure the feature.

Procedure

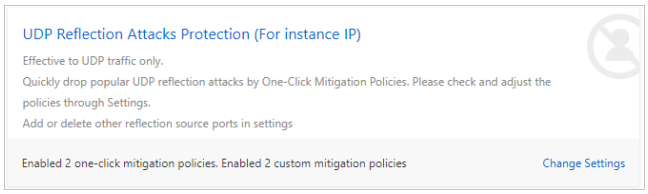
1.
2.
3.
4. On the **Protection for Infrastructure** tab, select the instance for which you want to configure the feature from the list on the left.

   You can search for the instance based on the instance ID or description.



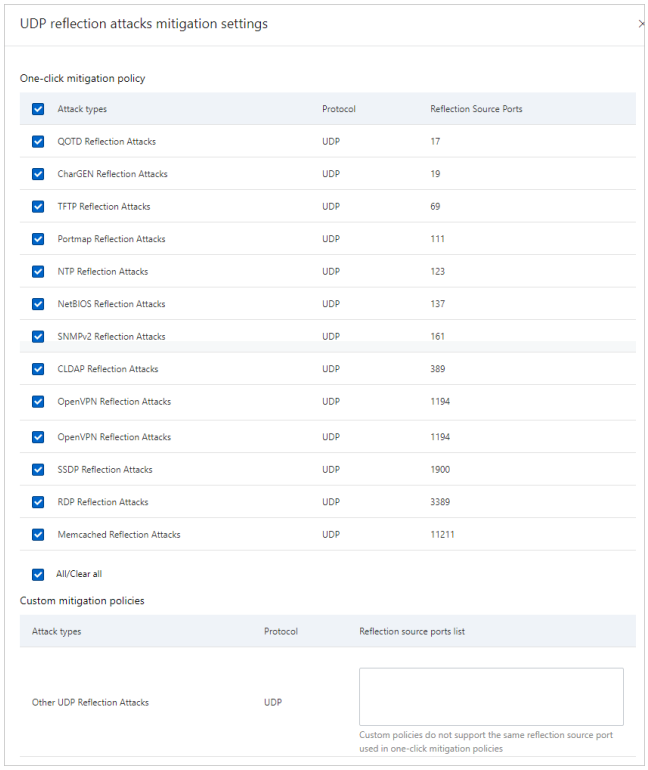
5. In the **UDP Reflection Attacks Protection (For instance IP)** section, click **Change Settings**.

> **Notice** The feature is available only for an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the Enhanced function plan. If you use an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the Standard function plan, click **Upgrade to Enhanced** to upgrade your instance.



6. In the **UDP reflection attacks mitigation settings** panel, configure filtering policies to specify ports over which UDP reflection attacks may be launched.

   After the filtering policies are configured, Anti-DDoS Pro or Anti-DDoS Premium discards the UDP traffic from the specified ports. If you configure forwarding rules over UDP for multiple UDP services, the filtering policies take effect on all the UDP services.



You can use one of the following methods to configure filtering policies based on your business requirements:

- **One-click mitigation policy**: Select policies from the list in the **One-click mitigation policy** section. We recommend that you use this method.

  A policy contains a common type of UDP reflection attack and the port over which the attack is launched. We recommend that you select all policies in the list to mitigate UDP reflection attacks that are launched over the ports.

- **Custom mitigation policies**: In the **Reflection source ports list** field of the **Custom mitigation policies** section, enter the ports over which you want Anti-DDoS Pro or Anti-DDoS Premium to discard the UDP traffic. The ports that you can enter must be within the range from 0 to 65535. You can enter up to 20 ports. Separate multiple ports with commas (,).

  You can use this method to configure filtering policies only for ports that are not in the list of the One-click mitigation policy section.

7. Click **OK**.
   After filtering policies are configured, Anti-DDoS Pro or Anti-DDoS Premium discards the UDP traffic over the ports that are specified in the filtering policies. This way, your UDP service is protected against UDP reflection attacks. You can modify the filtering policies in the Anti-DDoS Pro or Anti-DDoS Premium console based on your business requirements.

7.1.3. Configure diversion from the origin server

This topic describes how to configure the Diversion from Origin Server policy to block network traffic transmitted from regions outside mainland China through China Telecom or China Unicom lines. Each Alibaba Cloud account can enable this policy up to 10 times and disable it at any time.

Prerequisites

An Anti-DDoS Pro instance is available.

> **Note** The Diversion from Origin Server policy is available only for Anti-DDoS Pro.

Context

> **Note**

We recommend that you enable this policy if your Anti-DDoS Pro instance is under volumetric attacks that are about to exceed the protection capability. For example, if 30% of the attacks are launched from regions outside mainland China, you can use this policy to block these attacks in order to reduce the stress on your Anti-DDoS Pro instance.

After the Diversion from Origin Server policy is enabled, the specified network traffic is dropped at the data center. This minimizes the possibility of triggering a black hole. This way, you can protect your China Telecom or China Unicom lines. A black hole is triggered based on the same rules as Diversion from Origin Server, such as the volume of attack traffic and attack source. Therefore, the Diversion from Origin Server policy can minimize the possibility of triggering a black hole.

Procedure

1.

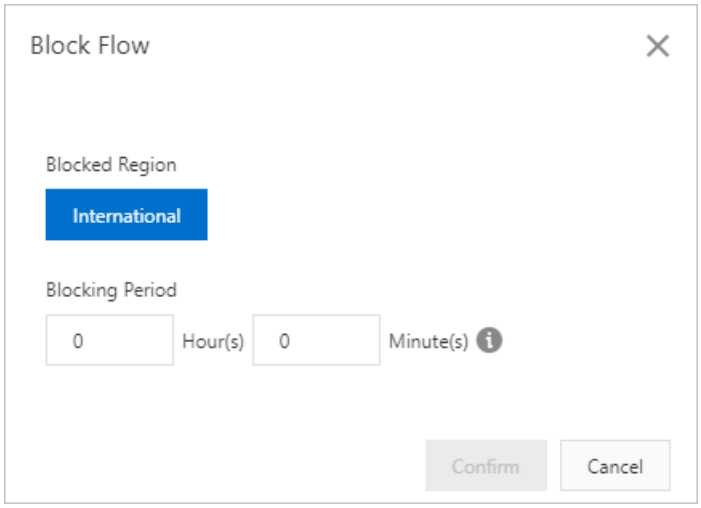
2. In the top navigation bar, select **Mainland China**.
3.
4. On the **Protection for Infrastructure** tab, select the target instance from the list on the left side.

   > **Note** You can also search for instances by instance ID or description.

5. In the **Diversion from Origin Server** section, perform the following operations as required.

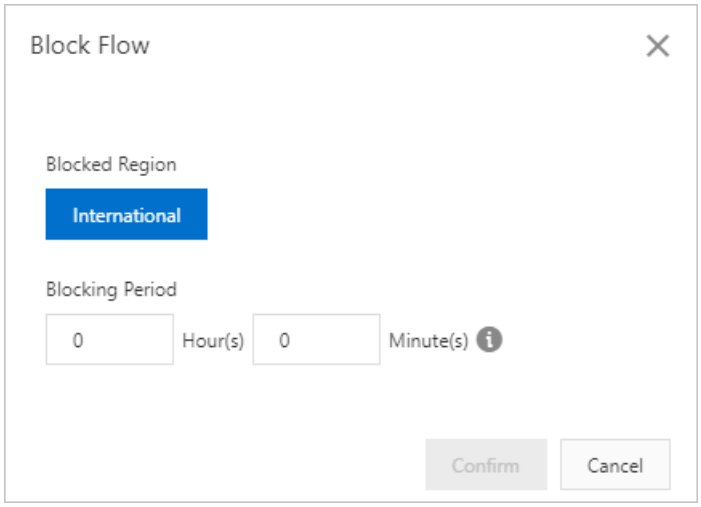
   - Block network traffic transmitted from regions outside mainland China through China Telecom lines: Click **Blocked** next to **Blocked Regions: China Telecom (International)**. In the **Block Flow** dialog box, set **Blocking Period** and click **Confirm**.

     > **Note** The minimum blocking period is 15 minutes, and the maximum is 23 hours and 59 minutes.



   - Block network traffic transmitted from regions outside mainland China through China Unicom lines: Click Blocked next to **Blocked Regions: China Unicom (International)**. In the **Block Flow** dialog box, set **Blocking Period** and click **Confirm**.

     > **Note** The minimum blocking period is 15 minutes, and the maximum is 23 hours and 59 minutes.

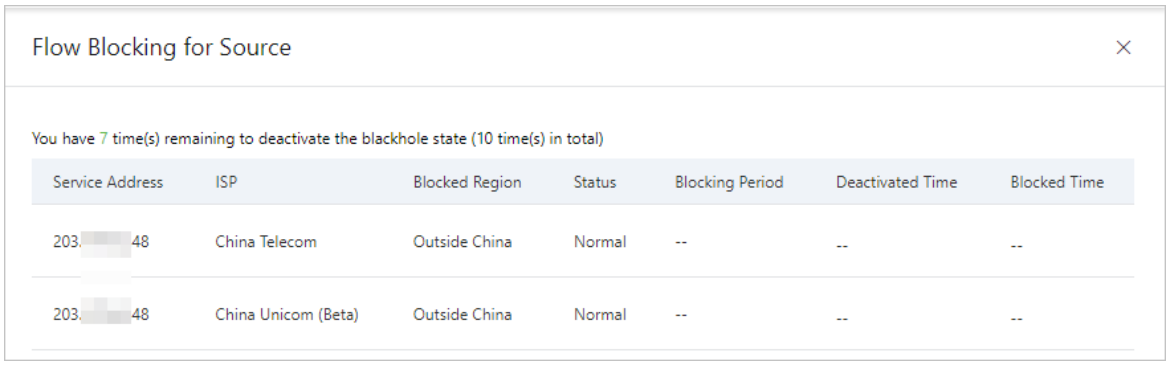


Note

- We recommend that you block network traffic transmitted from regions outside mainland China through China Telecom lines. You also need to monitor the changes in the volume of attack traffic. If the volume of attack traffic is about to exceed the protection capability of your instance, block the network traffic transmitted from regions outside mainland China through China Unicom lines.
- Each Alibaba Cloud account can enable this policy up to 10 times. Each time you enable this policy, the remaining quota is reduced by one.

If you fail to enable this policy, an error message appears. Follow the instructions to troubleshoot the error and try again. If no message appears, this policy is enabled.

6. (Optional)In the **Diversion from Origin Server** section, click **View Blocked Region**. In the **Flow Blocking for Source** pane, you can view the blocked regions and the blocking periods.



7. (Optional)Unblock network traffic.

   To **unblock** the network traffic that you have **blocked** before the blocking period expires, click **Deactivate Blackhole**.

7.1.4. Configure blocked regions

This topic describes how to configure and enable the Blocked Regions policy. This policy allows you to block requests to access Anti-DDoS Pro or Anti-DDoS Premium instances from IP addresses in specified regions. Anti-DDoS Pro or Anti-DDoS Premium instances that use the Enhanced function plan support this policy. After you enable this policy, requests to access Anti-DDoS Pro or Anti-DDoS Premium instances from the specified regions are dropped.

Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance that uses the Enhanced feature plan is available. For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

Context

The Blocked Regions policy drops the requests that are initiated from IP addresses of specific regions in China and specific countries and regions outside China. This way, requests from regions where your service is not involved are blocked. If all valid requests are initiated from regions inside China, you can configure the Blocked Regions policy to block requests from only regions outside China.

> **Note** This policy takes effect on Anti-DDoS Pro or Anti-DDoS Premium instances. You must configure this policy for each Anti-DDoS Pro or Anti-DDoS Premium instance.

Blocked Regions and Diversion from Origin Server

The Blocked Regions policy blocks requests from specific regions in scrubbing centers. This policy drops blocked requests near the destination servers. Anti-DDoS Pro or Anti-DDoS Premium instances identify and filter requests based on the region of the source IP addresses. This policy cannot reduce the volume of attack traffic. Therefore, it is suitable for mitigating connection flood attacks.

The Diversion from Origin Server policy drops requests from specific regions based on the attack source by using core routers on the network provided by an Internet Service Provider (ISP). For more information, see Configure diversion from the origin server.

> **Note** The Diversion from Origin Server policy is available only for Anti-DDoS Pro.

Blocked Regions and Blocked Regions (Domain Names)

The Blocked Regions policy configured for Anti-DDoS Pro or Anti-DDoS Premium instances has a higher priority than the Blocked Regions (Domain Names) policy when both the policies are in effect.

For example, if you configure the Blocked Regions policy for an Anti-DDoS Pro or Anti-DDoS Premium instance to block requests from regions outside China, users outside China cannot access domain names associated with this instance even if the Blocked Regions (Domain Names) policy is configured to allow access from these regions. If you want to block regions outside China for some services, we recommend that you configure blocked regions for domain names rather than for Anti-DDoS Pro or Anti-DDoS Premium instances. For more information, see Configure a location blacklist for a domain name.

Procedure

1.
2.
3.
4. On the **Protection for Infrastructure** tab, select the instance for which you want to configure blocked regions from the list on the left side.

> **Note** You can search for instances based on instance IDs or descriptions.

5. In the **Blocked Regions** section, click **Change Settings**.
6. In the **Configure Blocked Regions** panel, select the regions that you want to block and click **OK**.
7. Go back to the **Blocked Regions** section and turn on **Status** to apply the settings.

7.1.5. Deactivate blackhole filtering

If a service protected by Anti-DDoS Pro is attacked and the bandwidth of attack traffic exceeds the basic or burstable protection threshold, blackhole filtering is triggered. In this case, you can manually deactivate blackhole filtering in the Anti-DDoS Pro console to recover your service. We recommend that you increase the basic or burstable protection capability before you deactivate blackhole filtering. This prevents blackhole filtering from being triggered again.

Prerequisites

An Anti-DDoS Pro instance is purchased.

> **Note** Anti-DDoS Pro supports deactivation of blackhole filtering, but Anti-DDoS Premium does not.

Context

Each Alibaba Cloud account can deactivate blackhole filtering up to five times per day. The count is reset at 00:00:00 (UTC+8) the next day.

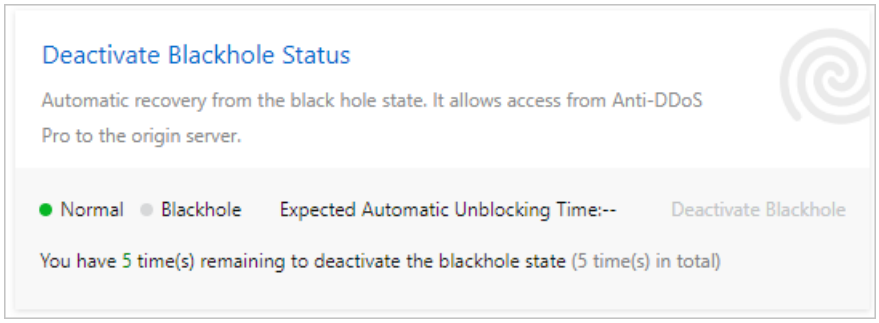
You consume a chance of deactivation only when you successfully deactivated blackhole filtering. The first deactivation in a day immediately takes effect. The interval of two deactivation operations must be greater than 10 minutes.

Procedure

1.
2. In the top navigation bar, select **Mainland China**.

   You can switch the region to manage and configure Anti-DDoS Pro or Anti-DDoS Premium instances. Make sure that you select the required region of Anti-DDoS Pro.
3.
4. On the **Protection for Infrastructure** tab, select the Anti-DDoS Pro instance from the list on the left.

   You can also search for the instance by its ID or description.
5. In the **Deactivate Blackhole Status** section, deactivate blackhole filtering based on the instance status.



- If the instance is in the **Blackhole** state, and you do not want to wait for blackhole filtering to be automatically deactivated, click **Deactivate Blackhole** and wait for blackhole filtering to be deactivated.
- If the instance is in the **Normal** state, the **Deactivate Blackhole** button is dimmed.

  The interval of two deactivation operations must be greater than 10 minutes.

Result

- Blackhole filtering is a risk management policy used by the backend servers of Alibaba Cloud. If your request to deactivate blackhole filtering fails, your deactivation chance for the day is not deducted. In this case, an error message appears. You can wait and try again later.
- If the message "Cannot deactivate the black hole status due to risk management. Wait 10 minutes and try again." appears, try again 10 minutes later.
- If no error message appears, blackhole filtering is deactivated. You can refresh the page to check whether network access is restored.

Related information

- ModifyBlackholeStatus

7.1.6. Connect to an ECS instance for which blackhole filtering is triggered

This topic describes how to connect to an ECS instance for which blackhole filtering is triggered from another ECS instance that resides in the same region.

Context

If your ECS instance encounters a volumetric attack that triggers blackhole filtering, all Internet traffic to the ECS instance is blocked. However, you can still access the ECS instance from Alibaba Cloud services that are in the same region as this ECS instance.

Therefore, after blackhole filtering is triggered for an ECS instance, you can connect to it from another ECS instance in the same region.

Procedure

1. Log on to a normal ECS instance that is in the same region as the ECS instance for which blackhole filtering is triggered.

> **Note** These two ECS instances must be in the same VPC and be able to communicate with each other. Make sure that communication is not blocked by security group rules. For more information, see Overview.

2. Use a tool or the command line interface to connect to the ECS instance for which blackhole filtering is triggered.
   After the connection is successful, you can modify configuration files on this ECS instance or transfer files to the normal ECS instance to which you log on.

7.2. Protection for website services

7.2.1. Use the intelligent protection feature

This topic describes how to use the intelligent protection feature provided by Anti-DDoS Pro and Anti-DDoS Premium to protect website services. The intelligent protection feature is developed based on the big data technologies of Alibaba Cloud. The feature automatically learns traffic patterns and uses algorithms to analyze attacks. Then, the feature apply accurate access control rules to adjust protection modes and to detect and block attacks at the earliest opportunity. The attacks include malicious bots and HTTP flood attacks.

Prerequisites

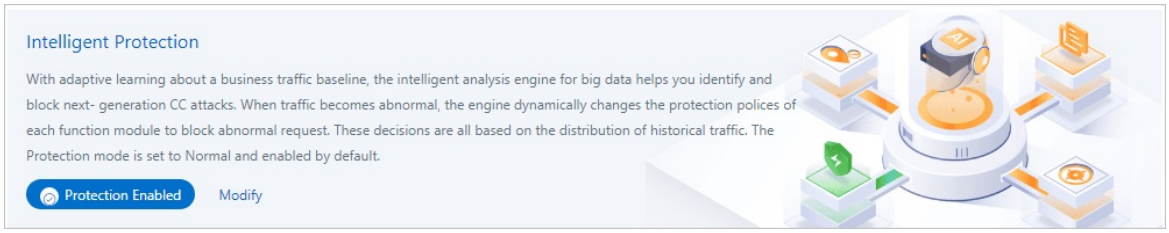
- A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.
- Mitigation settings are enabled in the latest version of Anti-DDoS Pro or Anti-DDoS Premium.

