

Alibaba Cloud

Anti-DDoS Basic

Anti-DDoS Pro Service

Issue: 20190424

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. |  Danger: 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. |  Warning: 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. |  Notice: 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. |  Note: You can use Ctrl + A to select all files. |
| > | Multi-level menu cascade. | Settings > Network > Set network type |
| Bold | 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 |
| 1 Product Introduction..... | 1 |
| 1.1 What is Anti-DDoS Pro..... | 1 |
| 1.2 How Anti-DDoS Pro works..... | 1 |
| 1.3 Features..... | 2 |
| 1.4 Benefits..... | 3 |
| 1.5 Scenarios..... | 4 |
| 2 Pricing..... | 5 |
| 2.1 Purchase guide..... | 5 |
| 2.2 Billing method..... | 6 |
| 2.3 Renew an instance..... | 11 |
| 2.4 Description of overdue status..... | 11 |
| 2.5 Improve protection capability..... | 11 |
| 3 Quick Start..... | 13 |
| 3.1 Web service..... | 13 |
| 3.1.1 Implement Anti-DDoS Pro for a website..... | 13 |
| 3.1.2 Enable Anti-DDoS Pro instances..... | 13 |
| 3.1.3 Step 1. Set up HTTP protection..... | 14 |
| 3.1.4 (Optional) Step 1: Set up HTTPS protection..... | 16 |
| 3.1.5 Step 2. Whitelist local IP subnet..... | 18 |
| 3.1.6 Step 3. Verify local settings..... | 19 |
| 3.1.7 Step 4. Update DNS settings..... | 20 |
| 3.2 Non-Web service..... | 20 |
| 3.2.1 Implement Anti-DDoS Pro for a non-web service..... | 20 |
| 3.2.2 Step 1. Set up layer 4 port protection..... | 21 |
| 3.2.3 Step 2. Whitelist local IP subnet..... | 22 |
| 3.2.4 Step 3. Verify local settings..... | 23 |
| 3.2.5 (Optional) Step 4. Update DNS settings..... | 24 |
| 4 User Guide..... | 26 |
| 4.1 Provisioning guide..... | 26 |
| 4.1.1 Website service provisioning with CNAME..... | 26 |
| 4.1.2 Non-website service provisioning with CNAME..... | 27 |
| 4.1.3 Description of CNAME access..... | 29 |
| 4.1.4 Enable CNAME auto switch..... | 30 |
| 4.1.5 Modify origin IP in provisioning settings..... | 30 |
| 4.1.6 Modify domain's forwarding line and origin settings..... | 31 |
| 4.1.7 Description of Anti-DDoS Pro ISP line resolution..... | 35 |
| 4.2 Layer-7 Protection Settings..... | 35 |

| | |
|--|-----------|
| 4.2.1 HTTP(S) flood protection mode..... | 35 |
| 4.2.2 Blacklist and whitelist settings..... | 38 |
| 4.2.3 Deactivate black hole..... | 39 |
| 4.2.4 Flow block..... | 41 |
| 4.3 Layer-4 Protection Settings..... | 42 |
| 4.3.1 Layer-4 cleaning mode..... | 42 |
| 4.3.2 Health check settings for non-website service..... | 45 |
| 4.3.3 DDoS defense police settings for non-website service..... | 47 |
| 4.3.4 Session persistence settings for non-website services..... | 49 |
| 4.4 Instance management..... | 49 |
| 4.4.1 Disable and remove certain lines..... | 49 |
| 4.4.2 Change ECS IP..... | 50 |
| 4.5 Reporting..... | 51 |
| 4.5.1 View the security report..... | 51 |
| 4.5.2 Set alarm notifications for DDoS events..... | 52 |
| 4.6 Logging..... | 52 |
| 4.6.1 Operation log..... | 52 |
| 4.6.2 Full log..... | 53 |
| 4.7 Managed Security Service of DDoS Protection..... | 56 |
| 5 Best Practice..... | 60 |
| 5.1 Configure a multi-line Anti-DDoS Pro instance to pass traffic back to multiple origin sites..... | 60 |
| 5.2 How can origins outside Alibaba Cloud get clients' real IP addresses?..... | 61 |
| 5.3 How to determine the attack type by using Anti-DDoS Pro?..... | 63 |
| 5.4 How to migrate the service from the original Anti-DDoS Pro instance to a new one?..... | 64 |
| 5.5 What measures I must take if the source IP gets exposed..... | 64 |
| 5.6 Obtain the real IP address of a visitor..... | 66 |
| 5.7 Protect origin sites that use Anti-DDoS Pro..... | 68 |
| 6 API Reference..... | 72 |
| 7 FAQ..... | 73 |
| 7.1 502 error reported after configuring Anti-DDoS Pro..... | 73 |
| 7.2 Anti-DDoS Pro FAQ..... | 75 |
| 7.3 Troubleshoot Anti-DDoS Pro access problems..... | 83 |
| 7.4 504 errors reported when handling requests with long processing time..... | 93 |
| 7.5 How to view the Anti-DDoS Pro IP addresses?..... | 94 |
| 7.6 Elastic protection FAQ..... | 94 |
| 7.7 Fail to upload large files on the website with Anti-DDoS Pro enabled..... | 96 |
| 7.8 Security group rule misconfiguration results into access exceptions..... | 97 |
| 7.9 HTTPS access exceptions arising from SNI compatibility..... | 97 |
| 7.10 How to convert an HTTPS certificate to the PEM format..... | 100 |
| 7.11 Description of HTTPS exception status..... | 102 |
| 7.12 Troubleshoot certain port access failure..... | 102 |

| | |
|---|-----|
| 7.13 Why does system prompt “Parameter format error” when I try to upload an HTTPS certificate..... | 104 |
| 7.14 What is the difference between Web Service and Non-Web Service?..... | 105 |

1 Product Introduction

1.1 What is Anti-DDoS Pro

Alibaba Cloud Anti-DDoS Pro is a paid service that features a set of high-defensive IPs, and acts as a protective barrier for the origin. It safeguards network servers under high volume DDoS attacks. After configuring the high defensive IPs for the network servers, all traffic passes through the Anti-DDoS Pro instance before rerouting to the origin.

Anti-DDoS Pro supports a peak protection bandwidth of 20Gbps ~ 600Gbps on servers inside and outside Alibaba Cloud. To make it more cost-effective, you are offered various flexible payment plans. Wherein, the fees are incurred according to the daily attack volumes.

Anti-DDoS Pro cleans all traffic, mitigates DDoS attacks, and then forward traffic to the origin. With malicious traffic mitigated, the origin gains higher availability and stability.

Additionally, with Anti-DDoS Pro enabled, traffic traction and re-injection are not necessary when your origin suffers DDoS attacks.

1.2 How Anti-DDoS Pro works

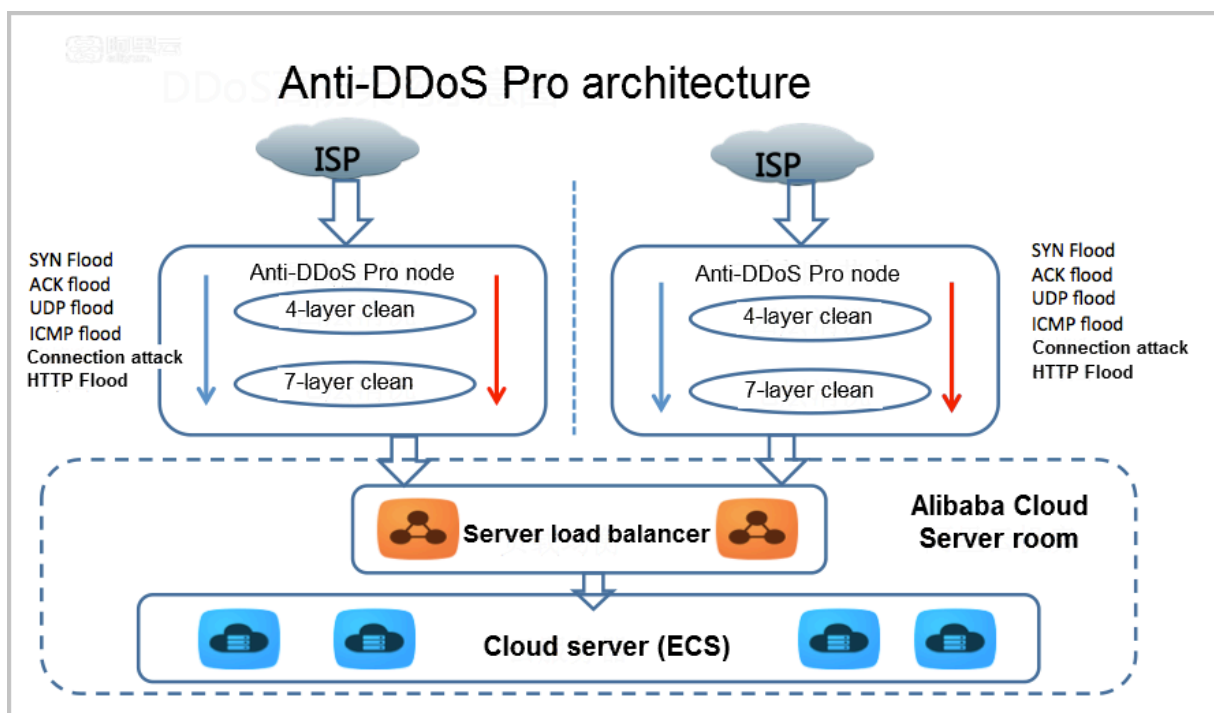
Alibaba Cloud Security Anti-DDoS Pro service is an attack protection service designed by the Alibaba Cloud research and development team.

Anti-DDoS Pro provides DDoS, HTTP flood, and WAF protection services, and is capable to defend against three to seven layers of DDoS attacks such as SYN flood, UDP flood, ACK flood, ICMP flood, DNS query flood, NTP reply flood, HTTP flood attack, and Web application attacks.

After purchasing the Anti-DDoS Pro service, you must resolve your domain name to the Anti-DDoS Pro IP and set forwarding rules to Anti-DDoS Pro. For web service, the domain name needs to be directed to the Anti-DDoS IP, and for non-web service, the service IP needs to be replaced with the Anti-DDoS Pro IP.

This configuration directs all public network traffic to the Anti-DDoS server room. The user access traffic is forwarded to the origin site IP by using port protocol

forwarding. Meanwhile, the malicious attack traffic is cleaned and filtered through the Anti-DDoS Pro service, and normal traffic is returned to the origin site IP. This entire process ascertains the stable access to the origin site IP and protects services.



1.3 Features

Alibaba Cloud Anti-DDoS Pro guarantees the stability of cloud service through the following features.

- Protects against most common DDoS attacks

The malicious attacks include but are not limited to: ICMP Flood, UDP Flood, TCP Flood, SYN Flood, and ACK Flood.

The detailed functions of Anti-DDoS Pro are as follows:

| Type | Feature | Description |
|-------------------|-----------------------------|--|
| Attack protection | Malformed message filtering | Filters out frag flood, smurf, stream flood, and land flood attacks. |
| Attack protection | Malformed message filtering | Filters out malformed IP packets, TCP packets, and UDP packets. |

| Type | Feature | Description |
|-------------------|---|--|
| Attack protection | DDoS attack protection on transport layer | Filters out Syn flood, Ack flood, UDP flood, ICMP flood, and Rstflood attacks. |
| Attack protection | DDoS attack protection on web application layer | Filters out HTTP Get flood, HTTP Post flood, and high frequency attacks, and supports HTTP feature filtering, URI filtering, and host filtering. |

- Configurable high-defensive IPs

The defense IPs can be modified at any time to achieve more diverse and targeted protection.

- Flexible management

The DDoS protection threshold can be configured to conduct more suitable protective measures. Without creating any interruptions to the entire process, it can be upgraded to a more advanced protection version.

- Detailed security report

The report helps to present all the necessary information to provide insights on the security environment. Moreover, the network traffic is monitored in real time that makes sure that the attacks are identified in time.

1.4 Benefits

Alibaba Cloud Anti-DDoS Pro has the following advantages.

- Protection against high-volume DDoS attacks

Proven successful is mitigating over 1 Tbps DDoS attacks.

Protects against all types of DDoS attacks based on network layer, transport layer, and application layer.

- Precisely targeted protection

Provides dedicated protection policies respectively for businesses such as e-commerce, encryption, 7-layer applications, intelligent terminals, and online protection service.

- Invisibility of origin resources

The origin IPs are replaced and concealed through the Alibaba Cloud Security service. The security resources work in front of the origin to prevent the attack from locating the origin resources.

- Flexible management

The DDoS protection can be upgraded to the professional edition with simple and quick operation. In addition, the process requires no physical equipment, and causes no interruption to the whole service.

- High availability and reliability

Based on auto detection, attack policy matching, real-time protection, and cleaning service, this service guarantees a 99.99% availability.

1.5 Scenarios

Alibaba Cloud Security Anti-DDoS Pro serves all customers in and out of Alibaba Cloud.

This service provides protection against the network attacks to the sector such as finance, entertainment (games), media, e-commerce, and government.

For businesses with high real-time user experience requirements, Anti-DDoS Pro provides excellent protection. These business include instant combat games, web games, online finance, e-commerce, online education, and O2O.

2 Pricing

2.1 Purchase guide

To purchase Anti-DDoS Pro instances, follow these steps.

Procedure

1. Log on to the [Anti-DDoS Pro purchase page](#).

Basic Configuration

ISP

CT, CU

CT, CU and CM

International

China Telecom and China Unicom are included

IP Count

2 ip

Each IP has independent resource reserved for DDoS protection. A post-pay bill will be generated when the attack traffic exceeds the basic capacity of protection.

Basic

| | | | | | |
|-------|-------|-------|------|------|------|
| 5Gb | 10Gb | 20Gb | 30Gb | 40Gb | 50Gb |
| 100Gb | 150Gb | 200Gb | | | |

This is the basic monthly pre-pay package. If you need more capacity, elastic protection packages are provided for mitigating attack which exceeds the basic capacity, additional fee will be charged based on each single day's maximum attack volume.
The maximum basic capacity of China Mobile is 150Gb!

Burstable

5Gb 30Gb

The cost of scaling bandwidth is post-pay mode, and based on consumption.

Ports

50

Domains

50

You can purchase additional domain name packages for website protection.

Clean Bandwidth

500M

1000M

2000M

100 M

Purchase Plan

Quantity

1

Plan

1 month

2

3

4

5

6

1 yr


2 yr

3 yr

☐ Auto Renew

?

2. Select ISP, Basic, Burstable, Ports, Domains, Clean Bandwidth, Quantity, and Plan according to your requirements.

| Parameters | Note |
|------------------------------|---|
| ISP | <p>Select the CT, CU or CT, CU and CM ISP line.</p> <div>  Note: If your service to be protected is not in the China Mainland region, go to purchase Anti-DDoS Premium. </div> |
| IP Count | <ul style="list-style-type: none"> Each CT, CU and CM ISP instance contains three IPs, one primary IP, and two backup IP. Each CT, CU ISP instance contains two IPs, one primary IP, and one backup IP. |
| Basic | Basic protection capacity of the Anti-DDoS Pro instance. |
| Elastic protection bandwidth | <p>Burstable protection capacity of the Anti-DDoS Pro instance. Burstable protection capacities are available when a network attack exceeds the basic capacity. An additional fee is then charged based on the daily maximum attack volume.</p> |
| Ports | The maximum number of non-web service ports that can be protected by the Anti-DDoS Pro instance. |
| Domains | The maximum number of web service domains that can be protected by the Anti-DDoS Pro instance. |
| Clean Bandwidth | The clean business bandwidth without DDoS attacks. |
| Quantity | The number of Anti-DDoS Pro instances to be purchased. |
| Length of purchase | The service duration of the Anti-DDoS Pro instance to be purchased. |

3. Click Buy Now to confirm your order and complete the payment.

2.2 Billing method

Anti-DDoS Pro uses a hybrid billing method.

Billing description

Billing type: Mixed

Unit: USD

Billing item: Basic protection and Elastic protection

Payment option: Subscription or Pay-As-You-Go

Billing cycle: Basic protection bandwidth (Unit: Gbps) and HTTP Flood protection capacity (Unit: QPS) are charged either monthly or yearly. A subscription bill is generated at purchase.

Settlement cycle: Elastic protection bandwidth (Unit: Gbps) and HTTP flood protection capacity (Unit: QPS) are charged daily. A Pay-As-You-Go bill is generated based on the actual attack peak that exceeds the basic DDoS protection capacity or HTTP flood protection capacity (only the larger billing range is counted) on the day before.

Expiry description

- You are sent reminder text messages/e-mails to renew your service seven days, three days, and one day before your upcoming expiry service.
- If you fail to renew the service after its expiry, the Anti-DDoS Pro service will be restored to the Anti-DDoS Basic protection capability.
- Your Anti-DDoS Pro configurations are retained for seven days after your service expires. If you renew the service within seven days, the protection continues without interruption. However, if the service is not renewed during this seven days grace period, your previous Anti-DDoS Pro IP gets auto released and the previous service configurations becomes unavailable.

Overdue instructions

- You receive inner-site notifications, three days before your Anti-DDoS Pro instance service expiration. You must renew your subscription. The Anti-DDoS Pro instance is disabled, if it is not renewed before its expiry. Moreover, the Anti-DDoS protection is restored to the default while having 5 GB capability offered for free.
- When your protection service expires, Anti-DDoS Pro saves your configuration for additional seven days. If the service is renewed within these seven days, the Anti-DDoS Pro protection continues. Otherwise, the IP address of the Anti-DDoS Pro instance is released and the service becomes unavailable.

Pricing

Basic protection (monthly subscription)

**Note:**

HTTP flood protection capacity is the protection capacity against HTTP flood attacks. If your normal business consumes a large number of QPS, choose an appropriate package accordingly.

| DDoS protection capacity | HTTP flood protection capacity | China Telecom + China Unicom (USD /Month) | China Telecom + China Unicom + China Mobile (USD/ Month) |
|--------------------------|--------------------------------|---|--|
| 5 Gbps | 15,000 QPS | 600 | - |
| 10 Gbps | 30,000 QPS | 1,310 | - |
| 20 Gbps | 60,000 QPS | 2,490 | 2,956 |
| 30 Gbps | 100,000 QPS | 3,970 | 4,686 |
| 40 Gbps | 130,000 QPS | 6,920 | 7,988 |
| 50 Gbps | 160,000 QPS | 9,880 | 11,290 |
| 100 Gbps | 300,000 QPS | 29,100 | 32,516 |
| 150 Gbps | 450,000 QPS | 36,490 | 41,164 |
| 200 Gbps | 600,000 QPS | 42,410 | 48,239 |
| 300 Gbps | 1,000,000 QPS | - | Discount Price: 62,580 Per Year |
| > 300 Gbps | > 1,000,000 QPS | Contact sales | |

Elastic protection (daily Pay-As-You-Go)

| DDoS attack peak | HTTP flood attack peak | China Telecom + China Unicom (USD /Day) | China Telecom + China Unicom + China Mobile (USD/ Day) |
|----------------------------------|--|---|--|
| Attack peak \leq 20 Gb | Attack peak \leq 60,000 QPS | Covered by monthly basic protection package | |
| 20 Gb < Attack peak \leq 30 Gb | 60,000 QPS < Attack peak \leq 100,000 QPS | 270 | 270 |
| 30 Gb < Attack peak \leq 40 Gb | 100,000 QPS < Attack peak \leq 130,000 QPS | 470 | 470 |
| 40 Gb < Attack peak \leq 50 Gb | 130,000 QPS < Attack peak \leq 160,000 QPS | 660 | 660 |

| | | | |
|-------------------------------|---|-------|-------|
| 50 Gb<Attack peak ≤60 Gb | 160,000 QPS<Attack peak≤200,000 QPS | 860 | 860 |
| 60 Gb<Attack peak ≤70 Gb | 200,000 QPS<Attack peak≤230,000 QPS | 1,350 | 1,350 |
| 70 Gb<Attack peak ≤80Gb | 230,000 QPS<Attack peak≤260,000QPS | 1,650 | 1,650 |
| 80Gb<Attack peak≤ 100Gb | 260,000QPS<Attack peak≤300,000 QPS | 1,940 | 1,940 |
| 100 Gb<Attack peak ≤150 Gb | 300,000 QPS<Attack peak≤450,000 QPS | 2,440 | 2,440 |
| 150 Gb<Attack peak ≤200 Gb | 450,000 QPS<Attack peak≤600,000 QPS | 2,830 | 2,830 |
| 200 Gb<Attack peak ≤300 Gb | 600,000 QPS<Attack peak≤1,000,000 QPS | 3,900 | 3,900 |
| 300 Gb<Attack peak ≤400 Gb | 1,000,000 QPS< Attack peak≤1,500, 000 QPS | 6,300 | 6,300 |
| 400 Gb<Attack peak ≤500 Gb | 1,500,000 QPS< Attack peak≤2,000, 000 QPS | 7,900 | 7,900 |
| 500 Gb<Attack peak ≤600 Gb | 2,000,000 QPS< Attack peak≤2,500, 000 QPS | 9,500 | 9,500 |

**Note:**

- Daily Pay-As-You-Go pricing of elastic protection is calculated for each individual Anti-DDoS Pro instance that has the elastic protection capacity enabled. If more than one Anti-DDoS Pro instances are attacked, then all the affected instances are charged.
- Elastic protection payment is calculated based on the actual attack peak that exceeds the basic DDoS protection capacity or HTTP flood protection capacity (only the larger billing range is counted) one day before.
- If you do not want to enable elastic protection, set the elastic protection bandwidth to the same as the basic protection bandwidth. After this action, Anti-DDoS Pro instance will no longer have the elastic protection capacity.

