

# Alibaba Cloud Anti-DDoS Pro

## Anti-DDoS Premium Service

Issue: 20190912

## Legal disclaimer

---

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

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

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.



# Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 <b>Danger:</b> Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 <b>Warning:</b> Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 <b>Notice:</b> Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 <b>Note:</b> You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
<b>Bold</b>	It is used for buttons, menus, page names, and other UI elements.	Click OK.
<code>Courier</code> font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[ ] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand   slave}</code>



# Contents

---

Legal disclaimer.....	I
Generic conventions.....	I
<b>1 Product Introduction.....</b>	<b>1</b>
1.1 What is Anti-DDoS Premium.....	1
1.2 Features.....	1
1.3 Scenarios.....	2
<b>2 Pricing.....</b>	<b>6</b>
2.1 Billing method.....	6
2.2 Global advanced mitigation.....	11
2.3 Mainland China Acceleration.....	14
2.4 Function plans.....	15
<b>3 Quick Start.....</b>	<b>20</b>
3.1 Enable Anti-DDoS Premium.....	20
3.2 Associate a website business with Anti-DDoS Premium for protection.....	20
3.3 Add a non-website business to Anti-DDoS Premium for protection.....	26
3.4 Configure Anti-DDoS Premium MCA.....	29
<b>4 User Guide.....</b>	<b>34</b>
4.1 Website configuration.....	34
4.1.1 Protection of non-standard ports.....	34
4.1.2 Upload an SSL certificate.....	35
4.1.3 Customize a TLS security policy.....	38
4.2 Layer 7 protection configuration.....	40
4.2.1 Configure the blacklist and whitelist.....	40
4.2.2 Block access requests from IP addresses in specific regions.....	42
4.2.3 Configure fine-grained access control rules.....	43
4.2.4 Configure HTTP(S) flood protection.....	51
4.2.5 Enable intelligent protection.....	54
4.2.6 Accelerate access to a static page.....	55
4.2.7 Change the public IP address of an ECS instance that hosts your origin site.....	57
4.3 Layer 4 protection configuration.....	58
4.3.1 Configure a Layer 4 mitigation policy.....	58
4.3.2 Configure health check rules.....	60
4.3.3 Configure session persistence rules.....	62
4.4 View Security Overview.....	63
4.5 Import or export provisioning settings.....	69



# 1 Product Introduction

---

## 1.1 What is Anti-DDoS Premium

For users who have business servers deployed outside the mainland China, Alibaba Cloud provides the Anti-DDoS Premium service to mitigate DDoS attacks.

By enabling Anti-DDoS Premium for your server that deployed outside the mainland China, all attack traffic against your server is pulled to your Anti-DDoS Premium's dedicated IP. Then, the Anti-DDoS Premium service filters attack traffic that diverted to global distributed scrubbing centers by using Anycast technology, and forward clean traffic back to the origin server. This mostly improves the stability of your business.

## 1.2 Features

Anti-DDoS Premium defends against the following types of DDoS attacks for you.

Functionality	Description
Malformed packets filtering	Defends against Frag flood, Smurf attack, stream flood and Land attacks, and filters malformed IP packet, TCP packet and UDP packet.
Transport layer DDoS protection	Defends against SYN flood, ACK flood, UDP flood, ICMP flood, and RST flood attacks.
Web application layer DDoS protection	Defends against HTTP Get flood, HTTP Post flood, and connection flood attacks by using filtering rules based on HTTP characteristics, URI and Host.

### Core features

Anti-DDoS Premium has the following features:

- Global DDoS Mitigation

Anti-DDoS Premium integrates capacities of all Alibaba Cloud scrubbing centers over the world as protection resources by using Anycast technology. With

distributed technology, Anti-DDoS Premium automatically diverts DDoS attack traffic to the nearest scrubbing center to the attacking source for mitigation.

- **Unlimited Protection**

Anti-DDoS Premium provides unlimited protection with full capacity to each user by comprehensively utilizing global near-source mitigation abilities.

In 2018, the total protection capacity of Alibaba Cloud International Anti-DDoS scrubbing centers increases to over 2 Tbps. Anti-DDoS Premium aims to defend against every single DDoS attack for you.



**Notice:**

Alibaba Cloud keeps rights of actions when attacks against your business impact the infrastructure of Alibaba Cloud International Anti-DDoS scrubbing centers. Once the actions are triggered on your Anti-DDoS Premium instance, your protected business may be affected. The action includes but not limited to “black hole” of the IP addresses being attacked, or alteration to the routing of the traffic destined to the IP addresses being attacked.

- **Dedicated IP Resource**

Anti-DDoS Premium provides a dedicated Anycast IP for each user. Each IP is isolated to avoid any impact by DDoS attacks against other users. This provides you a safer DDoS mitigation service.

- **Security Report**

Anti-DDoS Premium provides detail traffic report and attack protection report in real time for you to have a clear view on the security of your business.

## 1.3 Scenarios

The Internet is interconnected by local network operators to achieve global access. However, due to different policies of network operators in different regions, the actual network access and communication is different. Therefore, you have to use an appropriate DDoS protection solutions according to your business scenarios.



**Note:**

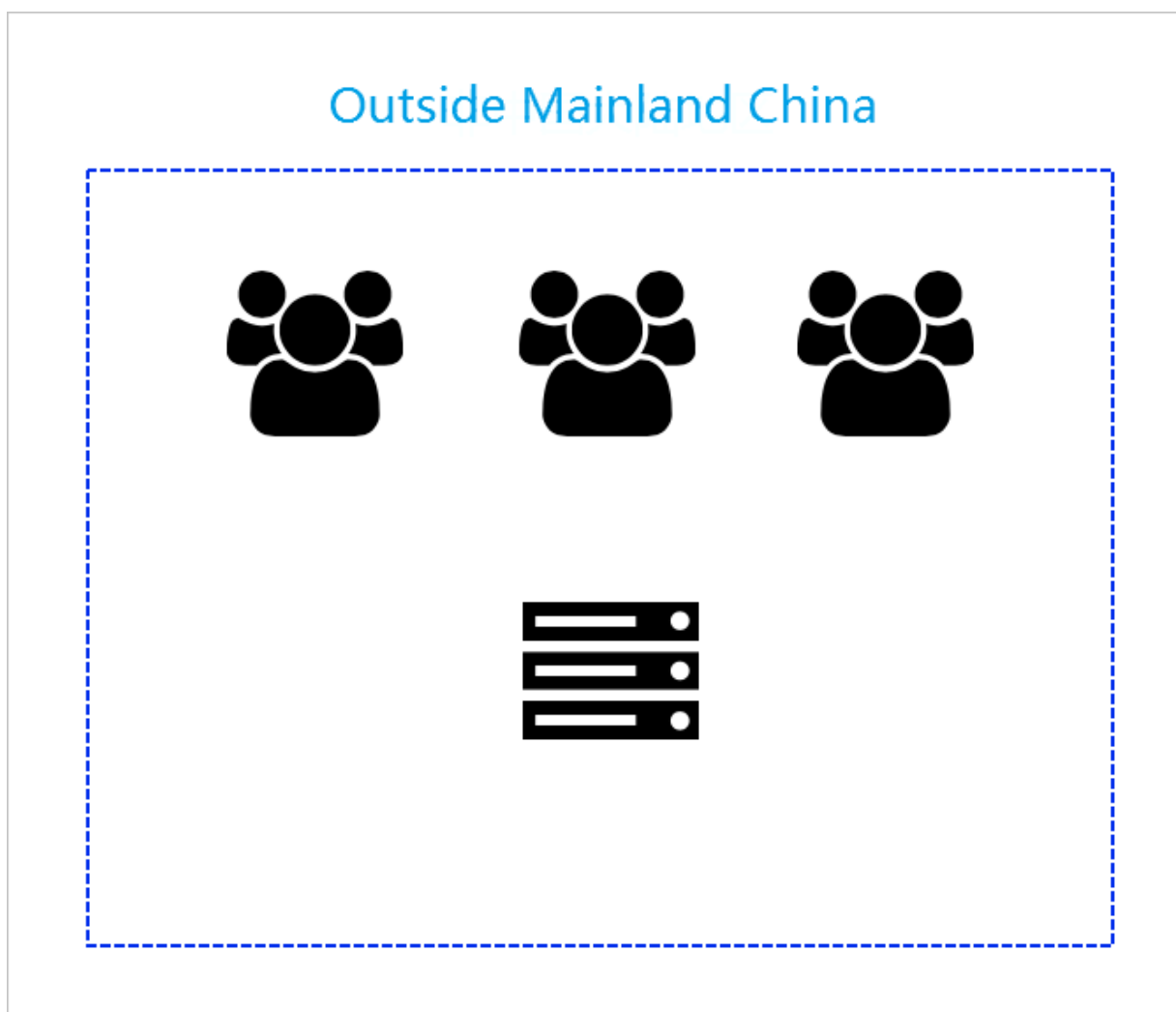
Because of the current routing and interconnection strategies of network operators , if only the Anti-DDoS Premium service is enabled, users in mainland China have to

access Anti-DDoS Premium resources deployed outside the mainland China, and the quality of the network link is affected.

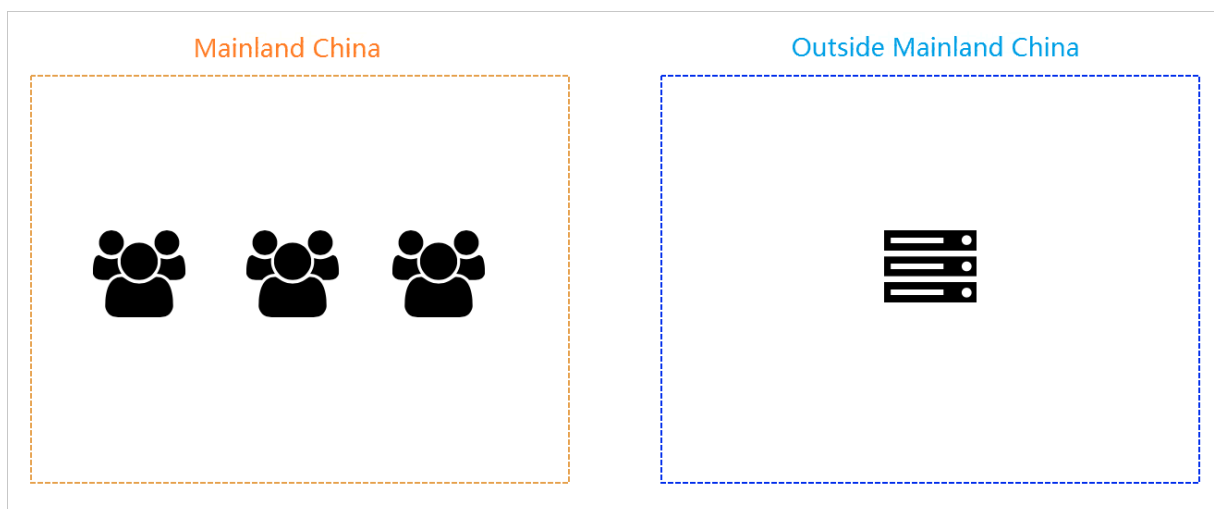
The average network delay time reaches 300 ms, and the network link is affected by international link congestion resulting in intermittent packet loss. Therefore, we strongly recommend that you deploy servers in mainland China to serve users in mainland China, use Anti-DDoS Pro service to mitigate DDoS attacks, and complete website registration and other compliance procedures to comply with relevant Chinese laws and regulations.

For servers that are deployed outside mainland China, see the following three scenarios:

Scenario 1: The Business Server is deployed in non-mainland China and mainly serves users from non-Mainland China



Purchase Anti-DDoS Premium, and add your business to the Anti-DDoS Premium instance for DDoS protection according to [Enable Anti-DDoS Premium](#).

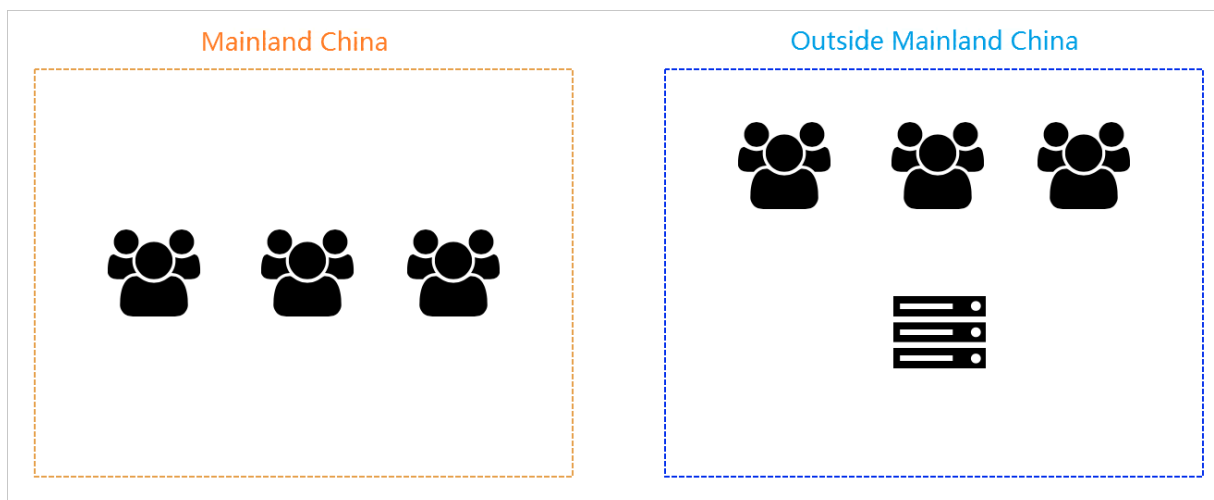
**Scenario 2: Servers deployed outside mainland China, while serving users in mainland China****Solutions:****· Solution A**

If your business has high requirements on network quality (for example, gaming servers), we recommend that you migrate your servers to the mainland China region that your major users located in, and purchase [the Anti-DDoS Pro service](#) to mitigate DDoS attacks.

**· Solution B**

If your business servers are not planned to be migrated to mainland China, contact our sales or submit a ticket to purchase the Mainland China Acceleration (MCA) plan of Anti-DDoS Premium. Then, our technical support helps you to deploy the Anti-DDoS Smart Switch solution to guarantee smooth access for users in mainland China by utilizing the acceleration lines when no DDoS attack happens. For more information about MCA, view [Configure Anti-DDoS Premium MCA](#).

**Scenario 3: Servers deployed outside mainland China, while serving users both in and outside mainland China**



**Solutions:**

- **Solution A**

We recommend that you deploy business servers separately for the two regions, using servers deployed in mainland China to serve users in mainland China and using servers deployed outside mainland China to serve users outside mainland China. Meanwhile, purchase [the Anti-DDoS Pro service](#) and the Anti-DDoS Premium service for businesses in and outside mainland China to mitigate DDoS attacks.

- **Solution B**

If you do not plan to deploy business servers in mainland China, contact our sales or submit a ticket to purchase the Mainland China Acceleration (MCA) plan of Anti-DDoS Premium. Then, our technical support helps you to deploy the Anti-DDoS Smart Switch solution to guarantee smooth access for users in mainland China by utilizing the acceleration lines when no DDoS attack happens. For more information about MCA, view [Configure Anti-DDoS Premium MCA](#).

## 2 Pricing

---

### 2.1 Billing method

Anti-DDoS Premium offers Insurance Plan and Unlimited Plan.

#### Advanced mitigation feature of Anti-DDoS Premium

Integrating all mitigation capacities of Alibaba Cloud Anti-DDoS scrubbing centers around the world, Anti-DDoS Premium defends against all DDoS attacks to secure your business.

In most cases, the chances of being attacked decrease significantly after you have successfully defended against DDoS attacks using the Anti-DDoS service. Typically, attackers launch DDoS attacks to cause financial losses to your business. Due to the cost of launching attacks, if the attackers fail to achieve this purpose, they will stop launching DDoS attack. Therefore, the advanced mitigation of Anti-DDoS Premium provides unlimited mitigation capacities and can integrate all mitigation capacities of Alibaba Cloud Anti-DDoS scrubbing centers around the world to secure your business.



