Anti-DDoS Advanced

Legacy Anti-DDoS Advanced

(Legacy)

Product Documentation

Contents

Legacy Anti-DDoS Advanced (Legacy) Product Introduction
Product Overview

Last updated：2020-07-30 11:33:07

Overview

Anti-DDoS Advanced is a paid protection service defending businesses such as games, internet services, and finance operations against high-volume distributed denial of service (DDoS) attacks that may disable user access. It can direct attack traffic to Anti-DDoS Advanced IPs for cleansing, thus ensuring business stability and availability of the real servers.
Anti-DDoS Advanced can be connected to through internet proxy and supports TCP, UDP, HTTP, HTTPS, and HTTP/2 protocols, making it ideal for finance, ecommerce, games, and other business scenarios.

Key Features

Multidimensional protection

Protection Type	Description
Malformed packet filtering	Filters out frag flood, smurf, stream flood, and land flood attacks as well as malformed IP, TCP, and UDP packets
DDoS protection at the network layer	Filters out UDP flood, SYN flood, TCP flood, ICMP flood, ACK flood, FIN flood, RST flood, and DNS/NTP/SSDP reflection attacks and null sessions.
DDoS protection at the application layer	Filters out CC attacks and slow HTTP attacks, and supports HTTP custom filtering such as host filtering, user-agent filtering, and referer filtering.

Flexible advanced protection policies

Anti-DDoS Advanced provides basic security policies by default on the basis of protection algorithms such as IP profiling, behavior pattern analysis, and AI-based smart recognition, effectively coping with common DDoS attacks. Meanwhile, it provides advanced DDoS protection policies such as IP blocklist/allowlist, protocol/port closing, packet characteristic filtering, and null session prevention to enable more targeted protection, and you can customize them as needed.

Custom cleansing mode

Anti-DDoS Advanced opens up its multiple protection levels and provides a custom cleansing threshold to allow flexible adjustment based on the attack characteristics, helping you swiftly respond to various types of DDoS attacks and meet your diversified business requirements.

Protection statistics and analysis

You can access multidimensional statistics of DDoS attacks, CC attacks, forwarded traffic, and other metrics, which helps you stay up to date with your business and attack conditions. In addition, Anti-DDoS Advanced supports automatic capture of attack packets, helping you quickly troubleshoot exceptions and problems.

Supported Regions

Anti-DDoS Advanced can protect all types of servers on the internet, including but not limited to those in customer IDCs, Tencent Cloud, and other clouds. It is currently available in following regions:

- Mainland China: South China (Guangzhou), East China (Shanghai), and North China (Beijing).
- Outside Mainland China: Hong Kong (China), Taiwan (China), Asia Pacific (Singapore, Seoul, Bangkok, India, and Japan), West US (Silicon Valley), East US (Virginia), North America (Toronto), and Europe (Frankfurt and Moscow).

The table below describes the protection bandwidth of Anti-DDoS Advanced for different regions.

Region	Base Protection	Elastic Protection	Maximum Protection Bandwidth
Guangzhou	20–50 Gbps	30–100 Gbps	100 Gbps
Beijing	20–50 Gbps	30–100 Gbps	100 Gbps
Shanghai	20–100 Gbps	30–300 Gbps	300 Gbps
Outside Mainland China	10–100 Gbps	30–400 Gbps	400 Gbps

You are recommended to choose a region closest to your real server so as to reduce access latency and accelerate access.

Product Strengths

Last updated：2020-05-09 18:03:48

Anti-DDoS Advanced is a paid product to protect your business from being affected by high-volume distributed denial-of-service (DDoS) attacks. It has the following advantages.

Massive Protection Resources

Connected with 30 ISPs across Mainland China and dozens of protection nodes overseas, Tencent Cloud's BGP linkage can provide protection bandwidth up to 900 Gbps for a single customer (point) in Mainland China and up to 400 Gbps outside Mainland China, enabling you to defend against all types of DDoS attacks with ease.

Leading Cleansing Capability

Leveraging the powerful protective clusters developed by Tencent and multi-dimensional algorithms, such as IP profiling, behavior pattern analysis, and cookie challenges, Anti-DDoS Advanced can accurately and promptly detect attack traffic. With the aid of a smart AI engine that continuously optimizes the algorithms, it is also flexible in coping with attack tricks.

Fast Access

With a 30-line BGP network encompassing various ISPs across Mainland China, Anti-DDoS Advanced features an extremely low delay in protection and fast access.

Hiding Real Server

Anti-DDoS Advanced replaces and hides your real server. It can be seen as a firewall before the real server for external access. All business access traffic passes through Anti-DDoS Advanced, which directly forwards normal traffic to the real server while cleansing attack traffic before it reaches the real server, helping boost the real server security.

Wide Applicability

Anti-DDoS Advanced fully supports website and non-website businesses and covers various businesses like finance, ecommerce, gaming, and government affairs, comprehensively satisfying the security protection needs in different application scenarios.

Cost Optimization

Anti-DDoS Advanced offers a "base protection + elastic protection" combo package where you are only charged by the amount of actual attack traffic. When the attack traffic exceeds the base protection bandwidth, it provides elastic protection to ensure the continuity of your business. Such seamless transition requires no additional devices and configuration on your side, reducing your daily protection costs.

Detailed Protection Report

Anti-DDoS Advanced can generate accurate and detailed protection reports. It can also capture attack packets automatically for troubleshooting.

Application Scenarios

Last updated：2020-04-03 14:35:43

Gaming

DDoS attacks are particularly common in the gaming industry. Anti-DDoS Advanced ensures the availability and continuity of the games to deliver a smooth experience for players. Meanwhile, it helps ensure that normal gaming continues throughout events, new game releases, and peak periods such as holidays.

Internet

Anti-DDoS Advanced ensures smooth and uninterrupted access to websites, especially during major ecommerce promotions.

Finance

Anti-DDoS Advanced helps the finance industry meet the compliance requirements and provide fast, secure, and reliable online transaction services to customers.

Government Affairs

Anti-DDoS Advanced satisfies the high security requirements of government clouds and provides high-level security for major government conferences and events especially during sensitive periods. It ensures the availability of public services and thus helps enhance government credibility.

Enterprises

Anti-DDoS Advanced ensures the availability of company websites to avoid potential financial losses and damage to brand reputation caused by DDoS attacks. In addition, you can save on investments in infrastructure, hardware, and maintenance.

Relevant Concepts

Last updated：2020-05-13 19:36:20

DDoS Attack

A Distributed Denial of Service (DDoS) attack is a malicious attempt to make a targeted server unavailable by blocking its network bandwidth or exhausting its system resources with a flood of attacking requests sent from large numbers of botnets.

Network-Layer DDoS Attack

A network-layer DDoS attack attempts to make a targeted server unavailable to its intended users by blocking its network bandwidth and exhausting its system-layer resources with a flood of internet traffic.
Common attacks include SYN flood, ACK flood, UDP flood, ICMP flood, and DNS/NTP/SSDP/Memcached reflection attacks.

CC Attack

A CC attack is a malicious attempt to make a targeted server unavailable by occupying its application-layer resources and exhausting its processing capacity.
Common attacks include HTTP/HTTPS-based GET/POST flood, layer-4 CC, and connection flood attacks, etc.

Protection Bandwidth

There are two types of protection bandwidth: base protection bandwidth and elastic protection bandwidth.

- Base protection bandwidth: base protection bandwidth of the Anti-DDoS service instance.
- Elastic protection bandwidth: the largest possible protection bandwidth of the Anti-DDoS service instance. The part in excess of the base protection bandwidth is billed daily in a pay-as-you-go manner.

If elastic protection is not enabled, the maximum bandwidth of an Anti-DDoS service instance will be the base protection bandwidth. If elastic protection is enabled, the maximum bandwidth will be the elastic protection bandwidth. Once the attack traffic exceeds the maximum protection bandwidth, IP blocking will be triggered.

> Elastic protection is disabled by default. If you need the feature, please check the pricing and billing information and enable it on your own. You can adjust the elastic protection bandwidth as required.

Benefits of Elastic Protection Bandwidth

With elastic protection enabled, when the attack traffic is higher than the base protection bandwidth but lower than the elastic protection bandwidth, Tencent Cloud Anti-DDoS Advanced will continue to protect your IPs to ensure your business continuity.

Elastic Protection Billing

With elastic protection enabled, elastic protection will be triggered and incur fees once the attack traffic goes over the base protection bandwidth. You will be billed on the following day based on the peak attack bandwidth of the current day.
For example, assume that you have purchased 20 Gbps of base protection bandwidth and set the elastic protection bandwidth as 50 Gbps. If the actual peak attack bandwidth of the day is 35 Gbps, you will need to pay for the elastic protection at the price of the 30–40 Gbps tier.
For more information, please see Billing Overview.

Cleansing

When the public network traffic of a target IP exceeds the threshold, Anti-DDoS will automatically cleanse the inbound traffic to the IP. The BGP routing protocol will be used to redirect the traffic from the original network route to the DDoS cleansing devices of Anti-DDoS, which will identify the traffic, discard attack traffic, and forward normal traffic to the IP. In general, cleansing does not affect normal access except on special occasions or when the cleansing policy is configured improperly.

Blocking

When the attack traffic suffered by a target IP exceeds the blocking threshold, Tencent Cloud will block all public network access requests to this IP through applicable ISP services to protect other Tencent Cloud users from being affected. This means that when the bandwidth of the attack traffic suffered by your IP exceeds the maximum protection bandwidth of your purchased Anti-DDoS package, Tencent Cloud will block all public network access requests to it. If your protected IP is blocked, you can log in to the console to unblock it.
Block

Blocking threshold

The blocking threshold of a protected IP equals the maximum protection bandwidth you have purchased. Anti-DDoS Advanced offers various specifications. For more information, please see Billing Overview.

Blocking period

An attacked IP is blocked for 2 hours by default. The actual duration can be up to 24 hours depending on how many times the IP is blocked and how high the peak attack bandwidth is.
The blocking duration is subject to the following factors:

- Continuity of the attack. The blocking period will extend if an attack continues. Once the period extends, a new blocking cycle will start.
- Frequency of the attack. Users that are frequently attacked are more likely to be attacked continuously. In such a case, the blocking period extends automatically.
- Traffic volume of the attack. The blocking period extends automatically in case of ultra-large volume of attack traffic.

> For IPs that are blocked too frequently, Tencent Cloud reserves the right to extend the duration and lower the threshold.

Why is my IP blocked?

Tencent Cloud reduces costs of cloud services by sharing the infrastructure, with one public IP shared by many users. When a high-traffic attack occurs, the entire Tencent Cloud network may be affected, not only the target servers. To protect other users and ensure network stability, the target server IP needs to be blocked.

Why isn't anti-DDoS service always free?

DDoS attacks threaten not only the targets but also the entire cloud network and affect non-attacked Tencent Cloud users as well. In addition, DDoS protection incurs high costs, including cleansing fees and bandwidth fees, among which bandwidth costs the most. Bandwidth fees are calculated based on the total amount of traffic, and there is no difference between fees incurred by normal traffic and attack traffic.
Therefore, Tencent Cloud provides Anti-DDoS Basic service free of charge for all users. However, once the attack traffic exceeds the free protection threshold, we will have to block the attacked IP from all public network access.
For more information on blocking, please see Blocking.

Purchase Guide
Billing Overview

Last updated：2021-03-18 10:46:46

Billing Mode

Anti-DDoS Advanced billing includes the fees of base protection bandwidth (frozen fees payment), elastic protection bandwidth (pay-as-you-go), and application bandwidth (frozen fees payment).

Billable Item	Billing Mode	Payment Method	Billing Description
Base protection bandwidth	Monthly subscription	Frozen fees payment	It provides base protection bandwidth. The amount of frozen fees is based on the base protection bandwidth and subscription plan period. Fees will be frozen at the time of successful purchase and settled on the 1st day of the next month.
Elastic protection bandwidth	Pay-as-you-go on a daily basis	Pay-as-you-go	If elastic protection is triggered, you will be billed on the following day based on the tiered price of the peak attack bandwidth of the current day. You will not be billed if elastic protection is not triggered. You can upgrade or downgrade the configuration.
Forwarding rules	Monthly subscription based on the rule quantity	Pay-as-you-go	60 forwarding rules are provided for free for each Anti-DDoS Advanced instance by default. 65 USD is charged per month for every additional 10 rules. Each Anti-DDoS Advanced instance can have up to 300 forwarding rules.
Application bandwidth	Bill-by-bandwidth on a monthly subscription basis	Frozen fees payment	The application bandwidth limit applies to both the inbound Anti-DDoS forwarding traffic and the outbound Anti-DDoS traffic. The application bandwidth needs to be higher than the peak bandwidth of the two, whichever is greater. If the actual application bandwidth is continuously higher than the application bandwidth selected when you purchased your Anti-DDoS Advanced instance, packet loss may occur. This might affect your service. We recommend adjusting your application bandwidth to avoid such occurrences.

Base protection

Base protection is on the monthly frozen fees payment. The detailed pricing is as follows:

Anti-DDoS Protection	Anti-CC Protection	Chinese mainland (USD/month)	Regions outside the Chinese mainland (USD/month)
10 Gbps	20,000 QPS	-	2,500
20 Gbps	40,000 QPS	2,400	4,800
30 Gbps	70,000 QPS	3,500	7,000
40 Gbps	100,000 QPS	-	8,200
50 Gbps	150,000 QPS	9,500	10,500
60 Gbps	200,000 QPS	-	12,000
80 Gbps	250,000 QPS	-	15,000
100 Gbps	300,000 QPS	28,000	16,500

Note：

- Query Per Second (QPS) here is used to measure the number of CC attack requests per second that an Anti-DDoS Advanced instance can defend against.
- Tencent Cloud provides up to TB-level protection capability. Contact your sales rep if necessary.

Elastic protection

You can enable elastic protection as needed.

- If elastic protection is not enabled for an instance, its base protection bandwidth will be the maximum protection bandwidth and no extra fees will be incurred.
- If elastic protection is enabled for an instance, its maximum protection bandwidth will be the elastic protection bandwidth.
  - If elastic protection is not triggered, no fees will be incurred.
  - If elastic protection is triggered and the attack traffic is higher than the base protection bandwidth but lower than the elastic protection bandwidth, you will be billed on the following day based on the tiered price of the peak attack bandwidth of the current day.

The detailed pricing of elastic protection is as follows:

Anti-DDoS Protection Peak	Chinese mainland (USD/day)	Regions outside the Chinese mainland (USD/day)

Bandwidth		
10 Gbps ≤ Peak attack bandwidth < 20 Gbps	-	320
20 Gbps ≤ Peak attack bandwidth < 30 Gbps	260	400
30 Gbps ≤ Peak attack bandwidth < 40 Gbps	450	700
40 Gbps ≤ Peak attack bandwidth < 50 Gbps	600	800
50 Gbps ≤ Peak attack bandwidth < 60 Gbps	800	1,200
60 Gbps ≤ Peak attack bandwidth < 70 Gbps	1,200	1,800
70 Gbps ≤ Peak attack bandwidth < 80 Gbps	1,500	2,200
80 Gbps ≤ Peak attack bandwidth < 90 Gbps	1,700	2,500
90 Gbps ≤ Peak attack bandwidth < 100 Gbps	1,900	2,700
100 Gbps ≤ Peak attack bandwidth < 120 Gbps	2,100	2,900
120 Gbps ≤ Peak attack bandwidth < 150 Gbps	2,300	3,200
150 Gbps ≤ Peak attack bandwidth <	2,700	4,000

200 Gbps		
200 Gbps ≤ Peak attack bandwidth < 250 Gbps	4,800	4,800
250 Gbps ≤ Peak attack bandwidth < 300 Gbps	5,600	5,600
300 Gbps ≤ Peak attack bandwidth < 400 Gbps	-	6,600

Forwarding rules

Number of Forwarding Rules	Price (USD/month/10 rules)
Number of ports (or protected domain names) ≤ 60	Free
Number of ports (or protected domain names) > 60	65

Note：

The number of forwarding rules is the total number of TCP/UDP ports (for non-website connections) and HTTP/HTTPS domain names (for website connections) that you configure for an Anti-DDoS Advanced instance.