Limits

| Specification | Limit | Description |
|-----------------------------|---------------------|--|
| Bandwidth | 100 Mbps/instance | Bandwidth consumed by normal business traffic in non-DDoS attack status. |
| QPS (For web service) | 3,000 QPS/instance | QPS consumed by normal business request in non-DDoS attack status. |
| Forwarding port volume | 50/IP address | Number of entries supported by TCP/UDP forwarding. |
| Protected domain volume | 50/IP address | Number of entries supported by HTTP/HTTPS forwarding. Wildcard domain name forwarding is supported and only occupies one forwarding entry. |
| Number of servers protected | 20 servers/instance | The total number of different IP addresses configurable for four-layer and seven-layer configuration. |
| New connection volume | 50,000/VIP | The number of new connections for single VIP. |
| Concurrent connection | 200,000/VIP | The number of concurrent connections for single VIP. |



Note:

- If you use an Alibaba Cloud web server, you can enjoy a maximum of business bandwidth of 200 Mbps.
- The bandwidth limits applies to both IN and OUT directions.
- The preceding plans are only available online. To meet the growing demands of your business, you can Contact sales for a customized solution.

Renew and upgrade service

You can renew or upgrade your service.

- **Renew:** After topping up your account, you can select to prolong the service cycle of the Anti-DDoS service.
- **Upgrade:** You can upgrade your instance to increase the bandwidth, domain or port volumes.

2.3 Renew an instance

Follow these steps to renew your Anti-DDoS Pro instance in the Anti-DDoS console.

Procedure

1. Log on to the [Alibaba Cloud Security](#) console.
2. Go to Anti-DDoS > Anti-DDoS Pro > Instance List, and then click Renew under the target instance.
3. Select an expected duration of the service, and then complete the payment.

2.4 Description of overdue status

You receive text message or email notifications, three days before your Anti-DDoS Pro instance service expiration. You must renew your subscription.

The Anti-DDoS Pro instance is disabled, if it is not renewed before its expiry.

Moreover, the Anti-DDoS protection is restored to the default while having 5 GB capability offered for free.

When your protection service expires, Anti-DDoS Pro saves your configuration for additional seven days. If the service is renewed within these seven days, the Anti-DDoS Pro protection continues. Otherwise, the IP address of the Anti-DDoS Pro instance is released and the service becomes unavailable.

2.5 Improve protection capability

You can increase the Anti-DDoS Pro bandwidth to increase the QPS of your HTTP and HTTPS services.



Note:

Because HTTPS consumes more resources, it may show less improvement in comparison to HTTP.

The default service bandwidth for each Anti-DDoS Pro instance is 100 Mbps, and the normal QPS limits for HTTP and HTTPS are both 3000. The default specifications can be improved as described in the following table.

| Additional bandwidth (Mbps) | HTTP QPS increment | HTTPS QPS increment |
|-----------------------------|--------------------|---------------------|
| 50 | 1,500 | 300 |
| 100 | 3,000 | 600 |
| 1,500 | 4,500 | 900 |
| 200 | 6,000 | 1,200 |
| 500 | 15,000 | 3,000 |
| 1,000 | 30,000 | 6,000 |
| 2,000 | 60,000 | 12,000 |

3 Quick Start

3.1 Web service

3.1.1 Implement Anti-DDoS Pro for a website

This tutorial explains a simple setup and verification process for Anti-DDoS Pro website protection through the Alibaba Cloud console. It does not cover all possible options.

Audience

This tutorial is suitable for users who:

- Are interested in learning how Anti-DDoS Pro works.
- Have purchased Anti-DDoS Pro and need to know how to set it up.
- Want to test, verify, modify, or delete Anti-DDoS Pro configurations.

Quick start flow

To set up basic website protection, complete the following tasks:



Note:

Before you begin, make sure that your Anti-DDoS Pro instance is enabled. To do this, see [Enable Anti-DDoS Pro instances](#).

1. [Set up HTTP protection](#) or [set up HTTPS protection \(optional\)](#).
2. [Whitelist local IP subnet](#).
3. [Verify local settings](#).
4. [Update DNS settings](#).

3.1.2 Enable Anti-DDoS Pro instances

After purchasing an Anti-DDoS Pro instance, you have to enable the instance before you set up website or non-website protection for your business.

Procedure

1. Log on to the [Anti-DDoS Pro console](#), and click Instance List.

2. Select the region, and then locate the Anti-DDoS Pro instance you want to enable.

The screenshot shows the 'Instance List' page in the Anti-DDoS Pro console. The 'International' tab is active. A search bar is at the top. Below it, a table lists instances. The first instance is 'ddosBag-cn-...' with a status of 'Normal' and 'Clean traffic: 100M'. The second instance is 'ddosBag-cn-...' with a status of '--' and 'Clean traffic: 100M'. The 'Enable immediately' link for the second instance is highlighted with a red box.

3. Click Enable immediately.

4. Select the line, and then click Enable now.

The screenshot shows the 'Enable now' dialog box. It contains a message: 'Before enabling, select the respective lines:'. Below this, a note says: 'Note: We suggest selecting the lines nearest to the users of your service. Once selected, this cannot be changed'. Under 'International Line', the 'East US' button is selected. At the bottom, the 'Enable now' button is highlighted with a red box, and a 'Cancel' button is also visible.

Result

After the Anti-DDoS Pro instance is enabled, you can now set up website or non-website protection for your business with the Anti-DDoS Pro instance.

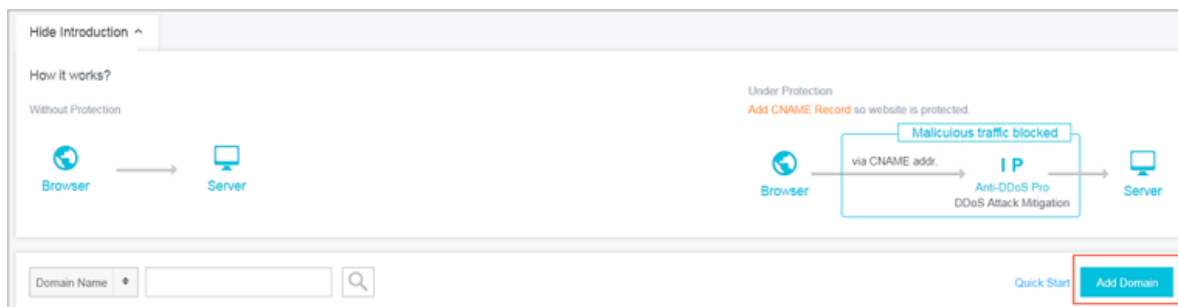
3.1.3 Step 1. Set up HTTP protection

HTTP website protection only supports TCP 80 port. If your web service needs to run on other ports, such as 8080, select layer 4 port (non-website access) protection.

Procedure

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

2. Go to Access > Web Service, and then click Add Domain to add the domain that you want to protect.



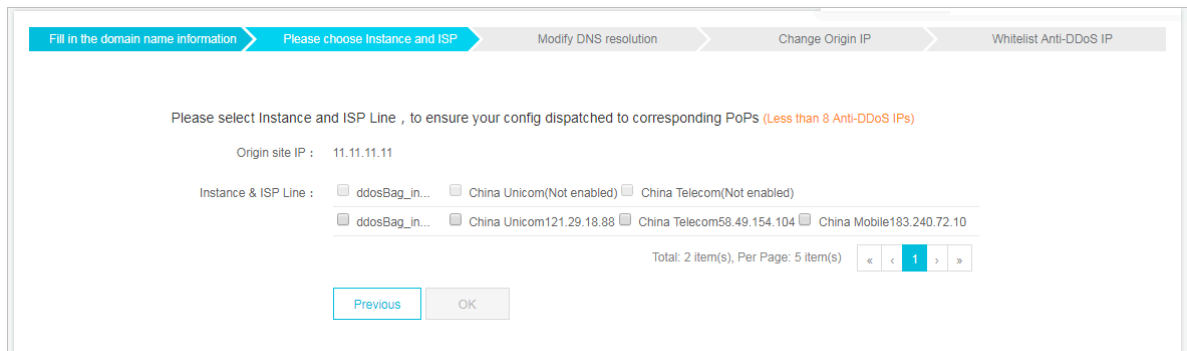
3. Input Domain Name, and Origin site domain or Origin site IP address accordingly.



Note:

- Domain name supports wildcard names. For example, “*.abc.com” can be used to match “www.abc.com”, “mail.abc.com”, and “blog.abc.com”.
- Up to 50 domain names can be added to a virtual IP address for HTTP forwarding.
- More than one origin IP address can be added. Multiple origin IP addresses must be separated by commas.
- Up to 20 origin IP addresses can be added to a domain name.

4. Click Next, and then select Anti-DDoS Pro instances and ISP lines for the domain.



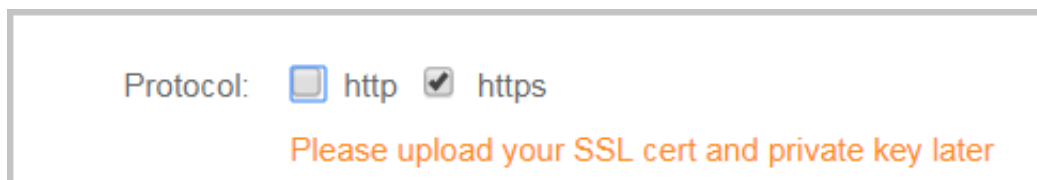
5. Click OK. A new domain entry will be added.
6. Click Setting under the created domain, and operate the HTTP Flood Protection switch to enable or disable corresponding protections, which is enabled by default.

3.1.4 (Optional) Step 1: Set up HTTPS protection

HTTPS website protection only supports TCP 443 port. If your web service needs to run on other ports such as 4433, select layer four port (non-website access) protection.

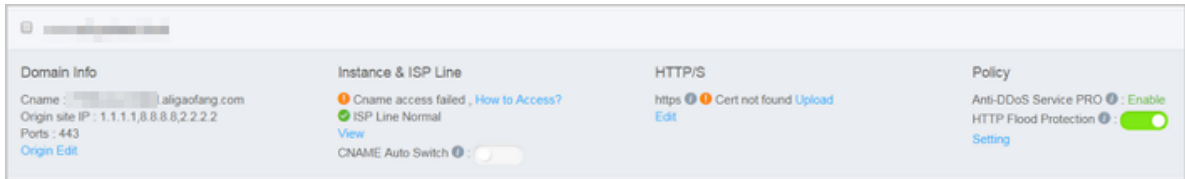
Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. Go to Access > Web Service, and then click Add Domain to add the HTTPS website domain that you want to protect.
3. Input Domain Name and Origin site domain or Origin site IP address accordingly.
4. For HTTPS protection, select https for the Protocol option, and Port 443 will be automatically added to Origin site port.



5. Click Next, and then select Anti-DDoS Pro instances and ISP lines for the domain.
6. Click OK. A new domain entry will be added.

- Click Upload under the HTTP/S column to enter the Upload certificate and private key page.



- Copy and paste the certificate and private key information, and click Upload.

General certificates, such as *.pem, *.cer, and *.crt certificates, can be opened in text editor tools. For other special certificate formats (for example, *.pfx, and *.p7b), you have to convert the certificate to *.pem format in advance.



Note:

If multiple certificate files (for example, certificate chain file) involved, you can combine the certificate information first and upload the certificate information.

Certificate file sample:

```
----- BEGIN CERTIFICATE -----
62EcYPWd20 y1vs6MTXcJ Sfn9Z7rZ9f mxWr2BFN2X bahgnsSXM4
8ixZJ4krc + 1M + j2kcubVpsE 2
cgHdj4v8H6 jUz9Ji4mr7 vMNS6dXv8P Ukl / qoDeNGCNdy TS5NIL5ir +
g92cL8IG0k jgvhlqt9vc
65Cgb4mL + n5 + DV9u0yTZTW / MojmlgfUek C2xiXa54nx Jf17Y1TADG
SbyJbsC0Q9 nIrHsPl8YK k
vRWvIAqYxX Z7wRwWwMv4 TMxFhWRiNY 7yZIo2ZUhl 02SIDNggIE eg ==
----- END CERTIFICATE -----
```

Private key sample:

```
----- BEGIN RSA PRIVATE KEY -----
DADTPZoOHd 9WtZ3UKHJT RgnQmioPQn 2bqdKHop + B / dn / 4VZL7Jt8zS
DGM9sTMThL yvsmLQKBgQ
Cr + ujntC1kN6p GBj2Fw2l / EA / W3rYEce2ty hjgmG7rZ + A /
jVE9fld5sQ ra6ZdwBcQJ aiyoIYo
aMF2EjRwc0 qWHalUq0C1 5f6ujSoHh2 e + D5zdmkTg / 3NKNjqNv6x
A2gYpinVDz FdZ9Zujxvu h9o
4Vqf0YF8bv 5UK5G04RtK ad0w ==
----- END RSA PRIVATE KEY -----
```

- Click OK to complete the certificate upload.



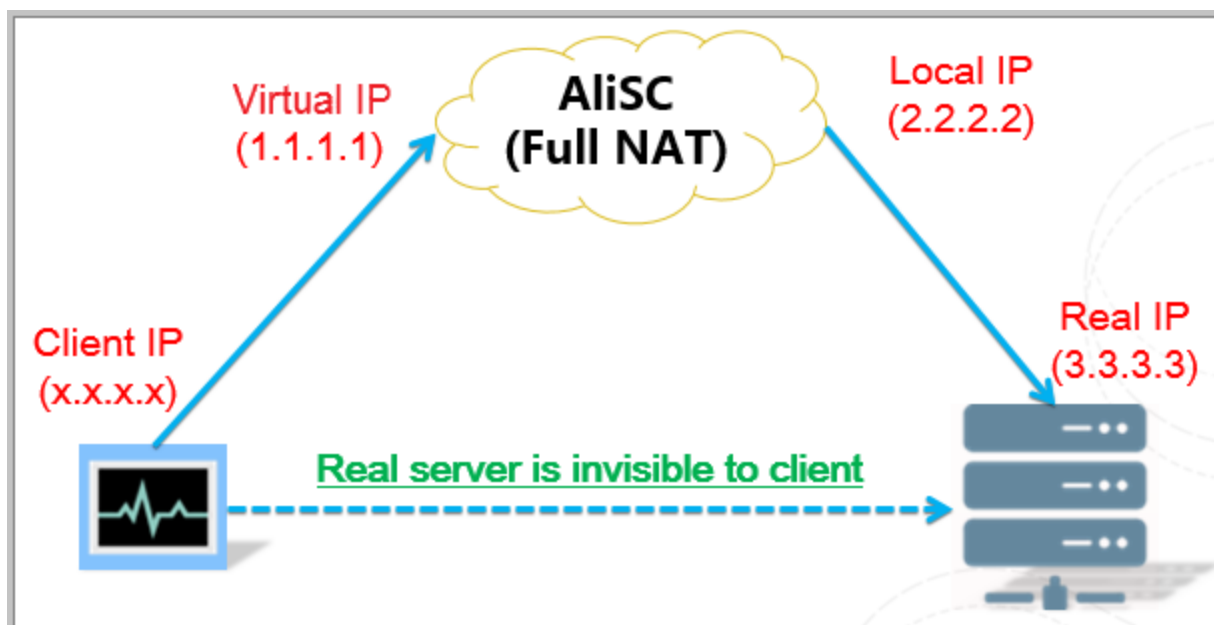
Note:

Up to five HTTPS forwarding rules can be added. This includes configuring both HTTP and HTTPS in one forwarding rule.

3.1.5 Step 2. Whitelist local IP subnet

The Alibaba scrubbing center (AliSC) of Anti-DDoS Pro acts as a reverse proxy. It makes sure the client server remains invisible to the origin server. AliSC handles all requests from clients by blocking malicious requests while forwarding legitimate requests to the origin. Therefore, malicious traffic is mitigated when it goes through Anti-DDoS Pro.

In Full-NAT proxy mode, Anti-DDoS Pro uses the local IP as the source IP to establish connection with the origin server, as illustrated in the following figure.



- Multiple local IP addresses are available because AliSC has multiple physical servers.
- In Full NAT mode, each packet's source IP address will be a local IP address.
- The origin server must whitelist all existing local IP addresses that are fixed to guarantee accessibility.
- AliSC uses local IP addresses to visit IDC network and keeps the real client IP address in HTTP/HTTPS header's X-forwarded-for field.

For origin, Anti-DDoS Pro makes source IP addresses more concentrated, and improves the transmission speed of packets from them. In this case, however, the local IPs may be determined as suspicious to the origin server's firewall or security software (if such software is applied). In case of the local IP being blocked or limited, make sure all the local IPs are whitelisted before being diverted to Alibaba Cloud.

For a deeper level of safety consideration, we recommend that you block all requests to the origin server from IP addresses except local IP addresses. By doing this, the origin is better protected even if the real IP addresses are disclosed.

Procedure

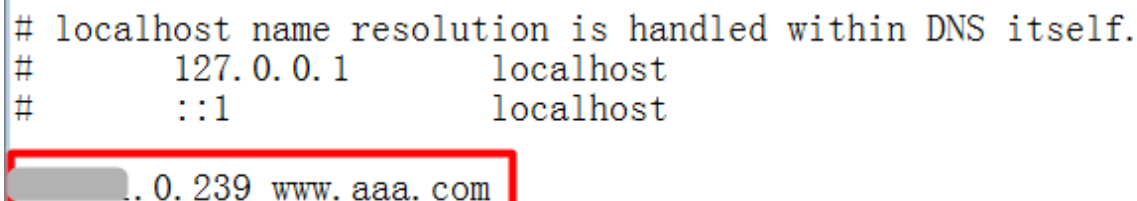
1. Log on to the [Anti-DDoS Pro console](#).
2. Go to Access > Web Service, and then select the domain name to be configured, and click Setting under the Policy column.
3. Click Setting of Black & White List, and then add the existing local IP addresses to the whitelist.

3.1.6 Step 3. Verify local settings

Before you update DNS settings and route all the traffic to Anti-DDoS Pro, we recommend that you verify the forwarding settings locally to guarantee availability.

Procedure

1. Manually bind the virtual IP address provided by Anti-DDoS Pro with the domain name in your local hosts file (for example, `C : \ Windows \ System32 \ drivers \ etc \ hosts`, in Windows). The domain name is then resolved to Alibaba Cloud' s IP address solely on your local device.



```
# localhost name resolution is handled within DNS itself.  
#          127.0.0.1      localhost  
#          ::1           localhost  
[redacted]. 0. 239 www. aaa. com
```

The domain name is then resolved to Alibaba Cloud' s IP address solely on your local device.

2. Refresh your local DNS cache. For example, run the `ipconfig / flushdns` command at the command line interface in Windows.
3. Browse your website through the domain name in your browser.
 - If the website is opened successfully, your configuration is properly set.
 - Otherwise, check your configuration or open a ticket to contact Alibaba Cloud Technical Support.

3.1.7 Step 4. Update DNS settings

Go to the DNS configuration panel and select either CNAME or A record to update the former DNS record, depending on your DNS service provider's configuration.

After that, the traffic can be redirected to another virtual IP address (for example, backup IP address) or even to the origin site to avoid further problems.



Note:

Although both CNAME and A record are supported for rerouting traffic, we recommend that you select CNAME rather than A record to guarantee a higher success rate.

- CNAME record

Update the former DNS record with the generated CNAME. The former A record can be deleted.

The recommended TTL value is 10 minutes.

- A record

Update the former A Record with the virtual IP address provided by Anti-DDoS Pro. If multiple virtual IP addresses are available, the domain name can be resolved to a different virtual IP address.

The recommended TTL value is 10 minutes.

3.2 Non-Web service

3.2.1 Implement Anti-DDoS Pro for a non-web service

This tutorial explains a simple setup and verification process of Anti-DDoS Pro non-website protection through the Alibaba Cloud console. It does not cover all possible options.

This tutorial is suitable for users who:

- Are interested in learning how Anti-DDoS Pro works.
- Have purchased Anti-DDoS Pro and need to know how to set it up.
- Want to test, verify, modify or delete Anti-DDoS Pro configuration.