#### Notice:

If the attacks against your business impact the infrastructure of Alibaba Cloud Anti-DDoS scrubbing centers, Alibaba Cloud has the right to control the traffic. Once the traffic control is triggered on your Anti-DDoS Premium instance, your protected business may be affected. The traffic control measures include but are not limited to black hole routing and limitations to the access traffic.

#### Plans of Anti-DDoS Premium

- Insurance Plan

Each month, Anti-DDoS Premium Insurance Plan offers two advanced mitigations by default, featuring unlimited mitigation capabilities. This protects your businesses against DDoS attacks with full capacity within 24 hours after an attack has been detected, and consumes one advanced mitigation. The number of

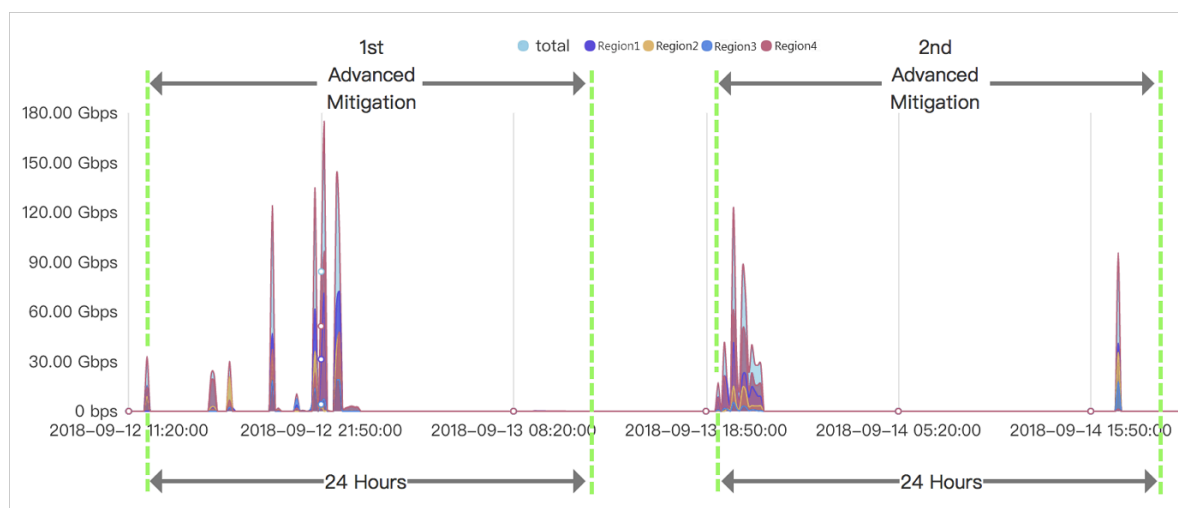
advanced mitigations is reset to two at the beginning of every month during the service period.



**Note:**

To purchase more advanced mitigations, see [Global advanced mitigation](#).

For example, a protected IP suffers DDoS attacks at 11:20:00 (UTC+8), September 12, and an advanced mitigation is triggered. Within 24 hours, Anti-DDoS Premium provides unlimited mitigation capacities for this IP. The protected IP suffers another DDoS attack at 18:50:00 (UTC+8), September 13, and an advanced mitigation is triggered again. 24 hours later, the advanced mitigation stops and the two advanced mitigation of the Anti-DDoS Premium Insurance Plan instance in September are exhausted. The number of advanced mitigations is automatically reset to two at the beginning of the following month, October 1.



Insurance Plan is a basic solution of Anti-DDoS Premium and applies to users who are less vulnerable to attacks.



**Note:**

Only when the DDoS attack against your business exceeds a specific threshold, namely the basic mitigation threshold, will the advanced mitigation of Anti-DDoS Premium be enabled.

- **Unlimited Plan**

Anti-DDoS Premium Unlimited Plan provides unlimited advanced mitigation capabilities for your business. After you purchase the Unlimited Plan instances,

Anti-DDoS Premium provides unlimited mitigation to protect your business against all DDoS attacks.

#### Pricing details of Anti-DDoS Premium

The pricing details of Anti-DDoS Premium instances are shown in the following table.

Plan	Business bandwidth	Advanced mitigation	Price (USD/month)
Insurance	100 Mbps	2/month	2,630
Unlimited		Unlimited	11,560
Insurance	150 Mbps	2/month	3,420
Unlimited		Unlimited	12,610
Insurance	200 Mbps	2/month	4,210
Unlimited		Unlimited	13,660
Insurance	250 Mbps	2/month	5,000
Unlimited		Unlimited	14,720
Insurance	300 Mbps	2/month	5,570
Unlimited		Unlimited	15,770



**Note:**

If you need a higher Clean bandwidth, contact Alibaba Cloud technical support.



**Note:**

Clean bandwidth refers to the maximum normal clean bandwidth that can be processed by Anti-DDoS Premium instances when your business is not under attack. Make sure that the Clean bandwidth of the instance is greater than the peak value of the inbound or outbound traffic of all services connected to the Anti-DDoS Premium instances. For more information about the Clean bandwidth, see [How to select a Clean bandwidth specification](#).

If the actual traffic volume exceeds the maximum Clean bandwidth, your business may be subject to traffic restrictions or random packet losses, and your normal business may be unavailable, slowed, or delayed for a certain period of time.

Anti-DDoS Premium instances provide the following business specifications by default:



**Note:**

If you need to expand the default business specifications based on actual needs, you can upgrade the instance or expand the corresponding specifications when purchasing the instance.

Business specifications	Descriptions	Default values	Price (USD/month )
Number of protected ports	The number of TCP /UDP ports that can be protected by the instance.	5	Every 5 ports: 150 USD/month
Number of protected domain names	The number of HTTP/ HTTPS domain names that can be protected by the instance.	10 <div> <b>Note:</b>            Contains only one top-level domain and the subdomains or wildcard domains of this top-level domain.         </div>	<ul style="list-style-type: none"> <li>For Standard Function Plan: 45 USD/month for every 10 domain names</li> <li>For Enhanced Function Plan: 75 USD/month for every 10 domain names</li> </ul> <div> <b>Note:</b>            Every 10 protected domain names contain only one top-level domain and the subdomains or wildcard domains of this top-level domain.         </div>
Clean QPS	The maximum concurrent HTTP/ HTTPS requests per second supported when the system is not under attack.	<ul style="list-style-type: none"> <li>Insurance Plan : 500 QPS</li> <li>Unlimited Plan : 1,000 QPS</li> </ul>	Every 100 QPS: 150 USD/month

## More information

### How to select a Clean bandwidth specification

You can select an appropriate Clean bandwidth specification based on the daily inbound or outbound traffic peaks of all businesses that have or will be connected to the Anti-DDoS Premium instance. Make sure that the Clean bandwidth of the instance is greater than the peak value of the inbound and outbound traffic of all businesses.



#### Note:

Typically, the outbound traffic is greater than the inbound traffic.

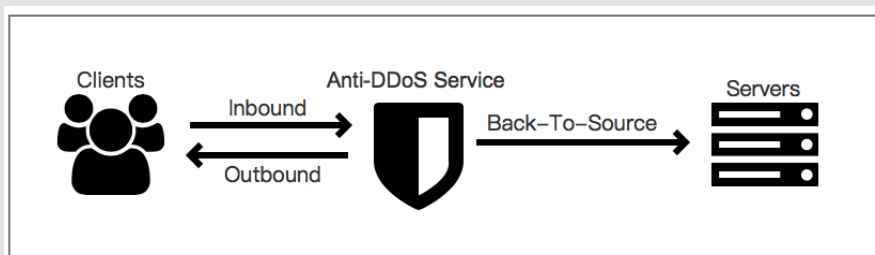
You can evaluate your business traffic by using ECS traffic statistics or other monitoring tools on your origin server.



#### Note:

The traffic here indicates the normal business traffic.

For example, you connect all access traffic of your external business to an Anti-DDoS Premium instance to secure your business. Anti-DDoS Premium will reroute the normal access traffic to the origin server when the business is normally accessed and without being attacked. When the business is attacked, Anti-DDoS Premium filters and blocks the malicious traffic, and only reroutes the normal traffic to the origin server. Therefore, the inbound and outbound traffic you view in the ECS console is normal traffic. If your business is deployed on multiple origin servers, you need to calculate the total traffic of all origin servers.



Assume that you need to connect the businesses of three websites to an Anti-DDoS Premium instance, the normal outbound traffic peak for each business does not exceed 50 Mbps, and the total business traffic does not exceed 150 Mbps. In this case, you only need to ensure that the maximum bandwidth of the purchased instance is greater than 150 Mbps.

### Domain name specifications

Anti-DDoS Premium instances support adding 10 domain names for protection by default, including one top-level domain and the subdomains or wildcard domains of the top-level domain.

Taking `abc . com` for example, you can add the top-level domain itself and a maximum of nine subdomains, such as `www . abc . com`, `*. abc . com`, `mail . abc . com`, `user . pay . abc . com`, and `x . y . z . abc . com`. Each domain name that you have added, including the top-level domain `abc . com` counts in the quota for protected domain names.

If you want to add two different top-level domains or their subdomains to connect to the Anti-DDoS Premium instance, you need to expand the quota for protected domain names. Assume that you have added `abc . com` or its subdomain for protection, when you try to add `xyz . com` (another top-level domain) or its subdomain, you will receive the following message:

The quota of top-level domains has been exceeded. Upgrade the instance to expand the quota for protected domain names.

In this case, you need to upgrade the Anti-DDoS Premium instance to expand the quota for domain name mitigation.



**Note:**

Adding 10 protected domain names each time allows you to have one more top-level domain in the quota for domain name mitigation. For example, you must set the number of protected domain names to 20 to protect the two top-level domains, `abc . com` and `xyz . com` in an Anti-DDoS Premium instance.

## 2.2 Global advanced mitigation

If the two advanced mitigations for the month of an Anti-DDoS Premium Insurance Plan instance has been used up, you can purchase additional global advanced mitigations to achieve more unlimited mitigation capabilities.

Each month, Anti-DDoS Premium Insurance Plan provides two advanced mitigations by default, featuring unlimited mitigation capabilities. This protects your businesses against DDoS attacks within 24 hours after an attack has been detected, and consumes one advanced mitigation.

If the business suffers from frequent large-traffic attacks, the two advanced mitigations of Anti-DDoS Premium Insurance Plan may be not enough to guarantee the service availability. In this case, you can purchase global advanced mitigations to obtain more advanced mitigations for the Anti-DDoS Premium instances in your account.

#### Notes

If the two advanced mitigations for the month have been used up and your business still suffers from large-traffic attacks, with the traffic volume exceeding the basic mitigation threshold, the additional global advanced mitigations you have purchased will be consumed to provide unlimited mitigation capacities.

You do not need to bind the global advanced mitigation to a specific instance. You can use the global advanced mitigation for all Anti-DDoS Premium Insurance Plan instances that meet the usage requirements.

#### Usage requirements

- The Insurance Plan instance is valid.
- The advanced mitigation feature of the account is not frozen.



#### Note:

When the number of advanced mitigations, including the number of global advanced mitigation, consumed by all instances in your account in the current month exceeds 10, the advanced mitigation feature will be automatically frozen. You must wait until the next calendar month to use this feature.

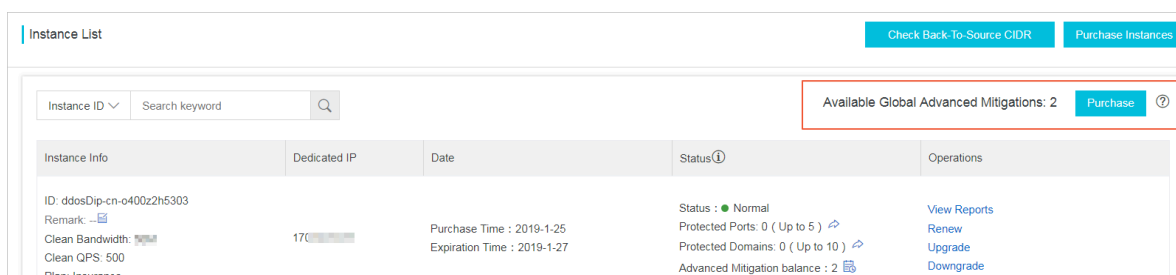
If your business is subject to frequent large-traffic attacks, we recommend that you purchase Unlimited Plan instances to protect your business.

#### Purchase global advanced mitigation

After you purchase an Anti-DDoS Premium instance, you can purchase additional global advanced mitigations in the Anti-DDoS Premium console at any time.

1. Log on to the [Anti-DDoS Premium console](#).

## 2. On the Instance List page, click Purchase.



Instance List

Check Back-To-Source CIDR Purchase Instances

Instance ID Search keyword

Available Global Advanced Mitigations: 2 Purchase ?

Instance Info	Dedicated IP	Date	Status①	Operations
ID: ddosDip-cn-o400z2h5303 Remark: <a href="#">...</a> Clean Bandwidth: <a href="#">...</a> Clean QPS: 500 Plan: Insurance	170	Purchase Time : 2019-1-25 Expiration Time : 2019-1-27	Status : ● Normal Protected Ports: 0 ( Up to 5 ) Protected Domains: 0 ( Up to 10 ) Advanced Mitigation balance : 2	<a href="#">View Reports</a> <a href="#">Renew</a> <a href="#">Upgrade</a> <a href="#">Downgrade</a>

## 3. On the Global Advanced Mitigation purchase page, select the quantity, and click Buy Now.



### Note:

Make sure that the Product is selected as Anti-DDoS Premium.

## Pricing

Pricing parameters	Description
Payment type	Subscription
Duration	1 Years
Unit price	1,580 USD




### Notice:

Refund is not supported for the global advanced mitigation.

## More information

### Global advanced mitigation and advanced mitigation of Anti-DDoS Premium instance

Type	Scope	Period of Validity	Quantity
Advanced mitigation of Unlimited Plan	Instance	Based on instance validity period	Unlimited

Type	Scope	Period of Validity	Quantity
Advanced mitigation of Insurance Plan	Instance	1 month  Note: Advanced mitigation that is unconsumed in the current month will be cleared at the beginning of next month.	Twice each month
Global advanced mitigation	Account	1 year	Purchase separately

## 2.3 Mainland China Acceleration

If your business servers are deployed in regions outside mainland China, you can purchase Mainland China Acceleration (MCA) for your Anti-DDoS Premium instances to accelerate the access to your business for users in mainland China.

MCA provides users in mainland China with low-latency access to the businesses deployed in regions outside mainland China. This significantly improves the response time when the business is not under attack.



Note:

MCA cannot be configured independently. MCA instances do not have any mitigation capabilities and must be used with Anti-DDoS Premium Insurance Plan or Unlimited Plan instances.

For more information about the applicable scenarios, see [#unique\\_15](#).

After purchasing MCA instances, you can use these instances with Anti-DDoS Premium Insurance Plan instances or Unlimited Plan instances to increase the access speed when your business is not under an attack, as shown in [#unique\\_9](#).

### Pricing

The pricing details of Anti-DDoS Premium MCA are shown in the following table.

Business bandwidth	Price (USD/month)
10 Mbps	1,548

Business bandwidth	Price (USD/month)
20 Mbps	3,096
30 Mbps	4,643
40 Mbps	6,191
50 Mbps	7,739
60 Mbps	9,287
70 Mbps	10,834
80 Mbps	12,382
90 Mbps	13,930
100 Mbps	15,478

**Note:**

Business bandwidth refers to the maximum normal business bandwidth that can be processed by Anti-DDoS Premium MCA instances when your business is not under attack. Make sure that the business bandwidth of the instance is greater than the peak value of the inbound and outbound traffic of all services connected to the MCA instance.

If the actual traffic volume exceeds the maximum business bandwidth, your business may be subject to traffic restrictions or random packet losses, and your normal business may be unavailable, slowed, or delayed for a certain period of time.

## 2.4 Function plans

Anti-DDoS Premium provides two function plans: standard function and enhanced function. In addition to the features provided by the standard function plan, the enhanced function plan also provides enhanced features such as website acceleration, non-standard service ports, and geo-blocking. These features enable Anti-DDoS Premium to be associated with more businesses and provide stronger protection against DDoS attacks. You can select an appropriate function plan based on your business conditions and security requirements.