Context

After you add your website to Anti-DDoS Pro or Anti-DDoS Premium, the intelligent protection feature is enabled by default. The intelligent protection engine automatically learns traffic patterns and protects the website against web attacks by using accurate access control rules.

Configure a policy for the intelligent protection feature

1.
2.
3.
4. On the **General Policies** page, click the **Protection for Website Services** tab. On the tab that appears, select a specific domain name from the list in the left side.
5. In the **Intelligent Protection** section, click **Modify**.



6. In the **Intelligent Protection** dialog box, configure **Mode** and **Level**, and turn on **Status**.
   - **Mode**: Set this parameter to **Warning** or **Defense**.

     This feature supports the following protection modes:

- **Warning**: In this mode, when Anti-DDoS Pro or Anti-DDoS Premium detects malicious requests, Anti-DDoS Pro or Anti-DDoS Premium records the attacks but does not block the requests. You can use this mode to learn how the feature safeguards your website.

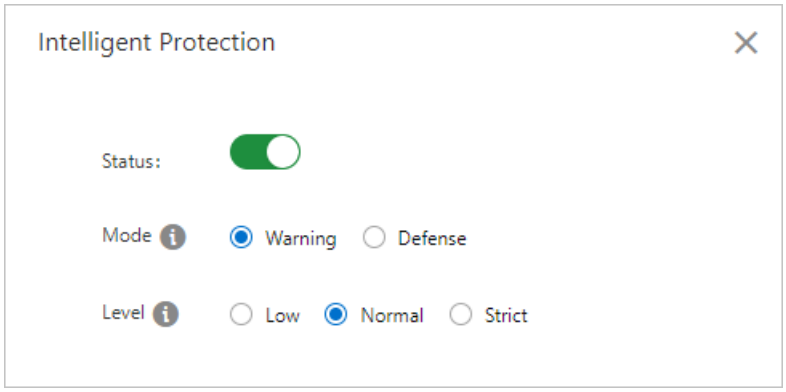
  You can use this mode and the Log Analysis feature to query warnings recorded by the feature and verify the protection capabilities of the feature. For more information, see View attack warning logs.

- **Defense**: In this mode, when Anti-DDoS Pro or Anti-DDoS Premium detects malicious requests, Anti-DDoS Pro or Anti-DDoS Premium applies accurate access control rules to block the malicious requests.

  > **Note** The feature uses accurate access control rules to trigger actions. To make sure that the feature works as expected, you must enable Accurate Access Control. For more information, see Configure accurate access control rules.

  We recommend that you use the Warning mode and the Log Analysis feature to analyze the attack logs. For this policy to take effect, enable the Defense mode only when the feature works as expected.

- **Level**: Set this parameter to **Low**, **Normal**, or **Strict**.



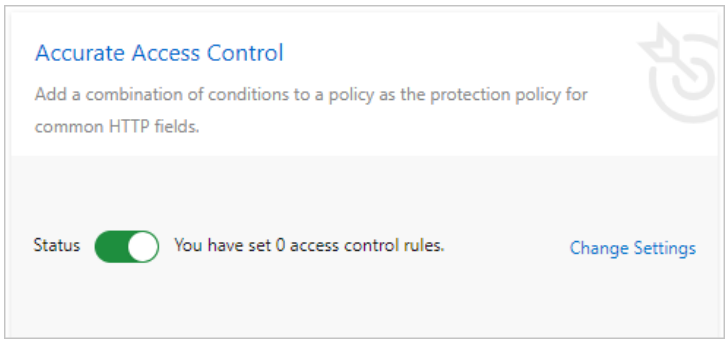
If you enable the feature, you can select a value for Level based on your business requirements. The following table describes the protection levels provided by the feature.

Level	Effect	Scenario
Low	Blocks specific attacks and allows normal requests.	Large websites that have high processing capabilities, and specific scenarios such as sales promotions
Normal (recommended)	Does not process requests in most cases. When Anti-DDoS Pro or Anti-DDoS Premium detects traffic that poses a threat to the protected website, Anti-DDoS Pro or Anti-DDoS Premium protects the website and minimizes the negative impacts on the website.	Scenarios in which the number of requests does not greatly fluctuate and the servers have additional resources other than managing normal network traffic
Strict	Strictly and intelligently blocks attacks. However, normal requests may also be blocked.	Websites that do not have sufficient processing or protection capabilities

After the feature is enabled, Anti-DDoS Pro or Anti-DDoS Premium automatically generates accurate access control rules when Anti-DDoS Pro or Anti-DDoS Premium detects malicious attacks. You can view the rules in the Accurate Access Control section.

View accurate access control rules

1.
2.
3.
4. On the **General Policies** page, click the **Protection for Website Services** tab. Select the required domain name from the list on the left side.
5. In the **Accurate Access Control** section, click **Change Settings**.



6. On the **Accurate Access Control** page, view the rules that start with **smartcc_**.

   Accurate access control rules created by Intelligent Protection start with smartcc_. Compared with custom accurate access control rules, the accurate access control rules created by the feature have the following characteristics:

   - The action of a rule may be warning. In Warning mode, the action specified in an accurate access control rule that is created by the feature is warning. In this case, Anti-DDoS Pro or Anti-DDoS Premium records attacks but does not block attacks.
   - Each rule has a validity period. After a rule expires, the rule becomes invalid and is automatically deleted.
   - Rules cannot be manually deleted. If you disable the feature, rules created by the feature are immediately deleted.

View attack warning logs

After the feature is enabled for your website, the Log Analysis feature records detected attacks that trigger the accurate access control rules. You can query the attack warning logs that are associated with the accurate access control rules on the Log Analysis page. This allows you to check the performance levels of the feature.

Prerequisites

- The Log Analysis feature is enabled for your website. For more information, see Overview.
- The intelligent protection feature is enabled for your website and is set to the Warning mode.

Queries

Log on to the Anti-DDoS Pro or Anti-DDoS Premium console and choose **Investigation > Log Analysis**. On the page that appears, select a domain name and enter the following query statement to view the attack warning logs related to the intelligent protection feature:

> **Note** Replace `aliyundoc.com` with the actual domain name of your website.

```
matched_host:"aliyundoc.com" and cc_action:alarm
```

Modify the policy for the intelligent protection feature

In the following business scenarios, we recommend that you modify the policy for the intelligent protection feature. This helps the feature learn traffic patterns to prevent false positives.

Scenario	Optimization method
Before you add your website to Anti-DDoS Pro or Anti-DDoS Premium, your website is configured with common throttling policies, or a large number of clients frequently reconnect to your website at the same time. Even if your website service is running normally, a large number of 4xx or 5xx HTTP status codes are returned.	1. On the **Protection for Website Services** tab, click **Modify** in the **Intelligent Protection** section. 2. In the **Intelligent Protection** dialog box, set **Mode** to **Warning**. 3. After three days, set **Mode** to **Defense**.
You want to launch a promotion event or stress test on your website, but the origin server of the website returns a large number of 4xx or 5xx HTTP status codes.	1. In the left-side navigation pane, choose **Mitigation Settings > Custom Policies**. On the page that appears, click **Create Policy** in the upper-left corner. 2. In the **Create Policy** dialog box, configure Policy Name and Validity Period and click **Confirm**. 3. Find the created policy in the policy list and click **Configure Policy** in the **Actions** column. 4. In the panel that appears, select websites or IP addresses that you want to protect.

7.2.2. Configure blacklists and whitelists for domain names

This topic describes how to configure the Black Lists and White Lists (Domain Names) policy in Anti-DDoS Pro or Anti-DDoS Premium to protect website services. After you enable this policy, access requests from the IP addresses or CIDR blocks in the blacklist are blocked, while access requests from the IP addresses or CIDR blocks in the whitelist are allowed.

Prerequisites

A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.

Context

> Note

After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect website services, you can add malicious IP addresses to the blacklist to block requests from them. You can add trusted IP addresses to the whitelist. Requests received from whitelisted IP addresses are forwarded directly to the website.

Precautions

- You can only enable the Black Lists and White Lists (Domain Names) policy for website services. You can configure a blacklist or whitelist on the Protection for Infrastructure tab for non-website services. For more information, see Configure the IP address blacklist and whitelist for an Anti-DDoS Pro or Anti-DDoS Premium instance.

  > Note The Black Lists and White Lists (Destination IP) policy is available only for Anti-DDoS Pro.

- The Black Lists and White Lists (Domain Names) policy only takes effect on a single domain name. It does not take effect on an Anti-DDoS Pro or Anti-DDoS Premium instance.
- You can configure up to 200 IP addresses or CIDR blocks in a blacklist or whitelist for a domain name.

Procedure

1.
2.
3.
4. On the **General Policies** page, click the **Protection for Website Services** tab and select the target domain name from the list on the left side.
5. In the **Black Lists and White Lists (Domain Names)** section, click **Change Settings**.

6. In the **Blacklist and Whitelist Settings** dialog box, configure the blacklist and whitelist and then click **OK**.
   - On the **Blacklist** tab, enter the malicious IP addresses or CIDR blocks that you want to block.
   - On the **Whitelist** tab, enter the IP addresses or CIDR blocks that you want to allow to pass through.

> **Note**
>
> - You can enter IP addresses or CIDR blocks. CIDR blocks must be in the format of IP address/Subnet mask.
> - You can add up to 200 IP addresses or CIDR blocks to a whitelist or blacklist. Separate multiple IP addresses or CIDR blocks with commas (,).
> - You can add 0.0.0.0/0 to the blacklist to block requests from all IP addresses except those added to the whitelist.

7. Go back to the **Black Lists and White Lists (Domain Names)** section and turn on **Status** to apply the settings.

> **Note** If you use an earlier version, you must enable HTTP flood prevention for the blacklist and whitelist to take effect.

Result

After the policy is enabled, the settings apply to each Anti-DDoS Pro or Anti-DDoS Premium instance associated with domain names and take effect on access to the domain names immediately.

> **Note** In some situations, the Black Lists and White Lists (Domain Names) policy takes effect only after your instance receives and processes certain inbound traffic. If the settings do not take effect after the policy is enabled, you can access the domain names several times to initiate the settings.

7.2.3. Configure a location blacklist for a domain name

This topic describes how to configure a location blacklist for a website that is protected by an Anti-DDoS Pro or Anti-DDoS Premium instance. After you enable the feature, you can add a location to the location blacklist to block requests from IP addresses that reside within the location with a few clicks.

Context

You can configure the location blacklist in the following scenarios:

- If your website is available only for users in a location, you can add other locations to the location blacklist after you add your website to Anti-DDoS Pro or Anti-DDoS Premium. For example, your website is available only for users in China, and you can add locations outside China to the location blacklist.
- If your website experiences frequent DDoS attacks from a location, you can add the location to the location blacklist after you add your website to Anti-DDoS Pro or Anti-DDoS Premium.

Precautions

- This feature is supported only for websites. We recommend that you configure traffic blocking policies on the Protection for Infrastructure tab to protect non-website services. For more information, see Configure diversion from the origin server and Configure blocked regions. Only Anti-DDoS Pro supports diversion from the origin server.
- You cannot configure location blacklists for multiple domain names at a time. If you want to configure location blacklists for multiple domain names, you must separately configure a location blacklist for each domain name.
- This feature identifies and filters only requests whose originating IP addresses reside in the blocked locations. This feature cannot reduce the volume of attack traffic.

Prerequisites

A website is added to Anti-DDoS Pro or Anti-DDoS Premium and is associated with an instance that uses the Enhanced function plan. For more information, see Add a website.

Procedure

1.
2.
3.
4. On the **General Policies** page, click the **Protection for Website Services** tab. In the left-side list of domain names, select a domain name.
5. In the **Location Blacklist (Domain Names)** section, click **Change Settings**.
6. In the **Configure Location Blacklist** panel, select the locations that you want to block and click **OK**.
7. Go back to the **Location Blacklist (Domain Names)** section and turn on **Status** to apply the configuration.

Result

After the feature is enabled, the configuration takes effect immediately on all Anti-DDoS Pro or Anti-DDoS Premium instances that are associated with the specified domain name.

7.2.4. Configure accurate access control rules

Both Anti-DDoS Pro and Anti-DDoS Premium allow you to create accurate access control rules for website services that they protect. After you enable Accurate Access Control, you can customize access control rules. These rules allow you to filter access requests based on commonly used HTTP fields, such as IP, URI, Referer, User-Agent, and Params. You can allow, block, or verify requests that match the rules. Accurate Access Control supports custom rules for different scenarios, such as hotlink protection and protection of the website management system.

Prerequisites

- The domain name of your website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.
- Protection settings are enabled in Anti-DDoS Pro or Anti-DDoS Premium.

Context

After you add your website service to Anti-DDoS Pro or Anti-DDoS Premium, you can enable Accurate Access Control and create accurate access control rules to manage requests that have specific characteristics. Each accurate access control rule consists of one or more conditions and one action.

- Conditions specify the HTTP fields, logic operators, and field values to be matched. The following table describes the HTTP fields supported by accurate access control rules.

  Note Different HTTP fields support different logical operators. For example, the source IP field supports the Is Part Of and Is Not Part Of logical operators. The URI field supports the Contains and Does Not Contain logical operators. For more information, see the Logical operator column in the following table.

Field	Field description	Supported logical operator
IP	The source IP address of the request.	Is Part Of and Is Not Part Of
URI	The request URI.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, and Is Longer Than
User-Agent	The information about the client browser that sends the request.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, and Is Longer Than
Cookie	The cookie in the request.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, Is Longer Than, and Does Not Exist
Referer	The source URL of the request, that is, the page from which the access request is redirected.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, Is Longer Than, and Does Not Exist
Content-Type	The HTTP content type of the response specified by the request, that is, MIME type information.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, and Is Longer Than

Field	Field description	Supported logical operator
X-Forwarded-For	The actual client IP address of the request.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, Is Longer Than, and Does Not Exist
Content-Length	The number of bytes in the request body.	Value Less Than, Value Equals, and Value More Than
Post-Body	The content of the request.	Contains, Does Not Contain, Equals, and Does Not Equal
Http-Method	The request method. Valid values: GET, POST, DELETE, PUT, OPTIONS, CONNECT, HEAD, and TRACE.	Equals and Does Not Equal
Header	The request header that is used to customize the HTTP header fields and values.	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, Is Longer Than, and Does Not Exist
Params	The parameters in the request URI. The parameters follows a question mark (`?`) in the URI. For example, the URI `example.aliyundoc.com/index.html?action=login` contains a parameter `action=login` .	Contains, Does Not Contain, Equals, Does Not Equal, Is Shorter Than, Has a Length Of, and Is Longer Than

- An action defines how a request is handled when it meets the conditions. Supported actions are Clear, Blocked, and JS Challenge. The JS Challenge action verifies source IP addresses by using JavaScript plug-ins.

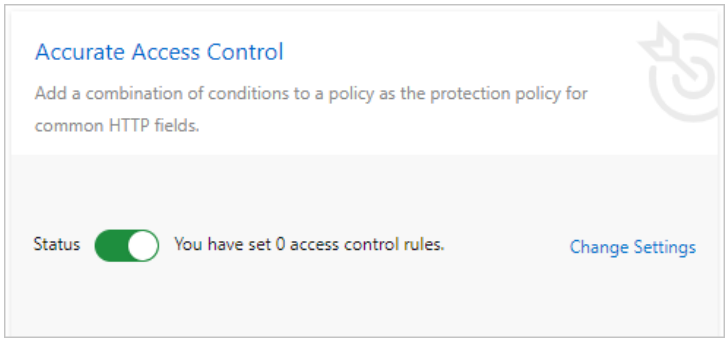
Limits

The following table describes the limits on Accurate Access Control based on the function plan of an Anti-DDoS Pro or Anti-DDoS Premium instance.

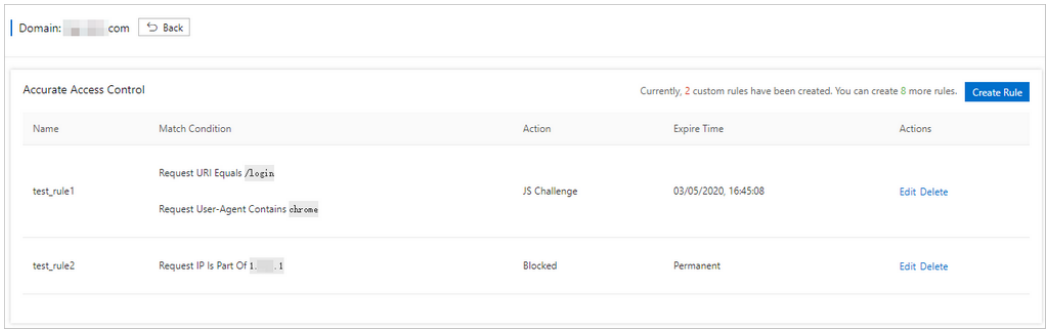
Limit	Standard function plan	Enhanced function plan
Number of custom rules	≤ 5	≤ 10
Supported match fields	IP, URI, Referer, and User-Agent	All fields that support matching

Procedure

1.
2.
3.
4. On the **General Policies** page, click the **Protection for Website Services** tab. Select the required domain name from the list on the left side.
5. In the **Accurate Access Control** section, click **Change Settings**.



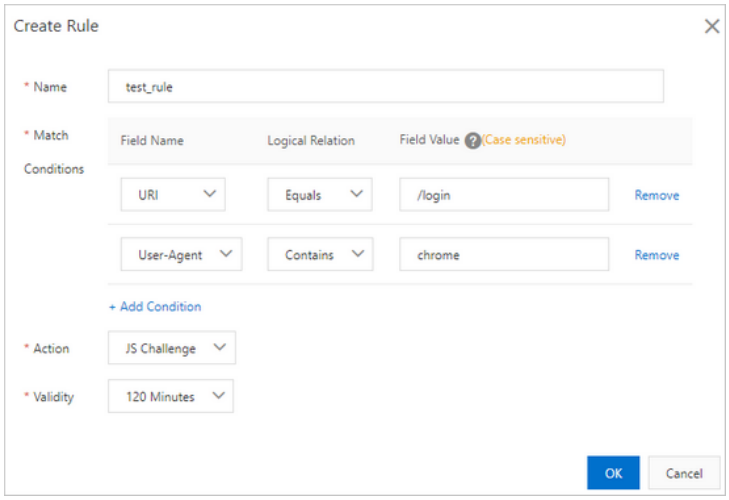
6. Create an accurate access control rule for the domain name.



- Create a rule
  a. Click **Create Rule**.

  > **Note** If the number of custom rules reaches the upper limit, the **Create Rule** button is not displayed.

  b. In the **Create Rule** dialog box, specify the required parameters and click **OK**.



Parameter	Description
Name	The name of the rule. The name can be up to 128 characters in length and can contain letters, digits, and underscores (_).