Note:

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.

Quick start flow

To set up basic website protection, complete the following tasks:



Note:

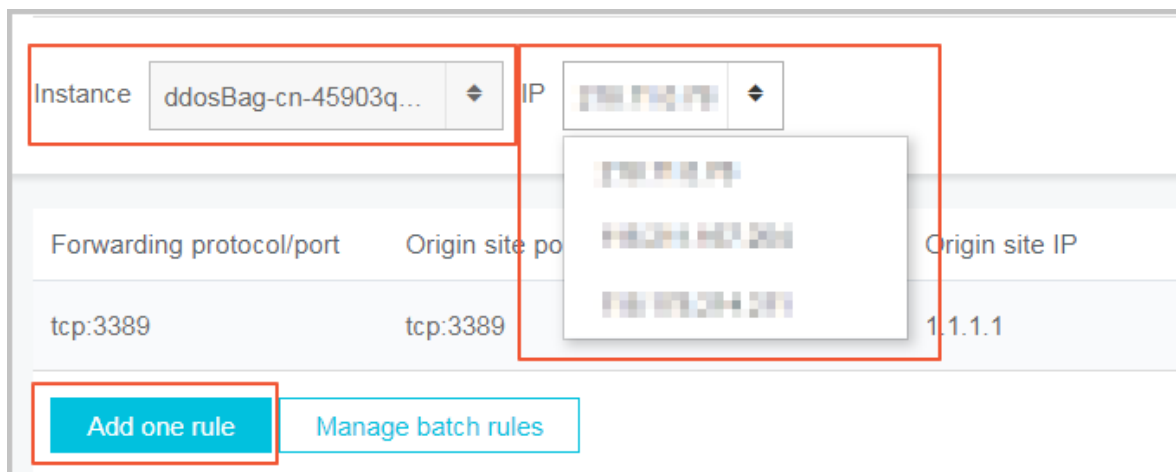
Before you begin, make sure that your Anti-DDoS Pro instance is enabled. To do this, see [Enable Anti-DDoS Pro instances](#).

1. [Set up layer 4 port protection](#).
2. [Whitelist local IP subnet](#).
3. [Verify local settings](#).
4. [Update DNS settings](#).

3.2.2 Step 1. Set up layer 4 port protection

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. Go to Access > Non-Web Service, and then select the Anti-DDoS Pro instance and IP.



3. Click Add one rule.

4. Select a protocol type under Forwarding protocol/port, and input the forwarding port.

| Forwarding protocol/port | Origin site port | LVS forwarding rule | Origin site IP |
|--------------------------|----------------------|---------------------|---|
| TCP <input type="text"/> | <input type="text"/> | Round Robin mode | <div>Use commas to separate up to 20 unique IP addresses</div> <input type="text"/> |
| <div>Add one rule</div> | | | |

5. Input Original site port and Original site IP. Use commas to separate multiple origin IP addresses.



Note:

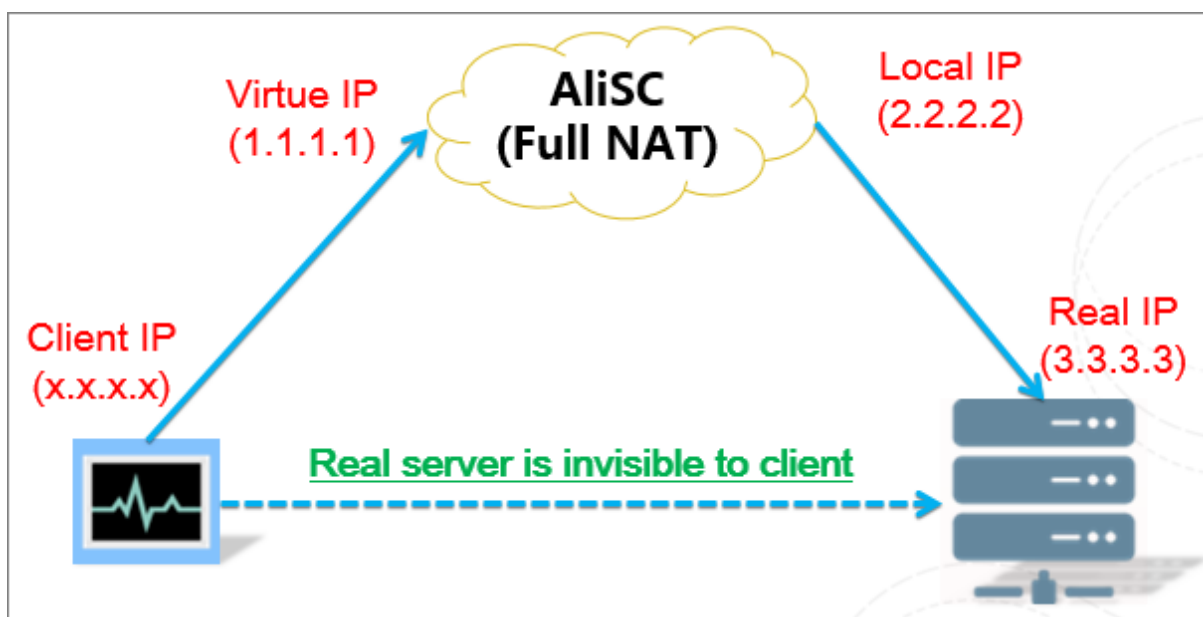
- UDP port 53 and TCP port 80 are not supported.
- Up to 50 layer-4 forwarding rules can be added to the list.
- Up to 20 origin IP addresses can be added to a layer-4 forwarding rule.

6. Click OK. A new rule entry will be added to the list.

3.2.3 Step 2. Whitelist local IP subnet

The Alibaba scrubbing center (AliSC) of Anti-DDoS Pro acts as a reverse proxy. It makes sure the client server remains invisible to the origin server. AliSC handles all requests from clients by blocking malicious requests while forwarding legitimate requests to the origin. Therefore, malicious traffic is mitigated when it goes through Anti-DDoS Pro.

In Full-NAT proxy mode, Anti-DDoS Pro uses the local IP as the source IP to establish connection with the origin server, as illustrated in the following figure.



- Multiple local IP addresses are available because AliSC has multiple physical servers.
- In Full NAT mode, each packet's source IP address will be a local IP address.
- The origin server must whitelist all existing local IP addresses that are fixed to guarantee accessibility.
- AliSC uses local IP addresses to visit IDC network and keeps the real client IP address in HTTP/HTTPS header's X-forwarded-for field.

For origin, Anti-DDoS Pro makes source IP addresses more concentrated, and improves the transmission speed of packets from them. Under this circumstance, however, the local IPs may be determined as suspicious to the origin server's firewall or security software (if such software is applied). In case of the local IP being blocked or limited, make sure all the local IPs are whitelisted before being diverted to Alibaba Cloud.

For a deeper level of safety considerations, we recommend that you block all requests to the origin server from IP addresses except local IP addresses. By doing this, the origin is better protected even if the real IP addresses are disclosed.

3.2.4 Step 3. Verify local settings

Before you update DNS settings and route all the traffic to Anti-DDoS Pro, we recommend that you verify the forwarding settings locally to guarantee availability.

To perform the verification, manually bind the virtual IP address provided by Anti-DDoS Pro with the domain name in your local hosts file (for example, C:\Windows

`\ System32 \ drivers \ etc \ hosts` , in Windows). The domain name is then resolved to Alibaba Cloud's IP address solely on your local device.

Anti-DDoS Pro refreshes your local DNS cache (for example, `ipconfig / flushdns` in Windows CMD) and loads this domain name in your browser. If your protection service does not have a domain name, you can directly replace the server's IP address with the virtual IP address acquired in the local testing environment.