When you purchase an Anti-DDoS Premium instance, the standard function is the default function plan. You can select the enhanced function to associate more businesses with Anti-DDoS Premium and increase the protection against DDoS

attacks. The enhanced function plan costs an extra 8,000 RMB per month. This cost is added to the price of the standard function plan for the instance.

You can upgrade the instances that have the standard function plan to activate the enhanced function plan.



**Note:**

After purchasing or upgrading to an enhanced function plan, you must edit the domain configuration to associate the domain with the Anti-DDoS Premium instance that has the enhanced function plan. This way, the enhanced features are available to the website.

### Comparison between the standard and enhanced function plans



Compared with the standard function plan, the enhanced function plan allows you to associate more businesses and increases protection against attacks.

Category	Feature	Description	Standard function	Enhanced function
Protection algorithm	Protection against DoS attacks	Supports protection against common DDoS attacks, including malformed packet attacks and various HTTP flood attacks.	✓	✓
	Protection against resource exhaustion attacks	Supports protection against common Layer 4 or Layer 7 resource exhaustion attacks, such as HTTP GET flood and HTTP POST flood attacks.  For more information, see <a href="#">#unique_17</a> .	✓	✓



Category	Feature	Description	Standard function	Enhanced function
	Intelligent protection	<ul style="list-style-type: none"> <li>· Supports intelligent protection against Layer 7 HTTP flood attacks at the application layer.</li> <li>· Supports intelligent protection against Layer 4 HTTP flood attacks and mitigates TCP connection exhaustion attacks.</li> </ul> <p>For more information, see <a href="#">#unique_18</a>.</p>	✓	✓
Protection rule	Blacklist and whitelist	<p>You can configure a whitelist and a blacklist for each domain associated with Anti-DDoS Premium. Each list can contain a maximum of 200 IP addresses or IP address ranges.</p> <p>For more information, see <a href="#">#unique_19</a>.</p>	✓	✓

Category	Feature	Description	Standard function	Enhanced function
	Accurate access control	Supports accurate matching of HTTP protection rules.  For more information, see <a href="#">#unique_20</a> .	A maximum of five rules can be configured for each domain associated with Anti-DDoS Premium, and only the IP, URL, Referer, and User-Agent field are supported.	A maximum of 10 rules can be configured for each domain associated with Anti-DDoS Premium.
	Geo-blocking	Supports the blocking of access traffic of each domain based on geographical locations.  For more information, see <a href="#">#unique_21</a> .	✗	✓
Connection method	Standard HTTP (80 or 8080) and HTTPS (443 or 8443) ports forwarding	Supports Anti-DDoS protection for HTTP (80 or 8080) and HTTPS (443 or 8443) ports.	✓	✓

Category	Feature	Description	Standard function	Enhanced function
	Non-standard HTTP and HTTPS ports forwarding	<p>Supports Anti-DDoS protection for non-standard HTTP and HTTPS ports (not limited to ports 80, 8080, 443, and 8443).</p> <div>  <b>Note:</b>  Each instance can be configured with 10 distinguished non-standard ports for forwarding. </div>	✗	✓
Others	Static page caching	<p>Supports static page website acceleration.</p> <div>  <b>Note:</b>  The custom cache rule function is under public review. You can configure a maximum of three rules for each domain associated with Anti-DDoS Premium. </div> <p>For more information, see <a href="#">#unique_22</a>.</p>	✗	✓

## 3 Quick Start

---

### 3.1 Enable Anti-DDoS Premium

You can add configurations for your domains (Layer 7) and ports (Layer 4) in Anti-DDoS Premium for DDoS protection.

After purchasing an Anti-DDoS Premium instance, you can add configurations in the console to add forwarding rules of domains and ports to specify the origin servers where clean traffic is forwarded to after DDoS attack mitigation.

After completing the configurations in the console, you change the DNS resolution record for domain or change your business application' s IP to the CNAME or IP assigned by your Anti-DDoS Premium instance, to switch all traffic to the Anti-DDoS Premium' s dedicated IP. Then, all traffic firstly passes through global scrubbing centers and the clean traffic is forwarded back to the origin servers. In this situation, the unlimited full-capacity protection has been enabled for your business.

### 3.2 Associate a website business with Anti-DDoS Premium for protection

After purchasing an Anti-DDoS Premium instance, you can associate your website domain with the instance to protect against DDoS attacks.

#### Context






#### Note:



If you want to associate a non-website business, such as a game client, a mobile game, or an app with Anti-DDoS Premium, see [Add a non-website business to Anti-DDoS Premium for protection](#).



#### Procedure

1. Log on to the [Anti-DDoS Premium console](#).
2. Go to the Provisioning > Website page, and click Add Website.

3. On the Website Configuration page that appears, set parameters for the website to be protected, and click Add website.

Parameter	Configuration method
Function Plan	<p>Select a function plan. Valid values:</p> <ul style="list-style-type: none"> <li>Standard Function</li> <li>Enhanced Function</li> </ul>
Instance	<p>Select an instance. Anti-DDoS Premium instances are displayed based on the specified function plan.</p> <div>  <b>Note:</b>            If no instances are displayed, instances that have the selected function plan are unavailable. You can choose to purchase an instance that has the enhanced function plan or upgrade an existing standard function instance.         </div> <p>This instance is to be associated with the website domain.</p> <div>  <b>Note:</b>            A domain can be associated with a maximum of eight Anti-DDoS Premium instances that have the same function plan.         </div>
Website domain	<p>Set the domain of the website that you want to protect.</p> <div>  <b>Note:</b> <ul style="list-style-type: none"> <li>You can set wildcard domains, such as *. aliyun . com . Anti-DDoS Premium automatically matches the subdomain of the wildcard domain.</li> <li>If you enter a wildcard domain and a specific domain, such as *. aliyun . com and www . aliyun . com , Anti-DDoS Premium will use the forwarding rules and protection policies of the specific domain whenever possible.</li> </ul> </div>

Parameter	Configuration method
Protocol	<p>Select the protocols supported by the website. Valid values:</p> <ul style="list-style-type: none"> <li>· HTTP (Selected by default)</li> <li>· HTTPS (Selected by default)</li> <li>· Websocket</li> <li>· Websockets</li> </ul> <div>  <b>Note:</b>            If your website supports HTTPS, you must select HTTPS. Select other protocols as needed.         </div>
Enable HTTP/2	<p>If your business supports HTTP/2, you can enable HTTP/2.</p> <div>  <b>Note:</b>            To enable HTTP/2 protection, the following requirements must be met:           <ul style="list-style-type: none"> <li>· Your website has been associated with an Anti-DDoS Premium instance of the enhanced function plan.</li> <li>· You have selected HTTPS.</li> </ul> </div>
Origin server	<p>Select the address type of the origin server and specify the address. Supported address types are as follows:</p> <ul style="list-style-type: none"> <li>· <b>IP:</b> You can enter a maximum of 20 IP addresses of the origin server. When multiple origin server IP addresses are specified, Anti-DDoS Premium uses IP Hash load balancing to forward traffic back to the origin server.</li> <li>· <b>Domain:</b> If you want to use Anti-DDoS Premium and WAF together for enhanced protection, you can select Domain and enter the CNAME record provided by your WAF instance.</li> </ul>

Parameter	Configuration method
Origin server ports	<p>Specify the server ports based on the protocols you have selected.</p> <div>  <b>Note:</b> The forwarding port is the same as the port of the origin server. </div> <ul style="list-style-type: none"> <li>When HTTP or Websocket is selected, the port is set to 80 by default.</li> <li>When HTTPS or Websockets is selected, the port is set to 443 by default.</li> </ul> <div>  <b>Note:</b> The port for HTTP/2 is the same as the port for HTTPS. </div> <p>You can customize ports. Click Custom to specify available ports.</p> <div> <div>Server Port: HTTP 80 HTTPS 443 <span>Custom</span></div> <div> <div>Server Port: HTTP HTTPS <span>Save Cancel</span></div> <div>80,8080</div> <div>If there are other ports, please add them and separate them by " <span>View optional range</span></div> </div> </div> <ul style="list-style-type: none"> <li>Instances that have the standard function plan: The port range is 80 or 8080 if you select HTTP or Websocket . The port range is 443 or 8443 if you select HTTPS or Websockets .</li> <li>Instances that have the enhanced function plan: The following figures show the available ports for HTTP and Websocket, and ports for HTTPS and Websockets in sequence.</li> </ul> <div> <div>Optional port range <span>×</span></div> <div> <div>http/websocket https/websockets <span>Search</span></div> <div> 80, 83, 84, 88, 89, 800, 808, 1000, 1090, 3333, 3501, 3601, 5000, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7060, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8106, 8181, 8334, 8336, 8800, 8686, 8787, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9999, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037, 9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48888, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702 </div> </div> </div> <div> <div>Optional port range <span>×</span></div> </div>

Website Configuration

Change DNS Records

\* Function Plan ⓘ

Standard Function

Enhanced Function

\* Instance

No appropriate instance. Please buy a new instance or upgrade your instance to the required specification, then do the domain configurations.

\* Website domain:

Please enter website domain, e.g. www.aliyun.com

Support Top Level Domain: e.g. "test.com" and Second Level Domain: e.g. www.test.com

\* Protocol:

☒ HTTP ☒ HTTPS ☐ Websocket ☐ Websockets

Enable HTTP/2 ⓘ

☐

This feature is only available to domains that are associated with Enhanced Function instances.

\* Origin server:

☒ IP ☐ Domain

Please input IP, separated with ",", cannot be repeated, up to 20.

Origin server ports:

HTTP 80 HTTPS 443

Custom (Port Custom is in public Beta Test stage now, and the Beta Test ends on May 31, 2019 )

4. Contact the DNS service provider of your website to modify the DNS record of the website domain.

Change the DNS record to the dedicated IP address of the Anti-DDoS Premium instance to redirect business traffic from your website to this instance.



**Note:**

If you want to verify whether the forwarding rule set for the Anti-DDoS Premium instance takes effect before business traffic redirection, click Return to Website



List. After you verify that the forwarding rule works as expected, change the DNS record to redirect business traffic to the Anti-DDoS Premium instance.

- a) Log on to the [Anti-DDoS Premium console](#). In the left-side navigation pane, click Instance List. On the page that appears, find the Anti-DDoS Premium instance that protects the website, and record the dedicated IP address of the instance.
- b) Contact the DNS service provider of your website to modify the A record of the website domain to point to the dedicated IP address.

The configuration pages of different DNS service providers are different. The following figure is for reference only.

The screenshot shows a web-based form titled "Add Record". It includes the following elements:

- Type:** A dropdown menu currently showing "A- IPV4 address".
- Host:** A text input field containing "Enter ...", followed by a ".com" domain and a help icon.
- ISP Line:** A dropdown menu showing "Default - Return to the default value when the query is not ...".
- \* Value:** A text input field containing "Enter ...".
- \* TTL:** A dropdown menu showing "10 minute(s)".
- Synchronize the Default Line:** An unchecked checkbox.
- Buttons:** "Cancel" and "OK" buttons at the bottom right.

- c) After the DNS configuration takes effect, all business traffic is redirected from your website to the Anti-DDoS Premium instance for protection.



**Note:**

It takes about 10 minutes for the DNS configurations to take effect. We recommend that you change the DNS record during the off-peak hours.

5. Optional: Configure origin server protection. For more information, see [Protect origin servers that use Anti-DDoS Pro](#).

**Note:**

DDoS attacks may send traffic that bypasses Anti-DDoS Premium to flood the origin server, which may throw the origin IP address into the black hole routing status. It can prevent your origin server against small-scale HTTP flood and Web attacks, but cannot prevent large-scale DDoS attacks.

### 3.3 Add a non-website business to Anti-DDoS Premium for protection

After purchasing an Anti-DDoS Premium instance, you can add your non-website business, such as client game, mobile game or APP, to the instance for DDoS protection.

#### Context

**Notice:**

Compared with website protection, non-website protection only provides layer 4 port protection, such as SYN, ACK, ICMP, and UDP floods. It cannot mitigate layer 7 attacks, such as HTTP floods, and web application attacks, such as SQL injection and XSS.

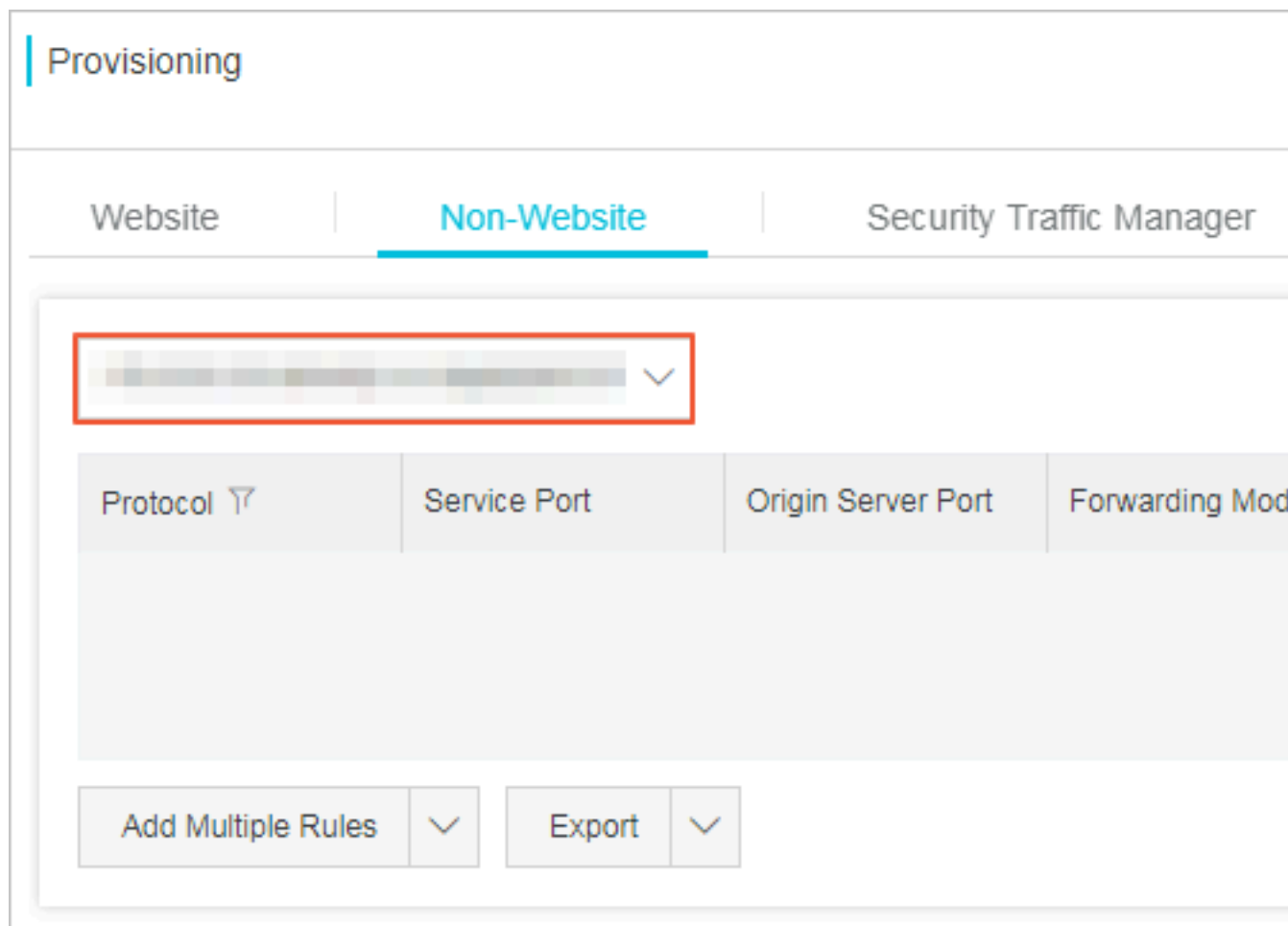
**Note:**

If you want to add a website domain to Anti-DDoS Premium, see [Add website to Anti-DDoS Premium for protection](#).