Application bandwidth

Application bandwidth is the bandwidth used for forwarding the application traffic that has been cleansed by the Tencent Cloud Anti-DDoS data center back to the data center on the real server.

It is on a monthly-subscribed frozen fees payment. **For non-Tencent Cloud users in the Chinese mainland, 100 Mbps forwarding bandwidth will be given free of cost after they purchase the base protection package.**

The detailed pricing is as follows:

Bandwidth	Price (USD/month)
50 Mbps	750

100 Mbps	1,500
150 Mbps	2,250
200 Mbps	3,000
500 Mbps	7,500
1 Gbps	15,000
2 Gbps	30,000

The relationship between the application bandwidth and the number of layer-7 requests is as follows:

Application Bandwidth	HTTP/HTTPS
50 Mbps	5,000 QPS
100 Mbps	10,000 QPS
150 Mbps	15,000 QPS
200 Mbps	20,000 QPS
500 Mbps	50,000 QPS
1 Gbps	100,000 QPS
2 Gbps	200,000 QPS

⚠ Note：

- The application bandwidth limit applies to both the inbound Anti-DDoS forwarding traffic and the outbound Anti-DDoS traffic. The application bandwidth needs to be higher than the peak bandwidth of the two, whichever is greater. If the actual application bandwidth is continuously higher than the application bandwidth selected when you purchased your Anti-DDoS Advanced instance, packet loss may occur. This might affect your application. We recommend upgrading your application bandwidth in time.
- The QPS metric used here is a general number of queries per second when there is no attack. If the actual QPS of your application is higher than the specification purchased, please adjust the specification of your Anti-DDoS Advanced instance to prevent packet loss. You can refer to the relationship table above to increase the application bandwidth of your Anti-DDoS Advanced instance and the general HTTP/HTTPS QPS metric.

Other Metrics

See the following table for descriptions of other metrics:

Metric	Specification	Description
Number of forwarding ports	60-300/Anti-DDoS Advanced instance	The total number of forwarding rules for TCP/UDP and HTTP/HTTPS. For TCP and UDP, if the same forwarding port number is used, two different forwarding rules need to be configured.
Number of supported domain names		
Number of real server IPs	20/instance	The total number of IP addresses for both layer-4 and layer-7 real servers.
Number of new connections per second	50,000/Anti-DDoS Advanced instance	The number of new connections per second for each Anti-DDoS Advanced instance.
Number of concurrent connections	200,000/Anti-DDoS Advanced instance	The number of concurrent connections per second for each Anti-DDoS Advanced instance.

Note：

The specifications above are only the ready-made ones. If you find the specifications are not ideal, please contact Tencent Cloud technical support to customize a higher specification.

Billing Example

Anti-DDoS Advanced uses a combined billing method. Below is a fee calculation example:
A user purchases an Anti-DDoS Advanced instance in the Shanghai region, with "20 Gbps base protection bandwidth" and "50 Gbps elastic protection bandwidth".
One day, DDoS attacks occur with a peak attack bandwidth of 45 Gbps, which exceeds the base protection bandwidth and triggers elastic protection. The peak attack bandwidth falls in the billing tier between 40 Gbps and 50 Gbps, and the elastic protection fee generated that day is 600 USD.
Therefore, the user needs to pay a total of 3,000 USD, including 2,400 USD of the monthly base protection fee and 600 USD of the elastic protection fee generated that day.

Purchase Guide

Last updated：2022-05-09 16:58:40

Prerequisites

Before purchasing an Anti-DDoS Advanced (Chinese Mainland) instance , you need to register a Tencent cloud account.

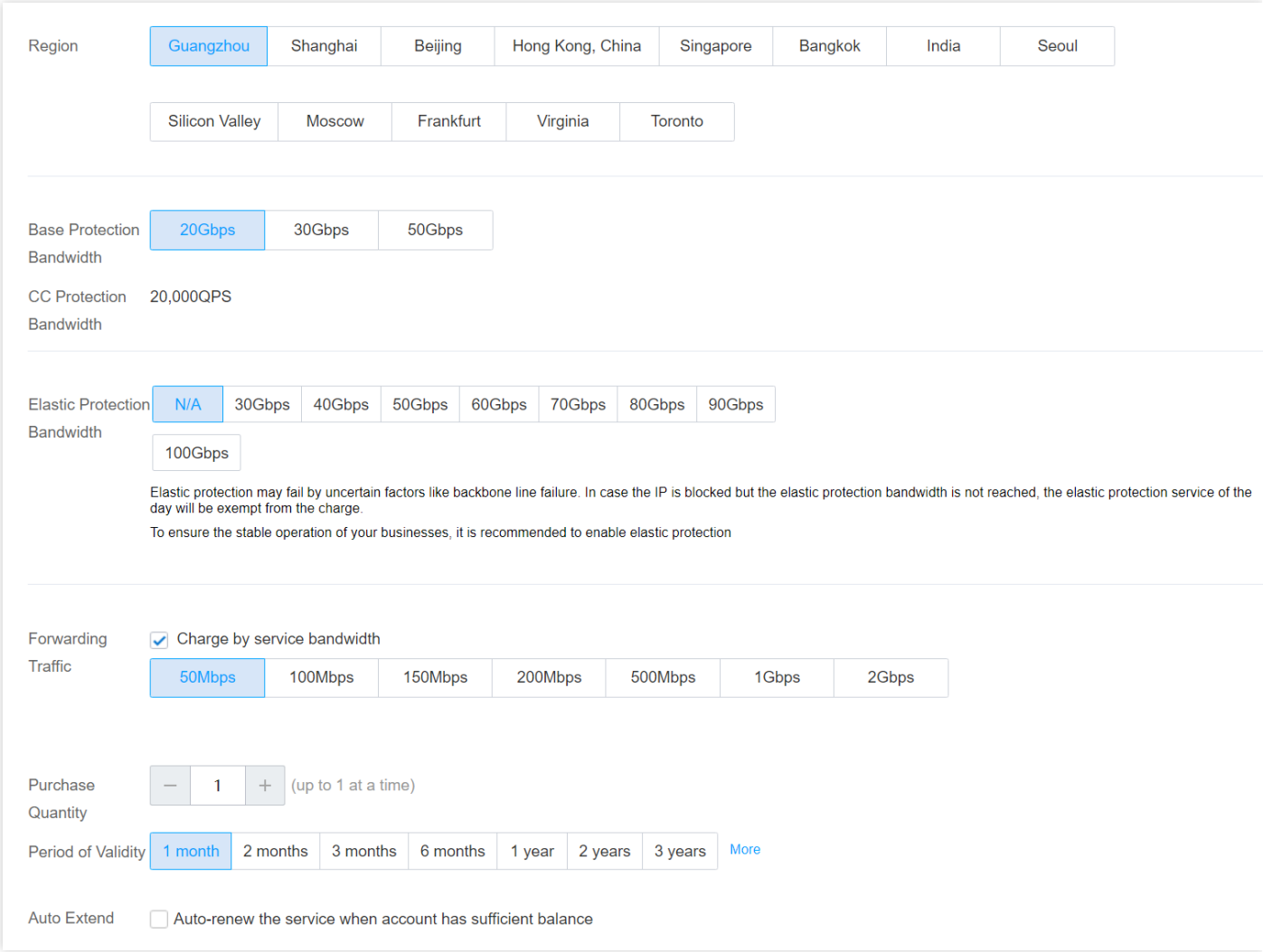
Steps

1. Log in to the Anti-DDoS Advanced console, and click ***Create***.

2. Select the protection configuration according to your business needs.

- Region: Anti-DDoS Advanced uses the forwarding proxy method. Please choose a location near the real server to reduce connection latency.
- Base protection bandwidth: Base protection capability for the instance. We recommend selecting a base protection bandwidth slightly higher than the average value of the historical attack traffic, which will allow you to handle normal attacks.
- Elastic protection bandwidth: Elastic protection capability for the instance. We recommend selecting an elastic protection bandwidth slightly higher than the historical largest attack traffic to defend against sudden increases in attack traffic, and avoid IP block caused by traffic exceeding the protection bandwidth limit. Elastic protection bandwidth is billed daily based on actual usage.
- Forwarding traffic: The normal traffic forwarded to the real server. We recommended selecting a bandwidth according to your normal traffic.
- Quantity: Select the number of instances you want to purchase.
- Contract duration: Select the length of the service plan you want to purchase. The fees are calculated based on the number of instances, the base protection bandwidth and the purchased usage period. Fees for the first month will be frozen in your account upon purchase.
- Auto renewal: Optional. When auto-renewal is activated, your subscription will be automatically renewed monthly on the expiration date given that your Tencent Cloud account has sufficient credits. This ensures consistent

protection for your business.



3. Click **Subscribe Now** and complete the payment.

More Information

- Anti-DDoS Advanced billing description
- Billing-related Questions

Expiration & Renewals

Last updated：2019-05-07 10:21:25

Expiration Reminder

Anti-DDoS Advanced will send expiration and renewal reminders to your root account and all collaborator accounts 7 days prior to expiration date of your monthly or yearly subscription via internal messages, SMS and emails.

Arrears Reminder

The system will send arrears reminders to your root account and all collaborator accounts when your monthly or yearly Anti-DDoS Advanced service subscription expires via internal messages, SMS and emails.

Renewal

- The system will send renewal reminder messages to the creator of the Tencent Cloud account and all collaborators 7 days prior to the expiration of the Anti-DDoS Advanced instance.
- When you have sufficient account credits and auto-renewal activated, the system will automatically charge your account and renew your subscription on the expiration date. When the service is successfully renewed, the fees for the first month will be frozen in your account and charged on the 1st day of the upcoming month.

Getting Started
Accessing Non-website Applications

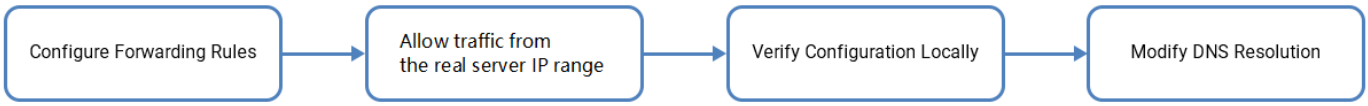
Last updated：2021-11-17 10:39:43

This document shows you how to connect non-website applications to Anti-DDoS Advanced instances and verify forwarding configurations.

Prerequisites

- Purchase an Anti-DDoS Advanced instance before adding a forwarding rule.
- Purchase a domain name resolution service before modifying the DNS information of your business domain name.

Process



Directions

Configuring a forwarding rule

1. Log in to the Anti-DDoS console and click **Anti-DDoS Advanced** -> **Access Configuration** on the left sidebar.

2. Open the **Non-website Scenarios** tab, find and select the target Anti-DDoS Advanced instance, and add a forwarding rule.

   - Create a single forwarding rule:

     a. Click **Create**.
     b. On the **Add forwarding rule** page, configure the following parameters as needed and click **OK**.

- Forwarding protocol: TCP and UDP are supported.
- Forwarding port: this is the Anti-DDoS Advanced port used for access. We recommend choosing the same port as that of the real server.
- Real server port: the real port of the business website.
- Forwarding method: **Forwarding via IP** and **Forwarding via domain name** are supported.
- Load balancing mode: only weighted polling is supported currently.
- Real server IP + weight/real server domain name: enter the real server IP + weight or real server domain name based on the **forwarding method**. Up to 20 pairs of IP + weight or domain name are supported.
  - If you tick **Forwarding via IP**, enter the real server IP address + weight, such as `1.1.1.1 50` . If a domain name corresponds to multiple pairs of real server IP + weight, you can enter all of them and separate them with carriage return. Up to 20 entries are supported.
  - If you tick **Forwarding via domain name**, enter the forwarding domain name. If a domain name corresponds to multiple real server domain names, you can enter all of them and separate them with carriage return. Up to 20 entries are supported.
    - Create multiple forwarding rules in batches:

      a. Click **Batch import** -> **Import forwarding rules**.
      b. Paste rules in the rule input box.

Note：

- From left to right, paste the forwarding protocol, forwarding port, real server port, real server IP, and weight (or forwarding domain name); separate each one with a space; only one forwarding rule can be entered per line.
- The number of forwarding rule entries added in batches cannot exceed the current quota. Within the quota limit, up to 30 entries can be imported at a time.

Allowing the forwarding IP range

To prevent the service unavailability that occurs when the real server blocks Anti-DDoS Advanced's forwarding IP, we recommend configuring allowlist policies for the real server infrastructure, including firewall, Web Application Firewall,

intrusion prevention system (IPS), and traffic management, and disabling the protection feature of the host firewall and other security software (such as Safedog) or setting allowlist policies, so that the forwarding IP will not be affected by the security policies of the real server.

To view the detailed Anti-DDoS Advanced forwarding IP range, you can log in to the Anti-DDoS console, click **Anti-DDoS Advanced** -> **Resource List** on the left sidebar, find the row of the target Anti-DDoS Advanced instance, and click its **ID/Name**.

Verifying the configuration locally

After the forwarding configuration is completed, the Anti-DDoS Advanced IP will forward the packets from the relevant port to the corresponding real server port by following the forwarding rules.

To ensure the stability of your business, a local test is recommended. The verification methods are as follows:

- **For applications accessed via IPs**
  For applications accessed via IPs (such as games), run `telnet` to check whether the Anti-DDoS Advanced port is accessible. You can also enter the Anti-DDoS Advanced IP as the server IP in your local client (if available) to check whether the local client can access the Anti-DDoS Advanced IP.
  For example, the Anti-DDoS Advanced IP is `10.1.1.1` with the forwarding port 1234. And the real server IP is `10.2.2.2` with the real server port 1234. Run `telnet` on your local client to connect to `10.1.1.1:1234` . If the address can be accessed, it means that the forwarding is successful.

- **For applications accessed via domain names**
  For applications accessed via domain names, please try the followings:

  i. Modify your local `hosts` file to direct local requests to the protected website to the Anti-DDoS Advanced IP.
  Take Windows operating system as an example:

  a. Open the `hosts` file in `C:\Windows\System32\drivers\etc` , and add the following content at the end of the text:
  `<anti-ddos advanced="" ip="" address=""> <domain name="" of="" the="" protected="" website="">`
  For example, if the Anti-DDoS Advanced IP is `10.1.1.1` and the domain name is `[www.qq.com](www.qq.com)` , add:
  `10.1.1.1 www.qq.com`
  b. Save the `hosts` file.

  ii. Run the `ping` command on the local computer to test the protected domain name.
  If the resolved IP address is the Anti-DDoS Advanced IP address bound in the `hosts` file, the forwarding is successful.

> Note：
> If the resolved IP address is still the real server IP address, try running the `ipconfig/flushdns` command in the Windows Command Prompt to clear the local DNS cache.

iii. After successful configuration of `hosts`, check whether the domain name can be accessed.
If yes, the configuration has taken effect.

> Note：
> If the verification still fails with the correct method, please log in to the Anti-DDoS console and check whether the configuration is correct. If the problem persists after you fix any incorrect configuration items, please contact Tencent Cloud technical support.