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1            localhost
[REDACTED]. 0. 239 www. aaa. com
```

- If the service is accessed successfully, your configuration is properly set.
- Otherwise, check your configuration or open a ticket to contact Alibaba Cloud Technical Support.

3.2.5 (Optional) Step 4. Update DNS settings

Rerouting traffic to Anti-DDoS Pro is available once all configuration is completed.

- If your service does not need a domain name, directly update the server's IP address by replacing it with the virtual IP address provided by Anti-DDoS Pro.
- If your service needs a domain name, go to your DNS configuration panel. Choose either CNAME or A record to update the former DNS record, depending on your DNS service provider's configuration. Traffic is then redirected to another virtual IP address (for example, backup IP address) or to the origin in order to minimize additional problems.



Note:

Although both CNAME and A record are supported for rerouting traffic, we recommend that you choose CNAME rather than A record to guarantee a higher success rate.

- CNAME

Update the former DNS record with the generated CNAME. The former A record can be deleted.

The recommended TTL value is 10 minutes.

- **A Record**

Update the former A Record with the virtual IP address provided by Anti-DDoS Pro . If multiple virtual IP addresses are available, the domain name can be resolved to a different virtual IP address. This is based on different ISPs.

The recommended TTL value is 10 minutes.

4 User Guide

4.1 Provisioning guide

4.1.1 Website service provisioning with CNAME

Currently, Anti-DDoS Pro supports CNAME and A record access modes. However, we recommend CNAME.

CNAME is a DNS alias record that can be considered as a redirection. For example, the real origin site IP address corresponding to the domain name `www.abc.com` is `1.1.1.1`, and the corresponding CNAME is `abcde12345.alicloudddos.com`.

As a result, when A record is used, DNS resolves `www.abc.com` to its A record `1.1.1.1`; when CNAME address is used, DNS resolves `www.abc.com` to its CNAME record `abcde12345.alicloudddos.com`.

You must not worry about or configure the real IP address corresponding to the CNAME address. The client auto queries the CNAME record and ultimately gets the IP address (`1.1.1.1`).

During the access to Anti-DDoS Pro, we suppose that the Anti-DDoS Pro IP addresses are `2.2.2.2`, `3.3.3.3`, and `4.4.4.4` (indicating different lines). For the same domain name, CNAME records generated in the three lines are the same. You only need to configure CNAME resolution for one line, resolving `www.abc.com` to the CNAME address, and Alibaba Cloud will handle the corresponding IP addresses for the CNAME record.

The point is that one CNAME record can correspond to multiple IP addresses which are changeable. The process is transparent and imperceptible to you. However, if you use A record, you must manually change the resolution configuration if you need to change the resolved IP address.

What is the advantage of CNAME access?

- CNAME access is more convenient. You only need to modify the resolution configuration once at your domain name resolution service provider (such as Alibaba cloud DNS or DNSPod) to make the change effective, with zero deployment and zero operation efforts.

- When the Anti-DDoS Pro service on a line suffers an exception, such as black hole, domain names using CNAME resolution can be automatically switched to another Anti-DDoS Pro line.

Procedure

1. Purchase an Anti-DDoS Pro instance.
2. Log on to the [Anti-DDoS Pro console](#), add the domain name, and then configure the forwarding rules.
3. Modify the DNS resolution configuration at your DNS service provider to resolve the domain name to the CNAME record of Anti-DDoS Pro.
4. Wait for DNS settings to come into effect (about a few minutes). Then the website is connected to Anti-DDoS Pro through CNAME.
5. Test if the website can be accessed normally.

How is the operator line resolved at Anti-DDoS Pro CNAME resolution?

In general, China Telecom and China Unicom lines are resolved to China Telecom and China Unicom Anti-DDoS Pro services respectively, and Hong Kong line is resolved to Hong Kong Anti-DDoS Pro service.

I have configured link-specific resolution. How to configure it after CNAME access?

Under normal circumstances, you only need the CNAME resolution of one default line to replace the previous link-specific resolution. The intelligent resolution is handled by Alibaba Cloud automatically.

The CNAME address offered by Anti-DDoS Pro is capable of link-specific resolution. We can check whether the domain name corresponding to the CNAME record has been configured in China Telecom, China Unicom, or Hong Kong lines. If so, we can perform link-specific resolution in the three lines automatically.

4.1.2 Non-website service provisioning with CNAME

This article takes an example to describe how to connect your layer-4 service to Anti-DDoS Pro by using CNAME resolution.

In most cases, you can directly specify the clients to access the Anti-DDoS Pro IP address for layer-4 access (non-web service protection). However, in some cases, you may need to use a domain name to connect your layer-4 service to Anti-DDoS Pro. In such cases, you can add a layer-7 domain name, and use the same CNAME to resolve the domain name to the different Anti-DDoS Pro lines for CNAME auto scheduling.

Assume that you want the traffic accessing the game server domain name (game.aliyundemo.com) to be redirected to your Anti-DDoS Pro IP address, the game's TCP ports are 1234 and 5678, and the origin site IP address is 1.1.1.1.

Step 1: Add the domain name to Web Service to obtain the CNAME.

Log on to the Anti-DDoS Pro console, and go to the **Access > Web Service** page. Click **Add Domain** to add game.aliyundemo.com under protection. When selecting ISP line, assign China Telecom, China Unicom, and BGP lines at the same time to the domain name so that Anti-DDoS Pro IP addresses on different lines use the same CNAME.



Note:

If this domain name does not relate to a real website business, you can select whatever Protocol and enter anything in Origin site IP. Because this rule does not affect the Port 1234 and Port 5678 that are required by the actual business. Access requests sent to these two ports are forwarded to the Anti-DDoS Pro IP addresses by the following Non-Web Service forwarding rules in Step 2.

If this domain name relates to a real website business, you must specify the correct protocol type and origin site IP. This CNAME can also be used in domain name resolution for layer-4 service protection.

Step 2: Configure a forwarding rule under Non-Web Service.

Follow [Non-website access](#) to configure two forwarding rules for the TCP ports 1234 and 5678.

You can use the **Export Rules** and **Add batch rules** functions to facilitate the operations.



Note:

You must configure the corresponding non-website forwarding rules for all the Anti-DDoS Pro IP addresses enabled in Step 1.

Step 3: Update the DNS settings of the domain name

Go to your DNS service provider to add a CNAME record for game.aliyundemo.com, resolving it to the CNAME generated in Step 1.

When the procedure is complete, requests from clients can be intelligently resolved to the Anti-DDoS Pro IP addresses based on their network types. Anti-DDoS Pro can

then correctly forward requests sent from the clients to origin based on the layer-4 forwarding configuration.

Additionally, you can enable [CNAME Auto switch](#) for layer-4 services on the Web Service page.

4.1.3 Description of CNAME access

When you connect your web service to Anti-DDoS, we recommend that you

[Access to Anti-DDoS Pro through CNAME](#) rather than A record.

Advantages of using CNAME are as follows:

- CNAME is more convenient to use. After you modify the resolution configuration once at your DNS service provider (such as Alibaba Cloud DNS or DNSPod), the change takes effect with no deployment and O&M efforts.
- When the Anti-DDoS Pro on a line encounters an exception, domain names using CNAME resolution can be automatically switched to protection under another Anti-DDoS Pro line. For example, if the China Unicom line fails or is congested, the domain names may get auto-scheduled to be protected under the China Telecom line.
- If you are using a “China Telecom + China Unicom” two-line subscription, when the China Unicom line suffers from attacks and is thrown into the black hole, CNAME can automatically schedule domain name resolution to the China Telecom line, which avoids affecting services that are previously resolved to the China Unicom line.

You can check if your domain name is connected to Anti-DDoS Pro through CNAME on the Web Service page.

- If the domain name is connected to Anti-DDoS Pro through CNAME, the Instance & ISP Line prompts CNAME access successful.
- If the domain name is not connected to Anti-DDoS Pro through CNAME (for example, A record is used, or the CNAME resolution was incorrectly configured), the Instance & ISP Line prompts CNAME access failed.



Note:

This prompt does not necessarily indicate that the domain name resolution or service encounters an exception. Domain names that cannot use CNAME

resolution can be configured normally using A record. If your business access is normal, you can ignore this prompt.

4.1.4 Enable CNAME auto switch

By default, the high-security IP Service provides CNAME automatic scheduling without additional opening.

CNAME Auto Switch provides the failover capability that when an ISP line of an Anti-DDoS Pro instance encounters a problem, the service can be automatically switched to a healthy line, ensuring the service continuity and availability. For example, you enable CNAME Auto Switch for a domain protected by an Anti-DDoS Pro instance that has China Telecom and China Unicom two lines.

For example, you enable CNAME Auto Switch for a domain protected by an Anti-DDoS Pro instance that has China Telecom and China Unicom two lines.

- When the IP address of the China Telecom line fails, the Anti-DDoS Pro service can automatically switch to the IP address of the China Unicom line that works normally.
- When both IP addresses of the China Telecom line and the China Unicom line fail, CNAME Auto Switch cannot work.



Note:

Assume that you enable CNAME Auto Switch. When an IP address fails or is thrown into a black hole, the auto switch can be completed within one minute. The same CNAME is resolved to another healthy IP address on the DNS server. However, the actual time required for the changes to come into effect on the client depends on local DNS caching and updating.

4.1.5 Modify origin IP in provisioning settings

You can modify the origin IP address as needed once you enable a non-web service or web service in Anti-DDoS Pro.

Follow these steps to modify the origin IP address for a non-Web service:

1. Log on to the [Anti-DDoS Pro console](#) and go to the Access > Non-Web Service page.
2. Select an Anti-DDoS instance and corresponding IP address.
3. Locate the target Forwarding protocol/port, and then click Edit under the Operation column of the protocol/port.

4. Enter a new Origin site IP, and then click OK under the Operation column.

**Note:**

If the non-Web service owns multiple lines, the forwarding rules for all the lines must be modified.

Web Service

Follow these steps to modify the origin IP address for a Web service:

1. Log on to the [Anti-DDoS Pro console](#) and go to the Access > Non-Web Service page.
2. Locate the domain name to be configured, and then click Origin Edit under the Domain Info column of the target domain name.
3. Click Edit Origin IP under the Operation column.
4. Enter a new Origin site IP, and then click OK.

**Note:**

When the modification is completed, the website takes some time to apply the configuration. During this period, the access requests are still forwarded to the former origin IP address. After the configuration is completed, access requests are forwarded to the new origin IP.

4.1.6 Modify domain's forwarding line and origin settings

Generally, each Anti-DDoS Pro instance has at least one Anti-DDoS Pro ISP line, and you may have multiple Anti-DDoS Pro instances under your Alibaba Cloud account. Therefore, you may have multiple available Anti-DDoS Pro ISP lines.

When you configure a domain to be protected by an Anti-DDoS Pro instance, at least one Anti-DDoS Pro ISP line and an origin site is set in the forwarding line.

However, in practice, you may change the domain's forwarding line and origin settings in Anti-DDoS Pro according to your business.

For example, you can change the domain's forwarding line and origin settings to fulfill the following requirements:

- Add Anti-DDoS Pro lines in a domain's forwarding line. For example, add a China Unicom forwarding line for one domain that has only one China Telecom forwarding line.

- Make all requests from China Unicom to be forwarded by the Anti-DDoS Pro China Unicom line, to avoid latency due to requests being forwarded by other Anti-DDoS Pro ISP lines.
- Make requests from China Unicom to be forwarded by multiple Anti-DDoS Pro China Unicom lines. Then, request flow can be assigned to multiple Anti-DDoS Pro lines evenly.

Prerequisites

Your domain must already be configured to be protected by Anti-DDoS Pro instances.



Note:

If your domain has not been configured in Anti-DDoS Pro, see [Set up HTTP protection for web service](#) or [Set up HTTPS protection for web service](#) to configure your domain to be protected by existing Anti-DDoS Pro instance.

To change the domain's forwarding line and origin settings in Anti-DDoS Pro, follow these steps:



Note:

We recommend that you get familiar with the procedure by using test domains before you change the settings for your business domains. Additionally, we recommend that you change the settings during low demand periods.

1. Log on to the [Anti-DDoS Pro console](#), go to Access > Web Service.
2. Locate the domain, click Origin Edit under the Domain Info area to open the Origin Edit webpage.



Note:

You can also click Edit under the Instance & ISP Line area of the domain, to open the Origin Edit webpage.

| Domain Name : ddosBag-cn-vj30kuu1p001.cn Back | | | | | Purchase |
|--|-------------------------|--|--|--------------------------------|--------------------------|
| Enable an unoccupied Anti-DDoS Pro ISP line by clicking Add forwarding line. Click Edit Origin or Edit Line to change the corresponding origins or Anti-DDoS Pro IP configurations. For more information, view related help documents. | | | | | |
| Origin Edit Add Forwarding Line | | | | | |
| ISP Line | Instance | Anti-DDoS IP /Domain Resolution Switch | Origin IP/Domain | Operation | |
| China Unicom | ddosBag-cn-vj30kuu1p001 | 121 View Edit Delete <input checked="" type="checkbox"/> | 111 View Edit Delete | Edit Origin IP | Edit IP |
| China Telecom | ddosBag-cn-vj30kuu1p001 | 58 View Edit Delete <input checked="" type="checkbox"/> | 111 View Edit Delete | Edit Origin IP | Edit IP |

3. Change the domain' s forwarding line and origin settings according to your requirements.

- Add a forwarding line

- a. Click Add Forwarding Line, to add a new forwarding line for the domain.

For example, add a China Unicom forwarding line on the basis of the existing China Telecom forwarding line.

- b. In the Add Forwarding Line dialog box, select Mode and enter the origin site information, and then click Next.
 - c. Choose unoccupied Anti-DDoS Pro lines, and click ON.



Note:

You can choose multiple Anti-DDoS Pro lines.



Note:

In the Add Forwarding Line dialog box, all Anti-DDoS Pro ISP lines that have the same ISP with the forwarding lines that are configured for the domain are grayed out and displayed as occupied. For example, if the domain has a China Unicom forwarding line configured, all Anti-DDoS Pro China Unicom lines are displayed as occupied. You can change the Anti-DDoS Pro lines for an ISP that has a forwarding line configured by using the Edit IP functionality. For more information, see the Edit IP section.

- d. Click OK, and the new forwarding line is displayed in the Origin Edit webpage.

- Edit Anti-DDoS Pro IP

- a. Locate a forwarding line, click Edit IP to change the Anti-DDoS Pro lines for the forwarding line.
 - Enable Anti-DDoS Pro IP: In the Edit IP dialog box, choose an Anti-DDoS Pro IP and click ON.



Note:

You can enable multiple Anti-DDoS Pro IPs for one forwarding line, and then requests can be assigned to multiple Anti-DDoS Pro IPs evenly.

- Remove Anti-DDoS Pro IP: In the Edit IP dialog box, choose an Anti-DDoS Pro IP and click remove.



Note:

If the remove button of an Anti-DDoS Pro IP is grayed out, the Anti-DDoS Pro IP has been used and the resolution switch is turned on in the forwarding line.

If you have to remove this Anti-DDoS IP, turn off the resolution switch of the Anti-DDoS Pro IP in the Origin Edit webpage, and then remove the Anti-DDoS Pro IP in the Edit IP dialog box.

- Edit origin IP
 - a. Locate a forwarding line, click Edit Origin IP to change the origin site information.
 - b. In the Edit Origin IP dialog box, select Mode and enter the origin site information, and then click OK.



Note:

The origin site information modification takes five minutes to take effect.

- Delete a forwarding line

Locate a forwarding line, click Delete to delete the forwarding line. After you delete the forwarding line, Anti-DDoS Pro ISP lines that have the same ISP with the forwarding line are no longer occupied in the Add Forwarding Line dialog box.



Note:

If the forwarding line is the last forwarding line of the domain, you cannot delete this line.

4.1.7 Description of Anti-DDoS Pro ISP line resolution

- By default, China Telecom and China Unicom lines will be resolved to China Telecom and China Unicom Anti-DDoS Pro services and Hong Kong line will be resolved to Hong Kong Anti-DDoS Pro service.
- When you stop China Telecom and China Unicom lines, China Telecom and China Unicom users will be resolved to Hong Kong Anti-DDoS Pro service by default.

4.2 Layer-7 Protection Settings

4.2.1 HTTP(S) flood protection mode

Anti-DDoS Pro provides four defense modes against HTTP(S) flood attacks.

- **Normal:** The default HTTP flood protection mode. It can be used when a website has normal traffic to avoid false positives.

This mode is used by default when you configure web service protection in Anti-DDoS Pro. Its policies are relatively loose and can defend against general HTTP flood attacks, without impairing normal requests.

- **Attack emergency:** You can switch to the emergency mode when you discover exceptions in website response, traffic, CPU, or memory indicators, but some normal traffic may be blocked in this mode.

This mode has relatively strict policies and can guard against more complex and sophisticated HTTP flood attacks. However, it may block a small part of normal requests.

- **High:** This mode uses relative strict policies. It enables a full-site level CAPTCHA verification for all requests to the protected website. Each visitor is verified, and can visit the website only after verified by the verification algorithm.



Note:

With the full-site algorithm verification, all requests from real visitors through browsers can have responses normally. However, for API/native app business, they cannot respond the algorithm verification correctly, and the website may be inaccessible.

- **Very High:** This mode uses very strict policies. It enables a full-site level CAPTCHA verification for all requests to the protected website. Each visitor is verified and can visit the website only after verified by the verification algorithm.

Comparing with the full-site algorithm verification of the High mode, anti-debugging and anti-machine authentication features are also enabled.



Note:

With the full-site algorithm verification in the Very High defense mode, requests from real visitors through browsers can have responses normally. (Exceptions may occur in few browsers and cause the website inaccessible. In this situation, re-visit the website after the browser is restarted.) However, for API/native app business, they cannot respond the algorithm verification correctly, and the website may be inaccessible.

Procedure

By default, your domain protected by the Anti-DDoS Pro instance uses the Normal HTTP flood protection mode. You can change the mode as you needed.


1. Log on to the [Anti-DDoS Pro console](#).
2. Go to Protection > Setting > Web Attack Protection page, select Instance, and select Domain.



Note:

You can also go to the Access > Web Service page, locate a protected domain, click Setting under the Policy column, to go to the Web Attack Protection page for the domain.

3. Locate the HTTP Flood Protection area, click to select the defense mode.



HTTP Flood Protection

Independent anti HTTP Flood Protection engine, blocking attacking IPs within 1 second by t...

Status : ●

Mode : ☒ Normal ☐ Attack emergency ☐ High ☐ Very High ⓘ

Custom : ●

Now have 2 customize rules, [Settings](#)

Custom HTTP Flood Protection Rule

Anti-DDoS Pro also supports custom HTTP flood protection rules for you to customize precise HTTP flood defense rules. You can configure defense rules for specific URLs with this functionality.

Go to the Web Attack Protection page of your protected domain, locate the HTTP Flood Protection area, enable custom HTTP flood protection rules, and then click Settings to set custom defense rules for specific URLs.

| Name | URL | Interval |
|-------|------|----------|
| test | /abc | 60 |
| test2 | /bac | 60 |

Best Practice for HTTP Flood Protection Settings

The sequence of defense effects with these four HTTP flood protection modes is: Very High > High > Attack emergency > Normal. Meanwhile, the possibility of false positives with these four HTTP flood protection modes is Very High > High > Attack emergency > Normal.

Generally, we recommend that you use the Normal HTTP flood protection mode for your protected domain. This mode uses relative loose defense policies, and only IPs with large access frequency are blocked. We recommend that you switch to the Emergency attack mode or the High mode when the Normal mode fails to deliver satisfactory performance or the website is under severe HTTP flood attacks. Do not forget to switch back to the normal mode after the attack is over.



Note:

If your website has API/native app business, they cannot respond the algorithm verification correctly, and the website cannot be protected with the High or Very

High HTTP flood protection mode. You have to configure custom HTTP flood defense rules for the URL being attacked to block those attack requests.

4.2.2 Blacklist and whitelist settings

Anti-DDoS Pro provides a blacklist and whitelist, which allows you to block and allow accesses to specified domains.

Context

- Requests from IPs (or IP segments) that are added to the whitelist are permitted to access the target domain and are not subject to any protection policies.
- Requests from IPs (or IP segments) that are added to the blacklist are blocked from accessing the target domain.



Note:

Blacklist and whitelist are effective for only the target domain, not for the whole Anti-DDoS Pro instance. You can separately add up to 200 IPs (or IP segments) to the blacklist or whitelist for a single domain.

You can add those malicious IPs that have huge access to the blacklist for blocking, and add those IPs within your internal office network, IPs called by business APIs or other trusted normal IPs to the whitelist. Requests from IPs (or IP segments) in the whitelist are permitted to access the protected domain and are not blocked.

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. Go to the Protection > Setting > Web Attack Protection page, select Instance, and select Domain.



Note:

You can also go to the Access > Web Service page, locate a protected domain, and click Setting under the Policy column, to open the Web Attack Protection page for the domain.

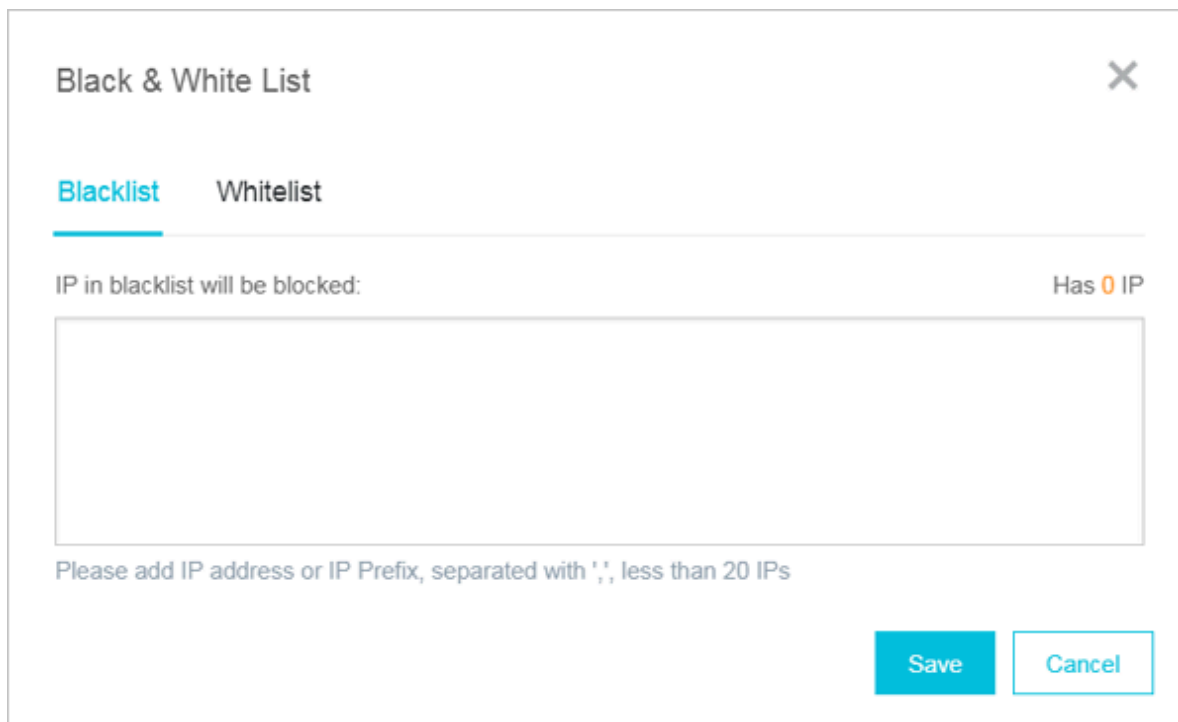
3. Locate the Black & White List area, click Settings.



Note:

To set the blacklist or whitelist, you have to enable HTTP Flood Protection.

- Select the Blacklist tab, add malicious IPs (or IP segments) to be blocked, and then click Save.
- Select the Whitelist tab, add IPs (or IP segments) that are permitted to access the domain, and then click Save.



Black & White List

Blacklist Whitelist

IP in blacklist will be blocked: Has 0 IP

Please add IP address or IP Prefix, separated with ',', less than 20 IPs

Save Cancel



Note:

- You can configure a maximum of 200 records each by using both individual IP address and IP/mask.
- Blacklist/Whitelist is not applicable to Non-Web Service.
- Blacklist/Whitelist is effective immediately if it is successfully configured. However, it becomes invalid when the configuration is deleted.
- Changes in the blacklist/whitelist affect all Anti-DDoS Pro IP addresses assigned to the target domain name in the forwarding rule configurations.

4.2.3 Deactivate black hole

Anti-DDoS Pro provides black hole deactivation to partial ISP lines of an Anti-DDoS Pro instance. You can deactivate the black hole status for the banned IP of your Anti-DDoS Pro instance.

Context

**Note:**

- Each Anti-DDoS Pro user has up to three chances to deactivate the black hole status in one day. You cannot do the deactivation after the chances exhausted. The deactivation chances are restored at midnight every day. The remaining chances cannot be accumulated to the next day.
- The black hole status deactivation can be affected by risk control policies of Alibaba Cloud. If the black hole status is not deactivated successfully, please try it later, and your deactivation chances are not deducted.
- Before you deactivate the black hole status, we recommend that you check the automatic reopened time first. If the automatic reopened time is acceptable, please wait until the Anti-DDoS Pro IP is unbanned.

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. Go to the Asset > Instance List, locate an ISP line under the black hole status, and click Setting under the Protection Info column.

**Note:**

You can also go to the Protection > Setting > DDoS Attack Protection page, locate the ISP line under the black hole status.

3. Click Deactivate Black Hole, locate the ISP line, and check the automatic reopened time.

**Note:**

If the automatic reopened time is acceptable, please wait until the Anti-DDoS Pro IP is unbanned.

4. Click Deactivate.

**Note:**

If the deactivation fails, you may receive an error message, and please try it later. If you do not receive any error message, the deactivation is successful, and you can refresh the status of your ISP lines to check whether it recovers.

4.2.4 Flow block

Anti-DDoS Pro provides an active flow blocking functionality to the China Telecom ISP line of Anti-DDoS Pro instances. You can manually block the flow to the China Telecom ISP line of your Anti-DDoS Pro instance.

Context

When the China Telecom ISP line of your Anti-DDoS Pro instance suffers huge traffic attacks, you can temporarily block the flow at the server side of the Anti-DDoS Pro service, to reduce the possibility of the black hole penalty against the China Telecom ISP line. Because the black hole policy considers multiple factors such as the size of traffic attacks and the attack origin, flow blocking can reduce the possibility of the black hole penalty under certain conditions.



Note:

- Currently, only the China Telecom ISP line supports flow blocking.
- Each Anti-DDoS Pro service user has totally three chances to block the flow to the China Telecom ISP line of an Anti-DDoS Pro instance that has more than 60 Gbps basic protection bandwidth.
- You can choose to block flow from the International ISPs or Chinese non-China Telecom ISPs two region. But, you cannot block flow from both regions at the same time.
- Single flow blocking can last from 5 minutes to 23 hours and 59 minutes. During the blocked period, you can actively reopen it at any time.

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. Go to Asset > Instance List, locate a China Telecom ISP line to be blocked, and click Setting under the Protection Info column.



Note:

You can also go to the Protection > Setting > DDoS Attack Protection page, and locate the China Telecom ISP line to be blocked.

3. Click Block Flow, select the China Telecom ISP line, click Block.

Instance ID

ddosBag-cn-v0h0f5e2801n

Cleaning Mode

Deactivate Black Hole

[Block Flow](#)

You have 12 times remaining to block traffic (19times in total)

| Instance Info | ISP Line | Service Address | Status | Blocked Region | Blocked Time | Reopened Time | Blocked Period | Action |
|---------------|---------------|-----------------|-----------------------|----------------|--------------|---------------|----------------|-----------------------|
| 流量封禁测试1 | China Unicom | 121.22.22.22 | -- | -- | -- | -- | -- | Not Supported |
| | China Telecom | 116.22.22.22 | ● Normal | -- | -- | -- | -- | Block |

4. In the Flow Block dialog box, select the Blocked Region, set the Blocked Time, and then click OK.

Flow Block

Blocked Region :

International ISPs

Domestic ISPs without China Telecom

Blocked Time :

23

Hour(s)

59

Minute(s)

OK

Cancel



Note:

If the flow blocking fails, you may receive an error message. Troubleshoot the issues accordingly and try it again. If you do not receive any error, the flow is blocked successfully, and you can see the blocked region and blocked period in the list. To reopen the flow, click Reopen.

4.3 Layer-4 Protection Settings

4.3.1 Layer-4 cleaning mode

Anti-DDoS Pro provides four layer-4 cleaning modes against the IP-level flow cleaning policies for your choice.

Context



Note:

Currently, cleaning mode change only supports CT/CU and International lines. Generally, new cleaning policies take effect several minutes after you change the cleaning mode.

- **Low:** This mode uses loose cleaning policies with a relatively large threshold of the speed limit.
 - Filters packages with defining DDoS characteristics, such as UDP reflection attack packages and attack packages that do not meet TCP characteristics.
 - Filters defining SYN flood and ACK flood attacks.
 - Applies easing restrictions on access IPs and destination IPs, mostly on the speed limit side.
- **Medium:** The default Medium mode uses normal cleaning policies.
 - Filters packages with defining DDoS characteristics, such as UDP reflection attack packages and attack packages that do not meet TCP characteristics.
 - Filters defining SYN flood and ACK flood attacks.
 - Applies restrictions on access IPs and destination IPs in a certain scope, mostly on the speed limit side.
 - Under circumstances, enables the reverse detection algorithm for the package filtering in a certain scope.
- **Emergency:** This mode uses relative strict cleaning policies. It enables connection detection for each IP to block IPs that have too many connections.
 - Filters packages with defining DDoS characteristics, such as UDP reflection attack packages and attack packages that do not meet TCP characteristics.
 - Filters defining SYN flood and ACK flood attacks.
 - Discards UDP packages.
 - Applies restrictions on access IPs and destination IPs in a certain scope. Speed limits, malicious IP blocking, and connection limits are enabled.

- **High:** This mode uses strict cleaning policies. It enables the origin authentication algorithm for package filtering under certain conditions.
 - Filters packages with defining DDoS characteristics, such as UDP reflection attack packages and attack packages that do not meet TCP characteristics.
 - Filters defining SYN flood and ACK flood attacks.
 - Discards UDP packages.
 - Applies restrictions on access IPs and destination IPs in a certain scope. Speed limits, malicious IP blocking, and connection limits are enabled.
 - Enables the reverse detection algorithm for the package filtering in a certain scope.

**Note:**

As some clients may not respond normally to this algorithm, partial normal requests can be blocked.

By default, your Anti-DDoS Pro instance uses the Medium cleaning mode. You can change the 4-layer cleaning mode as you needed.

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. Go to the Asset > Instance List, choose an ISP line of an Anti-DDoS Pro instance, click Setting in the Protection Info column to go to the DDoS Attack Protection page for the instance.

**Note:**

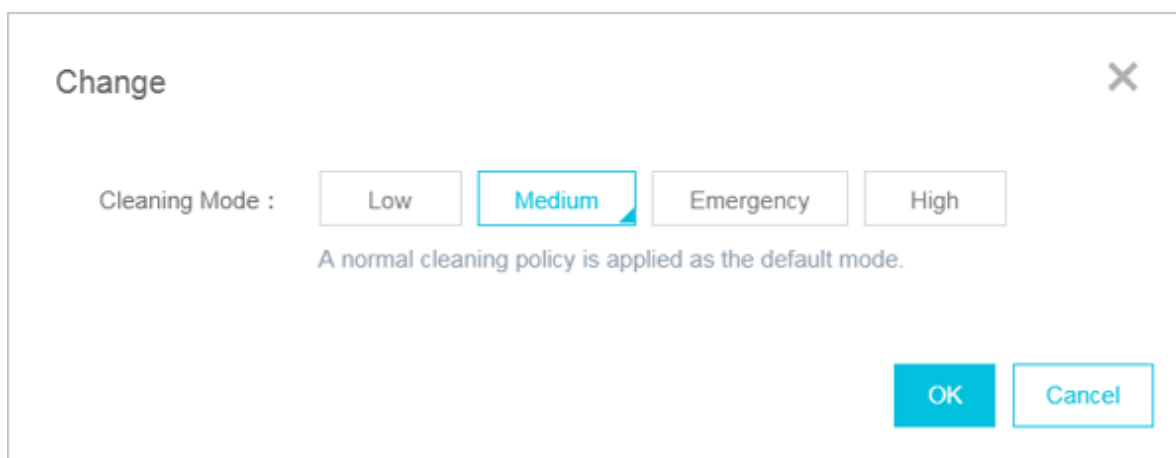
You can also go to the Protection > Setting > DDoS Attack Protection page, and manually locate the Anti-DDoS Pro instance.

| Instance Remarks <input type="text"/> <input type="button" value="Search"/> | | | |
|--|-------------------|---|--|
| Instance Info | ISP Line | Protection Info | Attack Statistics |
| ID : ddosBag-cn-45903q3r700o Expiration time : 2017-06-27 Clean traffic : 100M Renew Enable Auto Renew Service Update | China Unicom 218 | Status : Normal Setting No. of Port : 2 (At most 50) No. of Domains : 1 (At most 50) Mitigation BW : 20G (Burstable BW20G) edit | Max Attack Size : 0.00G Attack Events : 1 View reports |
| | China Telecom 116 | Status : Normal Setting No. of Port : 0 (At most 50) No. of Domains : 1 (At most 50) Mitigation BW : 20G (Burstable BW20G) edit | Max Attack Size : 0.00G Attack Events : 0 View reports |

3. Click Cleaning Mode, locate the ISP line that you want to change the cleaning mode for, and click Change.



4. Click to select a cleaning mode, and then click OK.



Result

After several minutes, the selected cleaning mode takes effect.

4.3.2 Health check settings for non-website service

This document describes how to configure health check for the Non-Web Service in Anti-DDoS Pro.

Follow these steps to configure health check rules for the Non-Web Service in the Anti-DDoS Pro console.

1. Log on to the [Anti-DDoS Pro console](#), and go to the Access > Non-Web Service page.
2. Select the target Anti-DDoS instance and IP.
3. Locate the corresponding Forwarding protocol/port, and click Configure under the Health Check column of the target protocol/port to configure health check. The health check feature is disabled by default.



Note:

If the forwarding protocol is TCP, you can select either TCP or HTTP as the health check method.

Parameter description

We recommend that you use the default values for health check configuration.

Table 4-1: Layer-4 health check

| Configuration | Description |
|---------------------|---|
| Port | Test port used by the health check service to access backend servers. The default port is the backend port specified in the listener configuration. |
| Response Timeout | Maximum timeout value for each health check response. If the backend server fails to respond correctly within the specified time period, the health check fails. |
| Check Interval | Interval between health checks. All nodes within the Anti-DDoS Pro cluster perform health checks on backend servers independently and in parallel based on this attribute. From individual statistics on a backend server, you may find that health-check requests sent from Anti-DDoS Pro do not strictly follow the specified time interval, because health-checks for different Anti-DDoS Pro nodes are not performed synchronously. |
| Unhealthy Threshold | This attribute specifies the number of consecutive health check failures allowed before a health check status is considered unhealthy. |
| Healthy Threshold | This attribute specifies the number of consecutive successful health check requests necessary for a health check status be considered as healthy. |

Table 4-2: Layer-7 health check

| Configuration | Description |
|---|--|
| Domain name and health-check path (only supports HTTP protocol) | <p>By default, layer-7 health check requests are HTTP HEAD requests sent by Anti-DDoS Pro to the default home page configured for the application server.</p> <ul style="list-style-type: none">· If the page for health check is not the default home page for the application server, you must specify the domain name and the specific health check path.· If the host field parameters are restricted for the HTTP head requests, you can only specify the health check path, that is, the page file URI for the health check. The domain name is not required, and it is the backend server IP address by default. |
| Normal status code | The normal HTTP status code for the health check. The default value is http_2xx, and cannot be changed. If the HTTP returns a non-2xx status code, then the server is considered as unhealthy by default. |
| Other parameter options | Same as the parameters for the layer-4 health check. |

4.3.3 DDoS defense police settings for non-website service

This topic describes the DDoS defense policies provided by Anti-DDoS Pro for the non-web service. You can refer this topic to optimize your non-web service' s anti-DDoS protection settings.

The DDoS defense policies for the non-web service in Anti-DDoS Pro is based on the IP and port protection. You can set the speed limit of connections and the length limit of packets for your IPs and ports of the non-web services that are protected by Anti-DDoS Pro, to relieve small-traffic connectivity attacks.

To set the DDoS defense policies for non-web service, follow these steps:

Log on to the [Anti-DDoS Pro console](#). Go to Access > Non-Web Service, select your anti-DDoS pro instance, and click Configure to set the DDoS defense policies.



Note:

The defense policies are based on the port level.

DDoS Defense Policies
✕

False Sources or Null Session Connections : ☐

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 : ☐

Packet Length Filtering ⓘ : Byte - Byte

Description of DDoS defense policies

| Policy name | Description |
|---|---|
| False Sources or Null Session Connections | Defense against false sources and null session connections . This policy only applies to TCP rules. |
| New Connection Speed Limits for Source IP | The maximum number of new connections per second from a single source IP. The new connections that exceed the limits are discarded. The new connection speed limits may have some deviation, because the protection device is deployed as clusters. |

| Policy name | Description |
|---|---|
| Concurrent Connection Speed Limits for Source | The maximum number of concurrent connections from a single source IP. The connections that exceed the limits are discarded. |
| New Connection Speed Limits for Destination IP | The maximum number of new connections per second to a single destination IP and port. The new connections that exceed the limits are discarded. The new connection speed limits may have some deviation, because the protection device is deployed as clusters. |
| Concurrent Connection Speed Limits for Destination IP | The maximum number of concurrent connections to a single destination IP and port. The connections that exceed the limits are discarded. |
| Packet Length Filtering | The length limit of payload included in packets (unit: byte). Packets that exceed the size limit are discarded. |

4.3.4 Session persistence settings for non-website services

Anti-DDoS Pro Non-Web Service protection provides IP-address-based session persistence, which supports forwarding requests from the same IP address to the same backend server.

Procedure

1. Log on to the [Anti-DDoS Pro console](#) and go to the Access > Non-Web Service page.
2. Select an Anti-DDoS Pro instance and the corresponding IP address.
3. Locate the target Forwarding protocol/port, and then click Configure under the Session Persistence column of the protocol/port. You can set session persistence at the port level.
4. Set the Connection Timeout, and then click Save.

4.4 Instance management

4.4.1 Disable and remove certain lines

This topic describes how to disable or remove a resolution line for the origins that use CNAME to access Anti-DDoS Pro.

Disable a line



Note:

This operation is only applicable to the origins that use CNAME to access Anti-DDoS Pro.

Follow these steps to disable a line:

1. Log on to the [Anti-DDoS Pro console](#) and go to the Access > Web Service page.
2. Locate the domain name to be configured, and click Origin Edit under the Domain Info of the target domain name.
3. In the Anti-DDoS IP /Domain Resolution Switch column, you can enable/disable a target line by using the corresponding toggle button.

When a line is disabled, no inbound website traffic passes through this line.

Remove a line



Note:

Before performing this operation, make sure that the website access traffic only passes through resolution lines that are enabled. If you are using a CNAME to access the Anti-DDoS Pro Web service, make sure that the line you want to delete is disabled first, which also means that the CNAME resolution is disabled.

Follow these steps to remove a line:

1. Log on to the [Anti-DDoS Pro console](#) and go to the Access > Web Service page.
2. Locate the domain name to be configured, and click Origin Edit under the Domain Info of the target domain name.
3. Click Edit IP in the Operation column.
4. On the Edit line page, click OFF under the target line to remove it, and then click OK.



Note:

Before removing a line, make sure that the website access traffic does not pass through this line.

4.4.2 Change ECS IP

If your source IP is disclosed already, we recommend that you use the IP we provide to you, which can prevent hackers from directly attacking the origin. You can change the backend ECS IP address for up to 10 times in the Anti-DDoS Pro console.

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. Go to the Access > Web Service page, and then click Change ECS IP.

**Notice:**

This operation temporarily interrupts your ECS service for a few minutes. We recommend that you back up your data first.

3. You must stop the ECS instance to change its IP. If the target instance is already stopped, go to step 4. Otherwise, click go to ECS in the Change ECS IP dialog box. In the ECS console, stop the target ECS.
 - a) Locate the target ECS from the Instance List, and then click its Instance ID.
 - b) On the Instance Details page, click Stop.
 - c) Select a stop method, and then click OK.

**Note:**

You will be required to enter a cellphone verification code to stop the instance.

- d) Wait until the status of the target instance becomes Stopped.
4. Return to the Change ECS IP dialog box, enter the target ECS Instance ID, and then click Next.
 5. Confirm that the target ECS instance information is correct (especially the ECS IP), select whether to restart the ECS after the IP is changed, and then click Release IP.
 6. After the previous IP is released, click Next to assign a new IP to the instance.
 7. After the IP is changed, click OK.

**Note:**

Once you change the ECS IP, enable Anti-DDoS Pro for the new IP. Make sure that you do not expose it.

4.5 Reporting

4.5.1 View the security report

Follow these steps to view the security reports.

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. Go to the Report > Security Report page.

3. On the Security Report page, you can click the Business, DDoS Protection, or HTTP Flood Protection tab to view the relevant summary charts and records.

**Note:**

All reports support the query condition that uses the start time and end time. Additionally, in the DDoS Protection report, Attack type and Attacker IP address are also displayed.

4.5.2 Set alarm notifications for DDoS events

You can configure Alarm notifications for Anti-DDoS Pro in the Message Center console. This article describes the detailed procedure.

Procedure

1. Log on to the [Message Center console](#).
2. Go to Message Settings > Common Message Settings, and click Manage Message Recipient.
3. On the Message Recipient Management page, click Add Message Recipient to add a contact. You can also select an existing contact, and click Modify/Delete on the Action list to perform the relevant operations.
4. Return to the Common Message Settings page. Go to Notification Type, and select Security Message > Security Notice to enable alarm notifications for Anti-DDoS Pro. In addition, select the corresponding notification methods (Internal Messages, Email, and Text Message), and click Modify under the Contact column to select the message recipient.

Result

Once you have set the alarm rules, the contacts selected by you will receive alarm notifications as and when the exception occurs.

4.6 Logging

4.6.1 Operation log

You can log on to the Anti-DDoS Pro console, and then go to the Log > Operation Log page to view operation log records about Anti-DDoS Pro service.

**Note:**

The Operation Log page only displays logs for important operations within the latest 30 days.

| Operation log | Status | Remark |
|---|-----------|---|
| ECS IP change log | Supported | - |
| CNAME scheduling log | Supported | - |
| Black hole deactivation log | Supported | Currently, black hole deactivation does not support BGP lines. |
| Flow block/reopen log | Supported | Currently, flow block only supports China Telecom lines of an Anti-DDoS Pro instance that has more than 60G basic protection bandwidth. |
| Cleaning mode change log | Supported | Four different modes can be chosen for 4-layer cleaning. Currently, cleaning mode change does not support BGP lines. |
| HTTP flood protection mode change log | Supported | Four different modes can be chosen for HTTP flood protection. |
| Elastic protection bandwidth change log | Supported | - |

4.6.2 Full log

According to APNIC DDoS threat landscape in 2017, more than 80% of DDoS attacks mix HTTP and HTTPS flood attacks, and have a high level of concealment. Therefore, it is especially important to analyze the access and attack behavior by using logs, and apply a protection strategy.

Now, Alibaba Cloud Anti-DDoS Pro has integrated with Log Service on website access logs (including HTTP flood attack logs), to provide real-time analysis and reporting center features.

Log Service supports the real-time collection of Alibaba Cloud Anti-DDoS Pro website access logs, HTTP flood attack logs, and supports real-time query and analysis of collected log data. The results of the query are displayed in the form of dashboards.

Enable the full log service

To enable the full log service for your protected website domain in Anti-DDoS Pro, follow these steps:



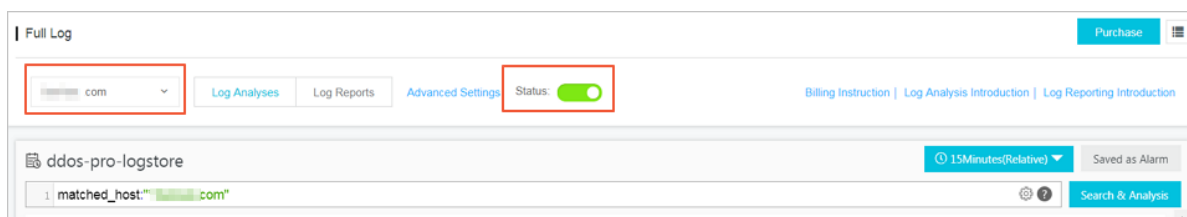
Note:

The usage of Anti-DDoS Pro full log service is charged according to the charge items of the Log Service. If no log data is generated, no billing is made. Log Service is billed by resource usage and provides the FreeTier quota for DDoS Logstore.

The payment of the Anti-DDoS Pro full log service is calculated mainly based on the collected log volume and log storage period factors. The Anti-DDoS Pro full log service provides 100 GB/day log volume and 3 days log storage period as the FreeTier quota. Meanwhile, index-based query analysis, reports, and alarms are not charged.

For example, you enabled the Anti-DDoS Pro full log service for a website whose average log size is about 1600 bytes, about 60 million logs are generated per day, and the storage period is 3 days. The total log volume is about 96 GB per day, not exceeding the FreeTier quota, and no charge is generated. However, if the access log volume of your website business exceeds the FreeTier quota, extra charges can appear. For more information about the billing method, view [Anti-DDoS Pro full log service - Billing method](#).

1. Log on to the [Anti-DDoS Pro console](#), and go to the Log > Full Log page.
2. Select the website for which you want to enable the Full Log service and click to turn on the Status switch.



After you turn on the Anti-DDoS Pro Full log service, you can query and analyze the collected logs in real time, view dashboards, and set alarms on the Full Log page. For more information about the Log Analysis and Log Reports features, see [Anti-DDoS Pro full log service - Log report](#) and [Anti-DDoS Pro full log service - Log analysis](#).

Use cases

By using the Anti-DDoS Pro Full log service, you can do the log analysis in the following scenarios.

- Troubleshoot website access exceptions

Log Service has been configured to collect Anti-DDoS Pro full logs, you can query and analyze the collected logs in real time. Using SQL statement to analyze the website access log, you can quickly check and analyze the website access exceptions, and view information such as read and write delays and operator distribution.

For example, view the website access log by using the following statement:

```
__topic__ : DDoS_access_log
```

- Track HTTP flood attack source

- For example, analyze the HTTP flood attack country distribution recorded in the access log by the following statement:

```
__topic__ : DDoS_access_log and cc_blocks > 0 | SELECT
  ip_to_country ( if ( real_client_ip = '-', remote_address ,
  real_client_ip ) ) as country , count ( 1 ) as " Attack
  Times " group by country
```

- For example, view the access PV by the following statement:

```
__topic__ : DDoS_access_log | select count ( 1 ) as PV
```

- Website operation analysis

Anti-DDoS Pro access log records the website access data in real time. You can perform SQL query analysis of the collected access log data to obtain real-time access status, such as determining the website popularity, the source and channel of the access, the client distribution, and assist in website operation analysis.

For example, view the visitor traffic distribution from different network providers:

```
__topic__ : DDoS_access_log | select ip_to_provider ( if (
  real_client_ip = '-', remote_address , real_client_ip ) ) as
  provider , round ( sum ( request_length ) / 1024 . 0 / 1024 . 0 ,
  3 ) as mb_in group by provider having ip_to_provider (
```

```
if ( real_client_ip = '-', remote_address, real_client_ip )) <>
' ' order by mb_in desc limit 10
```

4.7 Managed Security Service of DDoS Protection

Managed Security Service (MSS) is available in Alibaba Cloud Security DDoS Protection. Once you activate the MSS of DDoS Protection service, you can get professional and exclusive technical support from Alibaba Cloud Security experts with regard to implementing and using Alibaba Cloud DDoS Protection.

Overview

The MSS of DDoS Protection service is backed with Alibaba Cloud Security service team and helps you better use Alibaba Cloud DDoS Protection. With MSS of DDoS Protection, you can more effectively protect your Web assets against DDoS attacks, reduce Web business risk, and significantly reduce security maintenance costs.

The MSS of DDoS Protection service is suitable for situations where you have activated Alibaba Cloud DDoS Protection but lack continuous monitoring and security engineers to protect against vulnerabilities. The service is ideal for customers seeking outsourcing professionals to assist in the operation of security services.

Service scope

The MSS of DDoS Protection service provides a fully managed service for Alibaba Cloud DDoS Protection, including DDoS Protection configuration service, protection policy optimization, security monitoring and warning, security incident response, security consulting, security training and case study, and security reporting. These services are further described as follows.

Table 4-3: Service scope of MSS of DDoS Protection

| Service type | Description |
|--------------------------------|---|
| DDoS Protection configuration | <ul style="list-style-type: none"> Provides DDoS Protection configuration for implementing DDoS Protection for a website Assists in configuring and uploading the HTTPS certificate (Users can import the cert and private key by themselves) Adjusts the protection threshold according to the user's requirements Assists in configuring origin server protection for ECS and Server Load Balancer instances Performs adaptability verification and requesting test after website configuration is completed Assists in modifying the configuration and policies when the protected website changes |
| Protection policy optimization | <ul style="list-style-type: none"> Provides diagnosis and troubleshooting services when exceptions occur to services on DDoS Protection Optimizes user security protection policies by analyzing attack logs Adjusts protection policies and provides mitigation solutions in response to security incidents Provides suggestions on DDoS protection configuration for fault handling, HTTP flood protection, HTTP ACL policy, and data risk control |
| Monitoring and warming | <ul style="list-style-type: none"> Monitors the product availability, faults, and exceptional status Monitors high-risk security events and abnormal events caused by DDoS attacks Monitor protection status based on the user's or system's attack alerts and makes the adjustment to the protection policies |
| Security reporting | <ul style="list-style-type: none"> Provides customized security service reports for the user Sends the daily and monthly product operations and service report to the user |

Security incident response time

When a user encounters a security incident that requires urgent assistance, the service team responds to the user in a timely manner based on the security incident response time described as follows.

Table 4-4: Security incident response time

| No. | Priority | Definition | Response time |
|-----|-----------|--|---------------|
| 1 | Critical | The user's critical business or core components are significantly damaged or the service is unavailable, requiring immediate processing | 15 minutes |
| 2 | Emergency | The user's critical business or core components are severely affected or important features are unavailable and need to be processed as soon as possible | 30 minutes |
| 3 | High | The user's non-critical business is seriously damaged or unavailable | 2 hours |
| 4 | Medium | The user's non-critical business is abnormal | 4 hours |
| 5 | Low | General technical or advisory questions | 8 hours |

Service delivery description

The following table describes the service delivery method of MSS of DDoS Protection.

Table 4-5: Service delivery description

| Category | Description |
|-------------------------|---|
| Service delivery method | Remote online service |
| Service language | Chinese and English |
| Service period | Consistent with the user's purchase cycle |

| Category | Description |
|----------------------------|--|
| Supported service channels | <ul style="list-style-type: none">· Email· DingTalk· Phone |

Billing and purchasing method

The MSS of DDoS Protection service supports subscription and can be renewed on a monthly or yearly basis. To activate the MSS of DDoS Protection, go to the [sales page](#).



Notice:

Due to the special investment of the service support system and service human resources, refunds are not supported.

5 Best Practice

5.1 Configure a multi-line Anti-DDoS Pro instance to pass traffic back to multiple origin sites

In cases where compliance or high availability is required, you can deploy a multi-line Anti-DDoS Pro instance to pass traffic back to different origin sites, based on the type of line. For example, you can enable the China Telecom line of your Anti-DDoS Pro instance for a China Telecom origin, and the China Unicom line for a China Unicom origin. This topic describes the configuring method in the Anti-DDoS console.

Context

If your domain name is not connected to an Anti-DDoS Pro instance, follow [HTTP website access](#) or [HTTPS website access](#) to connect your domain name to Anti-DDoS Pro.



Note:

We recommend that you familiarize yourself with the configuration procedure, before performing the actual configuration and only do so during off-peak hours.

Procedure

1. Log on to the [Anti-DDoS Pro console](#) and go to the Access > Web Service page.
2. Locate the target domain name, and then click Origin Edit under Domain Info.
3. Disable certain lines for the current origin.
 - a) On the Anti-DDoS IP/Domain Resolution Switch column, toggle off one or more lines. For example, if you want to only use the BGP lines for domain name

- resolution for the current origin, you can disable the China Telecom and China Unicom lines.
- b) Click Edit IP in the Operation list.
 - c) On the Edit IP page, click OFF to disable certain lines, for which you have toggled domain name resolution off. In this case, disable China Telecom and China Unicom lines.
 - d) Click OK to go back to the Origin Edit page. When completing the configuration, you can find that the China Telecom and China Unicom lines are removed in the Anti-DDoS IP/Domain Resolution Switch column.
4. Add a new origin and enable other lines for it.
- a) On the Origin Edit page, click Add. For example, you can add a China Telecom origin, and enable the China Telecom line for it.
 - b) Select the Origin site IP mode and enter an IP address. Click ON under the China Telecom line. Click OK.
 - c) With the preceding configuration, your Anti-DDoS Pro instance's China Telecom line directs requests back to the newly added China Telecom origin.
5. Follow Step 4 to configure other lines of your Anti-DDoS Pro instance for the corresponding origins. Make sure that different lines are enabled for their corresponding origins.

5.2 How can origins outside Alibaba Cloud get clients' real IP addresses?

If you have configured Anti-DDoS Pro for your hosts outside Alibaba Cloud, you can use the methods introduced in this topic to obtain the clients' real IP addresses.

The methods described in this document support the following operating systems:

- Redhat Linux
- Centos 6.x

Consider these recommendations before you proceed with the steps:

- Perform a demo in a test environment. Make sure the business is stable before making the official release.
- Keep the original kernel. You can switch to the original kernel for recovery in case of restart failure.

Procedure

Follow these steps to obtain the clients' real IP addresses:

1. Download the following kernel installation files:

- [kernel-2.6.32-220.23.2.ali_github.el6.x86_64.rpm](#)
- [kernel-firmware-2.6.32-220.23.2.ali_github.el6.x86_64.rpm](#)

2. Install the kernel. Locate the installation directory and run the following command:

```
rpm -ivh kernel - 2 . 6 . 32 - 220 . 23 . 2 . ali_github . el6  
. x86_64 . rpm
```



Note:

You do not need to install kernel-firmware for CentOS 6.2 and later versions.

3. Configure the toa module to enable auto-load.

- a. Create a file `/etc/sysconfig/modules/toa.modules`, and add the following content:

```
! / bin / bash  
if [ - e / lib / modules / uname - r / kernel / net / toa /  
toa . ko ] ;  
then  
modprobe toa > / dev / null 2 >& 1  
fi
```

- b. Run the following command to grant the executable permission to the toa module.