Parameter	Description
Match Conditions	The match condition of the rule. To add match conditions for a rule, click **Add Condition**. Each condition consists of **Field Name**, **Logical Relation**, and **Field Value**. ■ Specify Field Name and Logical Relation based on the Supported match fields. ■ Specify Field Value based on Field Name. Field Value is case sensitive. This filed does not support regular expressions, but can be left empty. You can add multiple match conditions. If multiple conditions are specified, a request matches the rule only when all the conditions are met.
Action	The operation that is performed when a request meets the match conditions. Valid values: ■ **Blocked**: Requests that meet match conditions are blocked. ■ **Clear**: Requests that meet match conditions are allowed. ■ **JS Challenge**: Source IP addresses of requests that meet the match conditions are verified by using JavaScript plug-ins.
Validity	The validity period of the rule. You can set this parameter to 5 Minutes, 10 Minutes, 30 Minutes, 60 Minutes, 90 Minutes, 120 Minutes, or Permanent.

In this example, if a request is sent to a page that contains `/login` and the User-Agent field of the request contains `chrome`, the source IP address is verified. The rule remains valid 120 minutes after it is created.

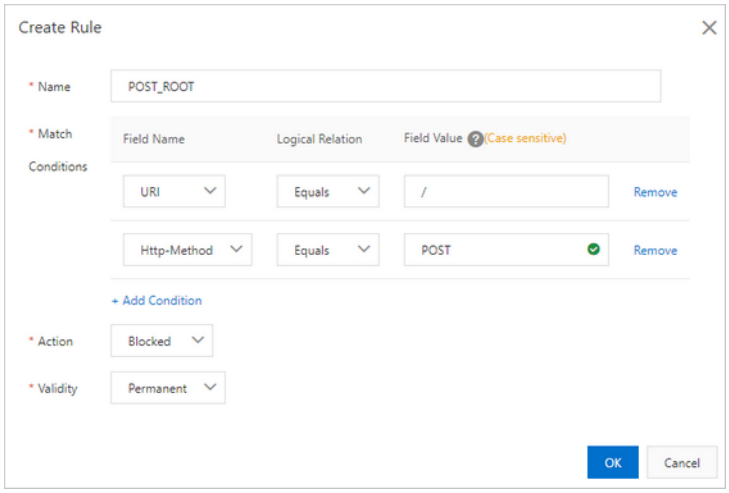
You can create multiple rules as required.

> **Note**
>
> ■ If you create multiple rules, the priority of a rule depends on its rank in the rule list. The higher the rank, the higher the priority. The system matches a request against rules in sequence based on their priorities. The higher the rule priority, the earlier the rule is matched.
>
> ■ If a request meets match conditions of multiple rules, the action of the rule with the highest priority takes effect.

Examples:

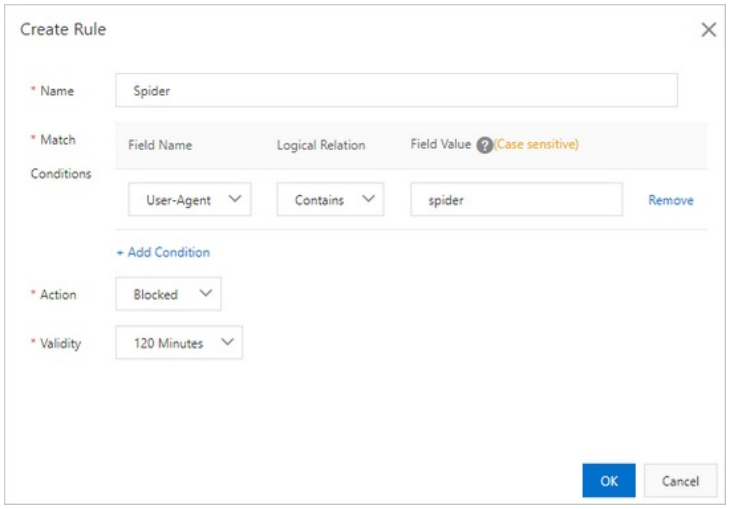
- Block specific requests.

  In most cases, the root directory of a website does not receive POST requests. If an HTTP flood attack occurs, your website may receive a large number of POST requests that access the root directory. We recommend that you check whether these requests are normal. If these requests are suspicious, you can use accurate access control rules to block them. The following figure shows the example configuration.



- Block web crawlers.

  If your website receives a large number of crawler requests within a period of time, an HTTP flood attack may be initiated from bots that simulate crawlers. You can use accurate access control rules to block these requests. The following figure shows the example configuration.



- Edit a rule.
  a. In the rule list, find the rule that you want to edit and click **Edit** in the Actions column.
  b. In the **Edit Rule** dialog box, modify the rule settings and click **OK**. Configure the rule settings the same way as you create a rule. You cannot change the value of **Name**.
- Delete a rule.
  a. In the rule list, find the rule that you want to delete and click **Delete** in the Actions column.
  b. In the message that appears, click **OK**.

7. Go back to the **Accurate Access Control** section and turn on **Status** to apply the rules.

7.2.5. Configure frequency control

Both Anti-DDoS Pro and Anti-DDoS Premium allow you to configure the Frequency Control policy for protected website services. You can use this policy to control the frequency of requests sent to your website from specific IP addresses. Frequency Control takes effect immediately after it is enabled. By default, the Normal mode is used to protect website services against common HTTP flood attacks. Frequency Control supports multiple modes for different scenarios. You can also create custom frequency control rules to prevent a specific IP address from frequently visiting a page in a short period of time.

Prerequisites

- A website is added to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.
- Protection settings in Anti-DDoS Pro or Anti-DDoS Premium of the latest version are enabled.

Context

> Note

After you set up an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your website service, you can enable Frequency Control to protect the website against HTTP flood attacks. Frequency Control supports multiple modes and allows you to adjust the mode in real time based on the traffic status of the website.

- Normal: We recommend that you use this mode if the website traffic is normal. By default, this mode is used. In this mode, Frequency Control protects websites against common HTTP flood attacks but does not block normal requests.
- Emergency: You can enable this mode when you detect HTTP response errors, traffic anomalies, or CPU and memory usage spikes. The Emergency mode provides relatively rigorous protection compared to the Normal mode. In this mode, Frequency Control protects websites against more complicated HTTP flood attacks but may block a few normal requests.
- Strict: This mode provides rigorous protection. It uses Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) to verify the identities of all visitors. Only verified visitors are allowed to access the website.

  > Note The CAPTCHA verification mechanism of this mode allows the requests that are initiated by real users from browsers. However, if the protected website provides API or native application services, requests to the website cannot pass the verification and will fail to access the services provided by the website.

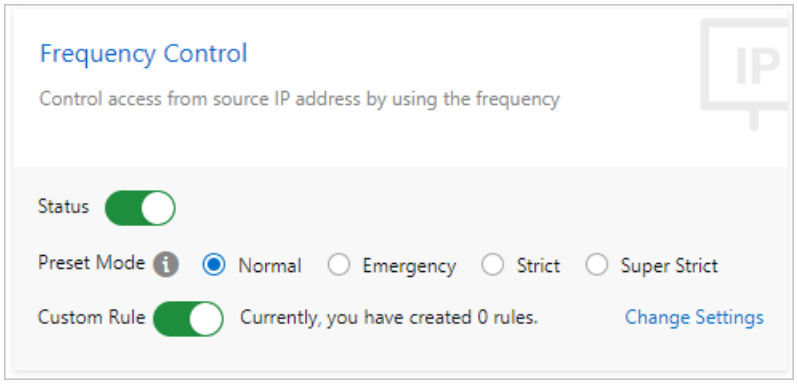
- Super Strict: This mode provides the most rigorous protection against HTTP flood attacks. It uses CAPTCHA to verify the identities of all visitors. Only verified visitors are allowed to access the website. Compared to the Strict mode, this mode combines CAPTCHA verification with anti-debugging and anti-machine verification technologies to enhance the protection of your website.

> **Note** The CAPTCHA verification mechanism of this mode allows the requests that are initiated by real users from browsers. Exceptions may occur in some browsers and cause the website to be inaccessible. In this case, you can restart the browser and revisit the website. However, if the protected website provides API or native application services, requests to the website cannot pass the verification and will fail to access the services provided by the website.

In addition to the protection modes, Frequency Control also allows you to create custom rules to block attacks more precisely. You can create a custom rule to protect a specific URL. After a custom rule is created, the specified IP address cannot frequently access the URL in a short period of time.

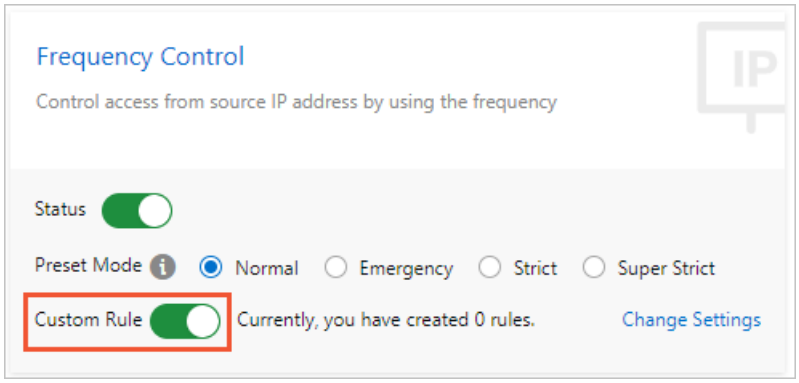
Configure a frequency control mode

1.
2.
3.
4. On the **General Policies** page, click the **Protection for Website Services** tab. On the tab that appears, select the target domain name from the list on the left side.
5. In the **Frequency Control** section, set **Preset Mode** as required and turn on **Status**. Supported modes include **Normal**, **Emergency**, **Strict**, and **Super Strict**.

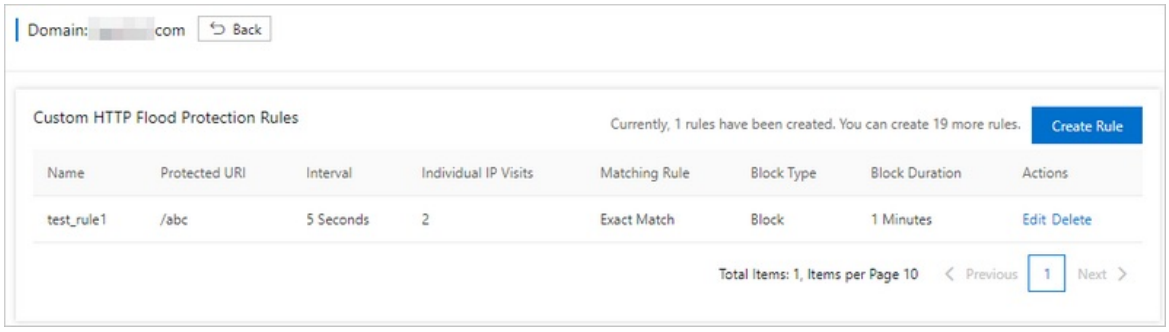


Create a custom frequency control rule

1.
2.
3.
4. On the **General Policies** page, click the **Protection for Website Services** tab. On the tab that appears, select the target domain name from the list on the left side.
5. In the **Frequency Control** section, turn on **Custom Rule** and then click **Change Settings**.



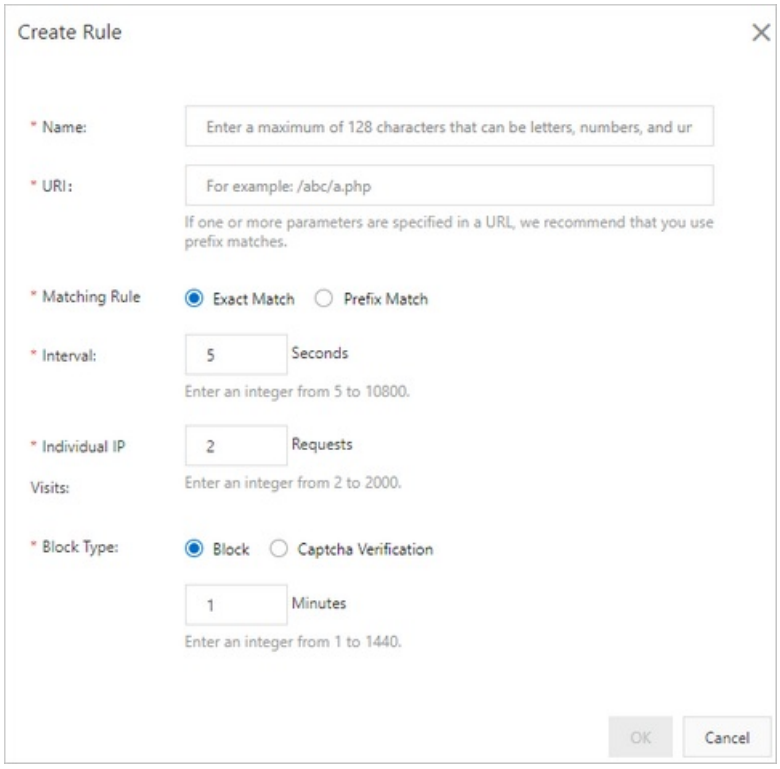
6. Create a frequency control rule for a domain name.



- Create a rule
  a. Click **Create Rule**.

  > **Note** A maximum of 20 rules can be created. If the number of rules reaches the upper limit, the **Create Rule** button is dimmed.

  b. In the **Create Rule** dialog box, specify the required parameters and then click **OK**.



Configuration	Description
Name	The name of this rule.
URI	The URI path to be protected. For example, */register*. The path can contain parameters connected by "?". For example, you can use */user?action=login*.
Matching rule	■ **Exact Match**: The request URI must be exactly the same as the configured URI here to get counted. ■ **URI Path Match**: When the request URI starts with the URI value configured here, the request is counted. For example, */register.html* is counted if you use */register* as the URI.
Interval	The cycle for calculating the number of visits. It works in sync with **Visits from one single IP address**.
Visits from a single IP address	The number of visits allowed from a single source IP address to the URL during the **Interval**.
Blocking type	The action to be performed after the condition is met. The operations can be Block or Human-Machine Identification. ■ **Block**: blocks accesses from the client after the condition is met. ■ **Man-Machine Identification**: accesses the client with redirection after the condition is met. Only the verified requests are forwarded to the origin.

You can create multiple rules as required.

- Edit a rule
  a. In the rule list, find the target rule and click **Edit** in the Actions column.
  b. In the **Edit Rule** dialog box, modify the settings and click **OK**. Specify the parameters in the same way you create a rule. However, you cannot change **Name** and **URI**.
- Delete a rule
  a. In the rule list, find the target rule and click **Delete** in the Actions column.
  b. In the message that appears, click **OK**.

7. Go back to the **Frequency Control** section and turn on **Status** to apply the rule.

Best practices

The protection intensities provided by different protection modes are listed in descending order: Super Strict > Strict > Emergency > Normal. The probabilities of false positives when you use these protection modes are listed in descending order: Super Strict > Strict > Emergency > Normal.

In normal situations, we recommend that you use the Normal mode for your protected website. In this mode, Frequency Control only blocks IP addresses that frequently send requests to your website. We recommend that you use the Emergency or Strict mode when your website is overwhelmed by HTTP flood attacks and the Normal mode fails to protect your website.

If your website provides API or native application services and the Strict or Super Strict mode is enabled, requests to the website cannot pass the verification. Therefore, these two modes are not suitable to protect this kind of website. You must create custom rules to protect specific URLs from HTTP flood attacks.

7.2.6. Configure the global mitigation policy

Anti-DDoS Pro or Anti-DDoS Premium provides the built-in global mitigation policy for websites that are added to Anti-DDoS Pro or Anti-DDoS Premium. The global mitigation policy supports three modes that are classified based on the intensity of traffic scrubbing. The policy helps you respond to volumetric attacks at the earliest opportunity. This topic describes how to configure the global mitigation policy.

Prerequisites

- An Anti-DDoS Pro instance or an Anti-DDoS Premium instance of the Insurance, Unlimited, or Secure Mainland China Acceleration (Sec-MCA) mitigation plan is purchased.

  For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.
- The website that you want to protect is added to the instance on the **Website Config** page.

  For more information, see Add a website.

Context

The global mitigation policy contains general protection rules that are accumulated when Anti-DDoS Pro or Anti-DDoS Premium handles common threats. After you enable the global mitigation policy, you can apply the general protection rules to the websites that are added to your instance. This reduces the risks that are caused by attacks on your websites.

You can separately enable the global mitigation policy for the domain name of each protected website. The global mitigation policy supports the following modes: **Normal**, **Low**, and **Strict**.

If you add a website to your instance on or after November 24, 2021, the global mitigation policy is automatically enabled for the domain name of the website and is in **Normal** mode. You can change the mode of the global mitigation policy based on your business requirements.

- If you require stronger traffic scrubbing capabilities to improve mitigation performance, we recommend that you use the **Strict** mode.

  > **Notice** To prevent negative impacts of mode adjustment on your business, we recommend that you submit a or contact customer service in the DingTalk group before you use the **Strict** mode.

- If you do not have high requirements for traffic scrubbing, we recommend that you use the **Low** mode. For example, you can use the Low mode during large-scale promotional events.

> **Notice** If you added a website to your instance before November 24, 2021, the global mitigation policy is disabled for the domain name of the website. We recommend that you enable the global mitigation policy for the domain name.

Procedure

1.
2.
3.
4. Click the **Protection for Website Services** tab. On the tab that appears, select a domain name from the list in the left side.

   The domain name list displays the domain names of the websites that are added to your instance. If the domain name list does not display the domain name of your website, add the website to your instance. For more information, see Add a website.

5. In the **Global Mitigation Policy** section, configure the parameters for the policy.

   You can configure the following parameters for the policy:

   - **Status**: You can turn on or off the switch to enable or disable the global mitigation policy. We recommend that you turn on the switch.
   - Mode: The **Low**, **Normal**, and **Strict** modes are supported. The following table describes the modes.

Mode	Effect	Scenario
Low	Blocks specific known attacks and allows normal requests.	This mode is suitable for large websites that have strong processing capabilities.
Normal (recommended)	Blocks attacks that are disclosed on the Internet but are not recorded in the historical traffic of your website. This mode has low impacts on business.	This mode is suitable for scenarios in which the number of requests does not greatly fluctuate and the business attributes and user sources are stable.

Mode	Effect	Scenario
Strict	Strictly blocks attacks. Normal requests may also be blocked.	This mode is suitable for websites that do not have sufficient processing capabilities.

7.3. Protection for non-website services

7.3.1. Configure intelligent protection

By default, the intelligent protection feature is enabled. This feature uses algorithms to learn historical traffic patterns of protected services and adjusts traffic scrubbing policies at Layer 4 to better safeguard the services. After your services are protected by Anti-DDoS Pro or Anti-DDoS Premium, intelligent protection of the normal level is enabled by default. If the normal-level protection cannot meet your requirements, you can set the level to Low or Strict as required.

Prerequisites

An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased. For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

Context

> Note

To protect your services against Layer 4 DDoS attacks, both Anti-DDoS Pro and Anti-DDoS Premium support the low, normal, and strict levels of intelligent protection. These levels are provided based on historical traffic patterns of services and technical experience of Alibaba Cloud security experts. By default, intelligent protection is enabled, and the protection level is set to Normal. You can change the level as required.