#### Procedure

1. Log on to the [Anti-DDoS Premium Service console](#).

2. Go to Provisioning > Non-Website page, select an Anti-DDoS Premium instance, and click Add Rule.



3. On the Add Rule page, configure the following rule, and click Confirm.

## Add Rule

\* Protocol: ☒ TCP ☐ UDP

\* Service Port:  +  
−  
Range 1- 65535

\* Origin Server Port:  +  
−  
Range 1- 65535

Forwarding Mode: Round Robin

\* Origin Server IP   
  
Separated with ",", cannot be repeated, up to 20.

Confirm

Parameter	Description	Note
Protocol	Protocols supported by the website.	The TCP and UDP protocols are supported.
Service Port	Port that used by the Anti-DDoS Premium instance to provide public service for the business. We recommend that you set the service port to the same port as the origin server port.	Any port from 1 to 65535 is supported.

Parameter	Description	Note
The port of the origin.	Origin server port that provides service for the business.	Any port from 1 to 65535 is supported.
Source station IP	IP address of the origin server.	You can set up to 20 origin server IPs. If multiple origin IPs are set, the system forwards traffic to these IPs by using the Round Robin mode to realize load balancing.

4. After you verify that the Anti-DDoS Premium forwarding rule works as expected, switch your business traffic to the Dedicated IP of the Anti-DDoS Premium instance.

**Note:**

Log on to the [Anti-DDoS Premium Service console](#). On the Instance Listpagepage, you can find the Dedicated IP of the Anti-DDoS Premium instance.

- If your business uses IP to access the origin server, change the business IP to the Dedicated IP of Anti-DDoS Premium.
- If your business also uses a domain to access the origin server (For example, you set the “aliyundemo.com” domain as the server address in the client program), go the DNS service provider of the domain and change the A record to point to the Dedicated IP of Anti-DDoS Premium.

## 3.4 Configure Anti-DDoS Premium MCA

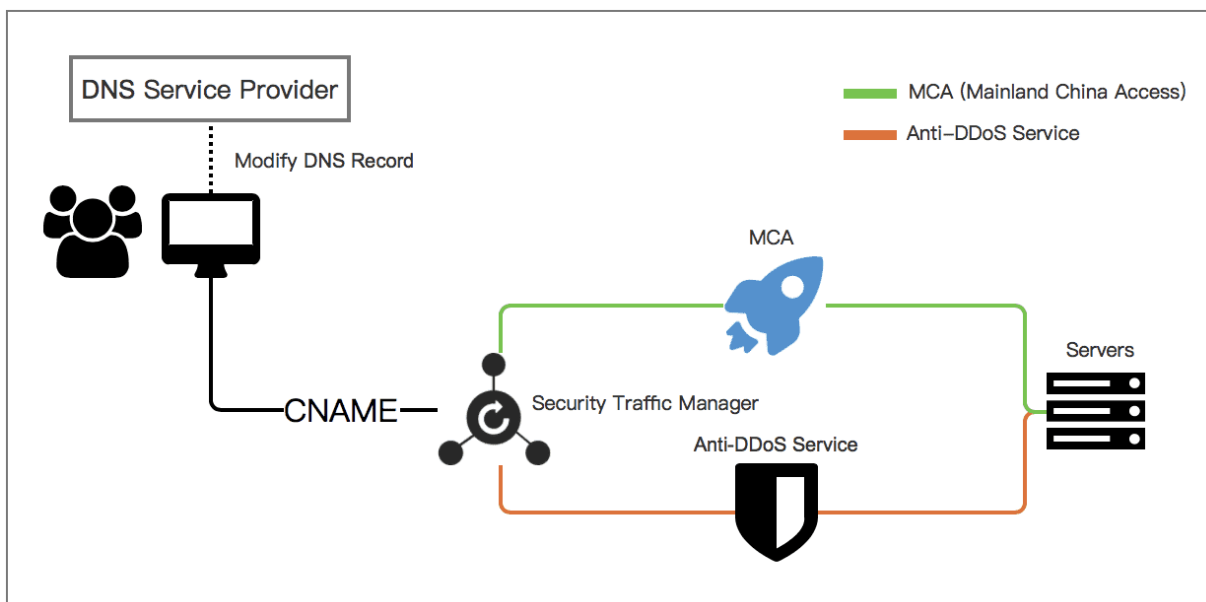
Anti-DDoS Premium mainland China acceleration (MCA) instance is used together with Anti-DDoS Premium Insurance/Unlimited instance, to realize quick access to your web service that deployed outside mainland China, especially for your Mainland China users.

### Context

After configuring MCA instance together with Anti-DDoS Premium Insurance/Unlimited instance, your web service can have the following features: Under no DDoS attack happens, Anti-DDoS Premium enables the MCA instance to accelerate web access to your service. When DDoS attack happens, Anti-DDoS Premium automatica

lly switches to the anti-DDoS instance (Insurance/Unlimited instance) to mitigate DDoS attacks for your web service.

For more information about recommended scenarios that require Anti-DDoS Premium MCA, refer to [Anti-DDoS Premium Use Cases](#).



You can configure an Anti-DDoS Premium MCA instance for domain (7-layer) or port (4-layer).

After purchasing Anti-DDoS Premium MCA and Insurance/Unlimited instances, complete provisioning of the instances for your website domain or service port on the Anti-DDoS Premium Management console, and then configure a Security Traffic Manager rule to enable the auto-switching between MCA and anti-DDoS instances. Finally, use the security service manager rule to forward non-attack traffic to the origin server of your web service.

## Procedure

1. Log on to the [Anti-DDoS Premium Service console](#).
2. Add your website or non-website service to both Anti-DDoS Premium Insurance/Unlimited and MCA instances.



### Note:

Only complete the provisioning configurations for your web service. Do not change the DNS resolution records of your domain at this step.

- For website domain: Refer to [Add website to Anti-DDoS Premium for protection](#) to complete the provisioning configuration. During the configuration, choose

both dedicated IPs of your Insurance/Unlimited and MCA instances when you choose dedicated IPs of Anti-DDoS Premium.

- For service port: Refer to [Add non-website business to Anti-DDoS Premium for protection](#) to complete the provisioning configuration. Add forwarding rules under both Anti-DDoS Premium Insurance/Unlimited and MCA instances for your non-website service. Thus, you have to add a forwarding rule for your non-website service for each instance that is supposed to be used.



**Note:**


To configure Anti-DDoS Premium MCA for non-website service, your service must have a domain bound with the origin server instead of using the server IP directly. Otherwise, traffic cannot be automatically scheduled by Security Traffic Manager.

3. After the provisioning configuration completes, select the Provisioning > Security Traffic Manager page, click Add Rule.





Website

Non-Website

Security Traffic Manager



Add Rule

Name	CNAME①	Nodes	Operations
jiasu1	 	Low Priority  High Priority 	<a href="#">Edit</a> <a href="#">Delete</a>

4. In the Add Rule dialog box, configure rule and then click Confirm.

**Add Rule** [X]

Name :

Nodes :

High Priority :  Select the Dedicated IP of MCA instance

Low Priority :  Select the Dedicated IP of Insurance/Unlimited instance

Important: Please make sure the Web/Non-Web provisioning settings have been done before using Security Traffic Manager.

Confirm Cancel

- The High Priority node: select the dedicated IP of the MCA instance.
- The Low Priority node: select the dedicated IP of the Insurance/Unlimited instance.

With this configuration, MCA instance is enabled with a high priority to accelerate web access when no DDoS attack happens, and the Security Traffic Manager automatically switch traffic to the anti-DDoS instance for DDoS attack mitigation when under DDoS attacks.

The system generates a CNAME record when the security traffic manager rule is added. After you change the DNS records of your service domain to resolve to the CNAME, the service traffic manager enables the traffic auto-scheduling for your service.



**Note:**

For those dedicated IPs that you select in the security traffic manager rule, make sure that you have completed the provisioning configurations for the dedicated IPs of the MCA and Insurance/Unlimited instances.



5. In the domain name resolution service provider, modify the DNS resolution record for that domain name.

After the DNS configuration is effective, all traffic to your web service is handled by the security traffic manager for auto-scheduling.



**Note:**

The traffic auto-scheduling is based on the CNAME record. Therefore, the DNS resolution of the service domain must use the CNAME record.

## 4 User Guide

---

### 4.1 Website configuration

#### 4.1.1 Protection of non-standard ports

Anti-DDoS Premium instances with the Standard Function plan support HTTP (80, 8080) and HTTPS (443, 8443) standard ports to help websites defend against DDoS attacks. The Enhanced Function plan supports non-standard HTTP and HTTPS ports. However, the number of ports used by each protected domain is limited.



**Note:**

To add non-standard HTTP or HTTPS ports, make sure that your domain is associated with an Anti-DDoS Premium instance with the Enhanced Function plan.

#### Limit on the total number of ports

The domains of an Anti-DDoS Premium instance with the Enhanced Function plan can use a maximum of 10 ports.

#### Supported ports



**Note:**

Anti-DDoS Pro Premium instances can only protect supported HTTP and HTTPS ports. The service does not protect or forward traffic from unsupported ports. For example, if an Anti-DDoS Premium instance receives a packet on port 4444, the packet will be discarded.

- For the HTTP and WebSocket protocols, instances with the Enhanced Function plan support the following ports:

80, 83, 84, 88, 89, 800, 808, 1000, 1090, 3333, 3501, 3601, 5000, 5111, 5222, 6001, 6666, 7000, 7001, 7002, 7003, 7004, 7005, 7006, 7009, 7010, 7011, 7012, 7013, 7014, 7015, 7016, 7018, 7019, 7020, 7021, 7022, 7023, 7024, 7025, 7026, 7060, 7070, 7081, 7082, 7083, 7088, 7097, 7777, 7800, 8000, 8001, 8002, 8003, 8008, 8009, 8020, 8021, 8022, 8025, 8026, 8077, 8078, 8080, 8081, 8082, 8083, 8084, 8085, 8086, 8087, 8088, 8089, 8090, 8091, 8106, 8181, 8334, 8336, 8800, 8686, 8787, 8888, 8889, 8999, 9000, 9001, 9002, 9003, 9080, 9200, 9999, 10000, 10001, 10080, 12601, 86, 9021, 9023, 9027, 9037,

9081, 9082, 9201, 9205, 9207, 9208, 9209, 9210, 9211, 9212, 9213, 48800, 87, 97, 7510, 9180, 9898, 9908, 9916, 9918, 9919, 9928, 9929, 9939, 28080, 33702

- For the HTTPS and WebSockets protocols, instances with the Enhanced Function plan support the following ports:

443, 4443, 5443, 6443, 7443, 7988, 8443, 9443, 8553, 8663, 9553, 9663, 10050, 10443, 18980, 30050

### 4.1.2 Upload an SSL certificate

To use Anti-DDoS Premium to scrub HTTPS traffic, you must select HTTPS on the Website Configuration page, and upload the SSL certificate. When your SSL certificate changes, you must update the certificate in the Anti-DDoS Premium console in a timely manner.

#### Prerequisites

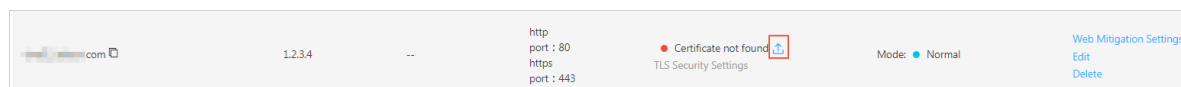
- You have added and configured a website that supports HTTPS. For more information about how to add and configure a website, see [#unique\\_29](#).
- You have prepared the certificate files.

If you have uploaded your certificate files to [Alibaba Cloud SSL Certificates Service](#), you can select the certificate directly. Otherwise, you need to prepare and upload the certificate files and private key files. The following files are required:

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

#### Procedure

1. Log on to the [Anti-DDoS Premium console](#).
2. In the left-side navigation pane, choose Provisioning > Website.
3. On the Website tab, click the upload icon in the Certificate Status column corresponding to the website to upload a certificate for.



4. In the Upload SSL Certificate and Private Key dialog box that appears, set Upload Method and the corresponding parameters. You can select either of the following methods to upload your certificate.

- Select Existing Certificates (Recommended)

If you have uploaded your certificate files to Alibaba Cloud SSL Certificates Service, you can directly select and upload an existing certificate.

If your certificate files have not been uploaded to SSL Certificates Service, you can click [Go to the SSL Certificates console](#) to upload your certificate first. For more information about how to upload certificates to SSL Certificates console, see [#unique\\_35](#).

- Manual Upload

Set Certificate Name, and copy the content of the certificate file to the Certificate File field and the content of the private key file to the Private Key field.



**Note:**

- If the certificate file is in PEM, CER, or CRT formats, you can use a text editor to open the file and copy its content. If the certificate file is in another format such as PFX and P7B, you need to convert the file format into PEM before you can use a text editor to open it and copy its content.

- If your SSL certificate has multiple certificate files, such as a certificate chain, you need to combine the content of multiple certificate files and paste the content to the Certificate File field.

Example of a certificate file:

```
----- BEGIN    CERTIFICAT  E -----
xxxxxxxxxxx  xxvs6MTXcJ  SfN9Z7rZ9f  mxWr2BFN2X  bahgnsSXM4
8ixZJ4krc + 1M + j2kcubVpsE  2cgHdj4v8H  6jUz9Ji4mr  7vMNS6dXv8
PUkl / qoDeNGCNDy  TS5NIL5ir + g92cl8IGOk  jgvhlqt9vc  65Cgb4mL +
n5 + DV9uOyTZTW / MojmlgfUek  C2xiXa54nx  Jf17Y1TADG  SbyJbsC0Q9
nIrHsPl8YK  kvRWvIAqYx  XZ7wRwWWmv  4TMxFhWRiN  Y7yZIo2ZUh
l02SIDNggI  Eeg ==
----- END    CERTIFICAT  E -----
```

Example of a private key file:

```
----- BEGIN    RSA    PRIVATE    KEY -----
xxxxxxxxxxx  xxtZ3UKHJT  RgNQmioPQn  2bqdKHop + B / dn /
4VZL7Jt8zS  DGM9sTMThL  yvsmLQKBgQ  Cr + ujntC1kN6p  GBj2Fw2l
/ EA / W3rYEce2ty  hjgmG7rZ + A / jVE9fld5sQ  ra6ZdwBcQJ
aiygoIYoaM  F2EjRwc0qw  Haluq0C15f  6ujSoHh2e + D5zdmkTg /
3NKNjqNv6x  A2gYpinVDz  FdZ9Zujxvu  h9o4Vqf0YF  8bv5UK5G04
RtKadOw ==
----- END    RSA    PRIVATE    KEY -----
```

Upload SSL Certificate and Private Key

Upload Method:

☒ Manual Upload
 ☐ Select Existing Certificates

Domain:

Certificate Name:

\* Certificate File ⓘ

62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4krc+

1M+j2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNGCNDyTS

5NIL5ir+g92cl8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZTW/MojmlgfUek

C2xiXa54nxJf17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvIAqYxXZ7wRwWWmv

4TMxFhWRiNY7yZIo2ZUhl02SIDNggIEeg==

-----END CERTIFICATE-----

\* Private Key ⓘ :

DADTPZoOHd9WtZ3UKHJTRgNQmioPQn2bqdKHop+B/dn/4VZL7Jt8zSDG

M9sTMThLyvsmLQKBgQCr+ujntC1kN6pGBj2Fw2l/EA/W3rYEce2tyhjgmG7rZ

+A/jVE9fld5sQra6ZdwBcQJaiygoIYoaMF2EjRwc0qwHaluq0C15f6ujSoHh2e+

D5zdmkTg/3NKNjqNv6xA2gYpinVDzFdZ9Zujxvuh9o4Vqf0YF8bv5UK5G04Rt

KadOw==

-----END RSA PRIVATE KEY-----

OK

Cancel

5. Click OK.

## Result

After the upload is complete, the certificate status is updated.

### 4.1.3 Customize a TLS security policy

Anti-DDoS Premium allows you to customize TLS security policies. You can select an appropriate TLS protocol as needed.