```
sudo chmod + x / etc / sysconfig / modules / toa . modules
```

4. Run the `reboot` command to restart the system.

Functional testing

In general, the host can obtain the clients' real IP addresses once you complete the installation. If the host cannot retrieve the clients' IP addresses, you can run the `lsmod | grep toa` command to check the loading status of the toa module.

If the toa module is not loaded, run the `modprobe toa` command to manually load it. When the module is loaded successfully, test the host again and see if it can get the clients' real IP addresses.

FAQ

- Will the network performance be slowed down when the network connection has to pass through the toa module?

The toa module is deployed on the supplementary access, and has little influence on the network performance.

- Do I need to worry about the stability after loading the new kernel module?

We recommend that you keep the original kernel. You can switch to the original kernel for recovery in case of restart failure. Additionally, you can find the source code of the current version on Github.

5.3 How to determine the attack type by using Anti-DDoS Pro?

This topic describes the method for you to identify the attack your Anti-DDoS Pro IP addresses suffer, from HTTP flood attack and DDoS attack.

- HTTP flood attack: mainly indicates layer-7 website connection attacks.
- DDoS attack: mainly indicates layer-4 heavy traffic attacks.

Procedure

You can log on to the [Anti-DDoS Pro console](#) and go to the Report > Security Report page to check attack records in the DDoS Protection and HTTP Flood Protection reports to determine the attack type.

- For DDoS attack, you can find attack traffic record in the DDoS Protection report, and traffic cleaning is triggered. However, no associated record can be found in the HTTP Flood Protection report.
- For HTTP flood attack, you can find attack traffic record in both of the DDoS Protection and HTTP Flood Protection reports, and traffic cleaning is triggered in the DDoS Protection report.

The DDoS Protection report only records layer-4 traffic. The HTTP flood attacks are layer-7 attacks, and the relevant protection result can only be viewed in the HTTP Flood Protection report.

5.4 How to migrate the service from the original Anti-DDoS Pro instance to a new one?

This topic describes the procedure to migrate your service to a new instance without experiencing any service interruption. This generally happens when your original Anti-DDoS Pro instance expires and you have a new Anti-DDoS Pro instance.

Procedure

1. Log on to the [Anti-DDoS Pro console](#).
2. Go to the Access > Web Service page.
3. Locate the target domain name, and click Origin Edit under Domain Info of the target domain name.
4. Click Edit IP in the Operation column.
5. In the Edit IP dialog box, select the Instance and Anti-DDoS IP to enable for the target domain name. You can click the corresponding ON button to apply the current domain name configuration to that IP.
6. Click OK. When the domain name configuration is effective, both the original and the new Anti-DDoS Pro instances become available.
7. Disable the Anti-DDoS IP of the original Anti-DDoS Pro instance on the Origin Edit page, and then remove that Anti-DDoS IP in the Edit IP dialog box by clicking the corresponding OFF button.

5.5 What measures I must take if the source IP gets exposed

If your source IP can still be attacked after being protected under Anti-DDoS Pro, you can change the source IP address.



Note:

Before changing the source IP address, make sure that you have eliminated all insecure factors that may expose the source IP address.

Insecure factors checklist

Follow this checklist to confirm that no insecure factor may expose your source IP address.

1. Check whether the origin server contains security risks such as Trojans or webshells.

2. Check whether Anti-DDoS Pro is enabled for all services in the origin server, especially the records other than Web records such as MX records for mail servers and bbs records.

**Note:**

Double-check your DNS records to confirm that no record points to the source IP.

3. Check whether the source code leaks your website information. For example, the `phpinfo ()` command may contain IP addresses and other information.
4. Check the origin server for malicious scanning. You can prevent this risk by only allowing the Anti-DDoS Pro IP addresses on the origin. Check if you have businesses resolved to the origin server. For more information, see [Protect the origin](#).
5. Make sure that no business is resolved to the origin.
 - a. Use a Ping tester (for example [DNS Checker](#)) to test the current domain name.
 - b. Check your DNS records again to make sure no record points to the source IP.

Change source IP

After eliminating all the insecure factors that may expose the source IP, you can change the exposed source IP. For more information, see [Change ECS IP](#).

Additional solution

If you do not want to change the source IP or have changed the source IP but still have a problem, we recommend that you deploy an SLB server in front of the backend of your ECS server.

You can deploy SLB by using the following architecture: Client > Anti-DDoS Pro > SLB > ECS

**Note:**

In this architecture, you must add the IP address of the load balancing server as the source IP in the Anti-DDoS Pro console.

With this architecture, even if the origin is put into a black hole after being attacked, to access the server through Anti-DDoS Pro remains unaffected. Because the traffic from the load balancing server to the origin is transmitted through the intranet, even if the origin IP is put into a black hole, Anti-DDoS Pro can still access the origin through the load balancing server.

5.6 Obtain the real IP address of a visitor

This topic describes how to obtain the real IP addresses of access requests to your origin after you enable Anti-DDoS Pro for the origin.

Non-Web Service (Layer-4 access)

Choose and apply the method best suitable for your origin to get the clients' IP addresses, based on different deployment architectures.

- Anti-DDoS Pro > Alibaba Cloud ECS

If you use the TCP port to forward flows, no special modification is required. IP addresses obtained by the origin server are the clients' real IP addresses. Additionally, you can configure the ECS security group directly targeted on the clients' real IP addresses.



Note:

If the UDP port is used to forward requests, then the origin ECS cannot obtain the real client IP addresses.

- Anti-DDoS Pro > SLB > ECS

If you use the TCP port to forward flows, no special modification is required. IP addresses obtained by the origin server are the clients' real IP addresses.



Note:

- You must add the [Anti-DDoS Pro's back-to-source CIDR block](#) to the whitelist of the Access Control settings in the SLB Management Console.
- If the UDP port is used to forward requests, then the origin ECS cannot obtain the real client IP addresses.



Notice:

- For ECS instances that are created after October 2018, clients' real IP addresses can be obtained directly on the origin ECS server by default.
- For ECS instances that are created before October 2018, the origin ECS server cannot obtain clients' real IP addresses. You have to submit a ticket to enable the corresponding feature.

- Anti-DDoS Pro > Non-Alibaba Cloud server

This architecture is partially supported to obtain clients' real IP addresses. For more information, see [How can origins outside Alibaba Cloud get the clients' real source IP addresses.](#)

Web service (Layer-7 access)

When a layer-7 proxy server (such as Anti-DDoS Pro) forwards users' access requests to the backend server, the origin retrieves the back-to-Source IP addresses of this layer-7 proxy server (such as Anti-DDoS Pro). The client's real IP address is placed into the HTTP header's X-Forwarded-For field by the layer-7 proxy server. The format is as follows: `X - Forwarded - For : Visitor ' s real IP address , Anti - DDoS Pro IP address .`

If more than one proxy server is adopted (for example, the requests pass through WAF, CDN, and other proxy servers), the format of the HTTP header's X-Forwarded-For field is as follows: `X - Forwarded - For : Visitor ' s real IP address , Proxy 1 - IP address , Proxy 2 - IP address , Proxy 3 - IP address ...`

The visitor's real IP address is placed in the first position, followed by all intermediate proxy servers' IP addresses. Therefore, the origin can obtain a visitor's real IP address from the HTTP header's X-Forwarded-For field.

Common methods for retrieving the X-Forwarded-For field

- ASP

```
Request . ServerVariables (" HTTP_X_FORWARDED_FOR ")
```

- ASP.NET(C#)