Modifying the DNS resolution of the business domain name

Before using Anti-DDoS Advanced, you need to configure the A record of your business domain name's DNS with an Anti-DDoS Advanced IP, so that all user access requests to your site will pass through Anti-DDoS Advanced first before arriving at the real server (that is, all traffic will be first directed to Anti-DDoS Advanced before getting to the real server).

> Note：
> The principle of domain name resolution configuration is consistent, but the configuration methods in different service providers may be different. Here the Tencent Cloud DNSPod is used.

1. Log in to the DNSPod console, click **Domain Name Resolution List** on the left sidebar, and click **Resolve** on the right of a domain name.
2. Open the **Record Management** tab, click **Add Records** to modify the IP address pointed to by the A record to the Anti-DDoS Advanced IP address, and click **Save**.

Accessing Website Applications

Last updated：2021-01-25 12:18:17

This document shows you how to connect website applications to Anti-DDoS Advanced instances and verify forwarding configurations.

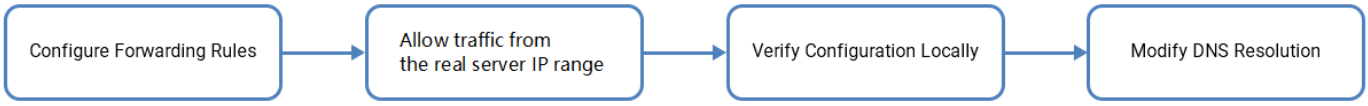
Note：

It currently supports connecting website applications in Beijing, Shanghai, and Guangzhou, while regions outside the Chinese mainland are not supported.

Prerequisites

- Purchase an Anti-DDoS Advanced instance before adding a forwarding rule.
- Purchase a domain name resolution service before modifying the DNS information of your business domain name.

Process



Directions

Configuring-a-forwarding-rule">

Configuring a forwarding rule

1. Log in to the Anti-DDoS console and click **Anti-DDoS Advanced** -> **Access Configuration** on the left sidebar.
2. Open the **Website Scenario** tab, find and select the target Anti-DDoS Advanced instance, and add a forwarding rule.
   - Create a single forwarding rule:

a. Click **Create**.

3. On the **Add forwarding rule** page, configure the following parameters as needed and click **OK**.

```
Parameter description:
```

- Domain: enter the domain name to be protected.
- Protocol: HTTP and HTTPS are supported, you can tick one as needed.

Scenario	Operation
Websites with HTTP only	Tick **HTTP**.
Websites with HTTPS only	▪ Tick **HTTPS**. ▪ Certificate source: the Tencent Cloud hosted certificate is selected by default. ▪ Certificate: select the corresponding SSL certificate.

- Forwarding method: **Forwarding via IP** and **Forwarding via domain name** are supported.
- Enter the real server IP or real server domain name based on the **forwarding method**.

```
- If you tick **Forwarding via IP**, enter the real server IP (or IP + port). If a domain name corresponds to multiple real server IPs (or multiple pairs of IP + port), you can enter all of them and separate them with carriage return. Up to 16 entries are supported.
- If you tick **Forwarding via domain name**, enter the forwarding domain name (CNAME) or domain name (CNAME) + port. If a domain name corresponds to multiple real server domain names (CNAME) or multiple pairs of domain name (CNAME) + port, you can enter all of them and separate them with carriage return. Up to 16 entries are supported.
```

- Create multiple forwarding rules in batches:

a. Click **Batch import** -> **Import forwarding rules**.

b. Paste rules in the rule input box.

> ⚠ **Note：**
>
> - From left to right, paste the domain name, protocol, real server IP (real server domain name is currently not supported), and real server port; separate the real server IP and real server port with `:` and others with spaces; only one forwarding rule can be entered per line.
> - The number of forwarding rule entries added in batches cannot exceed the current quota.

Allowing-the-forwarding-IP-range">

Allowing the forwarding IP range

To prevent the service unavailability that occurs when the real server blocks Anti-DDoS Advanced's forwarding IP, we recommend configuring allowlist policies for the real server infrastructure, including firewall, Web Application Firewall, intrusion prevention system (IPS), and traffic management, and disabling the protection feature of the host firewall and other security software (such as Safedog) or setting allowlist policies, so that the forwarding IP will not be affected by the security policies of the real server.
To view the detailed Anti-DDoS Advanced forwarding IP range, you can log in to the Anti-DDoS console, click **Anti-DDoS Advanced** -> **Resource List** on the left sidebar, find the row of the target Anti-DDoS Advanced instance, and click its **ID/Name**.

Verifying-the-configuration-locally">

Verifying the configuration locally

After the forwarding configuration is completed, the Anti-DDoS Advanced IP will forward the packets from the relevant port to the corresponding real server port by following the forwarding rules.
To ensure the stability of your business, a local test is recommended. The verification methods are as follows:

1. Modify your local `hosts` file to direct local requests to the protected website to the Anti-DDoS Advanced IP.
   Take Windows operating system as an example:
   i. Open the `hosts` file in `C:\Windows\System32\drivers\etc`, and add the following content at the end of the text:
   `<Anti-DDoS Advanced IP address> <Domain name of the protected website>`
   For example, if the Anti-DDoS Advanced IP is `10.1.1.1` and the domain name is `[www.qq.com](www.qq.com)`, add:
   `10.1.1.1 www.qq.com`
   ii. Save the `hosts` file.
2. Run the `ping` command on the local computer to test the protected domain name.
   If the resolved IP address is the Anti-DDoS Advanced IP address bound in the `hosts` file, the forwarding is successful.

> **Note：**
> If the resolved IP address is still the real server IP address, try running the `ipconfig/flushdns` command in the Windows Command Prompt to clear the local DNS cache.

3. After successful configuration of `hosts`, check whether the domain name can be accessed.
   If yes, the configuration has taken effect.

Note：

If the verification still fails with the correct method, please log in to the Anti-DDoS console and check whether the configuration is correct. If the problem persists after you fix any incorrect configuration items, please contact Tencent Cloud technical support.

Modifying-the-DNS-resolution-of-the-business-domain-name">

Modifying the DNS resolution of the business domain name

Before using Anti-DDoS Advanced, you need to configure the A record of your business domain name's DNS with an Anti-DDoS Advanced IP, so that all user access requests to your site will pass through Anti-DDoS Advanced first before arriving at the real server (that is, all traffic will be first directed to Anti-DDoS Advanced before getting to the real server).

Note：

The principle of domain name resolution configuration is consistent, but the configuration methods in different service providers may be different. Here the Tencent Cloud DNSPod is used.

1. Log in to the DNSPod console, click **Domain Name Resolution List** on the left sidebar, and click **Resolve** on the right of a domain name.
2. Open the **Record Management** tab, click **Add Records** to modify the IP address pointed to by the A record to the Anti-DDoS Advanced IP address, and click **Save**.

Operation Guide

Operation Overview

Last updated：2020-05-13 19:36:21

When you use Anti-DDoS Advanced, you may need to configure Anti-DDoS Advanced instances, view statistical reports, view operation logs, and set security event notifications. This document describes common operations in Anti-DDoS Advanced for your reference.

Instance Management

- Viewing instance details
- Setting resource name
- Configuring elastic protection
- Adjusting Anti-DDoS Advanced instance specification
- Unblocking protected IP

Protection Configuration

- Configuring scenario
- Configuring cleansing threshold and protection level
- Managing advanced DDoS protection Policy
- Configuring CC protection level
- Managing CC protection policy
- Configuring health check
- Configuring session persistence

Statistical Report

Viewing statistical report

Operation Log

Viewing operation log

Security Event Notification

Usage Limits

Last updated：2020-07-30 11:32:26

Scenario

Anti-DDoS Advanced can protect your IPs/domain names that are not deployed on Tencent Cloud. Both website and non-website applications are supported.

Capability

By default, each Anti-DDoS Advance instance supports up to 60 forwarding rules, and each rule supports up to 20 real server IPs/domain names.

Blocklist/Allowlist

- Up to 120 IPs allowed for one DDoS IP blocklist/allowlist
- Up to 50 IPs allowed for one CC IP blocklist/allowlist
- Up to 50 URLs allowed for one CC URL allowlist

Region availability

Anti-DDoS Advanced is available in the following regions:

- Mainland China: South China (Guangzhou), East China (Shanghai), North China (Beijing).
- Outside Mainland China: South China (Hong Kong), Asia-Pacific (Singapore, Seoul, Bangkok, India, Japan), Western U.S. (Silicon Valley), Eastern U.S. (Virginia), North America (Toronto), Europe (Frankfurt, Moscow).

Below is the protection bandwidth range in different regions.

Region	Base Protection	Elastic Protection	Maximum Protection Bandwidth
Guangzhou	20-50 Gbps	30-100 Gbps	100 Gbps
Beijing	20-50 Gbps	30-100 Gbps	100 Gbps
Shanghai	20-100 Gbps	30-300 Gbps	300 Gbps

Region	Base Protection	Elastic Protection	Maximum Protection Bandwidth
Outside Mainland China	10-100 Gbps	30-400 Gbps	400 Gbps

Protection Configuration
Configuring Scenarios

Last updated：2020-05-13 19:50:59

Use Cases

Anti-DDoS Advanced supports custom advanced DDoS protection policies. You can customize protection policies according to your business characteristics or the nature of attacks. In general, you can associate at most one advanced DDoS protection policy with an Anti-DDoS Advanced instance. If you have multiple instances, you can configure up to 5 advanced DDoS protection policies.
You may need to continuously optimize the policies to keep up with actual business needs and ever-changing attacks. To streamline the management of refined DDoS protection, Anti-DDoS Advanced allows you to create scenarios. You can create scenarios, and the backend can collect, identify, and automatically generate advanced protection policies for flexible configuration or maintenance of policies.

Creating Scenario

- **Method 1:**
  If you have not configured any scenario for your Anti-DDoS Advanced instance yet, when you log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar, you will see a message as shown below. Click **Create Now** to create a scenario.

> You can create up to 5 scenarios.

- **Method 2:**

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar. Select the **Advanced DDoS Protection Policy** tab and click **Create Scenario**.

2. On the scenario creation page, configure the following parameters according to your business characteristics and click **OK** to complete the configuration.
   - **Scenario Name:** required; enter a scenario name containing 1–32 characters of any type.

- **Platform:** select the development platform of your business. The options include PC client, mobile, TV, and CVM.
- **Category:** select a service category. The options include game, application, website, and others.
- **Basic Information:**
  - **Users outside China**
    Select **Yes**, **No**, or **Unknown**, indicating disabling or enabling **Reject traffic from outside China**.
  - **Actively initiate outbound TCP requests**
    Select **Yes**, **No**, or **Unknown**. If you select **Yes**, you need to enter the ports that initiate outbound TCP requests. Use commas (,) to separate multiple ports.
  - **Actively initiate outbound UDP requests, such as DNS, NTP requests**
    Select **Yes**, **No** or **Unknown**. If you select **Yes**, you need to enter the ports that initiate outbound UDP requests. Use commas (,) to separate multiple ports.
- **Other Info**: click **Expand** to configure more parameters.
  - **UDP payload with fixed characteristic**
    Select **Yes** or **No**. **No** is selected by default. If you select **Yes**, you need to enter the UDP payload characteristic.
  - **TCP payload with fixed characteristic**
    Select **Yes** or **No**. **No** is selected by default. If you select **Yes**, you need to enter the TCP payload characteristic.
  - **Web API application (separated with comma ",")**
    Select **Yes** or **No**. **No** is selected by default. If you selected **Yes**, you need to enter the API service URL(s). Use commas (,) to separate multiple URLs.

3. The backend will analyze the scenario you created and then automatically generate an advanced protection policy named in the format of `scenario name_policy_number`, such as `test_policy_1`. You can then configure or modify the protection policy as needed.

> - If you **have only one Anti-DDoS Advanced instance (resource)** and **have created only one scenario**, **the generated advanced protection policy will be automatically associated with the instance (resource)**.

- **If you modify the scenario information, the related configuration items in the corresponding advanced protection policy will be automatically modified to keep up with the changes to the scenario.** However, changes to the advanced policy will not be synchronized to the corresponding scenario.

- When one or more instances (resources) are bound to an advanced protection policy named "scenario name_policy_number.", if the forwarding rule parameters (such as the following parameters) of one instance (resource) are modified, **the corresponding configuration item information in the advanced protection policy will be automatically synced**.
- (Layer-4) Non-website business: TCP/UDP protocols; forwarding port range.
- (Layer-7) Website business: HTTP/HTTPS protocols; the forwarding ports are 80/443 by default.

Modifying and Deleting Scenario

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar.
2. Click **Advanced DDoS Protection Policy** and click **Configure** or **Delete** on the right of the target scenario to modify or delete the scenario.

If a scenario is deleted, the advanced protection policy corresponding to the scenario will also be deleted.

For more information, please see Managing Advanced DDoS Protection Policy.

Configuring Cleansing Threshold and Protection Level

Last updated：2020-07-30 11:59:28

Use Cases

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

> If you need to use the UDP protocol, please contact Tencent Cloud Technical Support to customize a policy and avoid impact on business operations when in strict mode.

Protection Level	Protection Operation	Description
Loose	• Filters SYN and ACK data packets with explicit attack characteristics. • Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specification. • Filters UDP data packets with explicit attack characteristics.	This cleansing policy is loose and only protects against explicit attack packets. You are recommended only to use this mode when requests are blocked mistakenly. Attack packets may pass through the security system in case of complex attacks.
Normal	• Filters SYN and ACK data packets with explicit attack characteristics. • Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specification. • Filters UDP data packets with explicit attack characteristics. • Filters common attack UDP data packets.	This cleansing policy applies to most businesses and effectively protects against common attacks. The normal mode is configured by default.

	• Actively verifies the source IPs of certain access requests.	
Strict	• Filters SYN and ACK data packets with explicit attack characteristics. • Filters TCP, UDP, and ICMP data packets that are not compliant with the protocol specification. • Filters UDP data packets with explicit attack characteristics. • Filters common attack UDP data packets. • Actively verifies the source IPs of certain access requests. • Filters ICMP attack packages. • Filters common UDP attack data packets. • Strictly checks UDP data packets.	This cleansing policy is strict. You are recommended to use this mode when attack packets pass through the security system in Normal mode.

By default, your purchased Anti-DDoS Advanced instance uses the Normal protection level, which can be changed based on your actual business needs. In addition, you can customize the cleansing threshold. If the attack traffic exceeds the threshold, the cleansing policy will be automatically triggered.

Configuration Samples

This section takes instance "bgpip-000002ai" in South China (Guangzhou) as an example to describe the configurations.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List** on the left sidebar, and click **South China (Guangzhou)** in the region selection box.
2. Find the Anti-DDoS Advanced instance whose ID is "bgpip-000002ai" and click **Protection Configuration** in the "Operation" column on the right.

3. In the pop-up Anti-DDoS configuration page, enable **Protection Status** to set the cleansing threshold and protection level.

> The configuration items are visible only when **Protection Status** is  . If you disable the protection, the configuration items will be hidden and will not take effect. After you enable the protection again, the items will be visible again and retain the original configurations.
> **Configuration parameter descriptions:**

- **Protection status**
  Protection is enabled by default. You can enable or disable it as needed and set the duration for disablement. Currently, the duration can only be 1–6 hours. The Anti-DDoS Advanced instance will automatically enable protection after the set duration elapses or when the attack traffic bandwidth exceeds 1 million pps or 2 Gbps.
  - **Cleansing threshold**
- It indicates the threshold to trigger cleansing. If the traffic is below the threshold, no cleansing operation will be executed even if attacks are detected.
- After protection is enabled, the Anti-DDoS Advanced instance, if just connected to your business, will use the default cleansing threshold value by default. As the business traffic changes, the system will automatically learn to calculate a baseline value. You can set the cleansing threshold based on your business protection needs at any time.
  If you have a clear concept about the threshold, set it as needed; otherwise, please use the default value. Anti-DDoS will automatically learn through AI algorithms and calculate the default threshold for you.