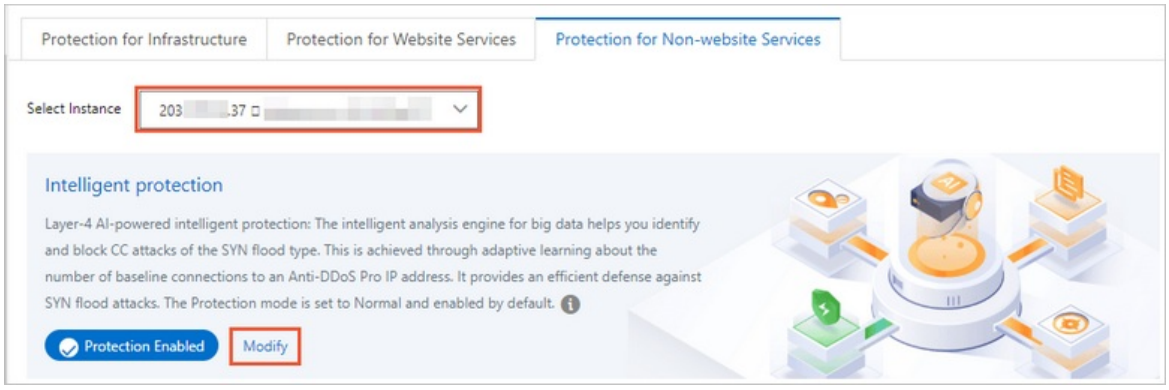
Intelligent protection works based on historical traffic patterns. If you use an Anti-DDoS Pro or Anti-DDoS Premium instance to protect your services for the first time, it takes about three days for Anti-DDoS Pro or Anti-DDoS Premium to learn the traffic patterns and provide optimal protection.

Intelligent protection algorithms automatically add malicious IP addresses to a blacklist and block all requests from these IP addresses within a specific time period. You can view, add, and remove IP addresses in the blacklist. You can also add IP addresses to a whitelist. This ensures that requests from these IP addresses are allowed. For more information, see Configure the IP address blacklist and whitelist for an Anti-DDoS Pro or Anti-DDoS Premium instance.

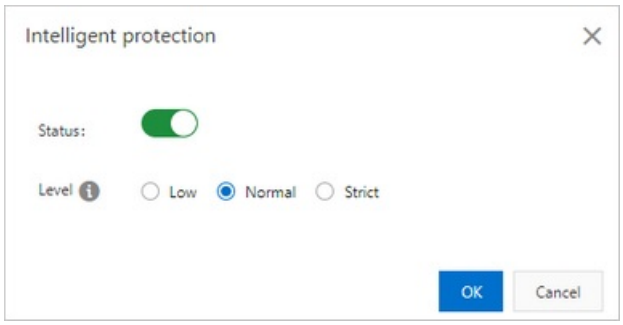
Procedure

1.
2.
3.
4. On the **General Policies** page, click the **Protection for Non-website Services** tab and select the target instance from the Select Instance drop-down list.

5. In the **Intelligent protection** section, click **Modify**.



6. In the **Intelligent protection** dialog box, set **Level** as required and then click **OK**.



Description of protection levels:

- **Low**: Intelligent protection automatically scrubs traffic from malicious IP addresses. It may not block all Layer 4 volumetric attacks but achieves a low false positive rate.
- **Normal**: Intelligent protection automatically scrubs traffic from malicious and suspicious IP addresses. This is the default level. Intelligent protection defends against DDoS attacks while maintains a low false positive rate at this level. We recommend that you use this level in common scenarios.
- **Strict**: Intelligent protection provides the strongest protection against DDoS attacks but may cause false positives.

After the protection level is changed, the Anti-DDoS Pro or Anti-DDoS Premium instance protects services based on the configured level.

7.3.2. Create an anti-DDoS protection policy

This topic describes how to create anti-DDoS protection policies. Both Anti-DDoS Pro and Anti-DDoS Premium allow you to create the following anti-DDoS protection policies to protect non-website services against Layer 4 DDoS attacks: False Source, Empty Connection, Speed Limit for Source, and Speed Limit for Destination. You can create an anti-DDoS protection policy for a specific port forwarding rule. This is applicable after you create port forwarding rules for an Anti-DDoS Pro or Anti-DDoS Premium instance and associate a non-website service with the instance. You can also create anti-DDoS protection policies for multiple port forwarding rules at a time.

Prerequisites

A port forwarding rule for a non-website service is configured on the Port Config page. For more information, see Create forwarding rules.

Context

Note

For non-website services, anti-DDoS protection policies are configured based on IP addresses and ports. To mitigate connection-oriented DDoS attacks, you can set the request rate, packet length, and other parameters as required. Anti-DDoS protection settings only apply to ports.

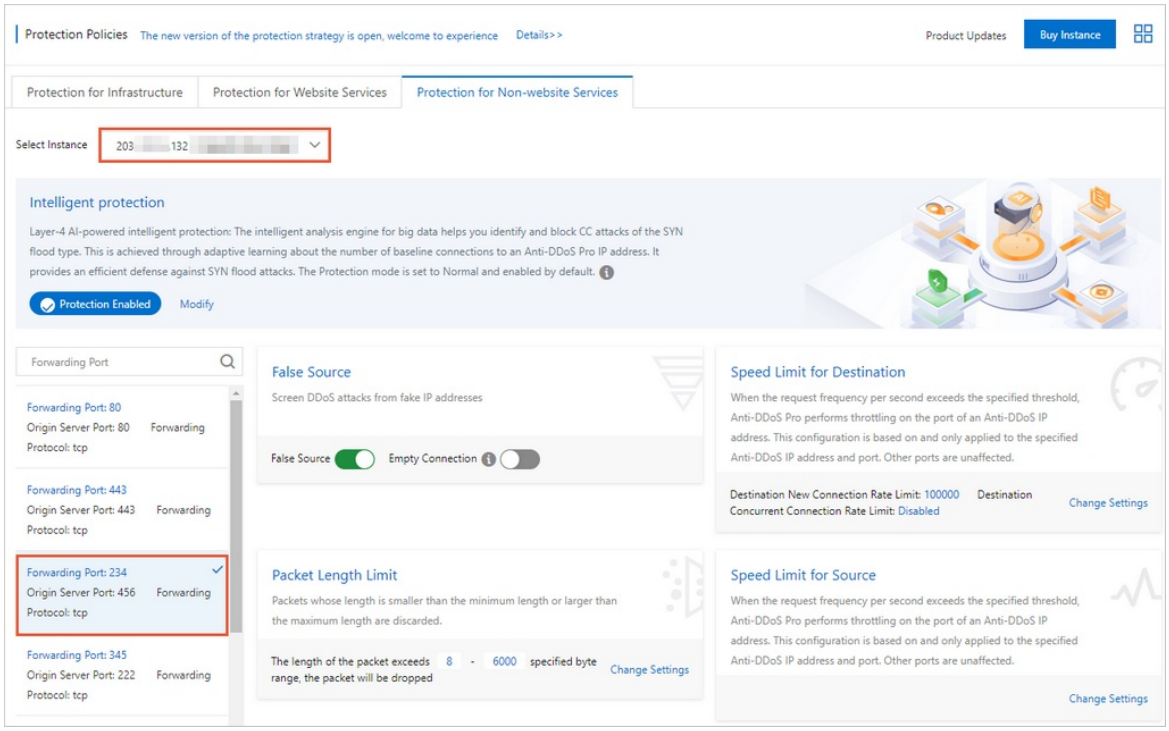
Both Anti-DDoS Pro and Anti-DDoS Premium allow you to create the following types of anti-DDoS protection policies for non-website services:

- False Source: verifies and filters DDoS attacks initiated from forged IP addresses.
- Speed Limit for Destination: The data transfer rate of the port that exceeds the maximum visit frequency is limited based on the IP address and port of your Anti-DDoS Pro or Anti-DDoS Premium instance. The data transfer rates of other ports are not limited.
- Packet Length Limit: specifies the minimum and maximum lengths of packets that are allowed to pass through. Packets with invalid lengths are dropped.
- Speed Limit for Source: The data transfer rate of a source IP address that exceeds the maximum visit frequency is limited based on the IP address and port of your Anti-DDoS Pro or Anti-DDoS Premium instance. The data transfer rates of other source IP addresses are not limited. This policy also supports the IP address blacklist policy. An IP address from which access requests exceed the maximum visit frequency five times within 60 seconds can be added to a blacklist. You can also specify the blocking period.

Create an anti-DDoS protection policy

The following procedure shows how to create an anti-DDoS protection policy for a specific port forwarding rule. You can also create anti-DDoS protection policies for multiple port forwarding rules at a time. For more information, see Create anti-DDoS protection policies for multiple port forwarding rules at a time.

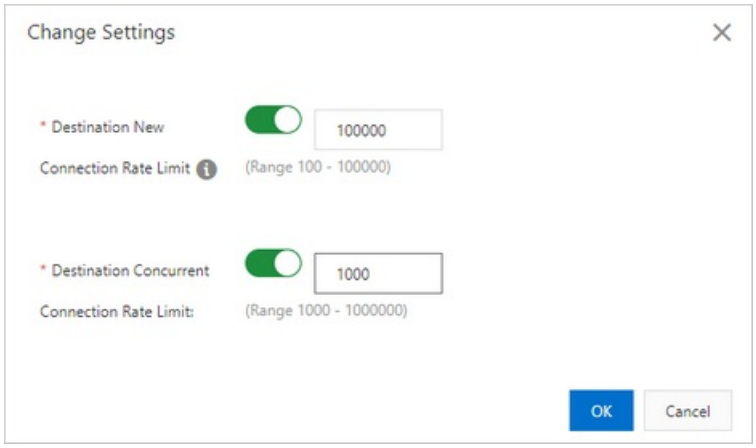
1.
2.
3.
4. On the **General Policies** page, click the **Protection for Non-website Services** tab. On the tab that appears, select the target instance from the Select Instance drop-down list.
5. Select the forwarding rule for which you want to create a policy from the list on the left side.



6. Configure settings in the **False Source**, **Speed Limit for Destination**, **Packet Length Limit**, and **Speed Limit for Source** sections.
   - **False Source**: In the **False Source** section, turn on or off **False Source** or **Empty Connection**.

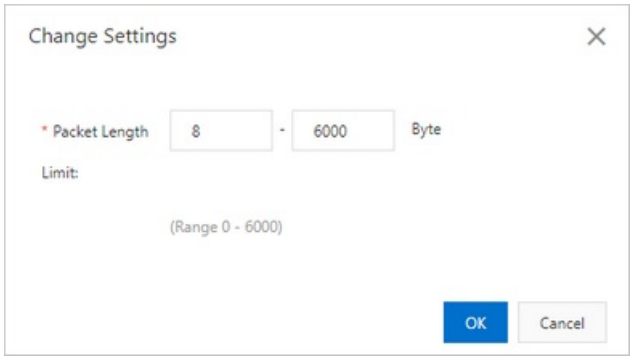
Parameter	Description
False Source	Turn on this switch to block requests from forged IP addresses. After you turn on the switch, Anti-DDoS Pro or Anti-DDoS Premium automatically filters requests initiated from forged IP addresses. **Note** This policy only applies to TCP rules.
Empty Connection	Turn on this switch to block requests that attempt to establish null sessions. After you turn on the switch, Anti-DDoS Pro or Anti-DDoS Premium automatically filters requests that attempt to establish null sessions. **Note** This policy only applies to TCP rules. To enable this policy, you must first enable the False Source policy.

   - **Speed Limit for Destination**: In the **Speed Limit for Destination** section, click **Change Settings**. In the **Change Settings** dialog box, specify the required parameters and then click **OK**.

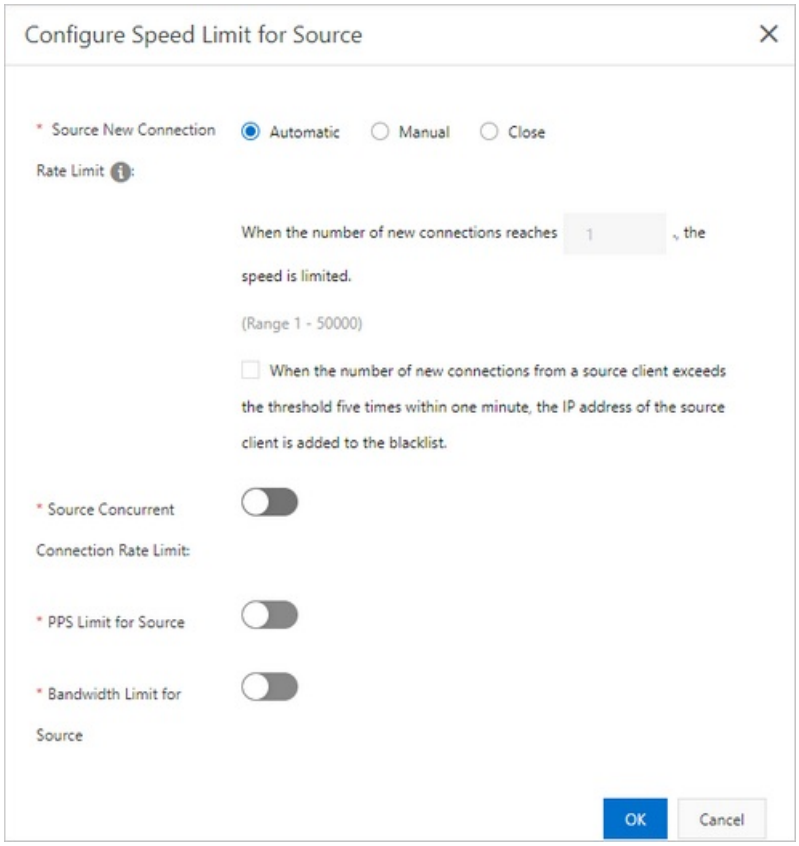


Parameter	Description
Destination New Connection Rate Limit	This parameter specifies the maximum number of new connections per second that can be established on an Anti-DDoS Pro or Anti-DDoS Premium port. The value ranges from 100 to 100000. Requests sent to the port after the upper limit is reached are dropped. **Note** The limit on new connections may be slightly different from actual scenarios because scrubbing nodes are deployed in clusters.
Destination Concurrent Connection Rate Limit	This parameter specifies the maximum number of concurrent connections that can be established on an Anti-DDoS Pro or Anti-DDoS Premium port. The value ranges from 1000 to 1000000. Requests sent to the port after the upper limit is reached are dropped.

- **Packet Length Limit**: In the **Packet Length Limit** section, click **Change Settings**. In the **Change Settings** dialog box, set the minimum and maximum lengths of the payload contained in a packet and then click **OK**. The value ranges from 0 to 6000. Unit: bytes.



- **Speed Limit for Source**: In the **Speed Limit for Source** section, click **Change Settings**. In the **Configure Speed Limit for Source** pane, specify the required parameters and then click **OK**.



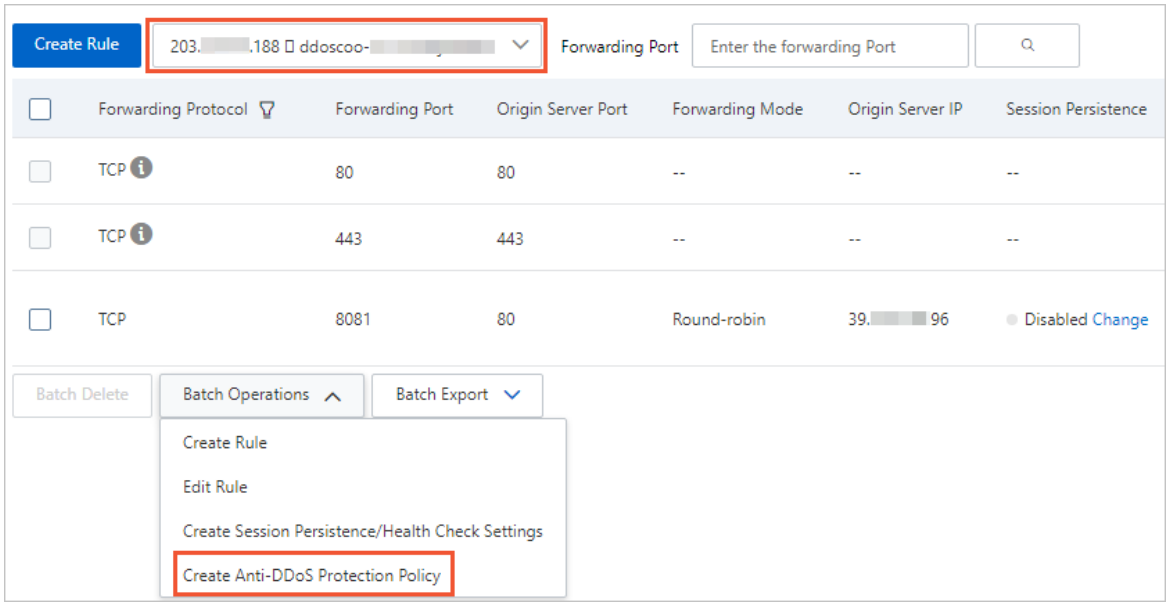
Parameter	Description

Parameter	Description
Source New Connection Rate Limit	This parameter specifies the maximum number of new connections per second that can be initiated from a single IP address. The value ranges from 1 to 50000. Requests initiated from the IP address after the upper limit is reached are dropped. This policy supports **Automatic** and **Manual** modes. ■ If you select Automatic, Anti-DDoS Pro or Anti-DDoS Premium dynamically calculates the maximum number of new connections per second that can be initiated from a single source IP address. ■ If you select Manual, you need to manually specify the maximum number of new connections per second that can be initiated from a single source IP address. **Note** The limit on new connections may be slightly different from actual scenarios because scrubbing nodes are deployed in clusters. Blacklist policy ■ If you select the **When the number of new connections from a source client exceeds the threshold five times within one minute, the IP address of the source client is added to the blacklist.** check box, all requests from IP addresses in the blacklist are dropped. ■ To enable the blacklist policy, you must set **Validity Period for Blacklist**. The value ranges from 1 to 10080. The default value is 30. Unit: minutes. An IP address added to a blacklist is removed from the blacklist when the validity period ends.
Source Concurrent Connection Rate Limit	This parameter specifies the maximum number of concurrent connections that can be initiated from a single IP address. The value ranges from 1 to 50000. Requests initiated from the IP address after the upper limit is reached are dropped. Blacklist policy ■ If you select the **When the number of concurrent connections from a source client exceeds the threshold five times within one minute, the IP address of the source client is added to the blacklist.** check box, all requests from IP addresses in the blacklist are dropped. ■ To enable the blacklist policy, you must set **Validity Period for Blacklist**. The value ranges from 1 to 10080. The default value is 30. Unit: minutes. An IP address added to a blacklist is removed from the blacklist when the validity period ends.