## Prerequisites

- Your website has been associated with an Anti-DDoS Premium instance of the enhanced function plan.
- You have added and configured a website that supports HTTPS. For more information about how to add and configure a website, see [#unique\\_29](#).
- You have uploaded the corresponding SSL certificate. For more information about how to upload an SSL certificate, see [#unique\\_37](#).

## Context

If your business needs to comply with PCI DSS 3.2, you must disable the TLS 1.0 protocol. However, the Web server of another business only supports the TLS 1.0 protocol, the TLS 1.0 must be enabled for this business. In this case, you can customize the TLS security policies for different businesses as needed.

## Procedure

1. Log on to the [Anti-DDoS Premium console](#).
2. In the left-side navigation pane, choose Provisioning > Website.
3. Click TLS Security Policy in the Certificate Status column corresponding to the added website.

4. In the TLS Security Settings dialog box that appears, set TLS Versions and Cipher Suites.

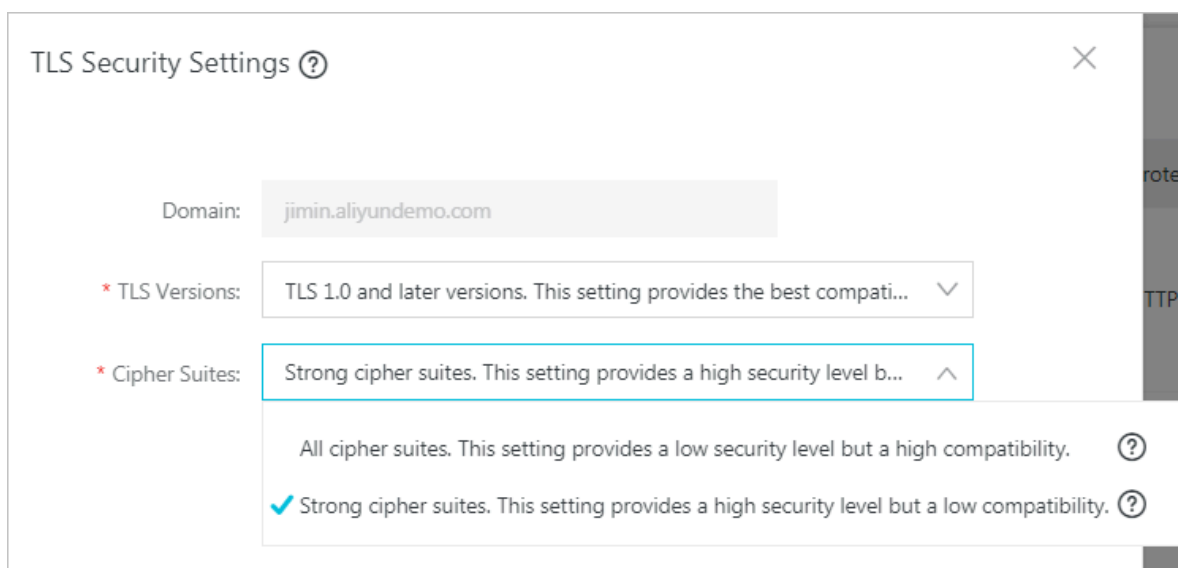
- **TLS Versions:** The default value is TLS 1.0 and later versions. This setting provides the best compatibility but a low security level. You can select V1.1 or V1.2 and later as needed.
- **Cipher Suites:**
  - **Strong cipher suites.** This setting provides a high security level but a low compatibility.

Only the following strong cipher suites are supported:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-WITH-CHACHA20-POLY1305
- ECDHE-RSA-WITH-CHACHA20-POLY1305
- ECDHE-RSA-AES256-CBC-SHA
- ECDHE-RSA-AES128-CBC-SHA
- ECDHE-ECDSA-AES256-CBC-SHA
- ECDHE-ECDSA-AES128-CBC-SHA
- **All cipher suites.** This setting provides a low security level but a high compatibility.

In addition to the preceding strong cipher suites, the following four weak cipher suites are also supported:

- RSA-AES256-CBC-SHA
- RSA-AES128-CBC-SHA
- ECDHE-RSA-3DES-EDE-CBC-SHA
- RSA-3DES-EDE-CBC-SHA



## 4.2 Layer 7 protection configuration

### 4.2.1 Configure the blacklist and whitelist

Anti-DDoS Premium allows you to configure a blacklist and whitelist to control access to your website domain.

- If you have configured a whitelist for a website domain, access requests from IP addresses or IP address ranges that are included in the whitelist are directly allowed without further inspection.
- If you have configured a blacklist for a website domain, access requests from IP addresses or IP address ranges that are included in the blacklist are directly blocked.



#### Note:

The whitelist and blacklist apply to an individual domain, not all domains associated with the Anti-DDoS Premium instance. For each domain, you can add up to 200 entries to the blacklist and whitelist, respectively. You can enter either IP addresses or IP address ranges to the blacklist and whitelist.

To block IP addresses that send large numbers of malicious requests to your server, you can add them to the blacklist. Meanwhile, you can add IP address ranges of intranet, business interface IP addresses, and verified IP addresses to the whitelist so that requests from these IP addresses are allowed.

1. Log on to the [Anti-DDoS Premium console](#).



2. In the left-side navigation pane, choose Provisioning > Website. On the page that appears, select a domain, and click Web Mitigation Settings.
3. On the HTTP Flood Protection Policies tab, click Change Settings in the Blacklist and Whitelist section.

**Note:**

To configure the blacklist and whitelist, you must enable HTTP Flood Protection.

- Click the Blacklist tab, enter the IP addresses or IP address ranges that you want to block, and click OK.
- Click the Whitelist tab, enter the IP addresses or IP address ranges that you want to allow access the website domain, and click OK.

**Note:**

You can enter up to 200 entries in the blacklist and whitelist, respectively. Each entry can be an IP address or IP address range. Separate multiple entries with commas (,).

Blacklist and Whitelist Settings

Blacklist

Whitelist

IP addresses in the blacklist will be blocked :

Enter IP addresses or IP address/CIDR. Separate multiple entries with commas (,). You can enter a maximum of 200 IP addresses.

OK

Cancel

**Note:**

- The blacklist and whitelist feature is only available in domain configurations.
- The blacklist and whitelist take effect immediately after they are configured.

**Notice:**

In some situations, it may take some access traffic and time for the configurations to take effect. If the blacklist and whitelist do not take effect immediately, wait a few minutes.

- You can add 0.0.0.0/0 to the blacklist to block requests from all IP addresses except the ones listed in the whitelist.
- After the blacklist and whitelist are configured, they apply to all Anti-DDoS Premium instances that are associated with the specified domain.

## 4.2.2 Block access requests from IP addresses in specific regions

Geo-blocking allows you to block all access requests from source IP addresses in specified regions (Mainland China, Hong Kong Special Administrative Region (SAR), Macao SAR, Taiwan, and other continents) with a single click. This feature is available only to specified domains.

### Prerequisites

Before enabling Geo-blocking, make sure that your website domain has been associated with an Anti-DDoS Premium instance that has the enhanced function plan.

### Context

Assume that normal requests to access `example.aliyundemo.com` are from China (including Hong Kong SAR, Macao SAR, and Taiwan). You can configure Geo-blocking for `example.aliyundemo.com` to block access requests from outside China regions.

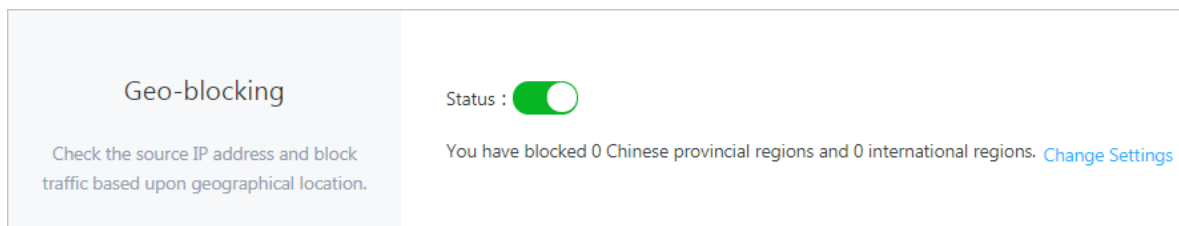
### Precautions

- Geo-blocking takes effect at the domain level. If you want to block multiple domains, you need to configure them separately.
- Geo-blocking uses Anti-DDoS Premium to identify and filter source IP addresses based on their regions. This method does not prevent DDoS attacks from sending traffic.

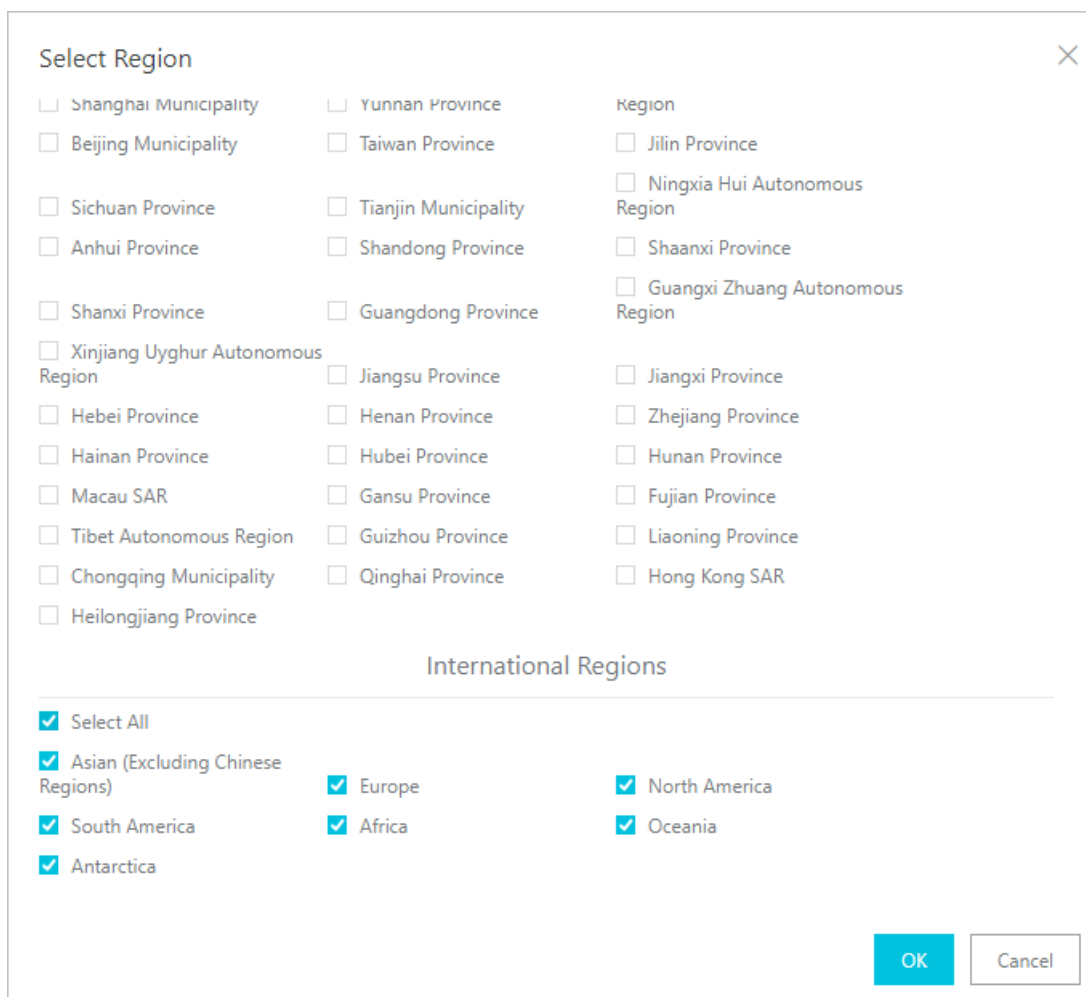
### Procedure

1. Log on to the [Anti-DDoS Premium console](#).
2. In the left-side navigation pane, choose Mitigation Settings > HTTP Flood Protection Policies.

3. Select the domain (example.aliyundemo.com is used as an example) for which you want to set Geo-blocking. Turn on Geo-blocking.



4. In the Geo-blocking section, click Change Settings. In the dialog box that appears, select the regions to be blocked. You can configure Geo-blocking as shown in the following figure. After the configuration takes effect, traffic from outside China regions cannot access example.aliyundemo.com.



5. After selecting regions, click OK to make the configuration take effect.

### 4.2.3 Configure fine-grained access control rules

Fine-grained 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 address, URL, Referer, User-Agent, and Params. For requests that meet the criteria, you can allow, block, or verify their access. This feature applies to custom business scenarios, such as hotlink protection and website administration console protection.

## Context

Each fine-grained access control rule consists of one or more match conditions and an action. When creating a rule, you can define match conditions by setting the field name, logical relation, and field value. Then, select an action to be triggered for access requests that meet the match conditions.

### Match conditions

Match conditions consist of the field name, logical relation, and field value. The field value does not support regular expressions, but can be set to null.

### Action

The fine-grained access control rule supports the following actions:

- **Block:** blocks the access request that meets the match conditions.
- **Allow:** allows the access request that meets the match conditions.
- **Challenge:** uses the CAPTCHA algorithm to verify the source IP address of the access request that meets the match conditions.

### Rule matching order

If multiple rules are configured, access requests are matched based on the order of the fine-grained access control rules. The rule with the higher ranking is matched first.

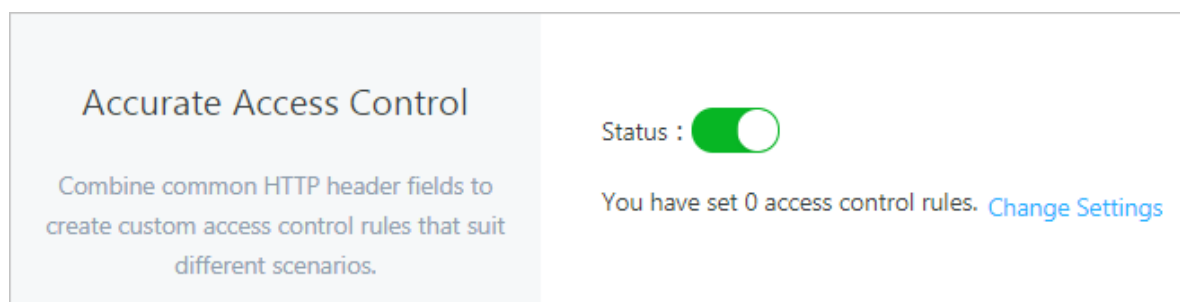
### Precautions

- There are limits to the number of fine-grained access control rules.
  - **Standard function instance:** A maximum of five rules can be configured for each website domain. Only IP address, URL, Referer, and User-Agent fields can be used as the criteria to match requests.
  - **Enhanced function instance:** A maximum of 10 rules can be configured for each website domain.
- Access requests are matched based on the display order of fine-grained access control rules in the rule list. The upper the display order, the higher the priority. If

a request meets the match conditions of multiple rules, the action of the rule that takes the highest priority is taken.

#### Procedure

1. Log on to the [Anti-DDoS Premium console](#).
2. In the left-side navigation pane, choose Mitigation Settings > HTTP Flood Protection Policies.
3. Select the domain (example.aliyundemo.com is used as an example) for which you want to configure fine-grained access control rules. Turn on Accurate Access Control.



4. In the Accurate Access Control section, click Change Settings to configure rules. You can configure a rule as shown in the following figure. After the rule is

configured, any request that contains MSIE in the User-Agent field to access the `/index.php` page will be blocked.

Create Rule ✕

\* Name

\* Match

Field Name	Logical Relation	Field Value	
URI	Equals	/index.php	Remove
User-Agent	Contains	MSIE	Remove

+ Add Condition

\* Action

\* Validity

## Supported fields



### Note:

Anti-DDoS Premium instances with the standard function plan only support using IP address, URL, Referer, and User-Agent fields as the criteria to match requests.