> - **Protection level**
>   After protection is enabled, the Anti-DDoS Advanced instance, if just connected to your business, will use the Normal protection level by default. You can adjust the level based on your business protection needs at any time.

- **Other configuration items**
- **Business scenario**
  You can select and modify a matched business scenario from the created ones as needed. When a business scenario is selected, the corresponding "advanced policy" will be automatically generated accordingly. For more information on how to create a business scenario, please see Configuring Business Scenarios.
  - **Advanced policy**
    You can select and modify a matched advanced policy from the created ones based on your business protection

characteristics. For more information on how to create an advanced policy, please see Managing Anti-DDoS Advanced Policies.

- **Alarm threshold for DDoS attacks**
  You can configure an alarm threshold for DDoS attacks. If the detected metric exceeds the set threshold, an alarm will be triggered and alarm notifications will be pushed to you. For more information on how to set an alarm threshold, please see Configuring Attack Alarm Thresholds.
- **AI-based enhanced protection for TCP business**
  For layer-4 TCP business, Anti-DDoS Advanced provides AI-based enhanced protection. After this feature is enabled, through self-learning of business routine characteristics with the aid of AI models, Anti-DDoS Advanced can automatically distinguish between business traffic and attack traffic, effectively defending your business against layer-4 CC attacks.
  Currently, AI-based enhanced protection for TCP business is only available to allowed users.

Manage DDoS advanced protection strategy

Last updated：2020-07-30 12:03:25

Anti-DDoS Advanced provides advanced protection policies against DDoS attacks. You can adjust and optimize the DDoS protection policy as required through blocklists/allowlists, disabling protocols, disabling (discarding) or opening ports, packet characteristic filtering, connection flood protection, and watermark protection.

Configuration Item Overview

Configuration Item	Description	Effective Time
Blocklist/Allowlist	It is IP-based protection. • It always allows requests from IPs in the allowlist. • It always blocks requests from IPs in the blocklist.	It takes effect immediately when the protected IPs are under attack.
Disabled protocol	It disables a protocol not used by the business. If attacks are detected, the Anti-DDoS cluster will cleanse the traffic under the protocol.	It takes effect immediately when the protected IPs are under attack.
Disabled (discarded) or passed port	You can disable or pass traffic from the specified type of ports.	When an attack is detected, the Anti-DDoS cluster will cleanse (or pass) the traffic on the specified port or specified port range.
Packet filter characteristic	It combines multiple criteria to set policy operations, such as the protocol, port range, packet range, whether to detect load, offset, detection depth, and whether to include characteristic strings based on the business or attack packets. If the packets match the policy criteria, operations such as direct forwarding, discarding, source IP blocking, or disconnecting can be executed.	It takes effect immediately when the protected IPs are under attack.
Speed limit	It is IP-based protection and limits the speed of the access protocol.	It takes effect immediately when the protected IPs are under attack.

Configuration Item	Description	Effective Time
Reject traffic from outside China	It rejects TCP traffic requests from outside China (including Mainland China, Hong Kong, Macao, and Taiwan).	It takes effect when the protected IPs are under attack.
Connection flood protection	It is IP-based protection, which limits the speed, packet length, and other parameters of connections accessing non-website IPs protected by Anti-DDoS Advanced to protect against light traffic connection attacks.	It takes effect immediately when the protected IPs are under attack.
Exceptional connection detection	When a source IP receives a TCP connection meeting the configured parameter characteristics, the connection will be regarded as exceptional. If the amount of exceptional connections received by the source IP exceeds the maximum allowable number, the IP will be added to the blocklist for a certain period and will not be accessible.	It takes effect immediately when the protected IPs are under attack.
Watermark protection	It supports UDP and TCP packets. Watermark detection and stripping will be executed for the payloads within the configured port range. Watermark protection can protect against layer-4 CC attacks, such as forged business packet attacks and replay attacks. • Customer client and Tencent Cloud Anti-DDoS Advanced system share the same watermark algorithm and key. • Each packet sent by the client is embedded with watermark characteristic which attack packets do not have. • The Anti-DDoS Advanced system will identify and discard attack packets.	It takes effect immediately when the protected IPs are under attack.

Adding Policies

> Configuration of advanced protection policy requires technical expertise. You are recommended to read the operation guide before configuring policies as needed.

Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Add Policy**. Configure the following parameters as needed and click **OK**.

- **Policy Name**
  Enter a policy name containing 1–32 characters of any type.

- **Blocklist/Allowlist**
  - If you need to set a blocklist, click **Add**, select **Blocklist**, enter IPs to block, and then click **OK**. Separate multiple IPs with carriage returns.
  - If you need to set a allowlist, click **Add**, select **Allowlist**, enter the IP to allow directly, and then click **OK**. Separate multiple IPs with carriage returns.

  > You can add up to 100 IPs for the blocklist and allowlist. The number of IPs to be added in batches cannot exceed the current available quota.

- **Disabled Protocol**

- Select the protocol to be disabled. The speed of ICMP, TCP, UDP and other protocols can be limited.

- **Port Number**
  Select the protocol and port type, enter the corresponding port, and choose the discarding or passing action according to your business needs. If you need to configure a continuous port range, you can use the "start port-end port" format.

- **Packet Filter Characteristic**
  Set conditions such as the protocol, port range, packet length, payload detection, offset, detection depth, and characteristic strings and configure the action to be taken for immediate effect.

  > - Offset: specifies the start position of the matched characteristics in the packet.
  > - Detection depth: specifies the packet length from the position set by the offset to the end of the matching content. It is used with the offset.
  > - Policy:
  >   - "Discard packet": discards the data packet matching the packet filter characteristic.
  >   - "Discard packet and block source IP": discards the data packet matching the packet filter characteristics and temporarily blocks the source IP.
  >   - "Discard packet and disconnect": discards the data packet matching the packet filter characteristics and closes the TCP connection.

- **Discard packet, disconnect, and block source IP**: discards the data packet matching the packet filter characteristics, closes the TCP connection, and temporarily blocks the source IP.
- **Directly forward**: directly forwards the data packets matching the packet filter characteristics.

- **Speed Limit**
  Click **Add**, select the protocol for speed limit, and then set the limit threshold. The speed of ICMP, TCP, UDP, and other protocols can be limited.

- **Reject Traffic from Outside China**
  Select "Enable" or "Disable". The protection engine of Anti-DDoS Advanced is embedded with an IP library containing IPs from outside China. If you enable this feature, source IPs in the library will be rejected. The **Enable** operation takes effect when attacks occur. The **Disable** operation takes effect immediately.

- **Connection Flood Protection**
  - **Null Session Protection**: select "Enable" or "Disable". The **Enable** operation takes effect when attacks occur. This feature is implemented based on TCP proxy and may affect the initial business access.
  - **Source New Connection Limit**: select "Enable" or "Disable". After selecting **Enable**, you need to set the rate threshold (unit: connection/sec) in the range of 0–∞. It specifies the number of new connections established by a source IP per second. New connections exceeding the upper limit will be discarded.
  - **Source Concurrent Connection Limit**: select "Enable" or "Disable". After selecting **Enable**, you need to set the quantity threshold in the range of 0–∞. It specifies the maximum allowed number of concurrent connections of a source IP. Concurrent connections exceeding the upper limit will be discarded.
  - **Destination New Connection Limit**: select "Enable" or "Disable". After selecting **Enable**, you need to set the rate threshold (unit: connection/sec) in the range of 0–∞. It specifies the maximum number of new connections established by a destination IP per second. New connections exceeding the upper limit will be discarded. Due to cluster-based deployment of the protection devices, deviation exists for the speed limit of new connections.
  - **Destination Concurrent Connection Limit**: select "Enable" or "Disable". After selecting **Enable**, you need to set the quantity threshold in the range of 0–∞. It specifies the maximum number of concurrent connections of a destination IP. Concurrent connections exceeding the upper limit will be discarded. Due to cluster-based deployment of the protection devices, deviation exists for the speed limit of concurrent connections.

- **Exceptional Connection Detection**
  - **Maximum Exceptional Source IP Connections**: click **Enable** and enter the maximum allowed number of exceptional source IP connections in the range of 0–∞. It specifies the maximum number of exceptional connections allowed for a source IP. If the number exceeds the threshold, the source IP will be identified as exceptional and will be blocked for a while.

> The following parameters can be configured only if **Maximum Number of Exceptional Source IP Connections** is enabled.

- **Syn Packet Ratio Detection**: select "Enable" or "Disable". After selecting **Enable**, you need to set the Syn packet ratio in the range of 0–100. It specifies the threshold ratio of Syn packets and Ack packets for a TCP connection to be identified as exceptional.
- **Syn Packet Number Detection**: select "Enable" or "Disable". After selecting **Enable**, you need to set the maximum allowed number of packets in the range of 0–65535. It specifies the threshold number of Syn packets for a TCP connection to be identified as exceptional.
- **Connection Timeout Detection**: select "Enable" or "Disable". After selecting **Enable**, you need to set the detection cycle (unit: second) in the range of 0–65535. It specifies the threshold period during which no packets are transmitted for an established TCP connection to be identified as exceptional.
- **Exceptional Null Session Detection**: select "Enable" or "Disable". It specifies that an established TCP connection will be identified as exceptional if it has no packets with payload.

- **Watermark Protection**

  Click **Enable** to configure watermark protection. Enter a specified TCP protection port and UDP protection port, and then click **OK** to make the watermark protection take effect. Adding an advanced DDoS protection policy will automatically generate a key. You need to add the watermark configuration to the client offline.

- **TCP Protection Port and UDP Protection Port**

  A TCP/UDP protection port can be configured with up to 5 port ranges. Different port ranges cannot overlap one another. If the starting and ending port numbers are the same, a range will be considered as one port. You need to configure at least one of the TCP or UDP port ranges.

  > Only when the UDP protocol port range is configured can UDP watermark be removed. You can also specify the offset of the watermark tag in the UDP packet.

- **UDP Watermark Removal**

  Select **Automatically Remove UDP Packet Watermark**. After the data packet passes through the security protection system, the watermark in a UDP packet will be automatically removed and then transferred to the real server.

> If the Anti-DDoS system is not required to remove the UDP watermark, then the client needs to be modified for watermark removal.

- **Offset**
  Specify the offset of the watermark tag in the UDP packet. The default value is 0, and the value range is 0–99. The offset only works after UDP watermark removal is enabled.

Binding and Unbinding Resource

Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Bind Resource** next to the target policy.

- Bind Resource: in the pop-up **Bind Resource** dialog box, select one or more resources as needed and click **OK**.
- Unbind Resource: in the pop-up **Bind Resource** dialog box, click ✕ to the right of a resource in the **Selected** section and click **OK**.

Adding Watermark to Client

Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Download Client Watermark File** next to the target policy to add the watermark to the client offline.

Adding, Deleting, or Disabling/Enabling Watermark Key

Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Watermark Key Configuration** next to the target policy.

- **Add Key**: in the pop-up **Key Information** dialog box, click **Add Key** to generate a key.
- **Disable**/**Enable Key**: you can disable or enable a key. In the pop-up **Key Information** dialog box, click **Disable** next to the target key. If you need to enable it again, click **Enable**.
- **Delete Key**: you can delete a disabled key. In the pop-up **Key Information** dialog box, click **Delete** next to the target key.

At most 2 keys can exist at one time. If you need to add more keys, please delete an existing one first. If only one key is activated, you cannot disable or delete it.

Configuring Policy

Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Configuration** next to the target policy. Update the following parameters as required, and then click **OK**.

You cannot modify a policy name in the "scenario name_policy_No." format.

- Policy Name
- Blocklist/Allowlist
- Disabled Protocol
- Port Number
- Packet Filter Characteristic
- Reject Traffic from Outside china
- Connection Flood Protection
- Exceptional Connection Detection
- Watermark Protection

Deleting Policy

- You can directly delete a policy without bound resources. To delete a policy with bound resources, unbind the resources first.
- If UDP watermark removal is enabled, deleting the policy will disable UDP watermark removal at the same time. Verify whether corresponding configuration or change has been completed on both the client and server first before deleting the policy.
- A deleted policy cannot be recovered.
- **You cannot delete an advanced protection policy automatically generated for your created scenario.**

Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the **Advanced DDoS Protection Policy** tab, click **Delete** next to the target policy. In the pop-up dialog box, click **OK**.

Configure CC protection level

Last updated：2021-01-27 11:11:39

Protection Description

In order to improve the protection effect and reduce the risk of false blocking during protection, Anti-DDoS Advanced has three protection levels for CC attacks for your choice, and the "normal" level is used by default.

- **Loose**: this level can be used when the protected website has no obviously exceptional traffic. It performs a looser human-machine recognition algorithm check on all requests made to the protected website, that is, each visitor is verified and only successfully authenticated visitors are allowed to access the website. As the CC protection policy at this level is relatively loose, there may be a risk of passing through a small number of exceptional requests.
- **Normal**: this level is the default CC protection level. It is recommended if you find that the protected website is under CC attacks. Compared with the loose level, the normal level of CC protection can cover most of attack scenarios and defend against most of CC attacks. In addition, it performs a human-machine recognition algorithm check on all requests made to the protected website, that is, each visitor is verified and only successfully authenticated visitors are allowed to access the website.
- **Strict**: the CC attack protection policy is stricter at this level and can defend against more complex CC attacks. In addition, it performs a strict human-machine recognition algorithm check on all requests made to the protected website, that is, each visitor is verified and only successfully authenticated visitors are allowed to access the website. Due to the strict authentication mechanism in this mode, some normal requests may be blocked by mistake.

  - The protection algorithms used at the above three CC protection levels are only applicable to webpages and HMTL5 pages.
  - If the business of the visited website is an API or a native app, as such businesses generally cannot respond to algorithm-based authentication normally, there is a great risk of false blocking.
  - If you need CC protection for API or native app businesses, please submit a ticket for protection policy customization.

Directions

By default, the normal level of CC protection is used for domain names of websites protected by Anti-DDoS Advanced instances. You can freely adjust the protection mode according to your actual business needs.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar, and click **CC Protection** on the protection policy page.
2. On the CC protection page, find the HTTP CC protection and HTTPS CC protection section at the bottom of the page, select the domain name that requires CC protection under the corresponding protocol, and set the CC protection level.

   - The CC protection level policy only takes effect for domain names with the access configured as website business (layer-7 access).
   - If you haven't connected the website domain name to be configured to an Anti-DDoS Advanced instance, please connect it first as instructed in Connecting Website Business.

For more information, please see Managing CC Protection Policy.

Manage CC protection policies

Last updated：2020-07-30 12:00:19

Anti-DDoS Advanced supports HTTP/HTTPS CC protection. When the number of HTTP/HTTPS requests recorded by Anti-DDoS Advanced exceeds the set **maximum number of HTTP/HTTPS requests**, HTTP/HTTPS CC protection will be automatically triggered.
Anti-DDoS Advanced allows you to set an ACL. By enabling HTTP/HTTPS CC protection, you can use common HTTP/HTTPS packet fields (such as host, CGI, Referer, and User-Agent parameters) to set matching conditions, so as to control access requests from internet users, i.e., blocking requests that hit the conditions or triggering CAPTCHA verification. You can also set speed limit rules to limit the speed of access IPs.
Anti-DDoS Advanced also allows you to configure URL allowlist, IP allowlist, and IP blocklist.