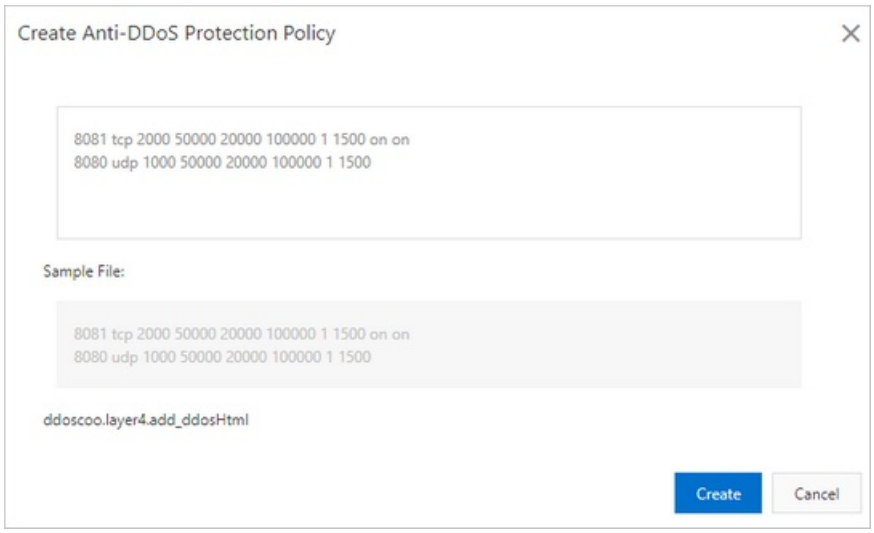
Parameter	Description
PPS Limit for Source	This parameter specifies the maximum number of packets per second that can be allowed from a single IP address. The value ranges from 1 to 100000. Unit: packet/s. Packets initiated from the IP address after the upper limit is reached are dropped. Blacklist policy ■ If you select the **When the source packets per second (PPS) of a source client exceeds the threshold five times within one minute, the IP address of the source client is added to the blacklist.** check box, all requests from IP addresses in the blacklist are dropped. ■ To enable the blacklist policy, you must set **Validity Period for Blacklist**. The value ranges from 1 to 10080. The default value is 30. Unit: minutes. An IP address added to a blacklist is removed from the blacklist when the validity period ends.
Bandwidth Limit for Source	This parameter specifies the maximum bandwidth of a single IP address. The value ranges from 1024 to 268435456. Unit: bytes/s. Blacklist policy ■ If you select the **When the source bandwidth of a source client exceeds the threshold five times within one minute, the IP address of the source client is added to the blacklist.** check box, all requests from IP addresses in the blacklist are dropped. ■ To enable the blacklist policy, you must set **Validity Period for Blacklist**. The value ranges from 1 to 10080. The default value is 30. Unit: minutes. An IP address added to a blacklist is removed from the blacklist when the validity period ends.

Create anti-DDoS protection policies for multiple port forwarding rules at a time

1.
2.
3.
4. On the **Port Config** page, select the target instance, click **Batch Operations** below the rule list, and select **Create Anti-DDoS Protection Policy**.



5. In the **Create Anti-DDoS Protection Policy** dialog box, follow the required formats to enter the content of anti-DDoS protection policies and then click **Create**.



The following section describes the formats of anti-DDoS protection policies.

> **Note** You can also export anti-DDoS protection policies to a TXT file, modify the content in the TXT file, and then copy and paste the modified content to the target fields. The formats of anti-DDoS protection policies in the exported file must be the same as those of the policies that you want to create. For more information, see Export multiple port configurations.

- Enter one policy in each row.
- Each anti-DDoS protection policy must contain the following fields from left to right: forwarding port, forwarding protocol, source new connection rate limit, source concurrent connection rate limit, destination new connection rate limit, destination concurrent connection rate limit, minimum packet length, maximum packet length, false source status, and empty connection status. The forwarding protocol can be TCP or UDP. For more information about the fields and valid values, see Parameters and descriptions of anti-DDoS protection policies. Fields are

separated with spaces.

- The forwarding port must be a port specified in a forwarding rule.
- The valid values of both False Source and Empty Connection are on and off. If any of these parameters is not set, the switch is turned off.

7.3.3. Configure the speed limit for source IP addresses

This topic describes how to configure and use the Speed Limit for Source policy. This policy allows you to set the maximum visit frequency and traffic volume from specific source IP addresses. If this policy is enabled, Anti-DDoS Pro or Anti-DDoS Premium adds IP addresses that exceed the maximum visit frequency or traffic volume to the blacklist or limits the data transfer rates from the IP addresses. After a source IP address is added to a blacklist, all requests from this IP address are dropped.

Prerequisites

A port forwarding rule for a non-website service is configured on the Port Config page. For more information, see Create forwarding rules.

Context

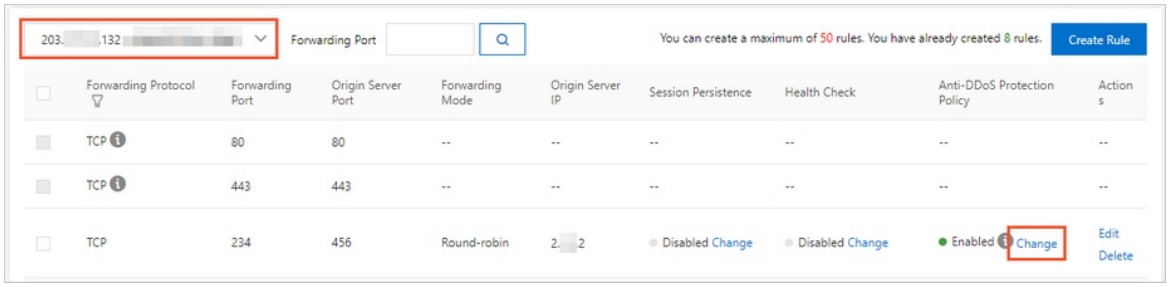
Both Anti-DDoS Pro and Anti-DDoS Premium allow you to set the maximum visit frequency from a source IP address to the port of your instance by limiting the numbers of new connections and concurrent connections. You can also limit the traffic volume to the port by limiting the bandwidth (bit/s) and packets per second (pps) of the source IP address. If an IP address exceeds the maximum visit frequency or traffic volume, Anti-DDoS Pro or Anti-DDoS Premium adds it to the blacklist or limits the data transfer rates. This policy can be used to block Layer 4 HTTP flood attacks that create a large number of connections. It can directly block the source IP addresses of attacks.

For example, assume that a source IP address accesses port 8000 of your instance, and the number of new connections is more than 10 times the normal level. You can set Source New Connection Rate Limit and enable the blacklist policy for port 8000. If the number of new connections from a source IP address repeatedly exceeds the limit, the IP address is added to the blacklist, and requests from this IP address are dropped.

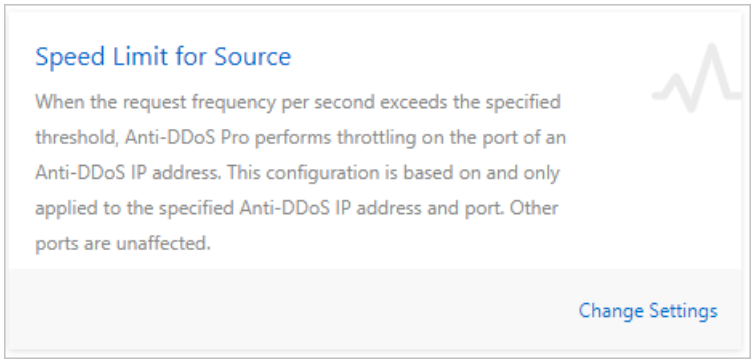
> **Note** The Speed Limit for Source policy takes effect on Anti-DDoS Pro or Anti-DDoS Premium ports. You must enable this policy for different Anti-DDoS Premium or Anti-DDoS Pro ports separately.

Procedure

1.
2.
3.
4. On the **Port Config** page, select the target instance.
5. Find the target forwarding rule and click **Change** in the **Anti-DDoS Protection Policy** column.

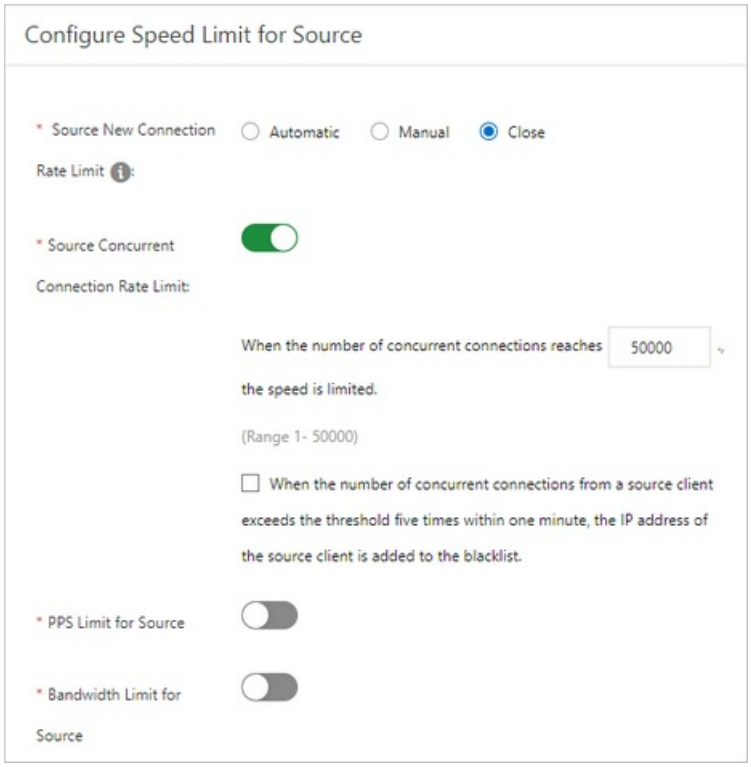


6. In the **Speed Limit for Source** section, click **Change Settings**.



7. In the **Configure Speed Limit for Source** pane, specify the required parameters.

   In this example, after the settings take effect, the number of concurrent connections from a source IP address cannot exceed 50,000 per second. It this threshold is reached, the data transfer rate of the IP address is limited. If you select the **When the number of concurrent connections from a source client exceeds the threshold five times within one minute, the IP address of the source client is added to the blacklist.** check box, your instance collects the number of times when the number of concurrent connections from a source IP address exceeds the threshold. If the number of times exceeds five, this IP address is added to the blacklist, and all requests from this IP address are dropped.



Source New Connection Rate Limit, PPS Limit for Source, and Bandwidth Limit for Source function the same way as Source Concurrent Connection Rate Limit. For more information, see Create an anti-DDoS protection policy.

8. Click **OK** to apply the settings.

7.4. Configure static page caching

Anti-DDoS Pro and Anti-DDoS Premium provide scrubbing centers that are integrated with web caching techniques to protect your website services against DDoS attacks and reduce page load time.

Prerequisites

Your website is added to an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the Enhanced function plan. For more information, see Add a website.

Context

After your website is added to an Anti-DDoS Pro or Anti-DDoS Premium instance, you can enable the static page caching feature for the website. After the feature is enabled, the Anti-DDoS Pro or Anti-DDoS Premium instance automatically detects whether the web pages that a client requests contain the resource types that are defined in the caching policy. If the web pages contain the resource types that are defined in the caching policy, the web pages are cached. The next time the client requests the same page, the Anti-DDoS Pro or Anti-DDoS Premium instance directly returns the pages. This accelerates client access.

You can customize caching rules for a specific page.

Procedure

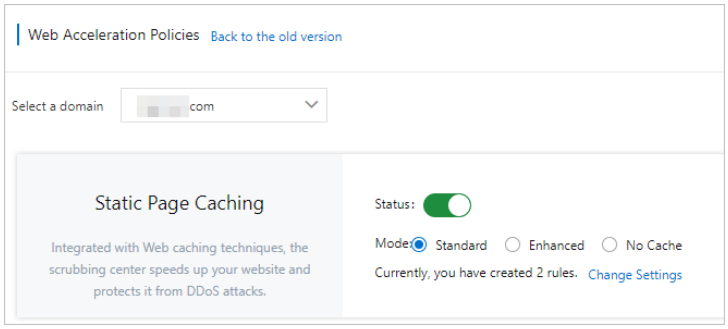
1.
2.
3.
4. In the upper part of the page that appears, select the required domain name.

   Notice You can enable the static page caching feature only for the domain names that are associated with an Anti-DDoS Pro or Anti-DDoS Premium instance that uses the Enhanced function plan.

5. In the **Static Page Caching** section, configure the **Mode** parameter and turn on **Status**.

   Valid values of the Mode parameter:

   - **Standard**: If the requested page contains static resources such as CSS, JavaScript, or TXT files, the page is cached.
   - **Enhanced**: All requested pages are cached.
   - **No Cache**: No requested pages are cached.

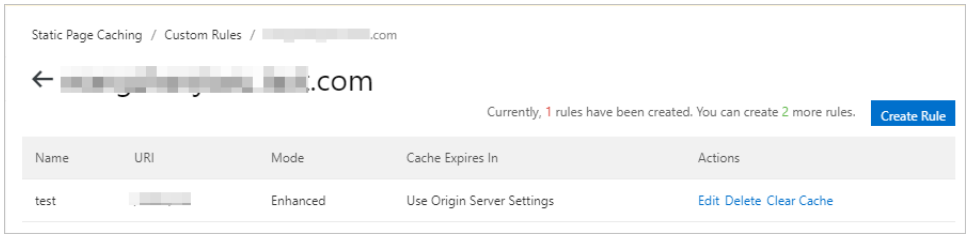


After you enable the static page caching feature for the domain name, the caching policy takes effect on all URIs in the domain name.

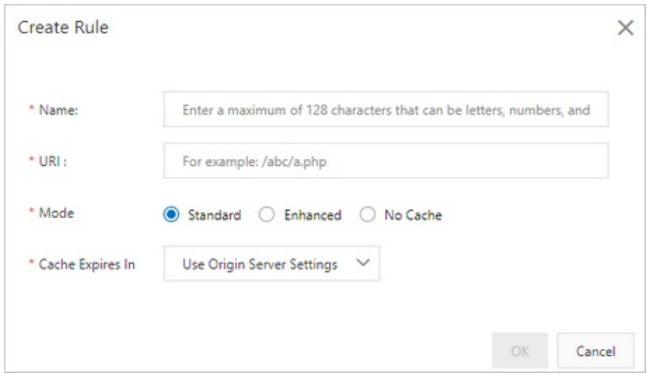
If you want to enable the static page caching feature for only a specific URI, we recommend that you set the **Mode** parameter to **No Cache** and perform the following steps to configure a custom caching rule.

6. (Optional)Configure a custom caching rule for a specific URI.
   i. In the **Static Page Caching** section, click **Change Settings**.
   ii. Click **Create Rule**.

> **Note** You can create a maximum of three custom caching rules.



iii. In the **Create Rule** dialog box, configure the parameters and click **OK**.



Parameter	Description
Name	The name of the caching rule. The name can contain letters, digits, and underscores (_). The name can be up to 128 characters in length.
URI	The URI of the page to be cached. Request parameters and wildcards are not allowed in the **URI** field. For example, `/a/` represents all pages in the path `<Domain name>/a/`.
Mode	The mode for the caching policy. Valid values: **Standard**, **Enhanced**, and **No Cache**. For more information about these values, see Step 5.
Cache Expires In	The validity period of the cached resources. Default value: **Use Origin Server Settings**. This value indicates that the validity period of the cached resources configured for the origin server is used. You can also select **1Hour(s)**, **1 Days**, **10 Days**, or **30 Days**.

After you create the custom caching rule for the specific URI, the custom caching rule preferentially takes effect over the caching policy of the domain name. You can view created rules and click **Modify** or **Delete** to manage the rules in the rule list. You can also click **Clear Cache** to manually refresh the cache of the page.

7.5. Create custom mitigation policies for specific scenarios

Both Anti-DDoS Pro and Anti-DDoS Premium allow you to create custom mitigation policies. A custom mitigation policy allows you to apply a scenario-specific template for high-traffic scenarios, such as new service launches and Double 11. You can create custom mitigation policies based on your business requirements.

Context

Scenario-specific templates are provided for you to create custom mitigation policies. When you create a custom mitigation policy, you must select a template and specify one or more assets for the policy. The assets include domain names and IP addresses that are added to Anti-DDoS Pro and Anti-DDoS Premium. A custom mitigation policy is valid only during a specified period of time. During the specified period, the custom mitigation policy takes effect instead of the standard mitigation policy.

Notice If no traffic surges happen, we recommend that you use standard mitigation policies instead of custom mitigation policies.

Supported templates

Only the **Important Activity** template is available. More templates will be provided in the future.

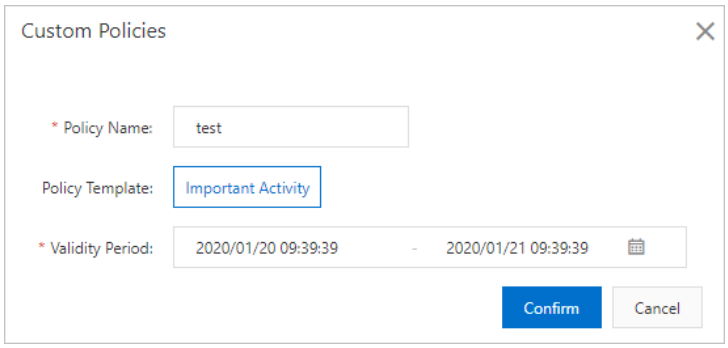
Example

If a large-scale event is held on a website, a large number of requests are sent to the website. As a result, the throughput of the website is much higher than usual. In this case, standard mitigation policies may report false positives. We recommend that you select the **Important Activity** template on the **Custom Policies** page. The Important Activity template automatically adjusts the standard mitigation policies during the specified period. Standard mitigation policies are adjusted based on the following rules:

- At the beginning of an activity, the Important Activity template saves the original configurations of the **Intelligent Protection** and **Frequency Control** features, and then automatically disables them to avoid false positives.
- At the end of the activity, the Important Activity template restores the configurations of these features.
- If you enable these features during the activity, the manual configuration takes effect.

Procedure

1.
2.
3.
4. Click **Custom Policies**.
5. In the **Custom Policies** dialog box, specify the parameters and then click **Confirm**.



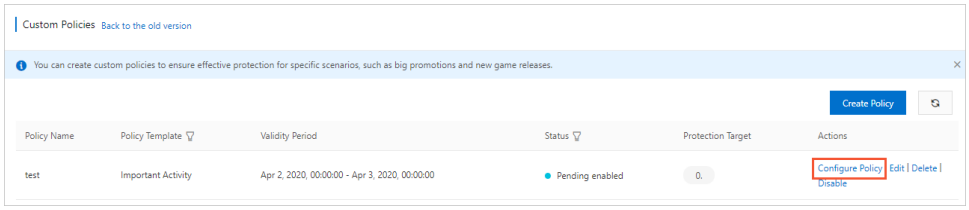
Parameter	Description
Policy Name	The name of the policy.

Parameter	Description
Policy Template	The template that you want to apply to the policy. Set the value to **Important Activity**.
Validity Period	The validity period of the policy. The policy takes effect during this period. **Note** If a template is applied to more than one policy, make sure that the values of **Validity Period** for these policies do not overlap with each other.