Field	Description	Applicable logical relation
IP	The source IP address in the access request.	<ul style="list-style-type: none"> <li>Is Part Of</li> <li>Is Not Part Of</li> </ul>
URI	The URI in the access request.	<ul style="list-style-type: none"> <li>Contains</li> <li>Does Not Contain</li> <li>Equals</li> <li>Does Not Equal</li> <li>Is Shorter Than</li> <li>Has a Length Of</li> <li>Is Longer Than</li> </ul>

Field	Description	Applicable logical relation
User-Agent	The information about the client that initiates the access request, such as the identifiers of the browser.	<ul style="list-style-type: none"> <li>• Contains</li> <li>• Does Not Contain</li> <li>• Equals</li> <li>• Does Not Equal</li> <li>• Is Shorter Than</li> <li>• Has a Length Of</li> <li>• Is Longer Than</li> </ul>
Cookie	The cookie information in the access request.	<ul style="list-style-type: none"> <li>• Contains</li> <li>• Does Not Contain</li> <li>• Equals</li> <li>• Does Not Equal</li> <li>• Is Shorter Than</li> <li>• Has a Length Of</li> <li>• Is Longer Than</li> <li>• Does Not Exist</li> </ul>
Referer	The source URL of the access request. This URL indicates the address of the webpage from which the access request is redirected.	<ul style="list-style-type: none"> <li>• Contains</li> <li>• Does Not Contain</li> <li>• Equals</li> <li>• Does Not Equal</li> <li>• Is Shorter Than</li> <li>• Has a Length Of</li> <li>• Is Longer Than</li> <li>• Does Not Exist</li> </ul>
Content-Type	The HTTP content type (MIME) specified in the response to the access request.	<ul style="list-style-type: none"> <li>• Contains</li> <li>• Does Not Contain</li> <li>• Equals</li> <li>• Does Not Equal</li> <li>• Is Shorter Than</li> <li>• Has a Length Of</li> <li>• Is Longer Than</li> </ul>

Field	Description	Applicable logical relation
X-Forwarded-For	The originating IP address of the client that initiates the access request.	<ul style="list-style-type: none"> <li>• Contains</li> <li>• Does Not Contain</li> <li>• Equals</li> <li>• Does Not Equal</li> <li>• Is Shorter Than</li> <li>• Has a Length Of</li> <li>• Is Longer Than</li> <li>• Does Not Exist</li> </ul>
Content-Length	The number of bytes in the access request.	<ul style="list-style-type: none"> <li>• Is Smaller Than</li> <li>• Has a Value Of</li> <li>• Is Larger Than</li> </ul>
Post-Body	The content of the access request.	<ul style="list-style-type: none"> <li>• Contains</li> <li>• Does Not Contain</li> <li>• Equals</li> <li>• Does Not Equal</li> </ul>
Http-Method	The method of the access request, such as GET and POST.	<ul style="list-style-type: none"> <li>• Equals</li> <li>• Does Not Equal</li> </ul>
Header	The header of the access request. You can customize the HTTP header fields and field values to be matched.	<ul style="list-style-type: none"> <li>• Contains</li> <li>• Does Not Contain</li> <li>• Equals</li> <li>• Does Not Equal</li> <li>• Is Shorter Than</li> <li>• Has a Length Of</li> <li>• Is Longer Than</li> <li>• Does Not Exist</li> </ul>



Field	Description	Applicable logical relation
Params	The parameter in the URL of the access request. It is the part following the question mark (?) in the URL. For example, in the <code>www.abc.com/index.html ? action=login</code> , <code>action=login</code> is the parameter.	<ul style="list-style-type: none"><li>• Contains</li><li>• Does Not Contain</li><li>• Equals</li><li>• Does Not Equal</li><li>• Is Shorter Than</li><li>• Has a Length Of</li><li>• Is Longer Than</li></ul>

### Other configuration examples

You can configure fine-grained access control rules based on the following configuration examples.

- Intercept malicious requests

In most cases, clients do not initiate POST requests to the root directory. During HTTP flood attacks, a large number of POST requests to the root directory are initiated by the client. The validity of these attacks can be evaluated. If the

requests are identified as abnormal, you can use fine-grained access control rules to intercept the request. A configuration example is as follows:

Edit Rule

\*

Name

Aliyun\_POSTROOT

\*

Match

Conditions

Field Name	Logical Relation	Field Value	
URI	Equals	/	Remove
Http-Method	Equals	POST	Remove

+ Add Condition

\*

Action

Blocked

\*

Validity

Permanent

OK

Cancel

- Intercept access requests of crawlers within a period of time

If the website traffic are used by a large number of crawler requests within a certain period of time, which may be HTTP flood attacks initiated by bots by simulating crawlers, you can intercept the crawler requests.

Create Rule

✕

\* Name

Aliyun\_Spider

\* Match

Field Name	Logical Relation	Field Value	
User-Agent	Contains	spider	Remove

+ Add Condition

\* Action

Blocked

\* Validity

Permanent

OK

Cancel

5. After the configuration is complete, click OK to make the configuration take effect.

## 4.2.4 Configure HTTP(S) flood protection

Anti-DDoS Premium provides four protection modes to help you prevent HTTP(S) flood attacks.

- **Normal:** The default HTTP(S) flood protection mode. You can use this mode when there are no apparent traffic exceptions to the website.

This mode prevent typical HTTP(S) flood attacks and does not block normal requests.

- **Emergency:** You can switch to the Emergency mode when you discover exceptions in metrics such as website response, traffic, CPU, and memory usage.

This mode has relatively strict policies. Compared with the Normal mode, the Emergency mode can prevent more complicated and sophisticated HTTP(S) flood attacks. However, it may block some normal requests.

- **Strict:** This mode uses strict protection policies. The mode implements CAPTCHA verification for all access requests to the protected website. Only verified visitors are allowed to access the website.



**Note:**

With the implementation of global CAPTCHA verification in Strict mode, all requests from real visitors through browsers are responded to normally. 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 uses the strictest protection policies. The mode implements CAPTCHA verification for all access requests to the protected website. Only verified visitors are allowed to access the website.

Compared with the Strict mode, the Super Strict mode combines the global CAPTCHA verification with anti-debugging techniques and anti-machine verification to enhance the protection of your website.



**Note:**

With the implementation of global CAPTCHA verification in Super Strict mode, all requests from real visitors through browsers are responded to normally. Exceptions may occur in some browsers and cause the website to be inaccessible. In this situation, 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.

## Procedure

By default, your domain protected by the Anti-DDoS Premium instance uses the Normal HTTP(S) flood protection mode. You can adjust the protection mode as needed.

1. Log on to the [Anti-DDoS Premium console](#).
2. In the left-side navigation pane, choose Provisioning > Website. On the page that appears, select a domain, and click Web Mitigation Settings.
3. On the HTTP Flood Protection Policies tab, select a mode in the HTTP Flood Protection section .



**Note:**

You can click Status to disable the HTTP(S) flood protection.

### HTTP Flood Protection

Advanced HTTP flood protection that blocks malicious traffic within several seconds.

Status : ☒

Mode ⓘ : ☒ Normal ☐ Emergency ☐ Strict ☐ Super Strict

Custom Rule : ☐

## Custom rules

The HTTP(S) flood protection feature also allows you to create custom rules to prevent HTTP(S) flood attacks. You can create custom rules for specific URLs.

In the left-side navigation pane, click Mitigation Settings. On the HTTP Flood Protection Policies page that appears, turn on Custom Rule in the HTTP Flood Protection section, and click Change Settings.

Domain: [redacted].com Back

Custom HTTP Flood Protection Rules

Name	Protected URI
------	---------------

Create Rule

Currently, 0 rules have been created. You can create 20 more rules.

Block Type Block Duration Actions

Total Items: 0, Items per Page 10 < 上一页 1 下一页 >

Create Rule

## Best practices for HTTP(S) flood protection

The levels of protection provided by different protection modes are as follows: Super Strict > Strict > Emergency > Normal. The chances of false positives when you use these protection modes are as follows: Super Strict > Strict > Emergency > Normal.

We recommend that you use the Normal mode for your protected website. This mode only blocks IP addresses that frequently send requests to your website. We recommend that you switch to the Emergency or Strict mode when your website is overwhelmed by HTTP(S) flood attacks and the Normal mode fails to protect your website.



Note:

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 websites. You must create custom HTTP(S) flood protection rules for specific URLs.

## 4.2.5 Enable intelligent protection

Intelligent protection is based on the big data processing capabilities of Alibaba Cloud. Through the intelligent analysis engine, it can learn business traffic baselines and dynamically adjust protection models to help you detect and block attacks in a timely manner, such as malicious bots and HTTP flood attacks.

### Context

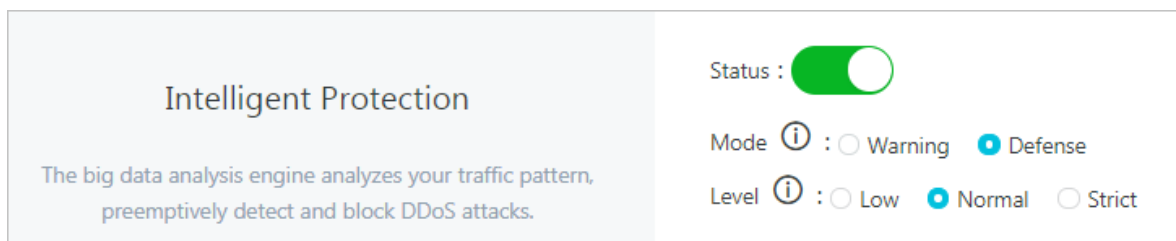


#### Notice:

When intelligent protection is enabled, the automatically issued intelligent rules cannot be manually deleted. If the intelligent protection rules are not suitable for your business scenarios, we recommend that you disable intelligent protection. After intelligent protection is disabled, the automatically issued intelligent rules are cleared instantly.

### Procedure

1. Log on to the [Anti-DDoS Premium console](#).
2. In the left-side navigation pane, choose Mitigation Settings > HTTP Flood Protection Policies.
3. Select the domain (example.aliyundemo.com is used as an example) for which you want to enable intelligent protection. Turn on Intelligent Protection.



### Result

If "The operation is successful" is displayed, this feature has been enabled.

After the intelligent protection feature is enabled, Anti-DDoS Premium instances automatically issue intelligent rules when attacks are detected. You can view specific

rule entries in the Accurate Access Control section. The rule name starts with "smartcc\_."



**Note:**

Each rule issued by intelligent protection has a validity period. If the validity period ends, the protection rule will automatically expire and be cleared.

## 4.2.6 Accelerate access to a static page

In addition to protection against DDoS attacks, Anti-DDoS Premium integrates the Web caching technology with its scrubbing center to provide a static page caching feature for access to your website.

### Prerequisites

Before enabling the static page caching feature, make sure that your website domain has been associated with an Anti-DDoS Premium instance that has the enhanced function plan.

### Context

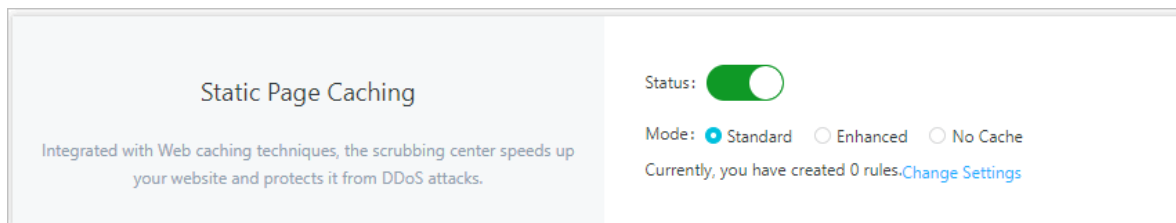
You can use the static page caching feature to accelerate the access to your website domain that has been associated with Anti-DDoS Premium. You can also create custom rules to set caching policies for specified pages linked to the website domain.

### Procedure

1. Log on to the [Anti-DDoS Premium console](#).
2. In the left-side navigation pane, choose Mitigation Settings > Web Acceleration Policies.
3. Select the domain for which you want to configure the static page caching feature. Turn on Static Page Caching.

#### 4. Select a static page caching mode.

- **Standard:** Only requests to access static files (.css, .js, and .txt) of the website domain are cached.
- **Enhanced:** All requests to access the website domain are cached.
- **No Cache:** No requests to access the website domain are cached.



#### 5. Click Change Settings to create custom rules for specified pages linked to the website domain.

##### a) Click Add Rule.

##### b) In the Add Rule dialog box that appears, enter the URI of the specified page, select a cache mode, and set the validity period of the page cache.



#### Note:

When setting a page caching rule, no parameters are required for URIs. However, the URI cannot contain wildcards. For example, when you enter /a/, all pages in the `www . a . com / a / path` are specified.

The 'Create Rule' dialog box has a title bar with a close button (X). It contains four fields, each with a red asterisk indicating it is required: 1. 'Name:' with a text input field containing the placeholder 'Enter a maximum of 128 characters that can be letters, numbers, and u'. 2. 'URI :' with a text input field containing the placeholder 'For example: /abc/a.php'. 3. 'Mode' with three radio buttons: 'Standard' (selected), 'Enhanced', and 'No Cache'. 4. 'Cache Expires In' with a dropdown menu showing 'Use Origin Server Settings' and a downward arrow. At the bottom right are 'OK' and 'Cancel' buttons.



## 4.2.7 Change the public IP address of an ECS instance that hosts your origin site

If the IP address of your origin site has been exposed, we recommend that you change the public IP address of the Alibaba Cloud ECS instance to prevent attackers from bypassing Anti-DDoS Premium and directly attacking the origin site. You can change the IP address of the back-end ECS instance in the Anti-DDoS Premium console. Each Alibaba Cloud account can change this IP address 10 times at most.

### Context



#### Note:

You can only change the IP address of an ECS instance that uses the public IP address on the classic network.

### Procedure

1. Log on to the [Anti-DDoS Premium console](#).
2. In the left-side navigation pane, choose Provisioning > Website.
3. Click Change ECS IP.



#### Notice:

During the IP change process, the business on your ECS instance is interrupted for several minutes. We recommend that you back up your data before performing this operation.

4. Stop the ECS instance before changing its IP address. Click Go to ECS in the Change ECS IP dialog box. In the ECS console, stop the ECS instance whose IP address needs to be changed.



#### Note:

If you have stopped the ECS instance whose IP address needs to be changed, skip this step.

- a) Find the target ECS instance in the instance list and click its ID.
- b) On the instance details page, click Stop.
- c) Select a stop mode and click OK.



#### Notice:

Exercise caution when you stop ECS instances. To ensure security, you must enter the verification code sent to your mobile phone.

- d) Wait until the ECS instance status changes to Stopped.
5. Return to the Change ECS IP dialog box, enter ECS Instance ID, and click Next.
6. Confirm that the current ECS instance information is correct (especially the ECS IP address). Click Release IP Address.
7. After the IP address of the ECS instance is released, click Next. A new IP address is automatically assigned to the ECS instance.
8. After the IP address of the ECS instance is changed, click OK to make the configurations take effect.



Note:

After the IP address is changed, you must associate the new IP address with Anti-DDoS Premium.

## 4.3 Layer 4 protection configuration

### 4.3.1 Configure a Layer 4 mitigation policy

Anti-DDoS Premium supports protection against Layer 4 DDoS attacks and provides multiple protection settings to safeguard your business.

#### Context

Anti-DDoS Premium provides protection against DDoS attacks based on IP addresses and ports for non-website business. You can set limits on parameters such as the request rate and packet length to mitigate DDoS attacks.

Anti-DDoS Premium supports the following mitigation items for you to choose from:

Item	Description
False Source	Detects and blocks false source IP addresses. This setting is applicable only to TCP.
Empty Connection	Detects and blocks null sessions. This setting is applicable only to TCP.

Item	Description
New Connection Speed Limits for Source IP Address	The maximum number of new connections per second from a single source IP address. All new connections exceeding the limit are discarded. The actual limit on the new connection rate may be slightly different because the protection servers are deployed in clusters.
Concurrent Connection Speed Limits for Source IP Address	The maximum number of concurrent connections from a single source IP address. All concurrent connections exceeding the limit are discarded.
New Connection Speed Limits for Destination IP Address	The maximum number of new connections per second to a single destination IP address and port. All new connections exceeding the limit are discarded. The actual limit on the new connection rate may be slightly different because the protection servers are deployed in clusters.
Concurrent Connection Speed Limits for Destination IP Address	The maximum number of concurrent connections to a single destination IP address and port. All concurrent connections exceeding the limit are discarded.
Packet Length Filtering	The limit on the payload size of a packet. Unit: Byte. All packets exceeding the size limit are discarded.