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

Enabling CC Protection

HTTP CC protection

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar. On the protection configuration page, click **CC Protection** and select the target instance.
2. In the **HTTP CC Protection** section, click  on the right of **Protection Status** to enable HTTP CC protection. Then, click the drop-down list on the right of **Maximum Number of HTTP Requests** to select an appropriate upper limit.

> CC protection is disabled by default. Only after it is enabled can the maximum number of HTTP requests be set.

HTTPS CC protection

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar. On the protection configuration page, click **CC Protection** and select the target instance.
2. In the **HTTPS CC Protection** section, select a protected domain name and click  on the right of **Protection Status** to enable HTTPS CC protection. Then, click the drop-down list on the right of **Maximum Number of**

HTTPS Requests to select an appropriate upper limit.

> CC protection is disabled by default. Only after it is enabled can the HTTPS requests threshold be set.

Customizing CC Protection Policies

- **Only after HTTP/HTTPS CC protection is enabled can you customize CC protection policies. Up to 5 policies can be added.**
- **A custom policy will take effect only when your Anti-DDoS Advanced instance is under attack.**
- In **match mode**, each custom policy may have up to **four** conditions for characteristic control, and the logical relationship between these conditions is "AND", which means all conditions must be matched before the policy will take effect.
- In **speed limit mode**, each custom policy can have only **one** condition.

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar to enter the protection configuration page. Click **CC Protection**, select the region, line, and target instance, and click **Add ACL**.
2. In the **Add ACL** pop-up window, set the following parameters as needed and click **OK**.

- Policy Name
  Enter the policy name, which can contain 1–20 characters of any type.
- Protocol
  Currently, HTTP and HTTPS are supported.
- Protected Domain Name
  Only when HTTPS is selected can a protected domain name be selected accordingly. You can select the protected domain name range, i.e., HTTPS website domain names in the configured forwarding rules.
- Mode
- Match mode: if an HTTP/HTTPS request with the specified field header is detected, it will be blocked or processed for CAPTCHA verification.
- Speed limit mode: the speed of access requests from the source IP will be limited. **This mode is not supported for HTTPS.**

- Policy
- **If the **match mode** is selected and the protocol is HTTP, multiple fields of an HTTP packet, namely, host, CGI, Referer, and User-Agent parameters, can be combined in various logical relationships such as "INCLUSIVE", "EXCLUSIVE", and "EQUAL TO", and you can set up to four policy conditions to combine the fields. **If the protocol is HTTPS**, multiple fields of an HTTPS packet, namely, CGI, Referer, and User-Agent parameters, can be combined in various logical relationships such as "INCLUSIVE", "EXCLUSIVE", and "EQUAL TO", and you can set up to three policy conditions to combine the fields. The fields are as described below:

Matched Field	Description	Applicable Logical Operators
host	Domain name of the access request.	INCLUSIVE, EXCLUSIVE, and EQUAL TO
CGI	URI of the access request.	INCLUSIVE, EXCLUSIVE, and EQUAL TO
Referer	Source website address of the access request, indicating the page from which the access request is generated.	INCLUSIVE, EXCLUSIVE, and EQUAL TO
User-Agent	Information such as browser identifier of the client that initiates the access request.	INCLUSIVE, EXCLUSIVE, and EQUAL TO

- When you select the **speed limit mode**, the speed of each source IP access request will be limited. You are allowed to set only one policy condition.
- Run
  This parameter is required only when the **match mode** is selected, indicating the action that needs to be performed after a policy is matched, such as blocking or CAPTCHA verification.

Setting Blocklist/Allowlist

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration** on the left sidebar to enter the protection configuration page. Click **CC Protection** and select the region, line, and target instance.
2. Select **HTTP** or **HTTPS** on the right of the page and select **URL allowlist**, **IP allowlist**, or **IP blocklist** to set the blocklist/allowlist. You can add or modify entries or export/import them in batches.

Configure Health check

Last updated：2020-05-13 19:51:00

Operation Scenarios

Anti-DDoS Advanced can automatically identify the running status of your real servers and isolate exceptional ones through health checks. This reduces the impact of real server exceptions on your overall business availability.

- **Non-website business (layer-4) health check**
  The health check mechanism for non-website business protection in Anti-DDoS Advanced is as follows: an Anti-DDoS cluster node initiates access requests to the server port specified in the configuration. If access to the port is normal, the real server will be considered healthy; otherwise, it will be considered exceptional.
  Under the TCP protocol, it detects whether the port can be connected. Under the UDP protocol, it uses ping for reachability check.
- **Website business (layer-7) health check**
  The health check mechanism for website business protection in Anti-DDoS Advanced is as follows: the Anti-DDoS forwarding cluster sends HTTP requests to the real server, and the Anti-DDoS system judges whether the server is normal according to the returned HTTP status codes.
  You can customize the status represented by the response code. For example, in a certain scenario, if HTTP returned values include http_1xx, http_2xx, http_3xx, http_4xx, and http_5xx, and you define http_1xx and http_2xx as normal status based on your business needs, then when a response code between http_3xx to http_5xx is returned, you can know that the server is exceptional.

> When configuring a layer-4 or layer-7 forwarding rule, if only one real server IP is configured in the rule, the health check feature will not be enabled, as it is suitable for scenarios with multiple real server IPs.

Directions

Health check configuration for non-website business

The following describes how to configure a health check rule for non-website business protection in Anti-DDoS Advanced.

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Access Configuration** to enter the management page.

2. Click **Non-Website Business**, select the target Anti-DDoS Advanced instance and corresponding rule, and click **Edit** in the "Health Check" column.

3. On the health check editing page, click **Show Advanced Options** to set the configuration items and click **OK**.

- Health check is enabled by default.
- When configuring health check, you are recommended to use the default values.
- The health check configuration information can be imported and exported in batches. After import, the system will match the rules one by one according to the imported "forwarding protocols and forwarding ports", and the "forwarding ports" must have rules configured.

Health check configuration for website business

The following describes how to configure a health check rule for website business protection in Anti-DDoS Advanced.

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Access Configuration** to enter the management page.

2. Click **Website Business**, select the target Anti-DDoS Advanced instance and corresponding rule, and click **Edit** in the "Health Check" column.

3. On the health check editing page, click to enable health check and click **Show Advanced Options** to set the configuration items. After confirming that everything is correct, click **OK**.

```
- Health check is disabled by default.
- When configuring health check, you are recommended to use the default values.
- The health check configuration information can be imported and exported in batc
hes. After import, the system will match the rules one by one according to the im
ported "forwarding protocols and business domain names", and the "business domain
names" must have rules configured.
```

Configuration Item Description

Layer-4 health check

Configuration Item	Description
Response timeout period	Maximum response timeout period for health check. If a real server fails to respond properly within the timeout period, the health check will be considered as failed.
Check interval	Interval between two health checks.
Unhealthy threshold	When the health check status is "succeeded", if the health check "failed" status is received for n times (n is the entered number) in a row, the real server will be considered as unhealthy, and an exception will be displayed in the console.
Healthy threshold	When the health check status is "failed", if the health check "succeeded" status is received for n times (n is the entered number) in a row, the real server will be considered as healthy, and nothing will be displayed in the console.

Layer-7 health check

Configuration Item	Description
Check interval	Interval between two health checks, which is 15 seconds by default.
Unhealthy threshold	When the health check status is "succeeded", if the health check "failed" status is received for n times (n is the entered number) in a row, the real server will be considered as unhealthy, and an exception will be displayed in the console.
Healthy threshold	When the health check status is "failed", if the health check "succeeded" status is received for n times (n is the entered number) in a row, the real server will be considered as healthy, and nothing will be displayed in the console.
HTTP request method and check path URL	The HEAD method is used by default, and the server will return only the header of the response packet. If the GET method is used, the server will return the complete response packet. The corresponding real server needs to support HEAD and GET. • If the page used for health check is not the default homepage of the application server, you need to specify a specific check path. • If the `host` field parameter is specified in the HTTP HEAD request, you need to specify the check path, i.e., the URI of the page file used for the health check.
HTTP status code detection	The HTTP status code used to determine whether the server is normal during health check. By default or if no selection is made, this value is http_1xx, http_2xx, http_3xx, and http_4xx. If the returned HTTP status code is not the default status value, the server will be considered as unhealthy. This value can be modified.

Configure Session to keep

Last updated：2020-05-13 19:51:00

Operation Scenarios

The non-website business protection service of Anti-DDoS Advanced provides IP-based session persistence to support forwarding requests from the same IP address to the same real server for processing.
Layer-4 forwarding supports simple session persistence. The session persistence duration can be set to any integer between 30 and 3600 seconds. If the time threshold is exceeded and the session has no new request, the connection will be automatically closed.

Directions

The following describes how to configure a session persistence rule for non-website business protection in Anti-DDoS Advanced.

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Access Configuration** on the left sidebar to enter the management page.

2. On the **Non-Website Business** tab, select the target Anti-DDoS Advanced instance and the corresponding rule, and click **Edit** in the "Session Persistence" column.

3. On the **Edit Session Persistence** page, click to enable session persistence, set the persistence duration, and click **OK**.

   - Session persistence is disabled by default.
   - When setting the persistence duration, you are recommended to use the default value.
   - The session persistence configuration information can be imported and exported in batches. After import, the system will match the rules one by one according to the imported "forwarding protocols and forwarding ports", and the "forwarding ports" must have rules configured.

Configuring Intelligent Scheduling

Last updated：2019-12-05 19:09:10

Use Cases

Each account can have multiple Anti-DDoS instances, and each instance has at least one protective line; therefore, there can be multiple protective lines under one account. Once your business is added to an Anti-DDoS instance, a protective line will be configured for it. If multiple protective lines have been configured, you need to choose the optimal business traffic scheduling method, i.e., how to schedule business traffic to the optimal line for protection while ensuring high business access speed and availability.
Anti-DDoS features priority-based CNAME intelligent scheduling, where you can select an Anti-DDoS instance and set the priority of its protective line as needed.

> Anti-DDoS Pro (includes single-IP and multi-IP instances) and Anti-DDoS Advanced instances support setting resolution.

Priority-based Scheduling

This refers to using the protective line of the highest priority to respond to all DNS requests, i.e., all access traffic will be scheduled to the protective line of the currently highest priority. You can adjust the priority value of protective line, which is 100 by default. The smaller the value, the higher the priority. The specific scheduling rules are as follows:

- If the protective instance configured for your business contains multiple protective lines from different ISPs and of the same priority, response will be made based on the ISP of the specific DNS request. If one of the lines is blocked, access traffic will be scheduled in the order of BGP > China Telecom > China Unicom > China Mobile > ISP outside Mainland China.
- If all the lines of the same priority are blocked, access traffic will be automatically scheduled to the currently available protective line of the second-highest priority.

> If no protective lines of the second-highest priority are available, automatic scheduling cannot be completed, and business access will be interrupted.

- If the protective instance configured for your business contains multiple protective lines from the same ISP and of the same priority, access traffic will be scheduled by way of load balancing, i.e., evenly distributed to such lines.

Example

Assume that you have the following Anti-DDoS instances: BGP protective IPs 1.1.1.1 and 1.1.1.2, China Telecom protective IP 2.2.2.2, and China Unicom protective IP 3.3.3.3, of which the priority of 1.1.1.2 is 2 and that of the rest is 1. Normally, all traffic will be scheduled to the protective lines with the current priority of 1. Specifically, traffic from China Unicom will be scheduled to 3.3.3.3, that from China Telecom to 2.2.2.2, and that from other ISPs to 1.1.1.1. If 1.1.1.1 is blocked, access traffic under this IP will be automatically scheduled to 2.2.2.2. If both 1.1.1.1 and 3.3.3.3 are blocked, traffic supposed to be scheduled to them will be distributed to 2.2.2.2, and if 2.2.2.2 is blocked too, traffic will be scheduled to 1.1.1.2.

Prerequisites

- Before enabling intelligent scheduling, please connect your business to be protected to your Anti-DDoS instance.

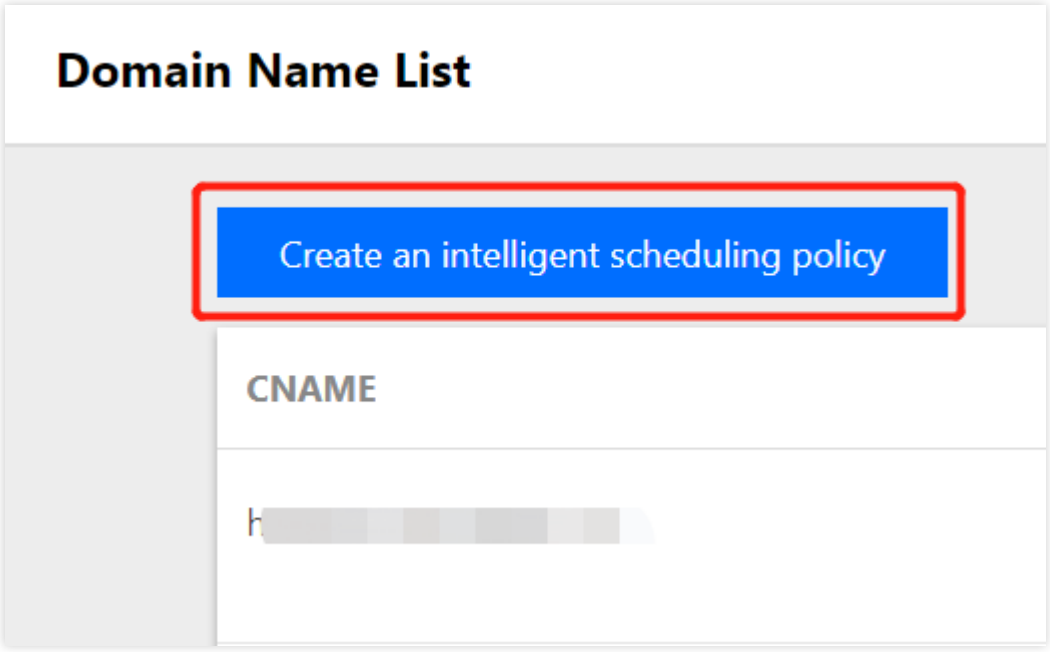
  - If you need to add the IP of your protected Tencent Cloud product to a purchased Anti-DDoS Pro instance, please see Getting Started with Anti-DDoS Pro.
  - If you need to connect your layer-4 or layer-7 application to a purchased Anti-DDoS Advanced instance, please see Anti-DDoS Advanced documents Connecting Non-website Application.

- Before modifying DNS information, you need to purchase a domain name resolution product.