After a policy is created, the policy is automatically enabled. You can view the policy on the Custom Policies page and check **Status** of the policy to determine whether the policy is in effect. A policy may have the following states:

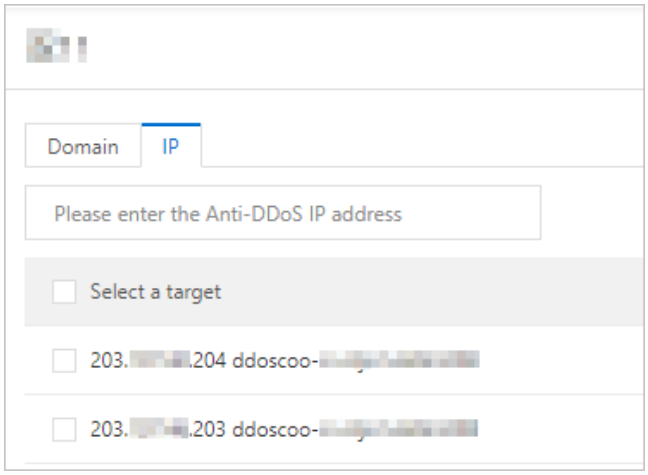
- **Pending Enabled**: indicates that the policy is still not in effect. The current time is earlier than the start time of the specified validity period.
- **Updating**: indicates that the policy is being issued. The process requires one or two minutes to complete.
- **Running**: indicates that the policy is in effect. The current time is within the specified validity period.
- **Expired**: indicates that the policy has expired. The current time is later than the specified validity period.
- **Disabled**: indicates that the policy is disabled. The policy does not take effect even if the current time is within the specified validity period.

6. In the list of custom mitigation policies, find the policy that you want to configure and click **Configure Policy** in the Actions column.



7. Select one or more domain names or IP addresses that are added to Anti-DDoS Pro or Anti-DDoS Premium for policy. Then, click **OK**.

Note If a website is added to Anti-DDoS Pro or Anti-DDoS Premium by using a domain name, we recommend that you enable the policy for the domain name. If a Layer 4 service is added to Anti-DDoS Pro or Anti-DDoS Premium by using an IP address, we recommend that you enable the policy for the IP address.



After the policy takes effect, information in the **Protection Target** column is automatically updated. You can move the pointer over the number in the Protection Target column to view the information.

8.Security Service

8.1. Security expert service

Anti-DDoS Pro and Anti-DDoS Premium provide free one-on-one expert service by using DingTalk groups. If you encounter any issues when you use Anti-DDoS Pro or Anti-DDoS Premium, you can click Meet Expert in the Anti-DDoS Pro or Anti-DDoS Premium console and obtain 24/7 support.

Prerequisites

- An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased. For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.
- DingTalk is installed on your mobile phone and a DingTalk account is created. For more information, visit the homepage of DingTalk.

Join a DingTalk group for Alibaba Cloud security services

1.
2. In the lower part of the left-side navigation pane, click Meet Expert.

> **Notice** **Meet Expert** is displayed in the Anti-DDoS Pro or Anti-DDoS Premium console only after an Anti-DDoS Pro or Anti-DDoS Premium instance is purchased.

3. Open the DingTalk app and scan the quick response (QR) code to join the DingTalk group for Anti-DDoS Pro or Anti-DDoS Premium.
   After you join the DingTalk group, you can ask any questions that you encounter when you use Anti-DDoS Pro or Anti-DDoS Premium. This way, you can enjoy one-on-one expert service from security experts.

8.2. Anti-DDoS Managed Service

Anti-DDoS Pro and Anti-DDoS Premium support Anti-DDoS Managed Service. After you purchase Anti-DDoS Managed Service, you can obtain technical support from Alibaba Cloud security experts to implement service configuration, implement security monitoring and inspection, and optimize mitigation policies. Anti-DDoS Managed Service also provides the following services: security incident response, security consultation, security training, case sharing, and security report analysis.

Overview

Anti-DDoS Managed Service is intended for Alibaba Cloud Anti-DDoS users and is delivered by the Alibaba Cloud security service team. Anti-DDoS Managed Service helps you effectively protect your web assets, lower security risks, and reduce O&M costs.

Anti-DDoS Managed Service is suitable for scenarios in which you have purchased Anti-DDoS Pro or Anti-DDoS Premium instances but cannot perform continuous service monitoring or do not have security engineers to defend against vulnerabilities. If you need to outsource security operations to professionals, you can purchase Anti-DDoS Managed Service.

> **Note** If you want to use some services of Anti-DDoS Managed Service, you must enable the Log Analysis feature of Anti-DDoS Pro or Anti-DDoS Premium. The services include mitigation policy optimization, monitoring and alerting configuration, and security report customization. If you do not enable the Log Analysis feature, these services may fail to be delivered. If you purchase Anti-DDoS Managed Service, we recommend that you enable the Log Analysis feature. For more information, see Overview.

Service scope

Anti-DDoS Managed Service provides end-to-end services covering provisioning and technical support. The following table describes the scope of Anti-DDoS Managed Service.

Service type	Description
Provisioning	• The security service team adds domain names to the Anti-DDoS Pro or Anti-DDoS Premium console for protection. • The security service team helps you configure and upload SSL certificates. You can also upload SSL certificates. • The security service team configures proper mitigation thresholds based on your business requirements. • The security service team helps you configure mitigation policies for Elastic Compute Service (ECS) instances and Server Load Balancer (SLB) instances. • The security service team verifies the forwarding configurations on your on-premises computer. • The security service team adjusts the relevant configurations when the protected domain names change.
Mitigation policy optimization	• The security service team diagnoses and troubleshoots exceptions in the services that are protected by Anti-DDoS Pro or Anti-DDoS Premium. • The security service team optimizes mitigation policies and configurations based on attack logs. • The security service team adjusts mitigation policies and provides solutions to mitigate the impact of security incidents. • The security service team provides suggestions on troubleshooting, HTTP flood protection, accurate access control, and data risk control.
Monitoring and alerting configuration	• The system automatically monitors the availability of Anti-DDoS Pro and Anti-DDoS Premium clusters. • The system automatically monitors high-risk events that are caused by DDoS attacks. • The security service team evaluates and filters alerts online.

Service type	Description
Security reports	• The security service team customizes security reports to meet your business requirements. • The security service team develops daily and monthly security reports. A daily security report provides operation data on the current day. A monthly security report provides operation data and data on attacks and defensive measures in the current month.

Response time for security incidents

After you purchase Anti-DDoS Managed Service, if you encounter a security incident, the security service team provides support within a specific period of time. The following table describes the response time for security incidents that have different priorities.

Response time for security incidents

No.	Priority	Definition	Response time
1	Critical	Your core business is severely damaged or completely unavailable.	15 minutes
2	Emergency	Your core business encounters single points of failure (SPOFs).	30 minutes
3	High	Your non-core business is severely damaged or unavailable.	2 hours
4	Medium	Your non-core business encounters SPOFs.	4 hours
5	Low	Daily technical consultation is required.	8 hours

Delivery of Anti-DDoS Managed Service

The following table describes the delivery of Anti-DDoS Managed Service.

Delivery of Anti-DDoS Managed Service

Category	Description
Delivery mode	Remote online service
Language	Chinese and English
Service period	Same as the validity period of Anti-DDoS Managed Service
Service channels	• Email • DingTalk • Phone call

Billing and purchasing

Anti-DDoS Managed Service supports the subscription billing method and can be renewed on a monthly or yearly basis. To purchase Anti-DDoS Managed Service, go to the Anti-DDoS Managed Service buy page.

> **Notice** Anti-DDoS Managed Service does not support refunds.

9.Best practices

9.1. Best practices to add a service to Anti-DDoS Pro or Anti-DDoS Premium

After you add a service to Anti-DDoS Pro or Anti-DDoS Premium, your service traffic is redirected to Anti-DDoS Pro or Anti-DDoS Premium to ensure stability and reliability of the origin server. This avoids service unavailability when volumetric DDoS attacks occur. This topic provides best practices to add a service to Anti-DDoS Pro or Anti-DDoS Premium and configure protection policies in various scenarios.

Scenarios to add a service to Anti-DDoS Pro or Anti-DDoS Premium

Scenario	Configuration process
Normal service configuration	1. Analyze the service 2. Prepare for the configuration 3. Add the service to Anti-DDoS Pro or Anti-DDoS Premium and configure protection policies
Emergency configuration when the service is under attack	Read Emergency scenarios to add a service and then add your service based on the process for normal service configuration.

Step 1: Analyze the service

Before you add a service to Anti-DDoS Pro or Anti-DDoS Premium, we recommend that you analyze the service status and data.

Item	Description	Suggestion
Website and service information		
Daily peak traffic of the website or application, such as bandwidth (Mbit/s) and QPS	Determine the point in time of risks.	This information is required to configure the service bandwidth and QPS of the Anti-DDoS Pro or Anti-DDoS Premium instance.
Major user groups, for example, the geographical locations of users	Determine attack sources.	This information is required to configure blocked regions. For more information, see Configure a location blacklist for a domain name.
Whether the service is deployed in the C/S architecture	If the C/S architecture is used, determine whether app clients, Windows clients, Linux clients, clients for other environments, or client callback is deployed.	None.

Item	Description	Suggestion
Whether the origin server is deployed in regions outside mainland China	Determine whether the Anti-DDoS Pro or Anti-DDoS Premium instance is suitable for your network architecture.	If the origin server is deployed outside mainland China, we recommend that you use Anti-DDoS Premium. For more information, see What are Anti-DDoS Pro and Anti-DDoS Premium?.
Operating system of the origin server (Linux or Windows) and web service middleware (such as Apache, NGINX, and IIS)	Determine whether access control policies are configured for the origin server. The policies may block traffic from the back-to-origin IP addresses of Anti-DDoS Pro or Anti-DDoS Premium.	If access control policies are configured, you must allow the back-to-origin IP addresses to access the origin server. For more information, see Allow back-to-origin IP addresses to access the origin server.
Whether the service needs to support IPv6	None.	If your service needs to support IPv6, we recommend that you use Anti-DDoS Origin. For more information, see What is Anti-DDoS Origin?.
Protocol used by the service	None.	This information is required to select a protocol for your website in Anti-DDoS Pro or Anti-DDoS Premium.
Service ports	None.	Determine whether service ports of the origin server are supported by Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Specify custom ports.
Whether the HTTP request header contains custom fields and whether the origin server provides a verification mechanism	Determine whether Anti-DDoS Pro or Anti-DDoS Premium affects the custom fields and causes verification failures on the origin server.	If yes, to obtain technical support.
Whether the origin server needs to obtain and verify the actual source IP addresses of requests	After you add the service to Anti-DDoS Pro or Anti-DDoS Premium, the actual source IP addresses of requests are changed. You must determine whether the origin server needs to obtain the actual source IP addresses to avoid service interruptions.	For more information, see Obtain the actual source IP addresses of requests.
Whether the service uses TLS 1.0 or a weak cipher suite	Determine whether the cipher suite of your service is supported.	After the service is added, you must configure TLS policies. For more information, see Customize a TLS policy.

Item	Description	Suggestion
(For HTTPS websites) Whether the origin server uses mutual authentication	None.	Anti-DDoS Pro and Anti-DDoS Premium do not support mutual authentication. You must change the authentication method.
(For HTTPS websites) Whether the clients support SNI	None.	After you add a domain name of an HTTPS website to Anti-DDoS Pro or Anti-DDoS Premium, both the clients and servers must support SNI.
(For HTTPS websites) Whether session persistence is enabled	The default connection timeout period for HTTP and HTTPS is 120 seconds.	If your service requires persistent sessions in scenarios such as file uploading and user logon, we recommend that you use cookies to implement session persistence at Layer 7.
Whether the service requires transmission of empty data packets	For example, the server sends empty packets to prevent session interruption. After you add the service to Anti-DDoS Pro or Anti-DDoS Premium, the service may be affected.	If yes, to obtain technical support.
Service interaction process	Determine the service interaction process and processing logic to configure suitable protection policies.	None.
Number of active users	Determine the severity of emergent attack events and take low-risk countermeasures.	None.
Service and attack information		
The type and characteristics of your service (for example, whether it is a gaming, website, or app service)	Analyze attack characteristics to take countermeasures.	None.
The volume of inbound service traffic	Determine whether there is malicious traffic. For example, the average volume of daily access traffic is 100 Mbit/s. If the traffic volume exceeds 100 Mbit/s, an attack may have occurred.	None.
The volume of outbound service traffic	Determine whether attacks occur and whether to increase service bandwidth.	None.

Item	Description	Suggestion
The volume and connections of inbound traffic for individual users or IP addresses	Determine whether throttling policies can be configured for individual IP addresses.	For more information, see Configure frequency control.
User sources	For example, users may visit your service from household LANs, Internet cafes, and proxy servers.	This information is required to determine whether concurrent requests are sent from a single egress IP address and prevent Anti-DDoS Pro or Anti-DDoS Premium from blocking normal service traffic.
Whether the service has suffered volumetric attacks and the types of the attacks	Configure targeted DDoS protection policies based on the types of historical attacks.	None.
The largest traffic volume of attacks suffered by the service	Select the specifications of the Anti-DDoS Pro or Anti-DDoS Premium instance based on the peak attack traffic.	For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.
Whether the service has suffered HTTP flood attacks	Configure preventive policies based on characteristics of historical attacks.	None.
The largest QPS of HTTP flood attacks suffered by the service	Configure preventive policies based on characteristics of historical attacks.	None.
Whether the service provides web APIs	None.	If web APIs are provided, we recommend that you do not use the frequency control feature of Anti-DDoS Pro or Anti-DDoS Premium. You can analyze API access characteristics and configure protection policies against HTTP flood attacks. This prevents normal API requests from being blocked.
Whether a stress test is performed for the service	Evaluate the request processing performance of the origin server and determine whether service exceptions are caused by attacks.	None.

Step 2: Prepare for the configuration

Notice We recommend that you add a service to Anti-DDoS Pro or Anti-DDoS Premium in a test environment first. After you verify that the service properly runs, perform the configuration in the production environment.

Before you add a service to Anti-DDoS Pro or Anti-DDoS Premium, make the following preparations.

Service type	Preparation
Website service	• Prepare information of the website that you want to add, including the domain names, public IP address of the origin server, and service ports. • Compete ICP filing for the domain names. • If the website supports HTTPS, prepare the certificate and private key, including a public key file in the .crt format or certificate file in the .pem format and a private key in the .key format. • Obtain an administrator account of the DNS service. This account is used to modify DNS records to redirect traffic to Anti-DDoS Pro or Anti-DDoS Premium. • Perform a stress test before you add the website to Anti-DDoS Pro or Anti-DDoS Premium. • List trusted clients of the website, such as the monitoring system, APIs that are called by using a fixed IP address or CIDR block, and specific client programs. After you add the website to Anti-DDoS Pro or Anti-DDoS Premium, you must add the IP addresses of these clients to a whitelist.
Non-website service	• Obtain the service port and protocol. • If the service is provided by using a domain name, obtain an administrator account that can change DNS records to redirect service traffic to Anti-DDoS Pro or Anti-DDoS Premium. • Perform a stress test before you add the service to Anti-DDoS Pro or Anti-DDoS Premium.

Step 3: Add the service to Anti-DDoS Pro or Anti-DDoS Premium and configure protection policies

1. Add the service to Anti-DDoS Pro or Anti-DDoS Premium.

   > **Note** If the service is already under attack before you add it to Anti-DDoS Pro or Anti-DDoS Premium, we recommend that you change the IP address of the origin server. Before you change the IP address, check whether the code of the client or app contains the IP address. If yes, update the code before you change the IP address to avoid impacts on normal service access. For more information, see Change the public IP address of an ECS origin server.

   Add the service based on the Anti-DDoS Pro or Anti-DDoS Premium instance and your service scenario:

   - Add a website service to Anti-DDoS Pro or Anti-DDoS Premium
   - Add a non-website service to Anti-DDoS Pro or Anti-DDoS Premium
   - Add a website service to Anti-DDoS Pro or Anti-DDoS Premium by using NS records

2. Configure protection for the origin server.

   To prevent attackers from bypassing Anti-DDoS Pro or Anti-DDoS Premium to attack the origin server, configure protection for the origin server. For more information, see Configure protection for an origin server.

3. Configure protection policies.
   - Website service provided by using domain names
     - HTTP flood protection
       - The service is running properly: Two or three days after you add the service to Anti-DDoS Pro or Anti-DDoS Premium, analyze service application logs, including information about URLs and the average QPS of individual source IP addresses. Based on the analysis, configure frequency control rules. This provides protection against attacks.
       - The service is suffering from an HTTP flood attack: Go to the **Security Overview** page in the Anti-DDoS Pro or Anti-DDoS Premium console to obtain information about your domain name, such as the most requested URLs and IP addresses, source IP addresses, and user agents. Based on the obtained information, configure frequency control rules and observe the protection effect. For more information, see Check the security overview and Create a custom frequency control rule.

         > **Notice** The **Emergency** mode of **Frequency Control** may block normal traffic of specific service types. We recommend that you do not set **Emergency** as the default mode of **Frequency Control**. If you provide the app or web API service, do not use the **Emergency** mode.
         >
         > If you use the **Normal** mode of **Frequency Control** but normal service traffic is still blocked, add the service IP addresses to a whitelist.

     - Intelligent protection for a website service

       The **Strict** mode of intelligent protection may block normal service traffic. After you add the domain name of your website to Anti-DDoS Pro or Anti-DDoS Premium, you do not need to be concerned about Layer-4 DDoS attacks. Therefore, we recommend that you use the **Normal** mode instead of the **Strict** mode. For more information, see Use the intelligent protection feature.

     - Log analysis

       We recommend that you enable the log analysis feature. For more information, see Quick start. If the service encounters Layer-7 DDoS attacks, you can use the log analysis feature to analyze attack characteristics and configure targeted protection policies.

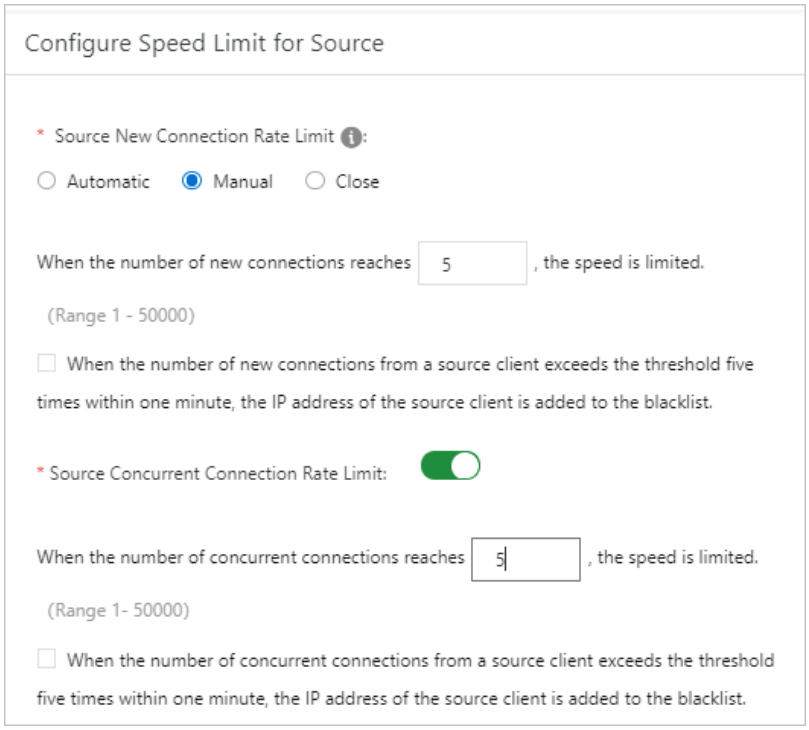
       > **Note** Enabling the log analysis feature incurs additional fees.