**You can configure mitigation policies for a specified port on a specified IP address.**



**Note:**

## Mitigation policies are configured based on ports.

## Procedure

1. Log on to the [Anti-DDoS Premium console](#).
2. In the left-side navigation pane, choose Provisioning > Non-Website. On the page that appears, select an Anti-DDoS Premium instance. Click Edit in the Mitigation Policies column corresponding to an existing forwarding rule.

Protocol	Service Port	Origin Server Port	Forwarding Mode	Origin Server IP	Session Persistence	Health Check	Mitigation Policies	Operations
TCP	100	100	Round Robin	1.1.1.1	Enabled	Disabled	Enabled	<a href="#">Edit</a> <a href="#">Delete</a>

3. In the Mitigation Policies dialog box that appears, configure Mitigation Policies for the selected IP address and port.

### 4.3.2 Configure health check rules

Anti-DDoS Premium provides health checks for protected non-website businesses.

Anti-DDoS Premium provides health checks for protected non-website business based on the settings of IP addresses and ports .

You can set health check rules for a specified port of a specified IP address.

#### Procedure

1. Log on to the [Anti-DDoS Premium console](#).
2. In the left-side navigation pane, choose Provisioning > Non-Website.
3. Select an Anti-DDoS Premium instance.
4. Click Edit in the Health Check column corresponding to an existing forwarding rule.



#### Note:

The health check feature is disabled by default. When the protocol specified in the forwarding rule is TCP, you can choose either Layer 4 or Layer 7 health check.

#### Health Check

TCP/UDP Health Check

Web Health Check

\* Port

100

Origin server port will be used by default 1- 65535

Advanced Options ^

\* Response Timeout

5

Timeout threshod for health check request (between 1 and 30 seconds)

\* Time Period

15

Time Period and Interval of health check (between 1 and 30 seconds), suggest to set value greater than 15s. It will cause server's load increasing if you set interval too small.

\* Unhealthy Threshold

3

Failed health check count, please enter integer between 1 and 10

#### Configuration items



#### Note:

We recommend that you use default values when configuring advanced settings for health check rules.

Table 4-1: Layer 4 health check

Health check setting	Description
Port	The port that the health check service uses to communicate with the back-end server. The back-end port configured for the listener is used by default.
Advanced setting	
Response Timeout	The maximum timeout period for each health check response. If the back-end server does not respond within the timeout period, the health check fails.
Check Interval	The interval between two consecutive health checks. All scrubbing nodes in the Anti-DDoS Premium cluster perform health checks on back-end servers at the specified interval independently and concurrently. Scrubbing nodes may perform health checks on the same back-end server at different points in time. This is the reason why the health check records on the back-end server do not indicate a check interval.
Unhealthy Threshold	The number of consecutive failed health checks performed by the same scrubbing node server that must occur before declaring a back-end server unhealthy.
Healthy Threshold	The number of consecutive successful health checks performed by the same scrubbing node that must occur before declaring a back-end server healthy.

Table 4-2: Layer 7 health check

Health check setting	Description
Domain Name and Health Check URI (HTTP only)	<p>During a Layer 7 health check, the Anti-DDoS Premium forwarding system sends an HTTP HEAD request to the default homepage of the back-end server.</p> <ul style="list-style-type: none"> <li>· If the page for health checks is not the default homepage of the back-end server, you must specify the domain name and URI for health checks.</li> <li>· If you have limited the host header field to specific values, you only need to specify the URI for health checks. The domain parameter is optional and set to the IP address of the back-end server by default.</li> </ul>

Health check setting	Description
Port	The port that the health check service uses to communicate with the back-end server. The back-end port configured for the listener is used by default.
Advanced setting	
Response Timeout	The maximum timeout period for each health check response. If the back-end server does not respond within the timeout period, the health check fails.
Check Interval	The interval between two consecutive health checks. All scrubbing nodes in the Anti-DDoS Premium cluster perform health checks on back-end servers at the specified interval independently and concurrently. Scrubbing nodes may perform health checks on the same back-end server at different points in time. This is the reason why the health check records on the back-end server do not indicate a check interval.
Unhealthy Threshold	The number of consecutive failed health checks performed by the same scrubbing node that must occur before declaring a back-end server unhealthy.
Healthy Threshold	The number of consecutive successful health checks performed by the same scrubbing node that must occur before declaring a back-end server healthy.

### 4.3.3 Configure session persistence rules

Anti-DDoS Premium provides the session persistence feature for protected non-website business. It supports forwarding requests from the same IP address to the same back-end server within a specified period of time.

#### Context

This feature is implemented based on the settings of IP addresses and ports for protected non-website business.

#### Procedure

1. Log on to the [Anti-DDoS Premium console](#).
2. In the left-side navigation pane, choose Provisioning > Non-Website.
3. Select an Anti-DDoS Premium instance.

4. Click Edit in the Session Persistence column corresponding to an existing forwarding rule.



Note:

Session persistence is configured based on ports.

5. In the Session Persistence dialog box that appears, set Timeout, and click Confirm.



Note:

If you want to disable the session persistence feature, click Disable Session Persistence.

## 4.4 View Security Overview

After you migrate your workloads to Anti-DDoS Premium and switch workload traffic to the Anti-DDoS Premium instance, you can go to the Security Overview page in the console. On this page, you can view the metrics and attack events in real time.

### Context

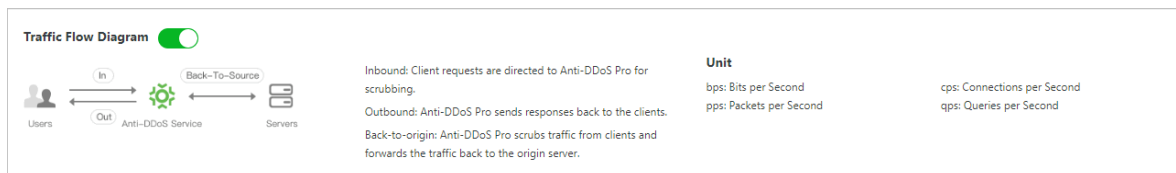
The Security Overview page provides an overview of the following metrics and DDoS attack events:

- Workload metrics: service bandwidth, request rate (QPS), connection rate (CPS), protected domains, and protected ports.
- Attack events: volumetric attacks, connection attacks, and application layer attacks
- 

### Procedure

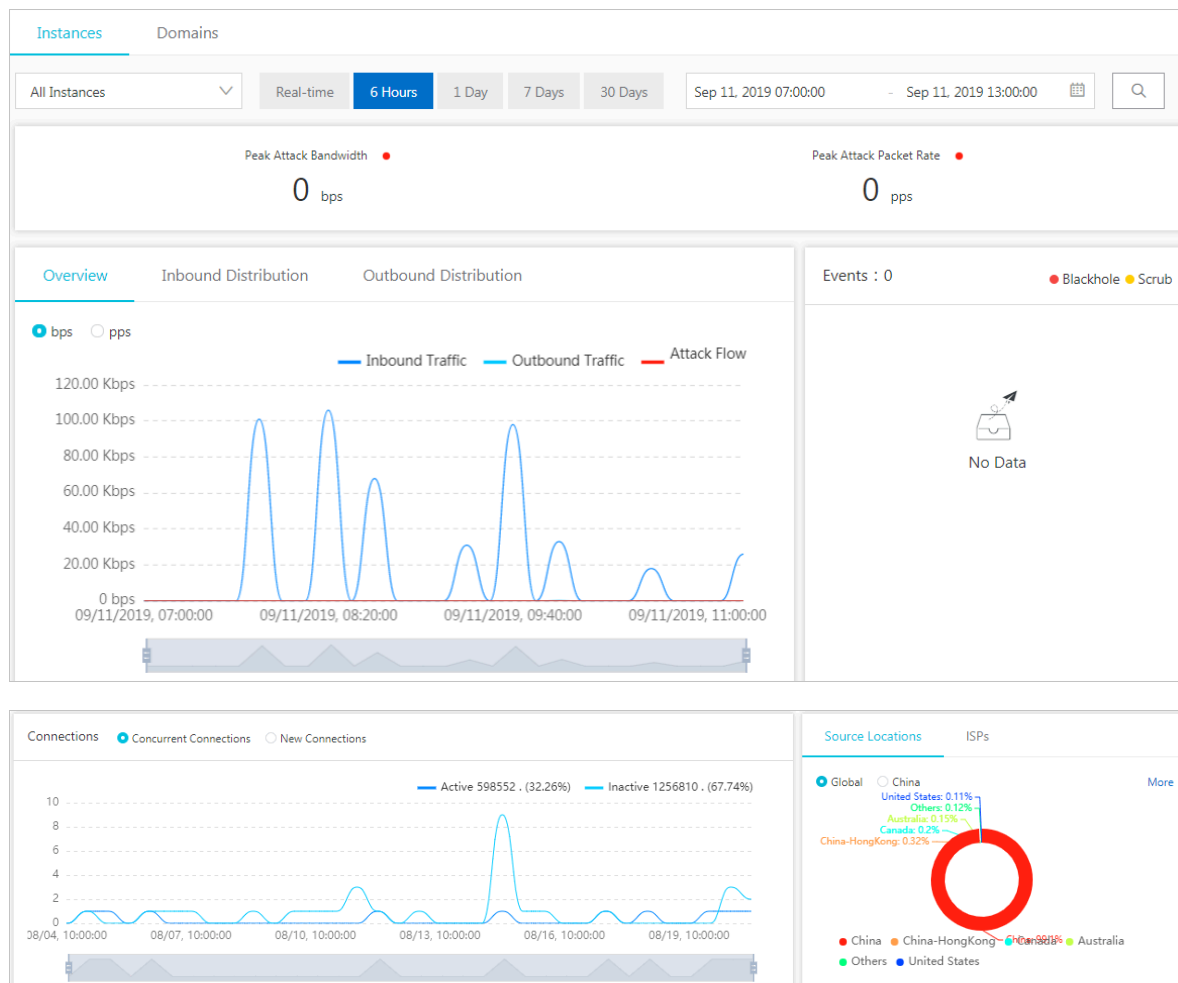
1. Log on to the [Anti-DDoS Premium console](#).
2. On the Security Overview page, you can learn more about the background information and related concepts.

In the top section of the Security Overview page, you can learn about traffic flow information, commonly used terms, and units of measurement.





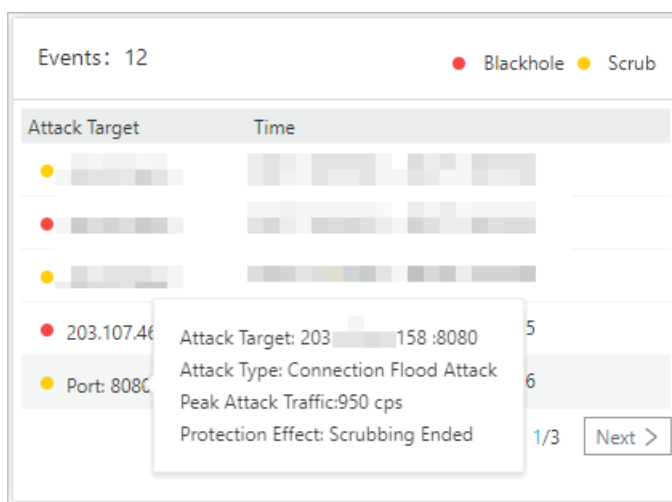
- Click the Instances tab, select one or more instances, and specify a time range to view the corresponding metrics.



You can view the following information about the selected instances:

- The Peak Attack Bandwidth and the Peak Attack Packet Rate
- The Bandwidth traffic, including inbound traffic, outbound traffic, and attack flow
- Attack Events

Move the pointer over an IP address to view the attack details, such as the attack type, peak attack traffic, and protection effect.



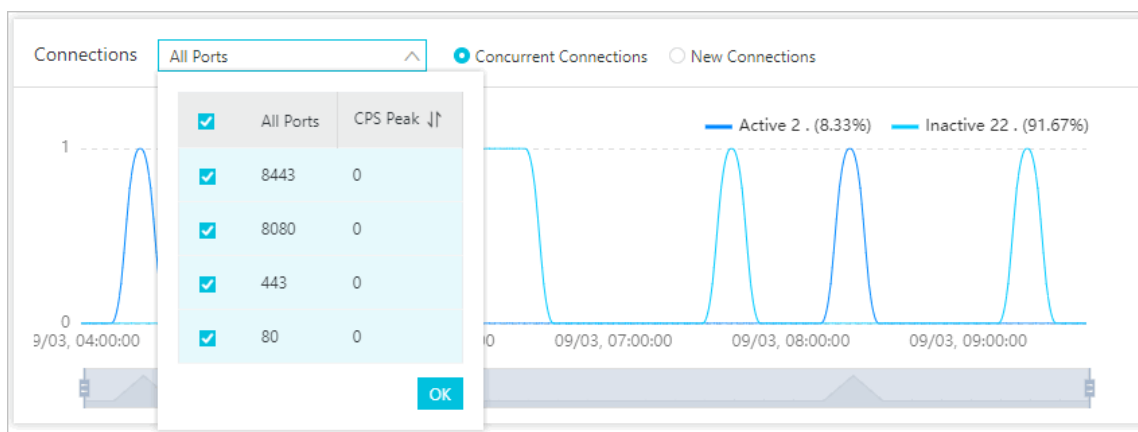
#### • Port Connections

- **Concurrent Connections:** The total number of concurrent TCP connections established between clients and the Anti-DDoS Premium instance.
- **New Connections:** The total number of new TCP connections established between clients and the Anti-DDoS Premium instance per second.



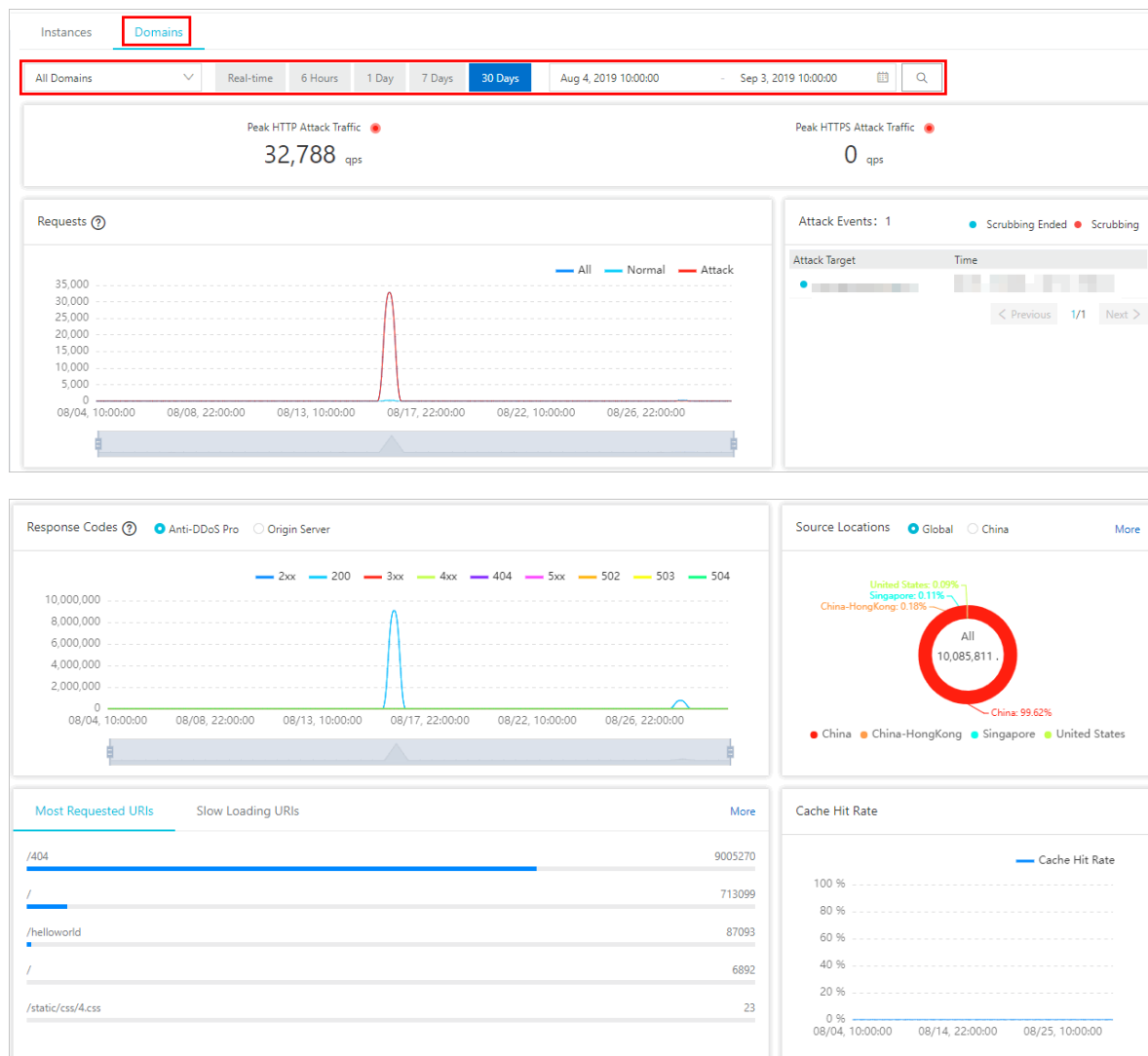
#### Note:

When only one instance is selected, the chart displays the numbers of different port connections to the instance. When two or more instances are selected, the chart displays the total number of port connections.