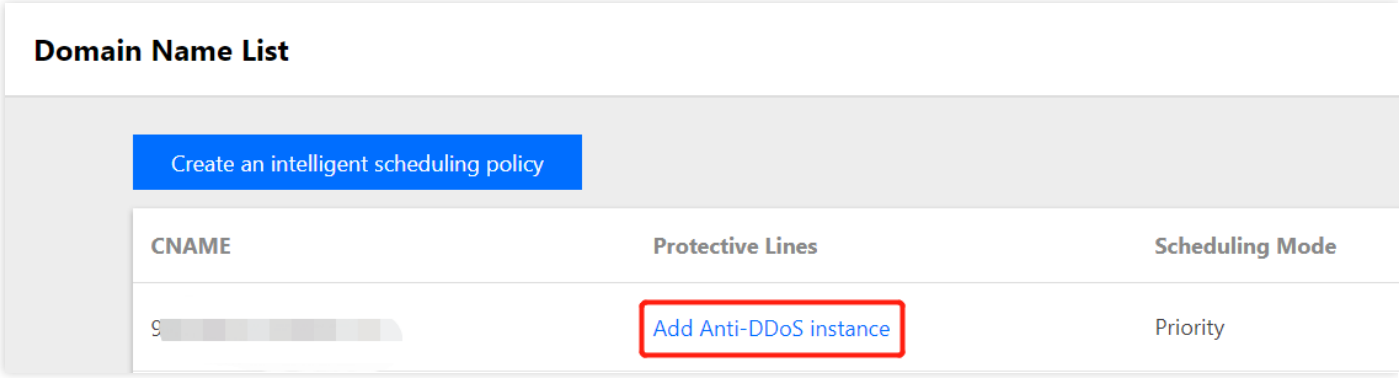
Setting Line Priority

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

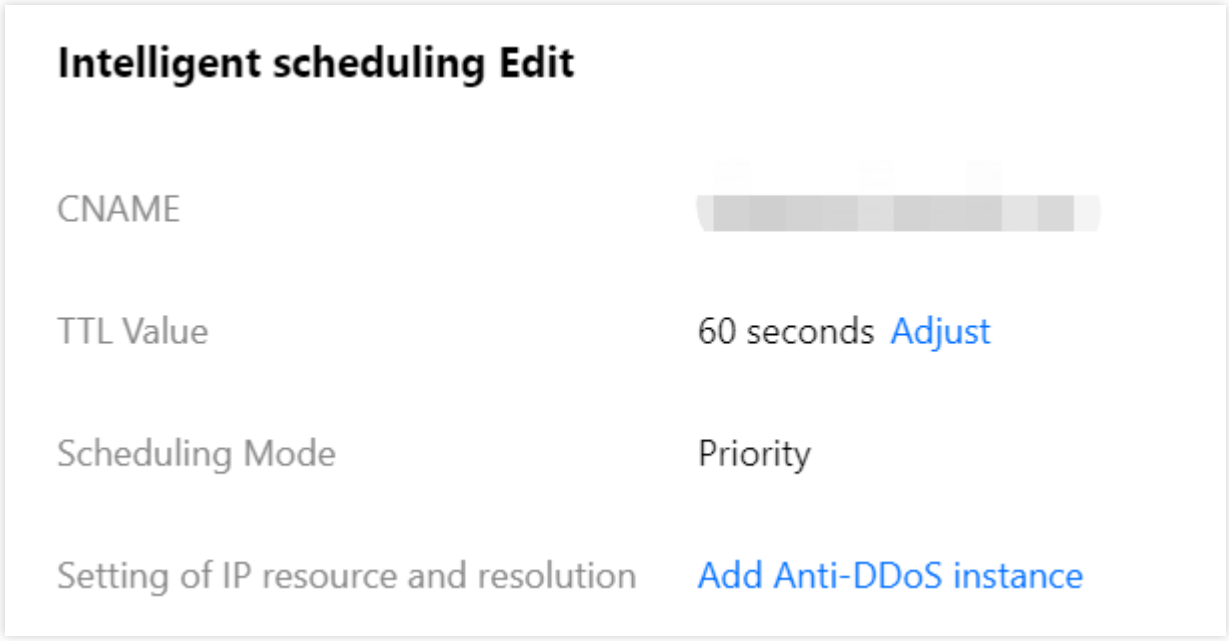
1. Log in to the Anti-DDoS Console, select **Intelligent Scheduling** > **Domain Name List** on the left sidebar, and click **Create Intelligent Scheduling**. Then, a CNAME record will be generated automatically by the system.



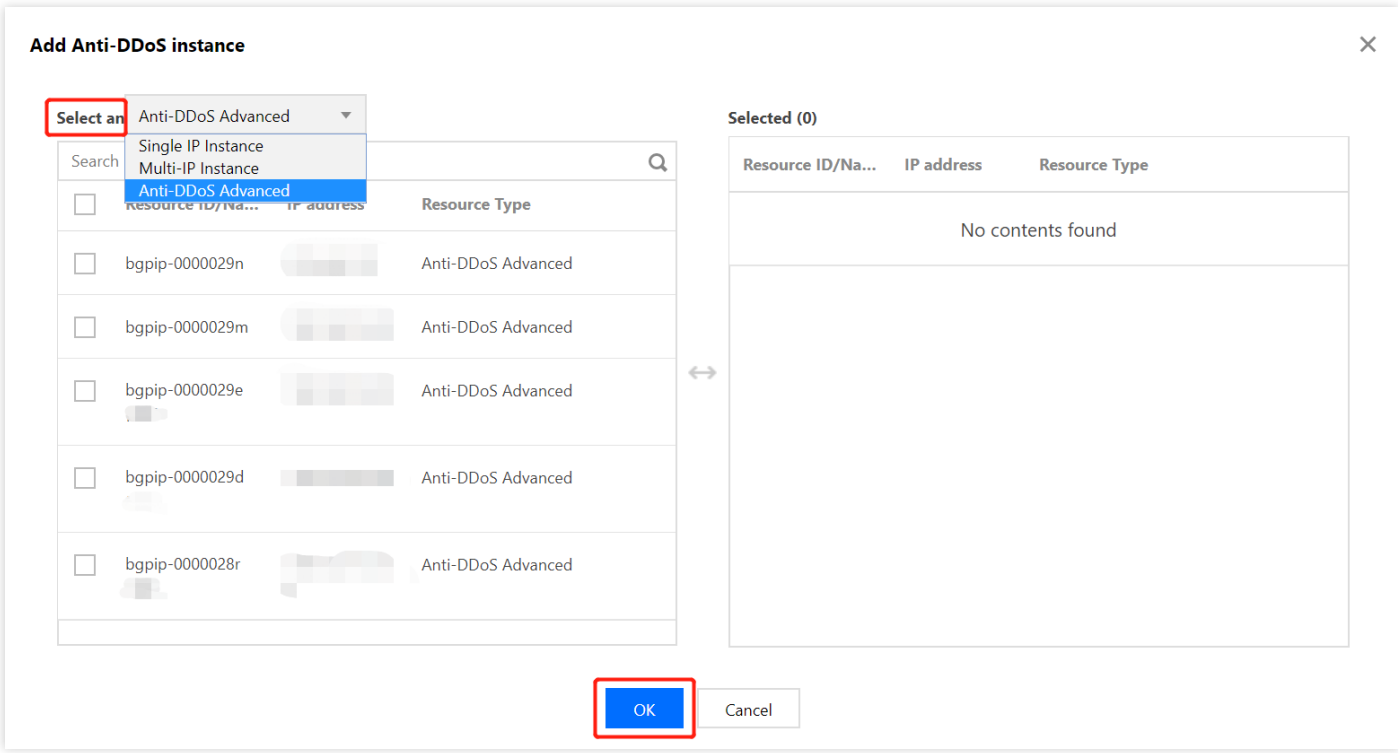
2. Locate the row of the CNAME record and click **Add Anti-DDoS Instance** to enter the intelligent scheduling editing page.



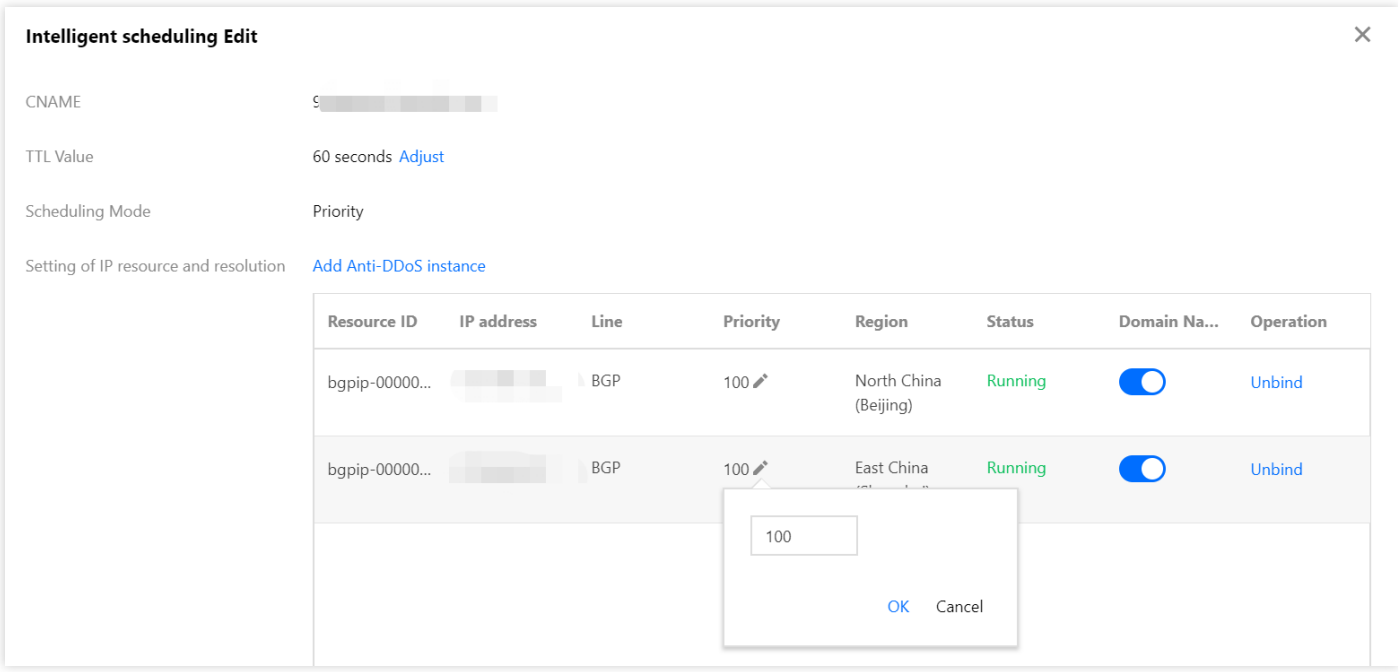
3. On the intelligent scheduling editing page, the TTL value is 60s by default, which can range from 1s to 3,600s, and the default scheduling method is priority-based.



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



5. After the instance is selected, DNS will be enabled for its protective line by default. At this point, you can set the line priority.



Modifying DNS

Before using a CNAME record for intelligent scheduling, you are recommended to change the CNAME record of your business domain name DNS to the CNAME record automatically generated by the intelligent scheduling system of Tencent Cloud Anti-DDoS, to which all access traffic will be directed.

Configure attack alarm threshold

Last updated：2020-05-13 19:51:00

Use Cases

When attacks against your Anti-DDoS Advanced resources start/end and your protected IPs are blocked/unblocked, you will get notifications through internal message, SMS, or email. Configuring proper attack alarm thresholds can help you know more about attacks instantly. This feature can also help prevent false alarming caused by normal business operations that bring traffic surges (such as data sync). For more information on how to receive alarm messages, please see Setting Security Event Notification.

Configuring DDoS Attack Alarm Threshold

This configuration example can achieve the following effect: after the attack traffic to the Anti-DDoS Advanced instance "bgpip-0000021y" exceeds the cleansing threshold and triggers DDoS attack cleansing, when the cumulative cleansed traffic (value) exceeds 1,000 Mbps, DDoS attack alarm messages will be sent to the specified user group.

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

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Resource List** on the left sidebar to enter the Anti-DDoS Advanced page, find the instance "bgpip-0000021y", and click **Protection Configuration** in the "Operation" column.

2. Enter the DDoS protection configuration page, select the alarm metric **Cleansed Traffic** in the drop-down list on the right of the DDoS attack alarm threshold, and set the threshold to 1,000 Mbps.

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

Configuring CC Attack Alarm Threshold

This configuration example can achieve the following effect: after the Anti-DDoS Advanced instance "bgpip-0000021y" triggers CC protection, when the HTTP CC protection bandwidth exceeds 2000 QPS, CC attack alarm messages will be sent to the specified user group.

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

1. Log in to the Anti-DDoS Console and select **Anti-DDoS Advanced** > **Protection Configuration**. On the protection configuration page, click **CC Protection**.
2. On the CC protection page, find the "HTTP CC Protection" section at the bottom of the page, and set the threshold to 2,000 QPS in "HTTP CC Attack Alarm Threshold".

Instance Management
Viewing Instance Details

Last updated：2020-04-25 11:34:54

Operation Scenarios

You can view the basic information (such as the base protection bandwidth and running status) and configure elastic protection of all purchased Anti-DDoS Advanced instances in the Anti-DDoS Console.

Directions

This document uses the Anti-DDoS Advanced instance "bgpip-0000020n" in Guangzhou as an example to describe how to view instance details.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List** on the left sidebar, and click **South China (Guangzhou)** in the region selection box. In the list below, click the Anti-DDoS Advanced instance whose ID is "bgpip-0000020n" to view its information.
2. On the pop-up page, you can view the following information:

Parameter description:

- **Basic information:**
  - **Name**

  This is the name of the Anti-DDoS Advanced instance for easier instance identification and management. You can set a custom instance name containing 1–20 character of any type as desired. For detailed directions, please see Setting Resource Name.
  - **IP**

    This is the protective IP provided by the Anti-DDoS Advanced instance, which is used as the frontend IP of the real server to provide services.
  - **Region**

    This is the **region** selected when the Anti-DDoS Advanced instance is purchased.
  - **Forwarding target**

    This is the location of the real business server protected by the Anti-DDoS Advanced instance.
  - **Base DDoS protection bandwidth**

    This is the base protection bandwidth of the Anti-DDoS Advanced instance, i.e., the **base protection**

bandwidth selected when the instance is purchased. If elastic protection is not enabled, this will be the maximum protection bandwidth of the instance.

- **CC protection bandwidth**
  This is the capability of the Anti-DDoS Advanced instance to defend against sudden CC attacks.
- **Current status**
  This is the current status of the Anti-DDoS Advanced instance, such as **Running**, **Cleansing**, and **Blocked**.
- **Expiration time**
  This is calculated based on the **purchase duration** selected when the instance is purchased and the order is paid, which is accurate to second. Tencent Cloud will send expiration and renewal reminders to the account creator and all collaborators through internal message, SMS, and email 7 days before the instance expires.
- **Intermediate IP range**
  This is the information of the intermediate IP range in the region of the current Anti-DDoS Advanced instance.

- **Elastic protection information**

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

This indicates whether elastic protection is enabled. If it is not enabled when you purchase the Anti-DDoS Advanced instance, you can enable it in a self-service manner when using the instance. For detailed directions, please see Configuring Elastic Protection.

- **Elastic bandwidth**
  This is the maximum elastic protection bandwidth of the Anti-DDoS Advanced instance. You can adjust it as needed at any time.

> This parameter is visible only after elastic protection is enabled.

Setting Resource Name

Last updated：2020-04-25 11:34:54

When multiple Anti-DDoS Advanced instances are used, you can set **resource names** to quickly identify and manage them.

Method 1

Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List**, select the region and line, click the name of the target instance in the **ID/Name** column, and then enter a name.

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

Method 2

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List**, and select a region in the top-left corner.
2. In the list below, click the ID of the target instance in the "ID/Name" column. In the **Basic Instance** section on the pop-up page, click **Modify**, enter or modify the name, and click **OK**.