```
Request . ServerVariables [" HTTP_X_FORWARDED_FOR "]
```

- PHP

```
`$_SERVER [" HTTP_X_FORWARDED_FOR "]
```

- JSP

```
request . getHeader (" HTTP_X_FORWARDED_FOR ")
```

After retrieving the HTTP header's X-Forwarded-For field, use “,” as the delimiter to capture the first IP address, which is the client's real IP address.

5.7 Protect origin sites that use Anti-DDoS Pro

This topic describes methods and principles for different scenarios to protect your origin sites under Anti-DDoS Pro.



Note:

The origin sites protection can prevent your origin against light-traffic HTTP flood and Web attacks, but cannot defend against heavy traffic DDoS attacks. In addition, it does not prevent DDoS attacks directly targeting the origin through traffic that bypasses Anti-DDoS Pro, which may even throw the origin IP address into the black hole.

Web service (layer-7 forwarding)

- Anti-DDoS Pro > ECS or origins outside Alibaba Cloud

Under this architecture, visitors' source IP addresses that send requests to ECS and non-Alibaba cloud origins are converted to Anti-DDoS Pro [back-to-source IP addresses](#).

You can use the origin's security software (such as iptables and firewall), to only allow Anti-DDoS Pro back-to-source IP addresses, and block all other IP addresses.

- Anti-DDoS Pro > SLB > ECS

Under this architecture, the IP address that sends requests to ECS becomes SLB's IP address.

We recommend that you use SLB's whitelist to only allow Anti-DDoS Pro to access SLB. For more information about whitelist settings, see [Configure a whitelist](#).

- Anti-DDoS Pro > WAF/CDN > ECS

Under this architecture, the IP address that sends requests to ECS becomes WAF or Alibaba Cloud CDN's IP address.

Whenever possible, we recommend that you configure relevant policies on WAF and Alibaba Cloud CDN, and configure origin policies based on the back-to-source IP addresses of WAF or Alibaba Cloud CDN.

Non-Web service (layer-4 protection)

Origin sites protection is not necessary for layer-4 forwarding. Because the attackers can always bypass Anti-DDoS Pro and directly attack the origin, which may bring congestion or trigger the back hole. Origin protection does not work in this case.

Configure ECS security group to protect the origin

Follow these steps to set up the security group for an ECS origin:

1. Log on to the [ECS console](#).
2. In the left-side navigation pane, click Security Group, select the target region (a security group can only be applied to ECS instances within the same region), and click Create Security Group.
3. Specify Security Group Name, Description, and Network Type, and then click OK.
4. Click Configure Rules under the Actions column of the newly added security group, and then click Add Security Group Rules.

5. Assume that the Anti-DDoS Pro IP segment is `1 . 1 . 1 . 0 / 24` , you can add the security group rules as shown in the following figure.

Add Security Group Rules

NIC: Intranet

Rule Direction: Inbound

Authorization Policy: Allow

Protocol Type: All

* Port Range: -1/-1 ⓘ

Priority: 10 ⓘ

Authorization Type: Address Field Access

* Authorization Object: 1.1.1.0/24 ⓘ Tutorial

Description: Anti-DDoS Pro

It must contain 2-256 characters and it cannot begin with http:// or https://

OK Cancel



Note:

- You can only add one IP address or IP segment in the Authorization Object field at one time. If you have more than one IP address or IP segment, you must add a corresponding rule for each of them.
- When the same authorization object matches multiple rules, the rule with the highest Priority overrides the rest of the rules.

6. Follow Step 4 to 5 to add security group rules for all Anti-DDoS Pro back-to-source IP segments to allow access from Anti-DDoS Pro. Add a security group rule to reject access from all IP addresses, and assign a lower priority (less than 10 in this example) to this rule.

7. When the security group rules are configured, assign this security group to the ECS instance that needs to allow access from the Anti-DDoS Pro back-to-source IP addresses. You can click **Manage Instances** under the **Actions** column of the security group, and then click **Add an ECS Instance** to add this ECS instance to the security group.

6 API Reference

7 FAQ

7.1 502 error reported after configuring Anti-DDoS Pro

This topic describes common causes and solutions to the 502 error reported when you attempt to access a domain name that is under the protection of Anti-DDoS Pro.

Anti-DDoS Pro IP blocked

- Symptoms

Anti-DDoS Pro acts as a reverse proxy between the client and origin site. This functionality makes the IP address of the origin site invisible to clients and all requests accessing the origin “looks like” coming from Anti-DDoS Pro IP addresses.

In addition, request traffic from each Anti-DDoS IP address is considerably large in amount, which makes the Anti-DDoS IP addresses much more suspicious to the origin site. However, if the source station IP is exposed, the client can request direct access to the source station, this bypasses the protection provided by high-security IP services.

- Analysis

In such cases, unless otherwise configured, the firewall or other security strategies in the origin site may regard Anti-DDoS IP addresses as abnormal or malicious visitors and thus blocks or imposes traffic restrictions on them. When Anti-DDoS Pro IP addresses are blocked or are subject to traffic restrictions, access requests passing through Anti-DDoS Pro are returned 502 errors.

- Resolution

You can resolve this issue by allowing all Anti-DDoS Pro IP addresses to access the origin site. The following methods are available to allow Anti-DDoS Pro IP addresses on the origin site:

- See [How to view the Anti-DDoS Pro IP addresses](#) to obtain all Anti-DDoS Pro IP addresses and add them to the whitelist of your origin site’s firewall and other host security protection software (such as a dongle).
- Disable the firewall and other host security protection software in the origin site.

Origin site exception

Origin site exception may cause response timeout when proceeding with an Anti-DDoS Pro request. Common origin site exceptions include the following cases:

- The origin site IP address is exposed and attacked, leading to an origin site crash.
- Physical failure in the origin site's server data center.
- Apache, Nginx, and other Web programs running on the origin site encounter a problem.
- High memory and CPU occupation on the server causes a sharp decrease in performance.
- The uplinks of the origin site are congested.

Analysis

Modify your local hosts file to redirect the domain name to the origin site IP address. If the origin site IP address cannot be accessed, ping the origin site IP address to check if any packet loss exists. If a packet loss exists, check if the telnet times out when attempting to access the server. If yes, chances are that the 502 error is caused by an origin site exception.

Resolution

Follow these steps to resolve this issue:

1. Check the origin site traffic and the request volume for a sharp increase, and compare the result with the Security Report data from the Anti-DDoS Pro console. If the origin site is under heavy traffic attack, but the Anti-DDoS Pro console shows no exceptions, it means that the attackers may have bypassed the Anti-DDoS Pro IP address, and attacked the origin site directly. In this case, we recommend that you [Change the origin site IP address](#).
2. After excluding the possibility of attacks, check the origin site server's process status, CPU/memory usage, bandwidth usage of the data center, and so on. In case of exceptions, we recommend that you contact server technicians or data center personnel to help you identify and fix the problem.
3. If only a limited number of clients have reported the 502 error, we recommend that you submit a ticket along with the clients' IP addresses and the time of error occurrence information. On the basis of information provided, the Alibaba Cloud technical professionals work on your ticket, take relevant steps, and assist to identify and resolve the issue.

Network congestion or jitter

Apart from the preceding two factors, occasional local network jitter, operator line failure, and some other factors may also cause the 502 error. Open a ticket to report this issue. The Alibaba Cloud technical professionals can also help you with the link quality monitoring information.

7.2 Anti-DDoS Pro FAQ

- *Can non-Alibaba Cloud users use Anti-DDoS Pro?*
- *Does Anti-DDoS Pro support upgrade from two-line subscription to three-line subscription?*
- *Does Anti-DDoS Pro support wildcard domain names?*
- *Can I upgrade to higher protection capabilities at any time if the 20 GB Anti-DDoS Basic capability of my Anti-DDoS Pro instance is insufficient?*
- *What will happen if my Anti-DDoS Pro instance expires?*
- *What is Anti-DDoS Pro bandwidth?*
- *Does it mean that each Anti-DDoS Pro IP address has a 500 Mbps service bandwidth if I purchase the Anti-DDoS Pro subscription with a service bandwidth of 500 Mbps?*
- *Is there any problem if the traffic exceeds the bandwidth of Anti-DDoS Pro?*
- *Does it support manual recovery if an Anti-DDoS Pro IP address has been thrown into the black hole?*
- *What is the role of the backup IP address for Anti-DDoS Pro (Hong Kong)?*
- *Will all Anti-DDoS Pro IP addresses be thrown into the black hole if the main IP address for Anti-DDoS Pro (Hong Kong) has been thrown into the back hole?*
- *What are the back-to-source IP addresses of Anti-DDoS Pro?*
- *Does Anti-DDoS Pro automatically add the Anti-DDoS Pro back-to-source IP addresses to the security group?*
- *Can I enter the intranet IP address as the origin IP address for Anti-DDoS Pro?*
- *Is there any delay when I modify the origin IP address for Anti-DDoS Pro?*
- *How long will it take for configuration modifications to come into effect, if the modifications are made from the Anti-DDoS Pro console?*
- *How can I view the attacker's IP address from the Anti-DDoS Pro console?*
- *How long will attack source IP address data be kept by Anti-DDoS Pro?*

- *Is it true that I can only retrieve the last month's data from the Anti-DDoS Pro security report?*
- *How can I know which website is attacked if I have configured multiple websites under the same Anti-DDoS Pro instance?*
- *What is the CNAME scheduling rule for Anti-DDoS Pro?*
- *How does a non-website CNAME use CNAME domain name scheduling?*
- *Does Anti-DDoS Pro support health check?*
- *How to balance the load if Anti-DDoS Pro is configured with multiple origins?*
- *Does Anti-DDoS Pro support packet capturing files?*
- *Does Anti-DDoS Pro support session persistence?*
- *How does Anti-DDoS Pro perform session persistence?*
- *What is the default TCP connection timeout value for Anti-DDoS Pro?*
- *What is the default HTTP/HTTPS connection timeout value for Anti-DDoS Pro?*
- *Does Anti-DDoS Pro support IPv6 protocol?*
- *Does Anti-DDoS Pro support WebSocket protocol?*
- *Does Anti-DDoS Pro support HTTPS two-way authentication?*
- *Why cannot old version browsers and Android clients normally access HTTPS sites?*
- *What are the SSL protocols and encryption suites supported by Anti-DDoS Pro?*
- *What are the total numbers of forwarding ports and domain names supported by Anti-DDoS Pro?*
- *The server's traffic does not reach the cleaning threshold. Why does some scrubbed traffic appear in the security report?*

Can non-Alibaba Cloud users use Anti-DDoS Pro?

Yes, non-Alibaba Cloud users can use Anti-DDoS Pro.

Anti-DDoS Pro uses a public network to return traffic back to origins, so all servers that are accessible to the public routes on Alibaba Cloud, other clouds, and IDC data centers can use Cloud Anti-DDoS Pro.

Does Anti-DDoS Pro support upgrade from two-line subscription to three-line subscription?

No, Anti-DDoS Pro does not support line upgrade. You can purchase the three-line Anti-DDoS Pro, and then migrate the original configuration to it. After confirming that the original two-line Anti-DDoS Pro has no business traffic, you can submit a ticket, indicating that you have already purchased the three-line Anti-DDoS Pro and

the services have been migrated, and apply a refund for the original two-line Anti-DDoS Pro.

Does Anti-DDoS Pro support wildcard domain names?

Yes, Anti-DDoS Pro website protection supports wildcard domain names. You can use wildcard domain names when configuring HTTP flood protection and Web application protection.

Wildcard domain name resolution indicates the operation that uses a wildcard character (asterisk) as the subdomains, and direct all subdomains to the same IP address. For example, if you configure wildcard domain name resolution for `www.taobao.com`, all requests that access `*.taobao.com` will be resolved to the IP address in the wildcard domain name resolution configuration.

Can I upgrade to higher protection capabilities at any time if the 20 GB Anti-DDoS Basic capability of my Anti-DDoS Pro instance is insufficient?

You can adjust Elastic Protection bandwidth on the Asset > Instance List page of the [Anti-DDoS Pro console](#) at any time to obtain higher DDoS protection capability. Elastic protection bandwidth adjustment becomes immediately effective.

What will happen if my Anti-DDoS Pro instance expires?

Anti-DDoS Pro loses protection capability after expiration, but the forwarding rule configuration still functions normally. When the traffic exceeds the limit, traffic restrictions are triggered, which may cause random packet loss. You can release the instance from the console.

What is Anti-DDoS Pro bandwidth?

Service protection bandwidth for Anti-DDoS Pro is a normal traffic value accumulated by an Anti-DDoS Pro instance (subject to the maximum value of the inbound traffic or outbound traffic) in the unit of Mbps. You can upgrade the service bandwidth for your Anti-DDoS Pro instance at any time from the Asset > Instance List page of the [Anti-DDoS Pro console](#). You can upgrade the service bandwidth up to 2 Gbps.

Does it mean that each Anti-DDoS Pro IP address has a 500 Mbps service bandwidth if I purchase the Anti-DDoS Pro subscription with a service bandwidth of 500 Mbps?

The purchased business bandwidth is for the entire high-security instance. No, the service bandwidth you have is for the entire Anti-DDoS Pro instance. If you have three

Anti-DDoS Pro IP addresses for your Anti-DDoS Pro instance, then the total service bandwidth of these three IP addresses cannot be greater than 500 Mbps.

Is there any problem if the traffic exceeds the bandwidth of Anti-DDoS Pro?

If your traffic exceeds the service bandwidth that you have purchased, the system will trigger traffic restrictions, which may cause random packet loss.

Does it support manual recovery if an Anti-DDoS Pro IP address has been thrown into the black hole?

Currently, Anti-DDoS Pro supports black hole deactivation to partial ISP lines. Each Anti-DDoS Pro user has up to three chances to deactivate the black hole status in one day. You cannot do the deactivation after the chances exhausted. For more information, see [Deactivate black hole](#).

What is the role of the backup IP address for Anti-DDoS Pro (Hong Kong)?

If the main IP address' data center crashes or is down, and cannot be quickly restored, you can use the backup IP address for failover. To guarantee smooth failover, make sure that the configuration for the backup IP address and that for the main IP address are synchronized.



Note:

Protection capability for the main and backup IP addresses are different. Please use the main IP address to protect your service. The backup IP address is only designed for use in failover, and is not recommended for use during normal occasions.

Will all Anti-DDoS Pro IP addresses be thrown into the black hole if the main IP address for Anti-DDoS Pro (Hong Kong) has been thrown into the back hole?

No. After the main IP address has been thrown into the black hole, the default backup IP address will not be thrown into the black hole. However, in this case, Anti-DDoS Pro does not automatically resolve your service to the backup IP address. The backup IP address' protection capability is only 500 MB. If you manually resolve your service to the backup IP address, then the backup IP address will also be thrown into the black hole when the attack traffic exceeds the protection capability.

What are the back-to-source IP addresses of Anti-DDoS Pro?

You can view the detailed back-to-source IP segments for Anti-DDoS Pro from the [Anti-DDoS Pro console](#). For more information, see [How to view the Anti-DDoS Pro back-to-source IP segment](#).

Does Anti-DDoS Pro automatically add the Anti-DDoS Pro back-to-source IP addresses to the security group?

No. Anti-DDoS Pro does not add the Anti-DDoS Pro back-to-source IP segment to the security group. You do not need to add them to your ECS or VPC security group either. However, if you have deployed a firewall or other host security protection software for your origin, you must add the Anti-DDoS Pro back-to-source IP segment to the corresponding whitelist.

Can I enter the intranet IP address as the origin IP address for Anti-DDoS Pro?

No. Anti-DDoS Pro is a public network back-to-source service, and does not support intranet IP addresses.

Is there any delay when I modify the origin IP address for Anti-DDoS Pro?

After you modify the origin IP address protected by Anti-DDoS Pro, the modifications will come into effect after approximately five minutes. We recommend that you perform modification during off-peak hours.

How long will it take for configuration modifications to come into effect, if the modifications are made from the Anti-DDoS Pro console?

Generally, the modified configuration comes into effect in 5 to 10 minutes.

How can I view the attacker's IP address from the Anti-DDoS Pro console?

You can view the attacker's IP address and the relevant attack information from the Security Report page on the Anti-DDoS Pro console.

How long will attack source IP address data be kept by Anti-DDoS Pro?

Anti-DDoS Pro keeps the attack source IP address data for 30 days. We recommend that you retrieve the relevant data from the Anti-DDoS Pro Security Report in a timely manner.

Is it true that I can only retrieve the last month's data from the Anti-DDoS Pro security report?

Yes. Currently, Anti-DDoS Pro Security Report can only support to retrieve the data of the previous month. We recommend that you retrieve the corresponding Security Report in a timely manner.

How can I know which website is attacked if I have configured multiple websites under the same Anti-DDoS Pro instance?

From the data packet layer, we cannot identify which of the websites protected by Anti-DDoS Pro is the target of heavy traffic DDoS attacks. We recommend that you use multiple Anti-DDoS Pro instances, and deploy your websites respectively on different Anti-DDoS Pro instances. Then you can identify the information about attacks against each website.

What is the CNAME scheduling rule for Anti-DDoS Pro?

When an Anti-DDoS Pro IP address is thrown into the black hole, CNAME Auto Switch function randomly forwards the traffic that has been sent to this IP address to the Anti-DDoS Pro IP address in another line. The effective time of such schedule is subject to the Local DNS cache update time.



Note:

You must enable CNAME Auto Switch to use it.

How does a non-website CNAME use CNAME domain name scheduling?

Website CNAME: Each domain name generates an independent CNAME, which has the automatic scheduling capability after an IP address is thrown into the black hole.



Note:

If the following conditions are met, the non-website configuration can achieve automatic scheduling function by using a website CNAME.

- Non-website forwarding configurations for three lines are consistent.
- The application supports domain name scheduling.

In this case, you can configure website access (for example, forward.example.com), and use this website configuration to generate a CNAME to use in non-website forwarding, achieving the CNAME automatic scheduling function.

Does Anti-DDoS Pro support health check?

Yes. Web service enables health check by default.

Non-web service disables health check by default, but you can enable it from the console. For more information, see [Anti-DDoS Pro health check configuration](#).

How to balance the load if Anti-DDoS Pro is configured with multiple origins?

- The web service uses the source address hashing method to perform load balancing.
- Non-web service uses the weighted round robin (wrr) method for round-robin scheduling, and the load weight is 1:1:1.

Does Anti-DDoS Pro support packet capturing files?

No. Anti-DDoS Pro in China Telecom and China Unicom lines does not support the download of packet capturing files. You can directly view the attack source IP information from the Alibaba Cloud Security console.

For BGP line Anti-DDoS Pro, you can submit a ticket, indicating the related IP addresses and the black hole time, to retrieve the sampling packet that captures files during the attack.

Does Anti-DDoS Pro support session persistence?

Yes. Anti-DDoS Pro supports session persistence, but this function is disabled by default. You can configure session persistence for non-web services from the console. For more information, see [Anti-DDoS Pro session persistence rules](#).

How does Anti-DDoS Pro perform session persistence?

After you enable session persistence, Anti-DDoS Pro constantly sends requests from the same IP address to the same server on the origin, during the period set for session persistence. However, if the client's network environment changes (for example, switching from a wired network to a wireless network, from the 4G network to a wireless network, and so on), session persistence may fail because of the change of the IP address.

What is the default TCP connection timeout value for Anti-DDoS Pro?

The default TCP connection timeout value for Anti-DDoS Pro is 900s. You can configure session persistence for non-web services from the console. For more information, see [Anti-DDoS Pro session persistence rules](#).

What is the default HTTP/HTTPS connection timeout value for Anti-DDoS Pro?

The default HTTP/HTTPS connection timeout value for Anti-DDoS Pro is 120s.

Does Anti-DDoS Pro support IPv6 protocol?

No, Anti-DDoS Pro currently does not support IPv6 protocol.

Does Anti-DDoS Pro support WebSocket protocol?

Yes, Web service of Anti-DDoS Pro supports WebSocket protocol.

Does Anti-DDoS Pro support HTTPS two-way authentication?

- Anti-DDoS Pro that uses the website access method does not support HTTPS two-way authentication.
- However, Anti-DDoS Pro that uses the non-website access method and TCP forwarding method supports HTTPS two-way authentication.

Why cannot old version browsers and Android clients normally access HTTPS sites?

Please check whether the clients support SNI authentication. For problems that SNI authentication may cause, see [HTTPS access exceptions arising from SNI compatibility](#).

What are the SSL protocols and encryption suites supported by Anti-DDoS Pro?

Supported SSL protocols

- TLSv1
- TLSv1.1
- TLSv1.2

Supported encryption suites

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- AES128-GCM-SHA256
- AES256-GCM-SHA384

- AES128-SHA256
- AES256-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-ECDSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-SHA
- AES128-SHA
- AES256-SHA
- DES-CBC3-SHA
- RSA+3DES

What are the total numbers of forwarding ports and domain names supported by Anti-DDoS Pro?

- Total number of forwarding ports: TCP and UDP protocols support 50 forwarding ports for each IP address by default, which can be extended to a maximum of 200 ports for each IP address.
- Total number of supported domain names: HTTP and HTTPS support forwarding a total of 50 domain names for each instance by default, which can be extended to a maximum of 200 domain names for each IP address.

The server's traffic does not reach the cleaning threshold. Why does some scrubbed traffic appear in the security report?

For services that have accessed in the Anti-DDoS Pro service, Anti-DDoS Pro automatically filters some malformed packets in the network traffic (for example , small SYN packets and SYN flag bit exceptions that do not conform to the TCP protocol). Thus, your server does not have to waste resources to deal with these obvious malformed packets. This type of filtered malformed packets are also counted in the scrubbed traffic, and that is the reason for that scrubbed traffic appears even if your server's traffic does not reach the cleaning threshold.

7.3 Troubleshoot Anti-DDoS Pro access problems

Symptoms

When a client attempts to access a website protected by Anti-DDoS Pro, the response becomes slow and choppy. It also suffers serious delay and packet loss.

Analysis

Collect the affected clients' source IP addresses, and perform link testing by using Traceroute/TRACERT, MTR, or network monitoring tools to determine the cause of this issue.

Resolution

- Cross-network accesses

Anti-DDoS Pro supports the following types of lines: China Telecom, China Unicom, and BGP lines. The BGP line is used to optimize the network quality of China Mobile and small telecommunication operators.

- When a non-China Telecom client (for example, a client using the China Unicom or China Mobile network) accesses the China Telecom line, delay and packet loss may occur.
- When a non-China Unicom client (for example, a client using the China Telecom or China Mobile network) accesses the China Unicom line, delay and packet loss may occur.

Solution: We recommend that you configure multiple lines for clients with different ISPs. For example, make the China Telecom clients access the China Telecom line, China Unicom clients access the China Unicom line, and clients using China Mobile and other networks access the BGP line.

- Backend server exceptions

Depending on the origin type, you can use the following troubleshooting methods to detect exceptions on your backend server.

- For Server Load Balancer (SLB) origins

Follow these steps to troubleshoot issues on a Server Load Balancer origin.

1. Run the `tcping` tool for SLB IP addresses and ports, to check for exceptions in the log.
2. Check the status of the SLB instance for exceptions. For example, you can check the connection count and backend server.
3. Check for a blacklist/whitelist or any other access control policies on the SLB . Make sure that the Anti-DDoS Pro back-to-source IP segments are allowed in these settings.
4. Check for security software or any other IP address blocking policies on ECS or VPC.



Note:

A security software may regard the Anti-DDoS Pro IP addresses as malicious IP addresses because all access requests are forwarded by Anti-DDoS Pro to the backend server after you enable the service. Therefore you must set rules in the security software to allow Anti-DDoS IP addresses to pass through.

5. Check if the SLB IP address is exposed.

- For cloud server (ECS/VPC) origins

Follow these steps to troubleshoot issues on an ECS or a VPC origin.

1. Run the `tcping` tool for server IP addresses and ports, to check for exceptions in the log.
2. Check for exceptions on the backend server. For example, the server IP address is in the black hole, the server is subject to traffic cleaning, the

CPU consumption is high, the database response is slow, and the outbound bandwidth is full.

3. Check for a blacklist/whitelist or any other access control policies on the server. Make sure that the Anti-DDoS Pro back-to-source IP segments are allowed in these settings.
 4. Check for any security software or other IP address blocking policies on the ECS or VPC instance. Make sure that the Anti-DDoS Pro back-to-source IP addresses are not blocked.
 5. Check if the server IP address is exposed.
- For non-Alibaba Cloud server origins

Follow these steps to troubleshoot issues on a non-Alibaba Cloud server origin.

1. Run the `tcping` tool for server IP address and ports, to check for exceptions in the log.
2. Check for exceptions on the server, such as high CPU consumption, slow database response, and full outbound bandwidth.
3. Check for a blacklist/whitelist or any other access control policies on the server. Make sure that the Anti-DDoS Pro back-to-source IP segments are allowed in these settings.
4. Check for any security software or other IP address blocking policies on the server.



Note:

Make sure that the Anti-DDoS Pro back-to-source IP addresses are not blocked.

5. Check if the server IP address is exposed.



Note:

We recommend that you replace your origin IP address after enabling Anti-DDoS Pro, and stop using the IP address that is already exposed.

- Traffic-cleaning events

In cases where Anti-DDoS Pro IP address is subject to a traffic-cleaning event, follow these steps to determine the issue:

1. Run the `tcpping` tool for the affected ports to detect delay or packet loss. Record the result.
2. Run the `tcpping` tool for the unaffected ports to detect delay or packet loss. Record the result.

Compare the recorded results with the following table to determine the issue.

| Delay or packet loss on affected ports | Delay or packet loss on unaffected ports | Analysis |
|--|--|---|
| Yes | No | The traffic cleaning policy causes no false positives. You can check the backend server's status and protection performance. If the server's protection capability is relatively weak, you must apply a more stringent protection policy. |
| Yes | Yes | The traffic cleaning policy causes false positives. You can submit a ticket for further backend inspection. |
| No | No | The issue is not caused by the traffic cleaning policy. |
| No | Yes | Generally, such a case does not exist. |

For the first two cases, we recommend that you submit a ticket to our after-sales technical support team and describe the issue in detail. Upon receiving a ticket, Alibaba Cloud technical professionals will help you solve the issue. If you want to apply a more stringent protection policy, you must contain the detailed parameters of your server's protection capability in the ticket. These parameters are:

- Description of normal user access
- Main service interaction process
- External service capability of your application

- Black hole events

In cases where Anti-DDoS Pro IP address is subject to a black hole event, identify the affected IP address and check if all affected requests pass through this IP address. Under certain circumstances, Anti-DDoS Pro supports automatic failover when an IP address is thrown into the black hole. But the actual time required for the changes to come into effect on clients depends on the time of DNS resolution, and local DNS caching and update.

- Web services

Go to the Anti-DDoS Pro > Web Service page, and check if the CNAME Auto Switch function is enabled. CNAME Auto Switch can switch the Anti-DDoS Pro service to a healthy line when the current line becomes unavailable. It provides the failover capability to guarantee the service continuity and availability.

- When the IP address of the China Telecom line is thrown into the black hole, CNAME automatically cancels resolution to the China Telecom IP address, and only resolves to China Unicom and BGP lines.
- When the IP address of the China Unicom line is thrown into the black hole, CNAME automatically cancels resolution to the China Unicom IP address, and only resolves to China Telecom and BGP lines.
- When the IP address of the China BGP line is thrown into the black hole, CNAME automatically cancels resolution to the BGP IP address, and only resolves to China Telecom and China Unicom lines.

- Non-web services

For non-website access, you can only depend on the built-in scheduling configuration because Anti-DDoS Pro does not provide CNAME automatic switching for it.

You can configure your application in a way that it is empowered with the failover capability. So that when the IP address of a line is thrown into the black hole, the application can switch to a healthy line.

- Other issues

If the issue persists, submit a ticket to contact the after-sales technical support team. We recommend that you include the following access information in the ticket to help our technical professionals quickly identify and analyze the issue.

| Line | Source IP address | Anti-DDoS Pro IP address | Ping info | Traceroute or MTR info | Tcping or port connection info |
|--------------------|-----------------------|----------------------------|--|---|--|
| China Telecom line | For example , 1.1.1.1 | For example , 180.97.163.0 | Results of more than 10 consecutive ping requests. | For example , Tracert or Traceroute info of accessing 180.97.163.0 from 1.1.1.1 | Results of more than 10 consecutive tcping requests. Or the port connection information. |
| China Unicom line | ... | ... | ... | ... | |

| Line | Source IP address | Anti-DDoS Pro IP address | Ping info | Traceroute or MTR info | Tcping or port connection info |
|----------|-------------------|--------------------------|-----------|------------------------|--------------------------------|
| BGP line | ... | ... | ... | ... | |

The following information also helps identify the issue:

- Configuration type of Anti-DDoS Pro back-to-source IP addresses, such as SLB, cloud server (ECS/VPC), and non-Alibaba Cloud server.
- Back-to-source IP addresses, and logs for the SLB, cloud server (ECS/VPC), or non-Alibaba Cloud server, including CPU, memory, bandwidth, and total connections.
- Access control policies applied in the origin.
- Security software installed in the origin, such as cloud locks, dongles, and the built-in iptables.
- Security policies applied in the origin, such as inspection and filtering for IP addresses.
- Traffic-cleaning or black hole events that Anti-DDoS Pro IP address is subject to.
- Service type, such as website, client games, web games, App, and so on.
- Operations that involve modifying or deleting the Anti-DDoS Pro instance during the occurrence of the issue.

Commonly used network monitoring tools

Traceroute command line tool

Traceroute is a network testing tool pre-installed on almost all versions of Linux. It tracks the path of transferring data packets to a target IP address using Internet Protocol (IP).

Traceroute firstly sends UDP testing packets whose maximum Time To Live (Max_TTL) period is short, and then listens to the ICMP TIME_EXCEEDED response on the entire link starting from the gateway. The testing starts when TTL=1 and continues as the TTL value increases until you receive the ICMP PORT_UNREACHABLE message. The ICMP PORT_UNREACHABLE message identifies if the target host is located, or if the maximum TTL value to track the path of transferring data packets is reached.

**Note:**

Traceroute sends UDP data packets for link testing by default. You can set the **-I** parameter so that traceroute sends an ICMP data packet for link testing.

Usage:

```
[ root @ centos ~]# traceroute -I 223 . 5 . 5 . 5
traceroute to 223 . 5 . 5 . 5 ( 223 . 5 . 5 . 5 ), 30 hops
max , 60 byte packets
 1 * * *
 2 192 . 168 . 17 . 20 ( 192 . 168 . 17 . 20 ) 3 . 965 ms
 4 . 252 ms 4 . 531 ms
 3 111 . 1 . 20 . 41 ( 111 . 1 . 20 . 41 ) 6 . 109 ms 6 .
 574 ms 6 . 996 ms
 4 111 . 1 . 34 . 197 ( 111 . 1 . 34 . 197 ) 2 . 407 ms 2
 . 451 ms 2 . 533 ms
 5 211 . 138 . 114 . 25 ( 211 . 138 . 114 . 25 ) 1 . 321 ms
 1 . 285 ms 1 . 304 ms
 6 211 . 138 . 114 . 70 ( 211 . 138 . 114 . 70 ) 2 . 417 ms
 211 . 138 . 114 . 66 ( 211 . 138 . 114 . 66 ) 1 . 857 ms 211 .
 138 . 114 . 70 ( 211 . 138 . 114 . 70 ) 2 . 002 ms
 7 42 . 120 . 244 . 194 ( 42 . 120 . 244 . 194 ) 2 . 570 ms
 2 . 536 ms 42 . 120 . 244 . 186 ( 42 . 120 . 244 . 186 ) 1 .
 585 ms
 8 42 . 120 . 244 . 246 ( 42 . 120 . 244 . 246 ) 2 . 706 ms
 2 . 666 ms 2 . 437 ms
 9 * * *
10 public1 . alidns . com ( 223 . 5 . 5 . 5 ) 2 . 817 ms 2
 . 676 ms 2 . 401 ms
```

TRACERT command line tool

TRACERT (or Trace Route) is a Windows command line utility for network diagnosis. It tracks the path of an IP data packet sent to the target IP address.

TRACERT sends ICMP data packets to determine the route to the target address. In these data packets, TRACERT uses different TTL values of IP addresses. Since routers along the data packet forwarding path must at least reduce the TTL by 1 before forwarding data packets, the TTL is actually equivalent to a hop counter. When the TTL of a packet reaches zero, the corresponding node sends an ICMP “timeout” message to the source computer.

TRACERT firstly sends the packet whose TTL value is 1, increases the TTL value by 1 and sends the corresponding packet in each subsequent transmission until the destination responds or the maximum TTL value is reached. The ICMP “timeout” messages sent back from intermediate routers contain information of corresponding nodes.

Usage:

```

C :\> tracert - d 223 . 5 . 5 . 5
Use at most 30 hops to track the routes of 223 .
5 . 5 . 5 .