   - **Non-website service provided by using ports**

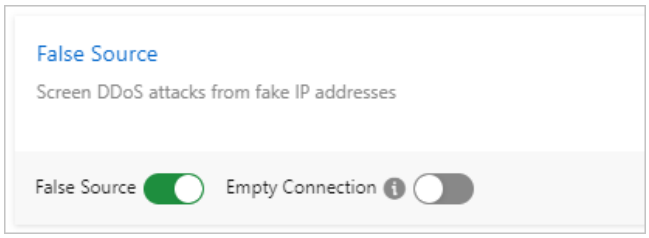
     In most cases, you can add a non-website service to Anti-DDoS Pro or Anti-DDoS Premium and use the default protection settings. After the service runs for two or three days, you can adjust the mode of Layer-4 intelligent protection based on the service characteristics. This optimizes protection against Layer-4 HTTP flood attacks. For more information, see Configure intelligent protection.

> **Note** If the service provides frequently called APIs or is visited from a single IP address, such as an egress IP address of an enterprise network or a server IP address, do not enable the **Strict** mode of Intelligent Protection. If you have to use the **Strict** mode, contact Alibaba Cloud technical support to analyze the service before you enable this mode to avoid service interruptions.

If attack traffic is transparently transmitted to the origin server, you can enable Speed Limit for Source and Speed Limit for Destination. For more information, see Create an anti-DDoS protection policy. At the beginning, we recommend that you set both Source New Connection Rate Limit and Source Concurrent Connection Rate Limit to 5. If normal service traffic is blocked, you can increase the limit values.



If the origin server of your service sends empty data packets, you must disable Empty Connection to avoid impacts on normal traffic. For more information, see Create an anti-DDoS protection policy.



4. Test the service.

   After you complete the configuration, test the accuracy of the configurations.

   > **Note** You can modify the *hosts* file on a local computer to perform the test.

   Check items of configuration accuracy

No.	Check item
Website service provided by using a domain name (required)	
1	Check whether the added domain name is correct.
2	Check whether the domain name has an ICP license.
3	Check whether the configured protocol is correct.
4	Check whether the configured port is correct.
5	Check whether the IP address of the origin server is correct. Make sure that you do not enter the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance or another service.
6	Check whether the uploaded certificate is correct.
7	Check whether the certificate is valid. For example, the encryption algorithm may be invalid or you have uploaded the certificate of another domain name.
8	Check whether the certificate chain is complete.
9	Make sure that you know the billing method of burstable protection in Anti-DDoS Pro or Anti-DDoS Premium.
10	Check whether WebSocket and WebSockets are enabled.
11	Check whether the Emergency mode of Frequency Control is enabled.
Non-website service provided by using a port (required)	
1	Check whether the service port can be accessed.
2	Check whether the UDP or TCP protocol is incorrectly configured.
3	Check whether the IP address of the origin server is correct. Make sure that you do not enter the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance or another service.
4	Make sure that you know the billing method of burstable protection in Anti-DDoS Pro or Anti-DDoS Premium.
5	Check whether the Strict mode of intelligent protection is enabled.

Check items of service availability

No.	Check item
1 (required)	Test whether the service can be normally accessed.
2 (required)	Test whether the session persistence function for user logon properly works.

No.	Check item
3 (required)	(For website services provided by using domain names) Check the number of 4XX and 5XX status codes in returned responses and make sure that the back-to-origin IP addresses are not blocked.
4 (required)	(For website services provided by using domain names) If you provide the app service, test whether HTTPS links are normal. Check whether SNI is properly configured.
5 (recommended)	Check whether the origin server is configured to obtain the actual source IP addresses of requests.
6 (recommended)	(For website services provided by using domain names) Check whether protection policies are configured for the origin server. This prevents attackers from bypassing Anti-DDoS Pro or Anti-DDoS Premium to attack the origin server.
7 (required)	Test whether the TCP service port is accessible.

5. Switch service traffic to Anti-DDoS Pro or Anti-DDoS Premium.

   After you verify all check items, we recommend that you change the DNS records one by one to gradually switch the service traffic to Anti-DDoS Pro or Anti-DDoS Premium. This prevents potential service exceptions in a large scale. If an exception occurs after you switch the traffic, restore the DNS records.

   > **Note** Changes to DNS records take effect in about 10 minutes.

   After you switch the service traffic, verify the check items of service availability again to make sure that the service properly runs.

6. Configure monitoring and alerts.

   Use Cloud Monitor to monitor availability and returned HTTP status codes (5XX and 4XX) for the domain names, forwarding ports, and origin server ports protected by Anti-DDoS Pro or Anti-DDoS Premium. This allows you to detect service exceptions in time. For more information, see Configure an alert rule for Anti-DDoS Pro or Anti-DDoS Premium.

7. Perform routine O&M.

   - **Use burstable protection of Anti-DDoS Pro and advanced mitigation in the Insurance plan of Anti-DDoS Premium.**
     - If you purchase an Anti-DDoS Pro instance for the first time, you can obtain three global advanced mitigation plans of 300 Gbit/s free of charge. For more information, see Apply for and use Anti-DDoS plans. Bind the plans to the Anti-DDoS Pro instance and set the burstable protection threshold to 300 Gbit/s. Anti-DDoS Pro then protects your service against attacks whose traffic volume does not exceed 300 Gbit/s and does not incur burstable protection fees within the day after you bind the plans.

       > **Note** If you do not want to enable burstable protection after the global advanced mitigation plans are used up or expire, change the protection threshold to the basic protection bandwidth of your Anti-DDoS Pro instance.

- If you want to enable burstable protection of Anti-DDoS Pro, view the billing methods to determine the costs. For more information, see Burstable protection: pay-as-you-go (billed daily).
- If you purchase an Anti-DDoS Premium instance with the Insurance mitigation plan, you can obtain two advanced mitigation plans (unlimited protection) each month free of charge. Select the mitigation plan based on your service needs.

- **Determine attack types.**

  If HTTP flood attacks and DDoS attacks occur, you can view attack information on the **Security Overview** page in the Anti-DDoS Pro or Anti-DDoS Premium console to determine the types of attacks. For more information, see Check the security overview.

  - DDoS attack: On the **Instances** tab, the protection reports show attack traffic fluctuations, and traffic scrubbing is triggered. However, on the **Domains** tab, the protection reports do not show fluctuations.
  - HTTP flood attack: On the **Instances** tab, the protection reports show attack traffic fluctuations, and traffic scrubbing is triggered. On the **Domains** tab, the protection reports also show fluctuations.

  For more information, see How do I identify the types of attacks against an Anti-DDoS Pro or Anti-DDoS Premium instance?.

- **Deal with service access latency and packet loss.**

  If the origin server is deployed outside mainland China and users of your service come from mainland China, the users may experience large latency and packet loss due to unstable links of cross-carrier network access. We recommend that you purchase an Anti-DDoS Premium instance and use the MCA mitigation plan.

- **Delete a domain name or port forwarding rule.**

  If you want to delete a domain name or port forwarding rule, check whether your service traffic is switched to Anti-DDoS Pro or Anti-DDoS Premium.

  - If no, delete the domain name or port forwarding rule in the Anti-DDoS Pro or Anti-DDoS Premium console.
  - If yes, go to the Alibaba Cloud DNS console to modify the DNS records to switch the traffic back to the origin server. Then, delete the domain name or port forwarding rule.

  > **Note**
  > - Before you delete the domain name or port forwarding rule, make sure that the DNS records or service traffic of the domain name is switched back to the origin server.
  > - After you delete the domain name or port forwarding rule, Anti-DDoS Pro or Anti-DDoS Premium no longer protects your service.

Emergency scenarios to add a service

If the service is already under attack, add it to Anti-DDoS Pro or Anti-DDoS Premium based on the following scenarios:

- The service suffers a DDoS attack.

In most cases, you can add the service to Anti-DDoS Pro or Anti-DDoS Premium and use the default protection settings.

If traffic of a Layer-4 HTTP flood attack is transparently transmitted to the origin server, you can enable Speed Limit for Source and Speed Limit for Destination. For more information, see Create an anti-DDoS protection policy.

- Blackhole filtering is triggered for the IP address of the origin server.

  You can use an ECS or SLB instance as the origin server. If you have not added the attacked service to Anti-DDoS Pro or Anti-DDoS Premium but blackhole filtering is triggered, you must change the public IP address of the origin server. For more information, see Change the public IP address of an ECS origin server. After you change the IP address, add the service to Anti-DDoS Pro or Anti-DDoS Premium as soon as possible to prevent the new IP address from being exposed.

  If you do not want to change the IP address of the origin server or the new IP address is already exposed, we recommend that you deploy an SLB instance as the origin server to connect the ECS instance and add the public IP address of the SLB instance to Anti-DDoS Pro or Anti-DDoS Premium.

  > **Note** If the service is under attack but the origin server is not deployed on Alibaba Cloud, make sure that the domain name of the service has an ICP license and contact technical support to add Alibaba Cloud as your service provider. Then, add the service to Anti-DDoS Pro or Anti-DDoS Premium.

- The service suffers an HTTP flood attack or crawler attack.

  If the service is under an HTTP flood or crawler attack, add the service to Anti-DDoS Pro or Anti-DDoS Premium. Then, analyze HTTP access logs to identify attack characteristics and configure protection policies. For example, you can check whether request fields, such as the source IP address, URL, Referer, User-Agent, Params, and Header are correct.

9.2. Add a website to both Anti-DDoS Pro or Anti-DDoS Premium and WAF

Anti-DDoS Pro or Anti-DDoS Premium and Web Application Firewall (WAF) can be used together to protect websites against both DDoS attacks and web application attacks. This topic describes how to add a website to both Anti-DDoS Pro or Anti-DDoS Premium and WAF.

Prerequisites

- An Anti-DDoS Pro or Anti-DDoS Premium instance is purchased. For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.
- A WAF instance is purchased. For more information, see Purchase a WAF instance.

Context

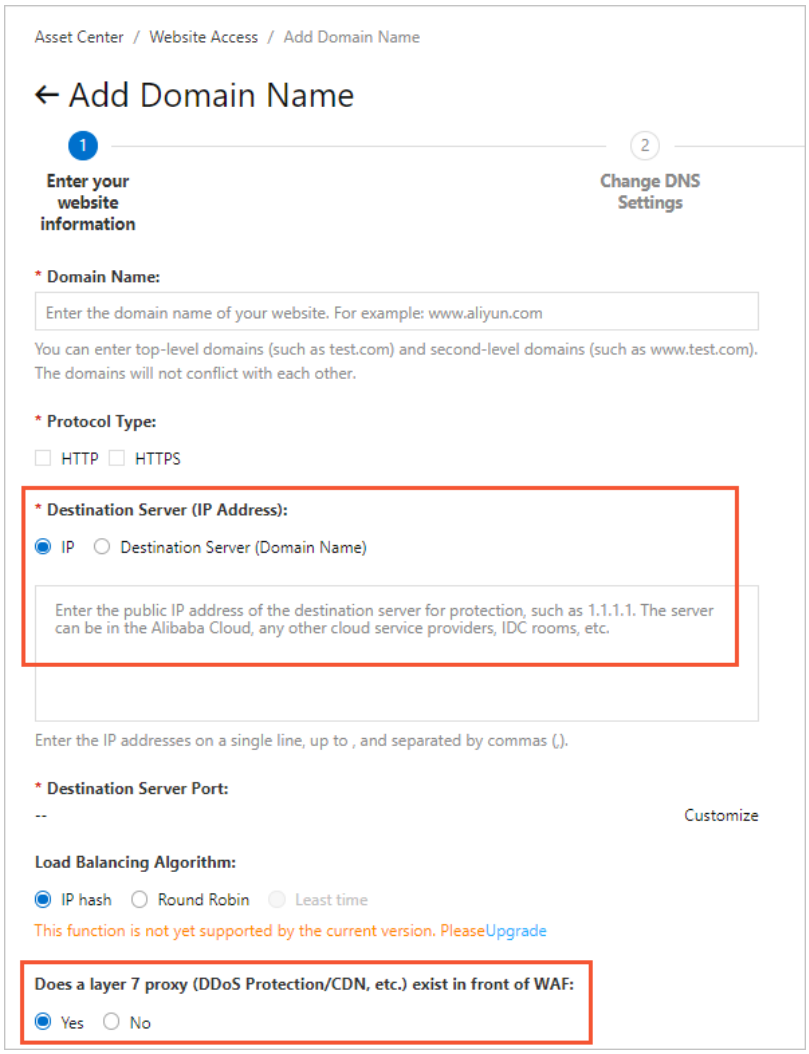
To configure Anti-DDoS Pro or Anti-DDoS Premium and WAF for your website, you can deploy the following network architecture: Use Anti-DDoS Pro or Anti-DDoS Premium at the ingress to defend against DDoS attacks. Use WAF at the intermediate layer to defend against web application attacks. Configure an ECS instance, SLB instance, or on-premises server as the origin server.

Note After you apply the preceding architecture, access requests are sent to multiple intermediate proxy servers before reaching the origin server. The origin server cannot directly obtain the actual source IP addresses of the requests. For more information about how to obtain the actual source IP addresses, see Obtain the actual source IP addresses of requests.

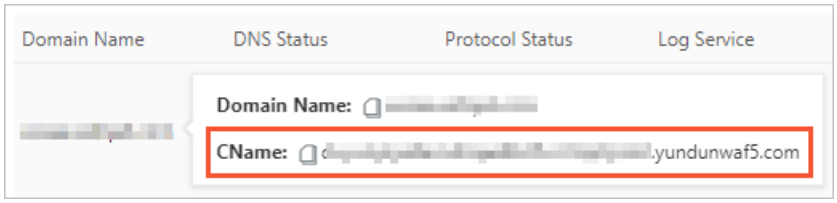
Procedure

1. Add the domain name of your website to WAF. For more information, see Add a domain name.

   In the **Enter your website information** step, set **Destination Server (IP Address)** to **IP** and enter the public IP address of the origin server. The origin server can be an SLB instance, ECS instance, or on-premises server. Set **Does a layer 7 proxy (DDoS Protection/CDN, etc.) exist in front of WAF** to **Yes**.

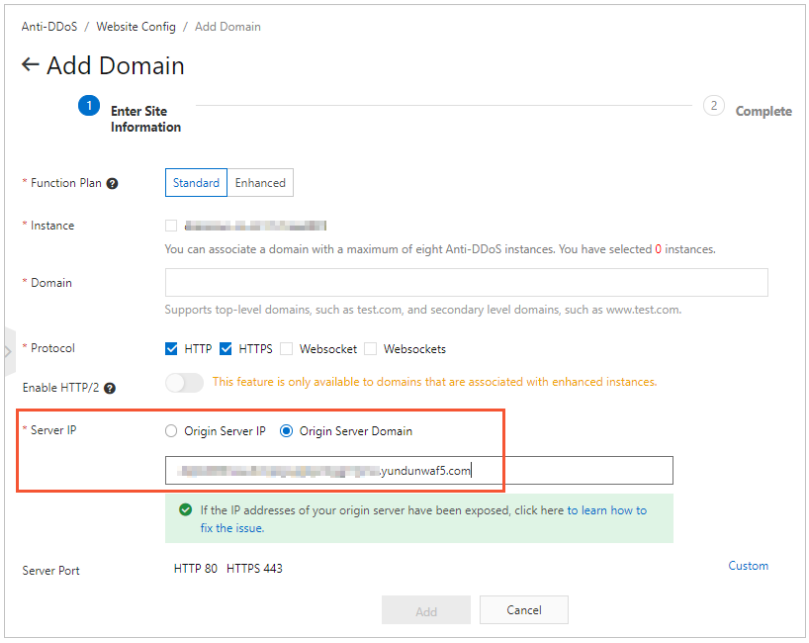


   After you add the domain name to WAF, go to the **Website Access** page in the WAF console to obtain the **CNAME** address of WAF.

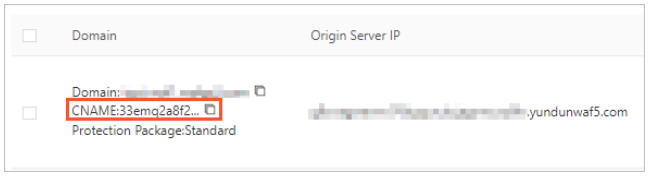


2. Add your website service to Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Add a website.

   In the **Enter Site Information** step, set **Server IP** to **Origin Server Domain** and enter the **CNAME** address of WAF obtained in the previous step.



   After you add the domain name to Anti-DDoS Pro or Anti-DDoS Premium, go to the **Website Config** page in the Anti-DDoS Pro or Anti-DDoS Premium console to obtain the **CNAME** address of Anti-DDoS Pro or Anti-DDoS Premium.



3. On the website of your DNS service provider, modify DNS records to point the domain name to the **CNAME** address of Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Change DNS records to protect website services.
   After the preceding configuration is complete, traffic to access your website is first scrubbed by Anti-DDoS Pro or Anti-DDoS Premium and then forwarded to WAF to filter out web application attacks. Only normal traffic is forwarded to the origin server.

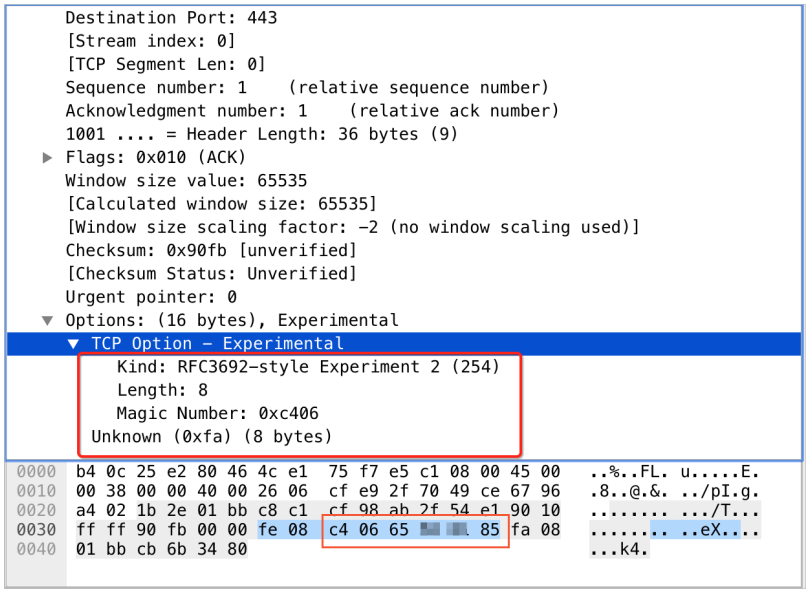
9.3. Obtain the actual source IP addresses of requests

After you add a service to Anti-DDoS Pro or Anti-DDoS Premium, Anti-DDoS Pro or Anti-DDoS Premium scrubs the traffic destined for the service and then forwards the traffic to the origin server. The source IP addresses of the requests are changed to the IP address of the Anti-DDoS Pro or Anti-DDoS Premium instance. This topic describes how to obtain the actual source IP addresses of requests.