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

Configuring Elastic Protection

Last updated：2020-04-25 11:34:55

After you enable elastic protection on the Anti-DDoS Advanced instance, when the attack traffic bandwidth exceeds the base protection bandwidth, Anti-DDoS Advanced will continue protection based on your elastic protection bandwidth.
If elastic protection is not enabled when you purchase the Anti-DDoS Advanced instance, you can enable it when using the instance. If elastic protection is not triggered on a day, no relevant fees will be incurred. When elastic protection is triggered (i.e., the attack bandwidth exceeds the base protection bandwidth), fees will be charged based on the billing tier corresponding to the actual attack bandwidth peak on the day and a bill will be generated the next day. You can modify the elastic protection bandwidth of the Anti-DDoS Advanced instance as needed with immediate effect.

Enabling Elastic Protection

> If elastic protection is not enabled when you purchase the Anti-DDoS Advanced instance, you can enable it when using the instance and set the elastic protection bandwidth to higher than the highest historical attack traffic bandwidth. This helps avoid potential IP blockage in case of excessive attacks.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List**, and click **Enable Elastic Protection** next to the target instance.
2. In the **Enable Elastic Protection** box, select the needed **Elastic Protection Bandwidth**.
3. Click **OK**.

Modifying Elastic Protection Bandwidth

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List**, and click the target instance ID to enter the basic information page of the instance.

2. In the "Elastic Protection" section, click **Modify** on the right of "Elastic Bandwidth".

3. In the **Modify Elastic Protection** box, select an appropriate **Elastic Protection Bandwidth**.

- You can increase or reduce the elastic protection bandwidth. The protection capability varies by region. For more information, please see Product Overview.
- Modification of the elastic protection bandwidth takes effect immediately.

4. Click **OK**.

Disabling Elastic Protection

If you disable elastic protection, the maximum protection bandwidth will degrade to the base protection bandwidth. Please ensure that the base protection bandwidth meets your actual needs before disabling elastic protection.

1. Log in to the Anti-DDoS Console, select **Anti-DDoS Advanced** > **Asset List**, and click **Disable Elastic Protection** next to the target instance.
2. In the **Disable Elastic Protection** box, click **OK**.

Adjust the specification of DDoS High Defense IP instance

Last updated：2020-05-13 19:50:59

Operation Scenarios

When using Anti-DDoS Advanced, if you find that the current specification (such as the base protection bandwidth, number of forwarding rules, or service bandwidth) cannot meet your actual business needs, you can upgrade the Anti-DDoS Advanced instance specification to improve the protection capabilities.
Specification adjustment in Anti-DDoS Advanced supports increasing the base protection bandwidth, the number of forwarding rules (protected domain names or ports), and the service bandwidth.

> Currently, specification downgrade of purchased Anti-DDoS Advanced instances is not supported.

Upgrading Anti-DDoS Advanced instance specification incurs additional fees. After the payment is made, the instance specification upgrade will take effect immediately.

Directions

1. Log in to the Anti-DDoS Console.
2. Select **Anti-DDoS Advanced** > **Resource List**.
3. Click **Upgrade** in the "Operation" column in the row of the target instance.
4. Set **Upgrade Base Protection**, **Upgrade Service Bandwidth**, or **Upgrade Forwarding Rule Quantity** as needed.
5. Click **Upgrade Now** to enter the **Check Information** page.
6. After confirming that everything is correct, determine whether to use vouchers according to your actual needs, and then click **Purchase**.
7. After making the payment, return to the Anti-DDoS Advanced resource list and you can see that the specification adjustment has taken effect.

Viewing Statistics Reports

Last updated：2020-04-25 11:34:56

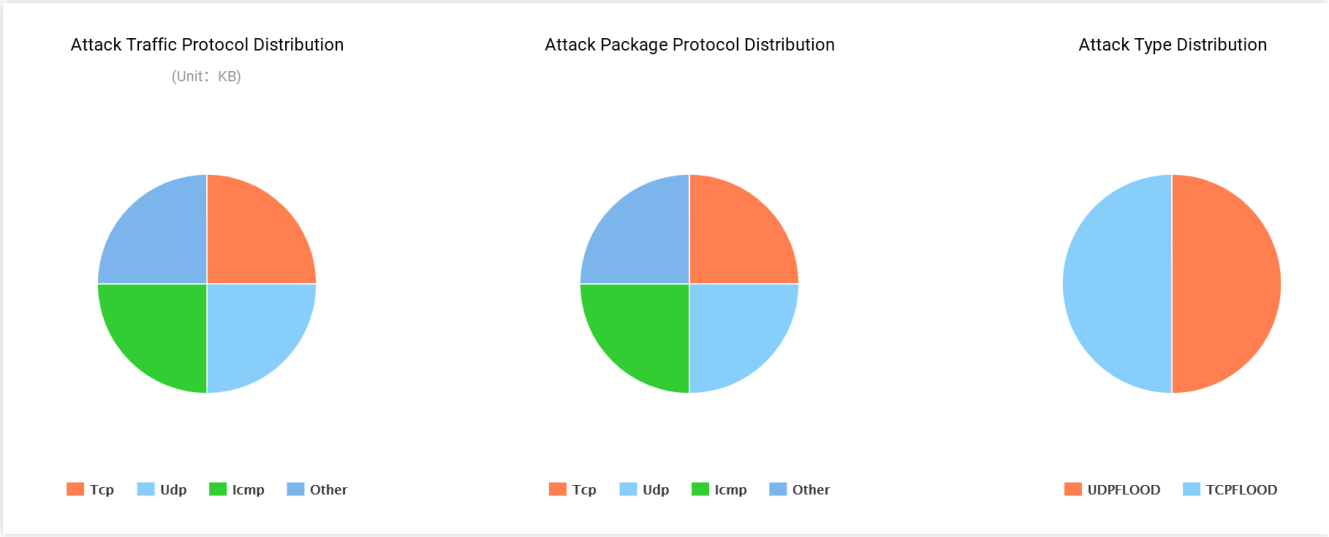
When you receive a DDoS attack alarm message or notice any issue with your business, you need to view details of the attacks, including the traffic and current protection effect. Enough information is critical for you to take measures in time to keep your business running smoothly.
The statistical reports in the Anti-DDoS Advanced Console provide rich information to help you easily stay up to date with the current business and attack conditions.

Viewing DDoS Protection Details

1. Log in to the Anti-DDoS Console.
2. Select **Anti-DDoS Advanced** > **Statistical Report**.
3. On the **DDoS Protection** tab, set the query period and select the region, line, target instance, and protected IP to check whether the instance has been attacked.

   > You can query the attack traffic and DDoS attack events in the last 180 days.

   - View the information of attacks suffered by the selected Anti-DDoS Advanced instance within the queried period, such as the trends of **attack traffic bandwidth/attack packet rate**. When the instance is under attack, you can intuitively view the attack bandwidth peak in the bandwidth trend diagram.
   - View how the attacks distribute across different attack traffic protocols, attack packet protocols, and attack types.
     - **Attack Traffic Protocol Distribution** displays how the attacks suffered by the selected Anti-DDoS Advanced instance distribute across different attack traffic protocols within the queried period.
     - **Attack Packet Protocol Distribution** displays how the attacks suffered by the selected Anti-DDoS Advanced instance distribute across different attack packet protocols within the queried period.
     - **Attack Type Distribution** displays how the attacks suffered by the selected Anti-DDoS Advanced instance distribute across different attack types within the queried period.



- **Attack Source Distribution**: in the **Attack Source Distribution** section, you can view the distribution of DDoS attack sources in and outside Mainland China within the queried period, so that you can take further protective measures based on the displayed information.

- In **DDoS Attack Records**, you can view details of the DDoS attack events within the queried period, including the start time, duration, type, and status of each attack event.
  - You can download DDoS attack packets to analyze and trace the attacks.
  - Click **Attack Details** to view the maximum packet rate, maximum attack traffic bandwidth, and total amount of traffic cleansed during the DDoS attack event.
  - Click **Attack Source Info** to view the attack source IP addresses, source regions, generated attack traffic, and attack packet size.

> Attack source information is sampled data, which is randomly collected for statistics. The data will be displayed around 2 hours after an attack ends.

Viewing CC Protection Conditions

1. Log in to the Anti-DDoS Console.

2. Select **Anti-DDoS Advanced** > **Statistical Report**.

3. Click the **CC Protection** tab, set the query period, and select the region, line, target instance, and protected IP to check whether the instance has been attacked.

You can query the number of attack requests and CC attack events in the last 180 days.

- You can select **Today** to view the trend in the number of attack requests to the selected Anti-DDoS Advanced instance. You can check whether the total number of requests is far higher than the normal QPS, whether the attack QPS has a value, and whether the value is extremely high.
- If the protected IP is under CC attack, the system will record the attack start time, end time, attacked domain names, attacked URLs, total request peak, attack request peak, and attack sources.
  - **Total request peak**: the peak of the total request traffic the Anti-DDoS Advanced instance receives when the attack occurs.
  - **Attack request peak**: the peak number of requests blocked by the instance when the attack occurs.

Viewing Business Traffic Conditions

1. Log in to the Anti-DDoS Console.
2. Select **Anti-DDoS Advanced** > **Statistical Report**.
3. Click the **Scenarios** tab, set the query period, and select the region, line, target instance, and protected IP to view the **inbound/outbound business traffic bandwidth trend**, **inbound/outbound business packet rate trend**, and **new connections or concurrent connections trend** in the selected period. In addition, you can view the peaks of inbound/outbound business traffic bandwidth and inbound/outbound business packet rate.
   - **Number of concurrent connections**: the total number of connections that exist in the system at a time point.
   - **Number of new connections**: the number of TCP connections that are established in the system in one second.

   You can query the business information in the last 180 days.

Viewing Operation Logs

Last updated：2020-05-13 19:36:22

Operation Scenarios

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

- Logs of forwarding policy change
- Logs of advanced DDoS protection policy change
- Logs of cleansing threshold adjustment
- Logs of protection level change
- Logs of CC protection policy change
- Logs of elastic protection bandwidth adjustment
- Logs of resource name change

Directions

1. Log in to the Anti-DDoS Console.
2. Select **Operation Logs** to enter the log query page.
3. Set the time range. View the corresponding operation history by filtering **Anti-DDoS Advanced** in **Product Type**.

Setting Security Event Notifications

Last updated：2020-04-25 11:34:56

Operation Scenarios

Alarm messages for Anti-DDoS Advanced will be sent to you through internal message, SMS, or email in the following conditions:

- An attack starts.
- An attack ended 15 minutes ago.
- An IP is blocked.
- An IP is unblocked.

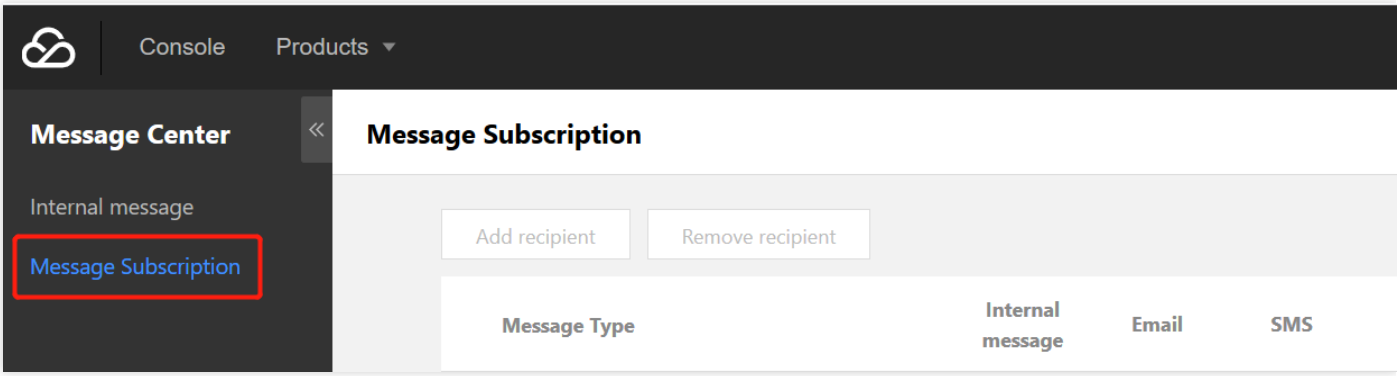
You can modify the recipients and how they receive the alarm messages as needed.

Directions

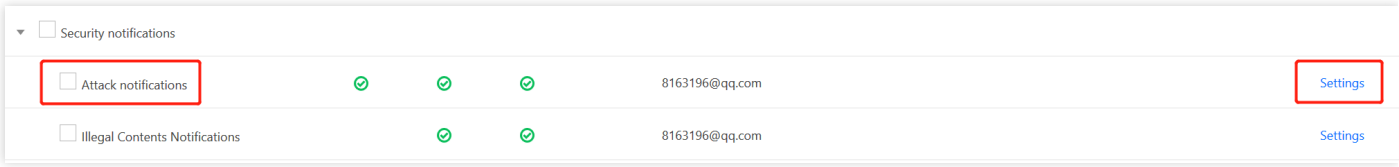
1. Log in to your Tencent Cloud account and go to the Message Center.

> Alternatively, you can log in to the console, click  in the top-right corner, and then click **Enter Message Center** at the bottom of the page.

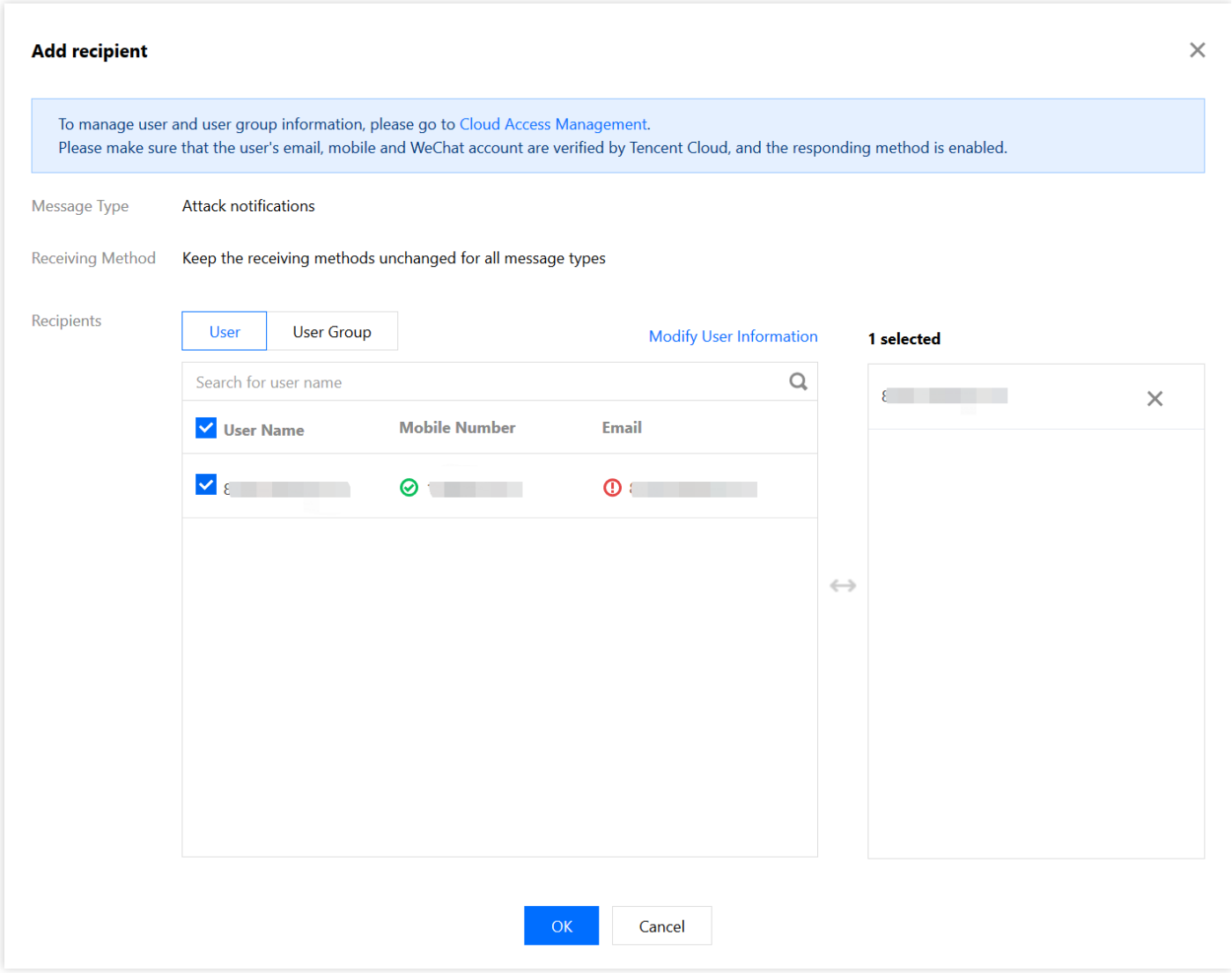
2. Click **Message Subscription** on the left sidebar to enter the message list.