#### • The distribution of traffic for Source Locations and ISPs

- Click the Domains tab, select one or more domains, and specify a time range to view the corresponding metrics.



You can view the following information about the selected domains:

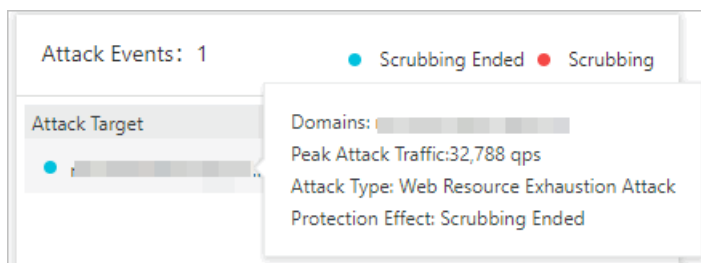
- The Peak HTTP Attack Traffic and the Peak HTTPS Attack Traffic
- The Requests trend chart

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

- If the time range is less than an hour, the granularity is one minute.
- If the time range is between 1 to 6 hours, the granularity is 10 minutes.
- If the time range is between 6 to 24 hours, the granularity is 30 minutes.
- If the time range is between 1 to 7 days, the granularity is one hour.
- If the time range is between 7 to 15 days, the granularity is 4 hours.

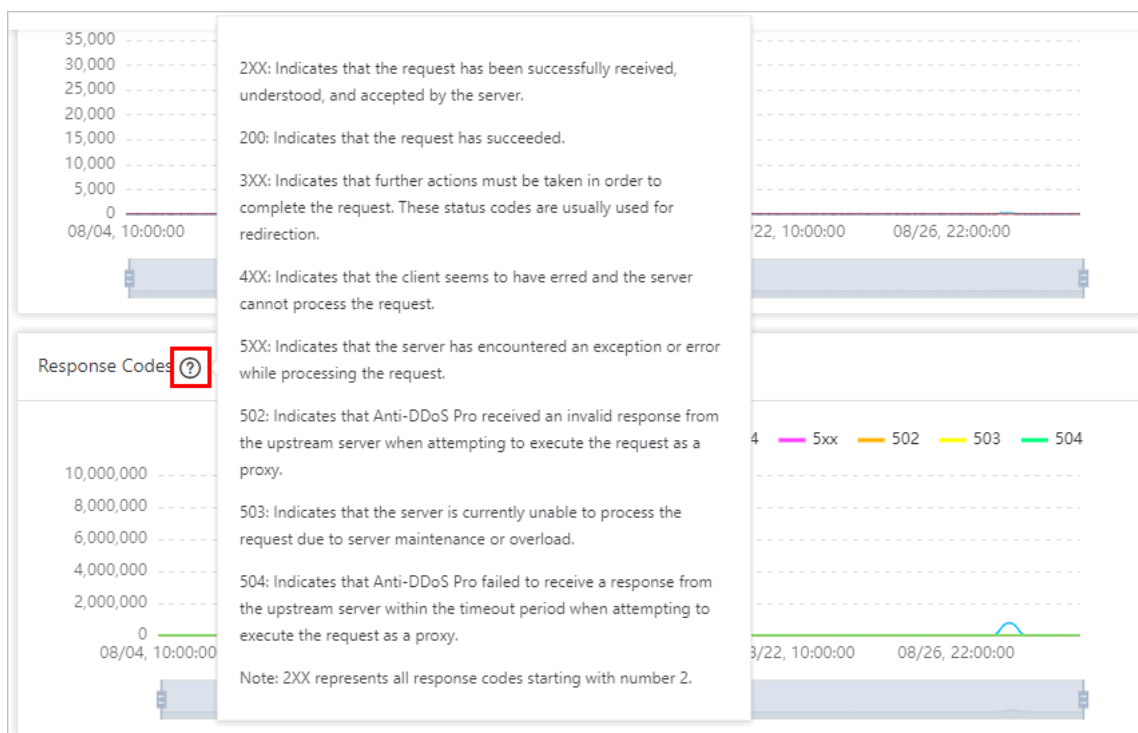
- For other time ranges, the granularity is 12 hours.
- Application Layer Attack Events

Move the pointer over a domain to view attack details, such as the attack type and peak attack traffic.



- Response Codes information

The trend of response codes displays the accumulated numbers of response codes within the queried time range. This range is the same as the time range used in the Requests trend chart. You can move the pointer over the question mark icon to find the explanation for the response codes.



- The traffic Source Locations
- Most Requested URIs and Slow Loading URIs
- The trend chart for the Cache Hit Rate



Note:

You must enable the Static Page Caching feature before you can view the trend for the cache hit rate. For more information, see [#unique\\_22](#).

## 4.5 Import or export provisioning settings

If you have multiple provisioning settings of website domain or layer-4 forwarding, and you want to back up or migrate the service provisioning settings, you can quickly complete such operations through the import/export functionalities of the provisioning settings.

- The import/export of layer-4 forwarding rule settings supports the TXT format.
- The import/export of website domain provisioning settings supports the XML format with high compatibility.

The XML format has more parameter extensibility and readability than the TXT format. Additionally, the import/export also supports the provisioning setting that uses a domain as the origin site.

### Bulk import website domain name Configuration

1. Log on to the [Anti-DDoS Premium Service console](#).
2. Go to Provisioning > Website, click Import at the bottom of the domain setting list to add provisioning settings for multiple domains.

3. In the Add Multiple Rules dialog box, enter the domain setting parameters in the specified XML format.

Add Multiple Rules

View the Sample

```

<DomainList>
<DomainConfig>
<Domain>a.com</Domain>
<ProtocolConfig>
<ProtocolList>http,https</ProtocolList>
</ProtocolConfig>
<InstanceConfig>
<InstanceList>ddosDip-cn-v0h0v9a3x07</InstanceList>
</InstanceConfig>
<RealServerConfig>
<ServerType>0</ServerType>
<ServerList>1.2.3.4</ServerList>
</RealServerConfig>
</DomainConfig>
<DomainConfig>
<Domain>b.com</Domain>
<ProtocolConfig>
<ProtocolList>http,websocket,websockets</ProtocolList>
</ProtocolConfig>
<InstanceConfig>
<InstanceList>ddosDip-cn-v0h0v9a3x07,ddosDip-cn-0pp0u9slr01</InstanceList>
</InstanceConfig>
<RealServerConfig>
<ServerType>1</ServerType>
<ServerList>q840a82zf2j23afs.qfvip05al.com</ServerList>
</RealServerConfig>
</DomainConfig>
</DomainList>

```

Next
Cancel





#### Note:

You can copy and paste the content in the text box.

#### • Parameter definition

The domain setting parameter content must start with `< DomainList >`, and end with `</ DomainList >`. Between these two tags, there is the domain provisioning setting parameters to be imported. The parameters of each domain provisioning setting start with `< DomainConf ig >` and end with

`</ DomainConf ig >`. For details about corresponding parameters for the domain provisioning setting, see the following table.

Parameter	Description
<code>&lt; Domain &gt; a . com &lt;/ Domain &gt;</code>	Domain name to be provisioned. You can enter only one domain in this parameter.
<code>&lt; ProtocolCo nfig &gt; &lt; ProtocolLi st &gt; http , https &lt;/ ProtocolLi st &gt; &lt;/ ProtocolCo nfig &gt;</code>	Protocol type. Separate multiple protocols with “,”. In this example, the protocols of the website domain are HTTP and HTTPS.
<code>&lt; InstanceCo nfig &gt; &lt; InstanceLi st &gt; ddoscoo - cn - 4590lwcn y0 01 &lt;/ InstanceLi st &gt; &lt;/ InstanceCo nfig &gt;</code>	Anti-DDoS Premium instance ID.   <b>Note:</b> Since each Anti-DDoS Premium instance has one dedicated anycast IP, just specify the Anti-DDoS Premium instance ID. Separate multiple Anti-DDoS Premium instance IDs with “,”.
<code>&lt; RealServer Config &gt; &lt; ServerType &gt; 0 &lt;/ ServerType &gt; &lt; ServerList &gt; 1 . 2 . 3 . 4 &lt;/ ServerList &gt; &lt;/ RealServer Config &gt;</code>	Origin site :  - <code>&lt; ServerType &gt; 0 &lt;/ ServerType &gt;</code> : For origin IP - <code>&lt; ServerType &gt; 1 &lt;/ ServerType &gt;</code> : For origin domain  In the <code>&lt; ServerList &gt; 1 . 2 . 3 . 4 &lt;/ ServerList &gt;</code> tags, specify the origin site address. Separate multiple origin site addresses with “,”.   <b>Note:</b> For one domain, you cannot set both IP and domain addresses as the origin site.

• Sample

```
< DomainList >
  < DomainConf ig >
    < Domain > a . com </ Domain >
    < ProtocolCo nfig >
      < ProtocolLi st > http , https </ ProtocolLi st >
    </ ProtocolCo nfig >
    < InstanceCo nfig >
      < InstanceLi st > ddosDip - cn - v0h0v9a3x0 7 </ InstanceLi st >
    </ InstanceCo nfig >
```

```

< RealServer Config >
< ServerType > 0 </ ServerType >
< ServerList > 1 . 2 . 3 . 4 </ ServerList >
</ RealServer Config >
</ DomainConfig >
< DomainConfig >
< Domain > b . com </ Domain >
< ProtocolConfig >
< ProtocolList > http , websocket , websockets </ ProtocolList >
</ ProtocolConfig >
< InstanceConfig >
< InstanceList > ddosDip - cn - v0h0v9a3x0 7 , ddosDip - cn -
0pp0u9slr0 1 </ InstanceList >
</ InstanceConfig >
< RealServer Config >
< ServerType > 1 </ ServerType >
< ServerList > q840a82zf2 j23afs . gfvip05al . com </ ServerList >
</ RealServer Config >
</ DomainConfig >
</ DomainList >

```

#### 4. Click Next.

After the XML content passes the validation, it is resolved to the domain provisioning settings to be imported.

#### 5. Select the domain provisioning settings to be added, and click OK to import these settings.

### Export provisioning settings of website domain

1. Go to Provisioning > Website, click Export at the bottom of the domain setting list.
2. Click OK to start an export task of current domain provisioning settings.
3. Click the Task List icon in the upper right corner of the Provisioning page, to view the progress of the export task.



- After the task completes, click Download in the Task List dialog box, to download the domain provisioning settings to your local computer.

Task List <span>×</span>			
Task	Status	Start Time	Operations
Conf Export: Webs...	<span>●</span> Preparing	01/07/2019 15:32:20	Delete
Conf Export: Webs...	<span>●</span> Done	12/27/2018 14:44:56	Delete Download

**Note:**

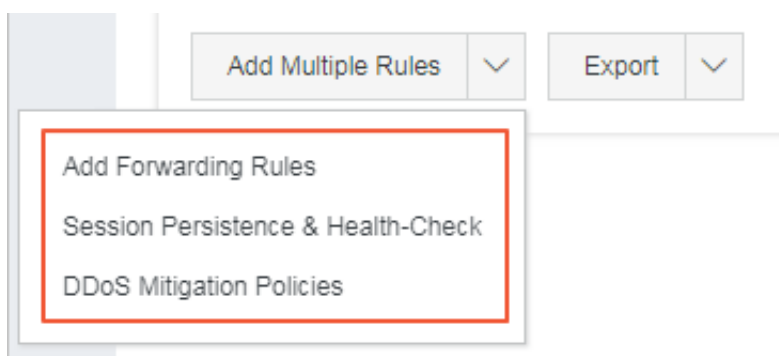
If the status of the tasks is Preparing, please be patient and wait for the export task to complete.

### Import forwarding rules

- Go to Provisioning > Non-Website page.
- Click Add Multiple Rules > Add Forwarding Rules at the bottom, to import multiple forwarding rules.

**Note:**

You can also select Session Persistence/Health-Check or DDoS Mitigation Policies to import corresponding settings.



- Refer to the samples to enter information about the settings.

- Forwarding rules

```
tcp    90    91    192 . 136 . 12 . 41
udp    22    13    12 . 14 . 1 . 23 , 10 . 23 . 4 . 12
```

From left to right, the above fields are Protocol, Forwarding Port, Origin site port, and Origin site IP.

- Session persistence/health-check settings

```
8081    tcp    4000    tcp    22    5    5    3    3
8080    tcp    4000    http   22    5    5    3    3 / search . php
www . baidu . com
```

From left to right, the above fields are Forwarding Port, Forwarding Protocol, Session Persistence Timeout, Health Check Type, Ports, Response Timeout, Check Interval, Unhealthy Threshold, Healthy Threshold, URI (Required when the health check type is http), domain (Optional when the health check type is http). "Forwarding Port" must be a forwarding port that has policies configured.

- DDoS mitigation policies

```
8081    tcp    2000    50000    20000    100000    1    1500    on    on
8080    udp    1000    50000    20000    100000    1    1500
```

From left to right, the above fields are Forwarding Port, Forwarding Protocol, New Connection Speed Limits for Source IP, Concurrent Connection Speed Limits for Source IP, New Connection Speed Limits for Destination IP, Concurrent Connection Speed Limits for Destination IP, Minimum Length of Packets, Maximum Length of Packets, and False Sources and Null Session Connections (This value is only effective for the TCP protocol. To enable the Null Session Connection setting, you must have the False Sources setting enabled).

4. Click Add to import the settings.

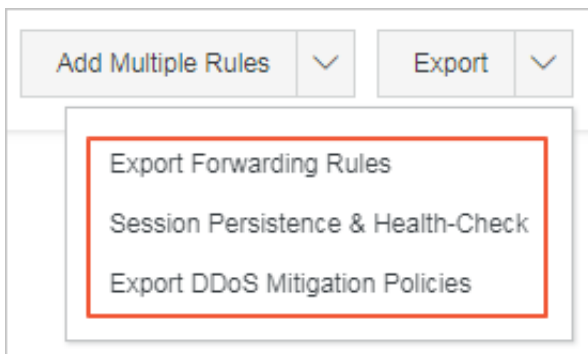
#### Export forwarding rules

1. Go to Provisioning > Non-Website page.
2. Click Export > Export Forwarding Rules at the bottom.



Note:

You can also select Session Persistence/Health-Check or DDoS Mitigation Policies to export corresponding settings.



3. In the prompt box, click OK, to start an export task for current forwarding rules.
4. Click the Task List icon in the upper right corner of the Provisioning page, to view the progress of the export task.
5. After the task completes, click Download in the Task List dialog box, to download the forwarding rule settings to your local computer.



**Note:**

If the status of the tasks is Preparing, please be patient and wait for the export task to complete.