 1      *      *      *      Request timeout .
 2      9 ms    3 ms    12 ms    192 . 168 . 17 . 20
 3      4 ms    9 ms    2 ms    111 . 1 . 20 . 41
 4      9 ms    2 ms    1 ms    111 . 1 . 34 . 197
 5     11 ms    *      *      211 . 140 . 0 . 57
 6      3 ms    2 ms    2 ms    211 . 138 . 114 . 62
 7      2 ms    2 ms    1 ms    42 . 120 . 244 . 190
 8     32 ms    4 ms    3 ms    42 . 120 . 244 . 238
 9      *      *      *      Request timeout .
10     3 ms    2 ms    2 ms    223 . 5 . 5 . 5

Tracking is finished .

```

For more information about TRACERT command line tool, see [Link testing tools for ping packet loss or ping failure](#).

TCPing tool

TCPing tool uses TCP method to view the port status and detect TCP delay and connection information. [Click to download the TCPing tool](#).

- Usage in Windows

Copy the TCPing tool to the specified Windows directory and run the following

command: `C :\> tcping . exe www . aliyun . com 80`

Example

```

C :\> tcping . exe www . aliyun . com 80

Probing 140 . 205 . 62 . 8 : 80 / tcp - Port is open -
time = 19 . 550ms
Probing 140 . 205 . 62 . 8 : 80 / tcp - Port is open -
time = 8 . 761ms
Probing 140 . 205 . 62 . 8 : 80 / tcp - Port is open -
time = 10 . 899ms
Probing 140 . 205 . 62 . 8 : 80 / tcp - Port is open -
time = 13 . 013ms

Ping statistics for 140 . 205 . 62 . 8 : 80
    4 probes sent .
    4 successful, 0 failed .
Approximate trip times in milli - seconds :

```

```
Minimum = 8 . 761ms , Maximum = 19 . 550ms , Average = 13 . 056ms
```

- Usage in Linux

Run the following command to install the TCping tool.

```
tar zxvf tcping - 1 . 3 . 5 . tar . gz
cd tcping - 1 . 3 . 5
make tcping . linux
```

Usage example:

```
[ root @ aliyun tcping - 1 . 3 . 5 ]# for (( i = 0 ; i < 10 ; +
+ i )) ; do ./ tcping www . aliyun . com 80 ; done
www . aliyun . com port 80 open .
www . aliyun . com port 80 open .
www . aliyun . com port 80 open .
www . aliyun . com port 80 open .
www . aliyun . com port 80 open .
www . aliyun . com port 80 open .
www . aliyun . com port 80 open .
www . aliyun . com port 80 open .
www . aliyun . com port 80 open .
www . aliyun . com port 80 open .
```

7.4 504 errors reported when handling requests with long processing time

While attempting to handle certain POST requests, the website protected by Anti-DDoS Pro waits for much longer time than required and returns a 504 error.

Analysis

This issue is because the request needs long processing time, which exceeds the connection threshold of Anti-DDoS Pro. As a result, Anti-DDoS Pro closes the connection. The default connection thresholds of Anti-DDoS are as follows:

- The TCP connection timeout value is 900s.
- The HTTP/HTTPS connection timeout value is 120s.

Resolution

We recommend that you configure a heartbeat detection for requests with long processing time. Enabling heartbeat detection can help make sure that the connection is active while you wait for a request to be handled.

Additionally, you can bypass Anti-DDoS Pro for certain requests, and have these requests directly access the backend ECS instance.

7.5 How to view the Anti-DDoS Pro IP addresses?

To avoid your Anti-DDoS Pro back-to-source IP segments from being blocked or being subject to traffic restrictions by the origin, you can add the Anti-DDoS Pro back-to-source IP segments to the whitelist of your origin's firewall or other host security protection software.

Follow these steps to view the Anti-DDoS Pro back-to-source IP segments.

1. Log on to the [Anti-DDoS Pro console](#).
2. Go to the **Access > Website** page.
3. Click **Back-to-source CIDR block** in the upper right corner of the page to view all the back-to-source IP segments of Anti-DDoS Pro.
4. You can add the corresponding Anti-DDoS Pro back-to-source IP segments to the whitelist of your origin's firewall or other host security protection software, based on the lines you use.

7.6 Elastic protection FAQ

- [Do I need to pay any fees for Elastic Protection when no attack occurs within one month?](#)
- [What is my final protection capability if I have purchased the 20 GB Anti-DDoS Basic and 50 GB Elastic Protection?](#)
- [What if the maximum Elastic Protection capability is exceeded?](#)
- [How will I be charged if I have purchased the 50 GB Elastic Protection, but the actual attack traffic is only 30 GB?](#)
- [Can I change the Elastic Protection capability from the current 100 GB to 200 GB?](#)
- [How to calculate the fees if an IP has been attacked multiple times in one day?](#)
- [Will I be charged based on the maximum attack traffic, if I have purchased a two-line subscription, and both the China Telecom and China Unicom IP addresses have been attacked?](#)
- [How do I stop using the Elastic Protection capability to avoid the post-payment fees after purchasing an anti-DDoS Pro instance?](#)

Do I need to pay any fees for Elastic Protection when no attack occurs within one month?

In this case, you only need to pay the subscription fee for the Anti-DDoS Basic bandwidth, and no additional fees are incurred.

**Note:**

If the service traffic exceeds the specification of Anti-DDoS Pro (200 Mbps for hosts inside Alibaba Cloud, and 100 Mbps for hosts outside Alibaba Cloud), corresponding traffic fees are incurred.

What is my final protection capability if I have purchased the 20 GB Anti-DDoS Basic and 50 GB Elastic Protection?

The final protection capability is 50 GB, which is subject to the Elastic Protection capability. For example, if you select the 20 GB Elastic Protection, you can only enjoy a protection capability of 20 GB, which is equivalent to without Elastic Protection.

What if the maximum Elastic Protection capability is exceeded?

When the attack traffic exceeds the maximum elastic protection capability for an IP address, this IP address is thrown into the black hole, and all traffic to/from it is blocked.

How will I be charged if I have purchased the 50 GB Elastic Protection, but the actual attack traffic is only 30 GB?

Basically, the fees are charged by the peak attack traffic. When the attack traffic is smaller than 20 GB (covered by Anti-DDoS Basic), no additional fee is charged. When the peak attack traffic is 30 GB, you only pay for protection of 30 GB. For specific fees, please contact our customer support representative.

Can I change the Elastic Protection capability from the current 100 GB to 200 GB?

Yes. You can adjust the Elastic Protection bandwidth in the Anti-DDoS Pro console, and you can either increase or decrease the bandwidth.

**Note:**

When the protection bandwidth is changed, the changes are effective from the following day because you are already charged for the attacks that occurred during the present day.

How to calculate the fees if an IP has been attacked multiple times in one day?

The fees are charged based on the peak attack traffic during the day (0:00-24:00), and is charged only once. If an IP address is attacked three times in a day, and the attack traffic is 50 GB, 100 GB, and 200 GB respectively, then the Elastic Protection fee is charged based on the attack traffic of 200 GB.

Will I be charged based on the maximum attack traffic, if I have purchased a two-line subscription, and both the China Telecom and China Unicom IP addresses have been attacked?

The fees are charged based on individual IP addresses, rather than the Anti-DDoS Pro instance. Therefore, both lines are separately charged for Elastic Protection based on the maximum attack traffic of these two IP addresses.

How do I stop using the Elastic Protection capability to avoid the post-payment fees after purchasing an anti-DDoS Pro instance?

You can set the Elastic Protection bandwidth for your Anti-DDoS Pro instance to the same value as the Anti-DDoS Basic bandwidth. In this case, the system does not enable Elastic Protection when your IP address suffers from attack traffic that is higher than the Anti-DDoS Basic bandwidth.

You can log on to the Anti-DDoS Pro console and go to the Asset > Instance List to adjust the Elastic Protection bandwidth for your Anti-DDoS Pro instance.

7.7 Fail to upload large files on the website with Anti-DDoS Pro enabled

After enabling Anti-DDoS Pro protection for the domain name, I cannot upload large files to the website, and the system throws a 413 error.

Analysis

Anti-DDoS Pro limits the maximum file size allowed to be uploaded to the website. If you attempt to upload a file that exceeds 300 Mb in size, a 413 error is thrown.

Resolution

- Method 1

Compress the file before uploading it, and make sure that the file you upload is smaller than 300 MB.

- Method 2

We recommend that you store large files in an Alibaba Cloud OSS bucket, rather than uploading it directly to the origin ECS server.

- Method 3

For occasional upload needs, you can temporarily map the HOST name to the IP address to bypass Anti-DDoS Pro, and directly access the ECS instance to upload the file.

7.8 Security group rule misconfiguration results into access exceptions

You can configure Non-Web Service of Anti-DDoS Pro for an origin site of Alibaba Cloud ECS or VPC. However, if the rule “Only allow Anti-DDoS Pro IP addresses, and block all other IP addresses” exists in the ECS/VPC security group, it can block the real IP address of the client.

Analysis

The latest security group version can obtain the visitors’ real IP addresses. Therefore, the “only allow/deny all” access rule can disturb the normal access traffic.

Resolution

Modify the ECS security group rules based on visitors’ real IP addresses.

Example

Assume that a complete access process is as follows: Client (real IP address: 1.1.1.1) > Anti-DDoS Pro (Back-to-source IP address: 2.2.2.2) > ECS

If you have set the rule in ECS security group to only allow IP address 2.2.2.2, then you must delete this rule. In addition, you have to decide whether to allow certain real client IP addresses based on your actual situation.

7.9 HTTPS access exceptions arising from SNI compatibility

What is SNI

The web hosting concept is introduced to HTTP servers to allow multiple domain names to use the same IP address, as the IPv4 addresses become scarce. A server can forward requests to different domain names (web hosts) based on the specified host in the request.

However, on an HTTPS server where an IP address is shared by multiple domain names (web hosts), the server doesn't know the specific host that a client requests at the start of the handshaking process. Therefore, the server cannot forward the request to the specific web host. But to complete the handshaking process, the server must obtain the certificate information in the web host's configuration.

Server name indication (SNI) is designed to resolve this issue. SNI requires the client to carry the host information of the domain name to be accessed before the handshake process with the server. The server can then choose the correct web host's certificate to establish a handshake and TLS connection with the client.

SNI was first introduced in 2014 and is now supported by all mainstream browsers, servers, and testing tools.

Why must the client support SNI to use Anti-DDoS Pro and WAF

When processing reverse proxy of HTTPS services, Anti-DDoS Pro and WAF interact with the real server (RS) on behalf of the client. So the certificates and private keys must be uploaded in the configurations of HTTPS protection. Because the Anti-DDoS Pro and WAF servers are limited in number, it is impossible to assign a physical server to a domain name. Therefore, the Anti-DDoS Pro and WAF clusters must contain servers that are shared by multiple domain names. As a result, the client must support SNI to interact normally with the Anti-DDoS Pro and WAF servers.

When you use a browser that does not support SNI to access a website protected by Anti-DDoS Pro or WAF, the Anti-DDoS Pro or WAF server fails to know the specific domain name which the client has requested. When the server cannot obtain the correct web host's certificate to interact with the client, the built-in certificate is adopted by default. In this case, the client browser prompts "Server certificate cannot be trusted" .



Note:

In theory, when an IP address is not shared by multiple domain names, it's not necessary for the client browser to support SNI. However, even if the real server serves only one domain name, the Anti-DDoS Pro or WAF server still need to conduct reverse proxy between the client and the origin. Therefore, the client still must support SNI to establish the connection with the Anti-DDoS Pro or WAF server.

Resolution

Server end

Configure your server to enable multiple HTTPS web hosts with one IP address.

Client end

If your client does not support SNI, consider the following suggestions:

- We recommend that you use the latest version of Google Chrome and Firefox browsers.
- Do not configure layer-7 website protection in Anti-DDoS Pro. Instead, configure website protection by using the layer-4 port 443 forwarding method.



Note:

The layer-4 protection does not protect your website against HTTP flood attacks.

SNI compatibility



Note:

SNI is compatible with the TLS 1.1 and later versions, but is not compatible with the SSL protocol.

SNI is supported by the following desktop browsers in clients:

- Chrome 5 and later versions
- Chrome 6 and later versions
- Firefox 2 and later versions
- Internet Explorer 7 and later versions (Only supports Windows Vista, Windows Server 2008, and later OS versions. In Windows XP, no IE browsers support SNI)
- Konqueror 4.7 and later versions
- Opera 8 and later versions
- Safari 3.0 and later versions (Only supports Windows Vista, Windows Server 2008, and later Windows versions, or Mac OS X 10.5.6 and later Mac versions)

SNI is supported by the following mobile phone browsers in clients:

- Android 3.0 Honeycomb and later versions
- iOS 4 and later versions
- Windows Phone 7 and later versions

SNI is supported by the following servers:

- Apache 2.2.12 and later versions
- Apache Traffic Server 3.2.0 and later versions
- Cherokee
- HAProxy 1.5 and later versions
- IIS 8.0 and later versions
- Lighttpd 1.4.24 and later versions
- LiteSpeed 4.1 and later versions
- Nginx 0.5.32 and later versions

SNI is supported by the following command lines:

- cURL 7.18.1 and later versions
- wget 1.14 and later versions

SNI is supported by the following libraries:

- GNU TLS
- JSSE (Oracle Java) 7 and later versions (only for use as a client)
- libcurl 7.18.1 and later versions
- NSS 3.1.1 and later versions
- OpenSSL 0.9.8j and later versions
- OpenSSL 0.9.8f and later versions (flag must be configured)
- QT 4.8 and later versions

7.10 How to convert an HTTPS certificate to the PEM format

A PEM certificate file (*.pem) usually takes the following format:



Note:

You can use notepad++ and other text editors to open PEM certificate files.

```
-----BEGIN CERTIFICATE-----
62EcYPWd2Oy1vs6MTXcJSfN9Z7rZ9fmxWr2BFN2XbahgnsSXM48ixZJ4k
rc+1M+j 2kcubVpsE2cgHdj4v8H6jUz9Ji4mr7vMNS6dXv8PUkl/qoDeNG
CNdyTS5NIL5ir+ g92cL8IGOkjgvhlqt9vc65Cgb4mL+n5+DV9uOyTZT
W/MojmlgfUekC2xiXa54nxJ f17Y1TADGSbyJbsC0Q9nIrHsPl8YKkvRWvI
AqYxXZ7wRwWWmv4TMxFhWRiNY7yZI o2ZUhl02SIDNggIEg==
-----END CERTIFICATE-----
```

CER/CRT certificates can be converted to the PEM format by directly modifying the file extension of the certificate file. For example, you can directly rename the server.crt certificate file as server.pem to convert it to the PEM format.

Convert PFX certificates to the PEM format

PFX certificates are generally used in Windows Server and can be converted by using the OpenSSL tool.

For example, you can run the following OpenSSL commands to convert the certname.pfx certificate to the PEM format:

- Extract the private key: `openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes`
- Extract the certificate: `openssl pkcs12 -in certname.pfx -nokeys -out cert.pem`

Convert P7B certificates to the PEM format

P7B certificates are generally used in Windows Server and Tomcat servers, and can be converted by using the OpenSSL tool.

Procedure

Follow these steps to convert a P7B certificate to the PEM format.

1. Convert the certificate. For example, run the `openssl pkcs7 -print_certificate -in incertificate.p7b -out outcertificate.cer` command to convert the `incertificate.p7b` certificate file to `outcertificate.cer`.
2. Extract the certificate content from `[----- BEGIN CERTIFICATE ----- to ----- END CERTIFICATE -----]` in the `outcertificate.cer` file.
3. Save the certificate content as the PEM format.

Convert DER certificates to the PEM format

DER certificates are generally used on Java platforms and can be converted to the PEM format by using the OpenSSL tool.

For example, you can run the following OpenSSL commands to convert the `certificate.cer` certificate to the PEM format:

- Extract the certificate: `openssl x509 -inform der -in certificate .cer -out certificate .pem`
- Extract the private key: `openssl rsa -inform DER -outform PEM -in privatekey .der -out privatekey .pem`

7.11 Description of HTTPS exception status

| Error log | Description | Note |
|--|---|------|
| Certificate and private key do not match | The uploaded certificate and private key do not match. | N/A |
| Incorrect certificate format | The certificate does not comply with the standard format. | N/A |

7.12 Troubleshoot certain port access failure

This topic is applicable to scenarios where certain port accesses are blocked for a long time.



Note:

If your Anti-DDoS Pro network links of all the three lines (BGP, China Telecom, and China Unicom) encounter failure at the same time, see [Troubleshoot Anti-DDoS Pro access problems](#).

A client fails to access the Anti-DDoS Pro IP address of a certain ISP (such as China Telecom) or a certain region (such as Lanzhou). However, the same client can access another Anti-DDoS Pro IP address of a different ISP or region.

Resolution

Follow these steps to resolve this issue:

1. Make sure that the client uses the same ISP network as the destination Anti-DDoS Pro IP address.
2. Collect the following basic information: client IP address, ISP information, and the port that cannot be accessed.

3. Perform further inspection and acquire the following diagnostic information:

- Screenshot of the Ping test result
- Screenshot of the Port telnet test result
- Full-screen screenshot of the specific error message
- Port route trace record, and result of the Port availability test
- Link testing result (If the ports cannot be pinged, you can use TRACERT or MTR to perform link testing.)

4. Once you have identified the issue based on the preceding information, contact the relevant team to solve it.

Case study

Symptoms

An Anti-DDoS Pro user has reported that a China Telecom user in ABC city, XYZ province has encountered an exception while accessing Port 80 of an Anti-DDoS Pro instance, but the access port 443 can be accessed normally.

Resolution

1. Collect the following basic information:

- This China Telecom user was in ABC city, XYZ province, and the faulty Anti-DDoS Pro port was 80. The scope of the issue is clear.
- This user can normally access Port 443, it means that the entire link is open, and the problem lies on certain ports.
- We contacted the end user to retrieve the specific IP address: x.x.x.x
- We contacted the end user to retrieve the ping/telnet error messages.
- We contacted the end user to retrieve the comparison between normal and abnormal port accesses.

2. Identify the problem. Based on the comparison between normal and abnormal port accesses, the tracking route was disconnected at a network exit in that city.

3. Resolve the problem. We contacted the operator to resolve the problem. The problem was caused because of the Municipal jurisdiction security regulation policy.

7.13 Why does system prompt “Parameter format error” when I try to upload an HTTPS certificate

When I upload the HTTPS certificate while configuring Anti-DDoS Pro, the system prompts “Parameter format error.”

Common issues, causes, and solutions to the “Parameter format error” upon uploading the certificate are listed as follows:

- The certificate name exceeds the length limit.

Solution: Modify the certificate name to contain less than 10 characters.

- The certificate file name contains special characters.

Solution: Only use English letters or numbers to name the certificate, and do not use spaces, underscores(_), delimiters, or other special characters.

- The certificate contains non-standard content. For example, the highlighted content of the following certificate file is invalid.

Example

[illegible]

Solution

Remove the certificate content before `--- BEGIN CERTIFICATE ---`.

- A standard certificate (.pem file) looks like the following:

-----BEGIN CERTIFICATE-----
62ECyPwHd2Qy1vSt6MTXcJSfNz9Zr9fmxWt28RfXQbahgnsXOH48o3Z4H
nc+1MgE2kzucbVspE2cQpHdYH8H0jL934rm7MNS6dVnBPuKlqgDeHfG
ChdyTSSNLSir+g92cLBJG0gJyqlh9rc65Cgb4mL+n5+Dv9uOyTZT
WfMoJmglfUekC2XoXs4S4rcf17Y1TADGSybJscQ9nblH8PnHk0wRWVd
Aq10CZ7wRwWmrm4TmdPWRNR7y2i oZUhh1K2SDNggEg==
-----END CERTIFICATE-----

- A standard private key (.key file) looks like the following:

```
-----BEGIN RSA PRIVATE KEY-----
DA0TP2oKH9W1Z3UKHTgRqNqmoPQn2bqdK0p+8/dn/4VZL738zSD
Gm95TmThL yvsnLQK8jQc+uhtC1N6pGB2FwZ/EAW3W9Ecal2yhg
mg7Z+A/V9F8f5zQa6Z2d8CQJahq0YoaMFZ2JwC0wHaluQc013f
6u5o4h2e+D5cdmK7/3Nk NvqN6A2gYV/DdG29Z9uoh9o4FqG0
YF8v5U5K3G04R2adQw==
-----END RSA PRIVATE KEY-----
```

For more information about HTTPS certificate format conversion, see [Convert an HTTPS certificate to the PEM format](#).

7.14 What is the difference between Web Service and Non-Web Service?

Web Service

Web service provides protection against various DDoS attacks from layer-3 to layer-7, including SYN flood, ACK flood, UDP flood, ICMP flood, and HTTP flood attacks. It is designed for HTTP and HTTPS protocols, and only supports Port 80 and Port 443.

Non-Web Service

Non-Web service provides protection against various DDoS attacks from layer-3 to layer-4, including SYN flood, ACK flood, UDP flood, and ICMP flood attacks. It cannot defend against layer 7 attacks, such as HTTP flood attacks. Non-Web service is designed for layer-4 TCP and UDP protocols, and does not support Port 80 and UDP Port 53. You can use this service for TCP connection establishment, concurrent TCP connection, and other traffic restriction control at the target IP address and port level.

Differences

Non-Web service (layer-4 protection) cannot resolve the layer-7 message content, therefore it does not provide protection policies for layer-7 content.



Note:

For special Web services (such as Web socket) or enabling non-standard ports (such as 8080, 8888, and 4433), you can use layer-4 forwarding rules to configure Anti-DDoS Pro.