Non-website service provided by using a port

> **Notice**
>
> - If your origin server is an Elastic Compute Service (ECS) instance that was created after October 2018, the source IP addresses that you obtain on the origin server are the actual source IP addresses of requests.
> - If your origin server is an ECS instance that was created before October 2018, you cannot directly obtain the actual source IP addresses of requests. You need to submit a to contact technical support.

For example, after you add a non-website service at Layer 4 to Anti-DDoS Pro or Anti-DDoS Premium, Anti-DDoS Pro or Anti-DDoS Premium connects to the origin server by using a three-way handshake process. Anti-DDoS Pro or Anti-DDoS Premium sends the last ACK packet that contains the information, such as the source port number and IP address, in the TCP Option field. The size of the information is 6 bytes. The following figure shows the information in the ACK packet.



The value of `Magic Number` indicates the source port number, which is a hexadecimal string. In this example, the source port number is `c4 06`. You can also obtain the source IP address, which is indicated by the next 4 bytes following the source port number. In this example, the source IP address is `65 ** ** 85`. Then, you can convert c4 06 and 65 ** ** 85 to decimal values to obtain the actual source port number and IP address. In this example, the actual source port number is 50182 and the actual source IP address is 101.***.***.133.

The methods that are used to obtain the actual source IP addresses of requests vary based on the network architecture of your services. For more information, see the following table.

Network architecture	Description

Network architecture	Description
Anti-DDoS Pro or Anti-DDoS Premium+ECS instance	• If service requests are forwarded by using a TCP port, the origin server can obtain the actual source IP addresses. You do not need to perform additional operations. You can configure security group rules for the ECS instance based on the source IP addresses of requests and the back-to-origin IP addresses of your Anti-DDoS Pro or Anti-DDoS Premium instance. For example, you can allow or deny inbound traffic from a specific IP address. • If service requests are forwarded by using a UDP port, the origin server cannot obtain the actual source IP addresses.
Anti-DDoS Pro or Anti-DDoS Premium+Server Load Balancer (SLB) instance+ECS instance	• If service requests are forwarded by using a TCP port, the origin server can obtain the actual source IP addresses. You do not need to perform additional operations. **Note** You must add the back-to-origin IP addresses of your Anti-DDoS Pro or Anti-DDoS Premium instance to the whitelist of the SLB instance. For more information, see Allow back-to-origin IP addresses to access the origin server and Enable access control. • If service requests are forwarded by using a UDP port, the origin server cannot obtain the actual source IP addresses. **Note** If the private IP address of the ECS instance is modified or the ownership of the ECS instance is transferred to you by another user, the origin server cannot obtain the actual source IP addresses. In this case, submit a to contact technical support.
Anti-DDoS Pro or Anti-DDoS Premium+Server that is not deployed on Alibaba Cloud	In some cases, the origin server can obtain the actual source IP addresses. For more information, see Obtain the actual source IP addresses of requests to an origin server that is not deployed on Alibaba Cloud.

Website service provided by using a domain name

By default, if service requests are forwarded to the origin server by a Layer 7 proxy server, such as an Anti-DDoS Pro or Anti-DDoS Premium instance, the source IP addresses obtained by the origin server are the back-to-origin IP addresses of the proxy server. The actual source IP addresses are recorded in the `X-Forwarded-For` field. The format is `X-Forwarded-For:Actual source IP address,Back-to-origin IP addresses of the Anti-DDoS Pro or Anti-DDoS Premium instance`.

If the requests pass through more than one proxy server, such as Web Application Firewall (WAF) and Alibaba Cloud CDN (CDN) instances, the `X-Forwarded-For` field in the HTTP request header records the actual source IP addresses and the IP addresses of all proxy servers. The format is `X-Forwarded-For:Actual source IP address,IP address of Proxy Server 1,IP address of Proxy Server 2,IP address of Proxy Server 3,...`

A common web application server can use the `X-Forwarded-For` field to obtain the actual source IP addresses of requests.

You can use the following methods to obtain the `X-Forwarded-For` field in different programming languages:

- ASP

```
Request.ServerVariables("HTTP_X_FORWARDED_FOR")
```

- ASP.NET (C#)

```
Request.ServerVariables["HTTP_X_FORWARDED_FOR"]
```

- PHP

```
`$_SERVER["HTTP_X_FORWARDED_FOR"]
```

- JSP

```
request.getHeader("HTTP_X_FORWARDED_FOR")
```

In the `X-Forwarded-For` field, the IP address before the first comma (,) is the actual source IP address of a request.

Note For more information about how to configure common web servers to obtain the actual source IP addresses, see Retrieve actual IP addresses of clients. Common web servers include NGINX, IIS 6, IIS 7, Apache, and Tomcat,

9.4. Obtain the actual source IP addresses of requests to an origin server that is not deployed on Alibaba Cloud

If you use a server in your data center as the origin server and use Anti-DDoS Pro or Anti-DDoS Premium to protect your service, requests are first scrubbed by Anti-DDoS Pro or Anti-DDoS Premium and then forwarded to the origin server. The origin server cannot directly obtain the actual source IP addresses of the requests. This topic describes how to configure the TOA module on the origin server to obtain the actual source IP addresses.

Scenario

The following table describes common deployment scenarios and whether the actual source IP addresses of requests can be obtained in each scenario.

Scenario	Description	Whether actual source IP addresses can be obtained

Scenario	Description	Whether actual source IP addresses can be obtained
Anti-DDoS Pro or Anti-DDoS Premium - Layer 7 SLB instance - Server in your data center	The origin server is deployed in your data center. Requests are first scrubbed by Anti-DDoS Pro or Anti-DDoS Premium. Then, a Layer 7 SLB instance forwards the requests to the origin server that is deployed in your data center.	Yes
Anti-DDoS Pro or Anti-DDoS Premium - Layer 4 instance SLB - Server in your data center	The origin server is deployed in your data center. Requests are first scrubbed by Anti-DDoS Pro or Anti-DDoS Premium. Then, a Layer 4 SLB instance forwards the requests to the origin server that is deployed in your data center.	No
Anti-DDoS Pro or Anti-DDoS Premium - Server in your data center	The origin server is deployed in your data center. Requests are first scrubbed by Anti-DDoS Pro or Anti-DDoS Premium and then forwarded to the origin server that is deployed in your data center.	Yes

Applicable operating systems

The method in this topic applies to the following operating systems:

- Red Hat Enterprise Linux
- CentOS 6.x
- CentOS 7.x

Procedure

Before you perform the following steps, take note of the following items:

> **Notice**
>
> - Before you use the method in a production environment, you can use the method in a test environment to check whether your service runs as expected.
> - We recommend that you keep the original kernel of the operating system. This way, you can use the original kernel to restore your service if a restart fails.

1. Download the required kernel installation file based on the operating system of your server.
   - CentOS 7.x: kernel-3.10.0-957.21.3.el7.toa.x86_64.rpm
   - CentOS 6.x or Red Hat Enterprise Linux:
     - kernel-firmware-2.6.32-696.13.2.el6.centos.plus.toa.x86_64
     - kernel-2.6.32-696.13.2.el6.centos.plus.toa.x86_64

2. Install the kernel.
   - CentOS 7.x

     Go to the directory of the installation file and run the following command:

     ```
     sudo yum localinstall kernel-3.10.0-957.21.3.el7.toa.x86_64.rpm
     ```

     > **Note** We recommend that you use the `yum localinstall` command to install the kernel to avoid dependency issues. You can also use the `sudo rpm -ivh kernel-3.10.0-957.21.3.el7.toa.x86_64.rpm` command.

   - CentOS 6.x or Red Hat Enterprise Linux

     Go to the directory of the installation file and run the following commands:

     ```
     sudo rpm -ivh kernel-firmware-2.6.32-696.13.2.el6.centos.plus.toa.x86_64.rpm
     sudo rpm -ivh kernel-2.6.32-696.13.2.el6.centos.plus.toa.x86_64.rpm
     ```

     > **Note**
     > - If kernel-firmware runs 2.6.32-696.13.2.el6.centos.plus.toa or later, use only the preceding second command.
     > - If dependency issues occur during installation, add the `--nodeps` parameter to the `rpm` command.
     > - If the kernel version is later than the TOA version, add the `--force` parameter to the `rpm` command to forcibly install the kernel.

3. Configure the TOA module to make sure that the module is automatically loaded when the operating system is started.
   i. Create the */etc/sysconfig/modules/toa.modules* file and add the following content to the file:
      - CentOS 7.x:

        ```
        #!/bin/bash
        if [ -e /lib/modules/`uname -r`/kernel/net/toa/toa.ko.xz ] ;
        then
        modprobe toa > /dev/null 2>&1
        fi
        ```

      - CentOS 6.x or Red Hat Enterprise Linux:

        ```
        #!/bin/bash
        if [ -e /lib/modules/`uname -r`/kernel/net/toa/toa.ko ] ;
        then
        modprobe toa > /dev/null 2>&1
        fi
        ```

   ii. Run the following command to grant execute permissions to the *toa.modules* file:

       ```
       sudo chmod +x /etc/sysconfig/modules/toa.modules
       ```

4. Run the `reboot` command to restart the operating system.
   After the installation is complete, the origin server can obtain the actual source IP addresses of requests.

   If the actual source IP addresses are not obtained, run the `lsmod|grep toa` command to check the loading status of the TOA module. If the TOA module is not loaded, run the `modprobe toa` command to manually load it. After the TOA module is loaded, you can view server access logs and test whether the origin server can obtain the actual source IP addresses.

References

- If I use the TOA module, does network performance deteriorate?

  No, the network performance does not deteriorate. The TOA module is deployed in bypass mode and has little impact on network performance.

- What do I do if the kernel is unstable after the TOA module is loaded?

  We recommend that you keep the original kernel of the operating system. This way, you can use the original kernel to restore your service if a restart fails.

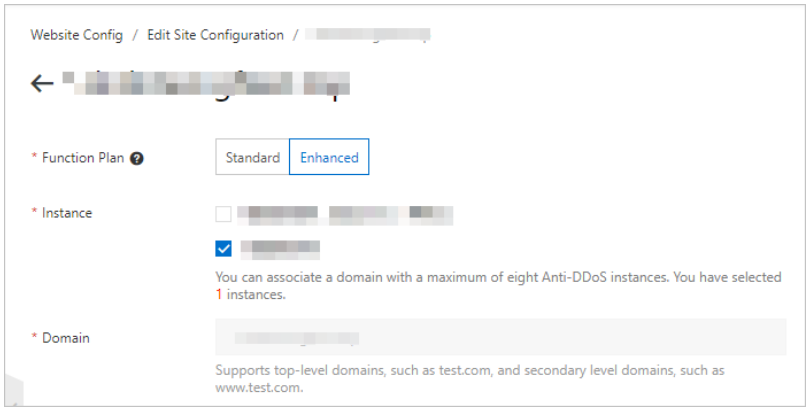
9.5. Switch service traffic to a new Anti-DDoS Pro or Anti-DDoS Premium instance

If the current Anti-DDoS Pro or Anti-DDoS Premium instance expires and you purchase a new instance, you can modify the settings of the added domain name to migrate your service to the new instance without service interruptions.

Procedure

1.
2.
3.
4. Find the required domain name, and click **Edit** in the Actions column.
5. Select the new instance for **Instance** and click **OK**.

> **Note**
>
> - You cannot add a domain name to instances of both the **Standard** and **Enhanced** function plan.
> - Each domain name can be added to a maximum of eight instances of the same **function plan**.



6. In the Confirm dialog box, confirm the selected Anti-DDoS Pro or Anti-DDoS Premium instance and click **OK**.

Result

After you modify the domain name settings, protection policies of the original Anti-DDoS Pro or Anti-DDoS Premium instance are applied to the new instance to protect your service.

9.6. Configure ACLs for the origin server

After you add your website to Anti-DDoS Pro or Anti-DDoS Premium, all traffic destined for the origin server of the website is forwarded by Anti-DDoS Pro or Anti-DDoS Premium. You can configure access control lists (ACLs) to protect the origin server. For example, you can allow inbound traffic only from the back-to-origin CIDR blocks of your Anti-DDoS Pro or Anti-DDoS Premium instance. This topic describes how to configure ACLs for origin servers based on different network architectures.

> **Note** ACLs for an origin server can help mitigate small volumes of HTTP flood attacks and web attacks. The ACLs cannot help mitigate volumetric DDoS attacks that bypass Anti-DDoS Pro or Anti-DDoS Premium and directly target the origin server. DDoS attacks may even trigger blackhole filtering for the origin server.

Network architecture of your website	ACL configuration description

Network architecture of your website	ACL configuration description
Anti-DDoS Pro or Anti-DDoS Premium + Elastic Compute Service (ECS) instance	The origin server is an ECS instance. The back-to-origin CIDR blocks of your Anti-DDoS Pro or Anti-DDoS Premium instance are the source IP addresses of the requests that are forwarded to the origin server. We recommend that you configure ACLs for the origin server by configuring the security group rules of the ECS instance. You can configure security group rules to allow traffic from only the back-to-origin CIDR blocks and deny all traffic from other IP addresses to protect the origin server. You can obtain the back-to-origin CIDR blocks of an Anti-DDoS Pro or Anti-DDoS Premium instance in the Anti-DDoS Pro or Anti-DDoS Premium console. For more information, see Allow back-to-origin IP addresses to access the origin server.
Anti-DDoS Pro or Anti-DDoS Premium + Origin server that is not deployed on Alibaba Cloud	The origin server is an ECS instance. The back-to-origin CIDR blocks of your Anti-DDoS Pro or Anti-DDoS Premium instance are the source IP addresses of the requests that are forwarded to the origin server. We recommend that you configure ACLs for the origin server in the security software installed on the origin server, such as iptables and a firewall, to allow traffic only from the back-to-origin CIDR blocks and deny all traffic from other IP addresses to protect the origin server.
Anti-DDoS Pro or Anti-DDoS Premium + Layer 4 Server Load Balancer (SLB) instance + ECS instance	The origin server is an ECS instance. The back-to-origin CIDR blocks of your Anti-DDoS Pro or Anti-DDoS Premium instance are the source IP addresses of the requests that are forwarded to the origin server. We recommend that you add the back-to-origin CIDR blocks of Anti-DDoS Pro or Anti-DDoS Premium to the whitelist of the SLB instance to configure ACLs for the origin server. Then, enable access control to allow traffic only from the back-to-origin CIDR blocks to protect the origin server. For more information, see Enable access control.
Anti-DDoS Pro or Anti-DDoS Premium + Layer 7 Application Load Balancer (ALB) instance + ECS instance	The origin server is an ECS instance. The back-to-origin CIDR blocks of the ALB instance are the source IP addresses of the requests that are forwarded to the origin server. We recommend that you add the back-to-origin CIDR blocks of your Anti-DDoS Pro or Anti-DDoS Premium instance to the whitelist of the ALB instance to configure ACLs for the origin server. Then, enable access control to allow traffic only from the back-to-origin CIDR blocks to protect the origin server. For more information, see Access control.
Anti-DDoS Pro or Anti-DDoS Premium + Web Application Firewall (WAF) or Alibaba Cloud CDN (CDN) + ECS instance	The origin server is an ECS instance. The back-to-origin CIDR blocks of WAF or CDN are the source IP addresses of the requests that are forwarded to the origin server.

Network architecture of your website	ACL configuration description We recommend that you configure ACLs for the origin server in WAF or CDN. For more information, see Configure protection for an origin server.
Anti-DDoS Pro or Anti-DDoS Premium + WAF or CDN + Origin server that is not deployed on Alibaba Cloud	

9.7. Best practices to configure an ECS instance as the origin server of a non-website service

If you add a non-website service, such as a port-based service that uses TCP, to Anti-DDoS Pro or Anti-DDoS Premium and the origin server of the service is an Elastic Compute Service (ECS) instance or a virtual private cloud (VPC), your service traffic may be directly forwarded to the origin server. In this case, Anti-DDoS Pro or Anti-DDoS Premium cannot protect your service, and risks may occur. To prevent the risks, we recommend that you perform the following operations:

- Configure a security group rule for the ECS instance that is used as the origin server. This rule allows only the back-to-origin CIDR blocks of an Anti-DDoS Pro or Anti-DDoS Premium instance to access your ECS instance and denies the traffic from other IP addresses.

  You can obtain the back-to-origin CIDR blocks of an Anti-DDoS Pro or Anti-DDoS Premium instance in the Anti-DDoS Pro or Anti-DDoS Premium console. For more information, see Allow back-to-origin IP addresses to access the origin server.
- If an IP address such as the egress IP address of your internal network is trusted and you want to use the IP address to access your ECS instance, configure a security group rule to allow the traffic from the trusted IP address.

9.8. Handle exposure of the origin IP address

After you add your service to Anti-DDoS Pro or Anti-DDoS Premium, if attack traffic is not scrubbed and directly targets the origin server, the IP address of the origin server may have been exposed. In this case, you must change the IP address of the origin server.

Check for risks that cause IP address exposure

Before you change the IP address of the origin server, make sure that you eliminate all risks to prevent the IP address from being exposed again. You can check for the following exposure risks:

- Check whether the origin server contains security risks, such as trojans and backdoors.

  We recommend that you use Alibaba Cloud Security Center to check and fix security vulnerabilities. For more information, see What is Security Center?.
- Check whether the origin server runs services that are not added to Anti-DDoS Pro or Anti-DDoS Premium. For example, you have added MX records to configure an email server or other DNS records to configure a BBS website for the origin server.

> **Notice** Make sure that no DNS records map a domain name to the IP address of the origin server.

- Check whether the source code of the website is exposed. For example, the `phpinfo()` function may contain the IP address of the origin server.
- Check whether the origin server encounters malicious scanning. You can allow inbound traffic only from the back-to-origin IP addresses of Anti-DDoS Pro or Anti-DDoS Premium to access the origin server. For more information, see Configure ACLs for the origin server.

Change the IP address of the origin server

After you eliminate all risks that may cause the exposure, you can change the IP address of the origin server. For more information, see Change the public IP address of an ECS origin server.

If you do not want to change the IP address or the new IP address is also exposed, we recommend that you deploy an SLB instance to connect the ECS instance. For more information, see Quick Start of SLB. You can adopt the following network architecture: Client > Anti-DDoS Pro or Anti-DDoS Premium > SLB instance > ECS instance.

In this architecture, even if the origin server encounters attacks that trigger blackhole filtering, the service is not interrupted. Traffic from the SLB instance to the origin server is transmitted over the internal network. If blackhole filtering is triggered for the public IP address of the origin server, Anti-DDoS Pro or Anti-DDoS Premium can still access the origin server through the SLB instance.

> **Note** To apply the preceding network architecture, you must set the origin server address to the IP address of the SLB instance in the Anti-DDoS Pro or Anti-DDoS Premium console.