3. In the message list, click **Settings** on the row of **Security Event Notifications** to enter the settings page.



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



Best Practices
Migrating Applications to Anti-DDoS Advanced

Last updated：2020-05-09 18:03:48

Background

There could be many special configurations and restrictions for currently running online applications, and service downtime may have negative impact on business. Therefore, you are recommended to follow the suggestions below to adopt appropriate switching mode and avoid possible risks before integrating Anti-DDoS Advanced to your online applications.

Suggestions

Please note that the following suggestions are based on what we have learned from serving other Tencent Cloud customers. You are recommended to adjust or improve the scheme according to your actual situation to minimize risks.

Technical suggestions

- Modify local hosts file instead of the DNS A record. The testing team should locally test and measure relevant performance metrics such as availability and latency.
- With an intelligent DNS product, you can change the A record for specified ISPs or regions, redirect a little amount of traffic to Anti-DDoS Advanced IP for test before fully applying Anti-DDoS Advanced to your business applications.
- Shorten the TTL of the DNS record for faster disaster recovery.
- Prepare a rollback plan in advance and back off as soon as any problem arises.

Priority

- Migrate standby and non-critical business applications first.
- Migrate the applications during off-hours.

In Case of Real Server IP Exposed

Last updated：2020-04-03 14:35:44

Some attackers may record real server IP history, and the exposed IPs allow them to bypass Anti-DDoS Advanced and directly attack your real server. In this case, you are recommended to change the actual real server IP.
If you don't want to change the IP of your real server or have already done so but the IP is still exposed, in order to prevent attacker from bypassing Anti-DDoS and directly attack your real server IP, please follow the steps below:

- To prevent attackers from scanning C range or other similar IP ranges, do not use the same IP or an IP similar to the old IP as the new real server IP.
- Prepare the standby linkage and standby IP in advance.
- Set the scope of access sources to prevent malicious scans.
- Follow the instructions in Real Server-Based Defense Scheduling Solution and apply the solution based on your actual needs.

> Before changing the real server IP, be sure to confirm that all factors that may expose the IP have been eliminated.

You can refer to the following steps before changing the real server IP to check the risk factors and prevent the new IP from disclosure.

Checklist

Checking DNS resolution history

Check all the DNS resolution records of the attacked real server IP, including resolution records of sub-domain names, MX (Mail Exchanger) records of mail servers, and NS (Name Server) records. Make sure that all those records are configured for protection by Anti-DDoS Advanced, so that none of them will be resolved to the new real server IP.

Checking for information disclosure and command execution vulnerabilities

- Check your websites or business systems for possible information disclosure vulnerabilities, such as phpinfo() disclosure and sensitive information leakage on GitHub.
- Check your websites or business systems for command execution vulnerabilities.

Checking for trojans and backdoors

Check your real server for potential trojans, backdoors, and other hidden risks.

Obtaining Real Client IP

Last updated：2020-04-21 11:34:57

Using Non-Website Traffic Forwarding Rules

When Anti-DDoS Advanced uses non-website traffic forwarding rules, the real server needs to get the real client IP through the TOA module.
After the business request is forwarded through layer 4 of the protective IP, the source IP address that the business server sees after receiving the packet is the egress IP address of the protective IP. In order for the server to get the real client IP, you can use the following TOA scheme. On the Linux server of the business, install the corresponding TOA kernel package and reboot the server. Then, the server can get the real client IP.

How TOA works

Once forwarded, the data packet will undergo SNAT and DNAT at the same time, and its source and destination addresses will be modified.
Under the TCP protocol, in order to pass the client IP to the server, the client's IP and port are placed in the custom `tcp option` field during forwarding.

```
#define TCPOPT_ADDR 200
#define TCPOLEN_ADDR 8 /* |opcode|size|ip+port| = 1 + 1 + 6 */

/*
*insert client ip in tcp option, now only support IPV4,
*must be 4 bytes alignment.
*/
struct ip_vs_tcpo_addr {
__u8 opcode;
__u8 opsize;
__u16 port;
__u32 addr;
};
```

The Linux kernel's state transits from `SYN_REVC` to `TCP_ESTABLISHED` after the listening socket receives the ACK packet of three-way handshake. At this point, the kernel will invoke the `tcp_v4_syn_recv_sock` function. The Hook function `tcp_v4_syn_recv_sock_toa` will first invoke the original `tcp_v4_syn_recv_sock` function, then invoke the `get_toa_data` function to extract the `TOA OPTION` from the `TCP OPTION` , and store it in the `sk_user_data` field.

Then, `inet_getname_toa hook inet_getname` will be used. When the source IP address and port is obtained, the original `inet_getname` function will be invoked first, and then it will be checked whether `sk_user_data` is empty. If real IP and port can be extracted from this field, the returned values of `inet_getname` will be replaced with these two values.

The client program calls `getpeername` in the user mode, and the client's original IP and port will be returned.

Kernel package installation steps

CentOS 6.x/7.x

1. Download the installation package:
   - Download for CentOS 6.x
   - Download for CentOS 7.x
2. Install the package file.

```
rpm -hiv kernel-2.6.32-220.23.1.el6.toa.x86_64.rpm --force
```

3. Reboot the server after the installation is completed.

```
reboot
```

4. Run the following command to check whether the TOA module is successfully loaded.

```
lsmod | grep toa
```

5. If not, manually start it.

```
modprobe toa
```

6. Run the following command to enable automatic loading of the TOA module.

```
echo "modprobe toa" >> /etc/rc.d/rc.local
```

Ubuntu 16.04

1. Download the installation package:
   - Download the kernel package
   - Download the kernel header package
2. Run the following command:

```
dpkg -i linux-image-4.4.87.toa_1.0_amd64.deb
```

The header package is optional. If needed for relevant development, install it.

3. After the installation is completed, reboot the server, then run the `lsmod | grep toa` command to check whether the TOA module is loaded, and if not, start it by running the `modprobe toa` command.
   Run the following command to enable loading of the TOA module:

```
echo "modprobe toa" >> /etc/rc.d/rc.local
```

Debian 8

1. Download the installation package:
   - Download the kernel package
   - Download the kernel header package
2. The installation method is the same as that for Ubuntu.
   Please download the appropriate kernel package according to the type and version of the Linux OS of your business server and follow the steps below. If there is no kernel package for your OS, please see the **TOA source code installation guide** below.

TOA source code installation guide

Source code installation

1. Download the source code package containing the TOA patch and click the TOA patch to download the installation package.
2. Decompress it.
3. Edit `.config` by changing `CONFIG_IPV6=M` to `CONFIG_IPV6=y` .
4. If you need to add some custom descriptions, you can edit `Makefile` .
5. Run `make -jn` (n is the number of threads).
6. Run `make modules_install` .
7. Run `make install` .
8. Modify `/boot/grub/menu.lst` by changing `default` to the newly installed kernel (the `title` order starts at 0).
9. Reboot and the kernel will have TOA.
0. Run `lsmode | grep toa` to check whether the TOA module is loaded, and if not, start it by running `modprobe toa` .

Kernel package production

You can make your own rpm package or use the one we provide.

1. Install `kernel-2.6.32-220.23.1.el6.src.rpm` .

```
rpm -hiv kernel-2.6.32-220.23.1.el6.src.rpm
```

2. Generate the kernel source code directory.

```
rpmbuild -bp ~/rpmbuild/SPECS/kernel.spec
```

3. Copy the source code directory.

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/ cp -a linux-2.6.32-220.23.1.el
6.x86_64/ linux-2.6.32-220.23.1.el6.x86_64_new
```

4. Apply the TOA patch to the copied source directory.

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/linux-2.6.32-220.23.1.el6.x86_64
_new/
patch -p1 < /usr/local/src/linux-2.6.32-220.23.1.el6.x86_64.rs/toa-2.6.32-220.2
3.1.el6.patch
```

5. Edit `.config` and copy it to the `SOURCE` directory.

```
sed -i 's/CONFIG_IPV6=m/CONFIG_IPV6=y/g' .config
echo -e '\n# toa\nCONFIG_TOA=m' >> .config
cp .config ~/rpmbuild/SOURCES/config-x86_64-generic
```

6. Delete `.config` from the original source code.

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/linux-2.6.32-220.23.1.el6.x86_64

rm -rf .config
```

7. Generate the final patch.

```
cd ~/rpmbuild/BUILD/kernel-2.6.32-220.23.1.el6/
diff -uNr linux-2.6.32-220.23.1.el6.x86_64 linux-2.6.32-220.23.1.el6.x86_64_ne
w/ >
~/rpmbuild/SOURCES/toa.patch
```

8. Edit `kernel.spec` .

```
vim ~/rpmbuild/SPECS/kernel.spec
```

Add the following lines to `ApplyOptionPath` (you can also modify the names of custom kernel packages such as `buildid`):

```
Patch999999: toa.patch
ApplyOptionalPatch toa.patch
```

9. Make an rpm package.

```
rpmbuild -bb --with baseonly --without kabichk --with firmware --without debugi
nfo --target=x86_64 ~/rpmbuild/SPECS/kernel.spec
```

0. Install the kernel rpm package.

```
rpm -hiv kernel-xxxx.rpm --force
```

1. Reboot to load the TOA module

Using Website Traffic Forwarding Rules

When Anti-DDoS Advanced uses website traffic forwarding rules, the `X-Forwarded-For` field in the HTTP header can be used to get the real client IP.

`X-Forwarded-For` is an extended field in the HTTP header used to enable the server to identify the real IP of the clients accessing the server through proxies.

Format:

`X-Forwarded-For: Client, proxy1, proxy2, proxy3……`

When forwarding the user access request to the real server, Anti-DDoS Advanced will record the real IP of the requesting user at the beginning of the `X-Forwarded-For` field. Therefore, the application on the real server only needs to get the content of the `X-Forwarded-For` field in the HTTP header.

For more information, please see How to Get Real Client IP Based on Layer-7 Forwarding Rules.

Real Server-based Defense Scheduling Solution

Last updated：2020-05-09 18:03:49

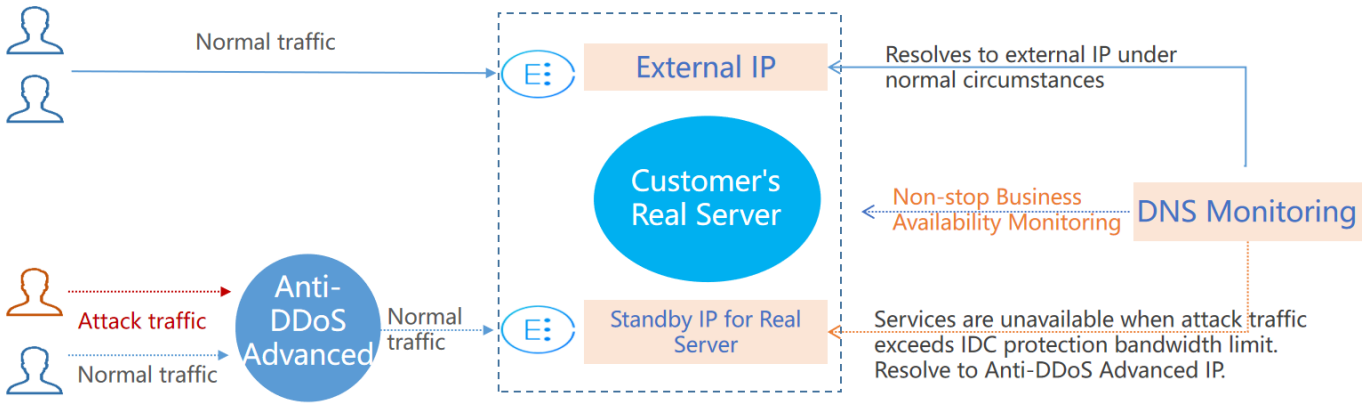
Background

You may consider real server-based protection scheduling if your customers have low tolerance for connection latency or if your business requires normal traffic to directly access the real server.
This scheme can quickly schedule protection after attacks occur, while allowing normal traffic to access the real server.

Protection Scheme

The figure below illustrates how real server-based protection scheduling works:

> This scheme requires monitoring and intelligent switching provided by DNS service providers.



Scheme Description

To implement this scheme, you need an Anti-DDoS Advanced IP, a DNS monitor, an external business IP, and a standby IP of the real server.

- Under normal circumstances, your business domain name is resolved to the outbound IP. Requests access the real server directly. DNS monitors watch over whether the applications are accessible on the real server in real time. As soon as the DNS monitor detects that the outbound IP is not accessible, DNS will resolve the business domain name to the Anti-DDoS Advanced IP according to the preset switching rules. Anti-DDoS Advanced will cleanse and remove the attack traffic and forward normal traffic to the standby IP of the real server, thus ensuring service availability.

  > To avoid faulty switching caused by uncontrollable factors such as network jitter, manual switching is recommended.

Benefits

- Meets the needs of direct access to the real server under normal circumstances.
- Applies to businesses that require very low connection latency.
- When the traffic volume is beyond the protection capability of the real server, the domain name will be automatically resolved to the Anti-DDoS Advanced IP.

Tips and Precautions

- Configure the forwarding rules of real server standby IP and Anti-DDoS Advanced IP in advance.
- Deploy the standby IP and primary IP of the real server with different physical addresses for better protection results.
- Practice and test regularly and familiarize yourself with scheme details to solve potential problems.

Suggestions on Stress Test

Last updated：2020-05-09 18:03:49

A stress test is designed to simulate DDoS attacks. To ensure the quality of the test, you are recommended to read this document carefully before conducting a stress test.

> The following suggestions are mainly about the impact of DDoS protection on stress testing. You may also need to consider other test-related factors, such as network bandwidth, linkage loads, and other basic resources.

Adjusting Protection Policies

- Disable CC protection policies, or set the HTTP request threshold for CC protection to a value higher than the maximum value of your stress test.
- Disable DDoS protection policies, or set the cleansing threshold for DDoS protection to a value higher than the maximum value of your stress test.

Limiting Traffic and Number of Requests in Stress Test

- The bandwidth of your stress test should be lower than 1 Gbps; otherwise, attack protection may be triggered.
- The number of HTTP requests in your stress test should be no more than 20,000 requests per second (QPS); otherwise, attack protection may be triggered.
- The number of new connections established per second, the maximum number of connections, and the number of inbound packets per second in your stress test should be less than 50,000, 2,000,000, and 200,000, respectively.

> If the traffic and number of requests in your stress test will exceed the above ranges, please contact Tencent Cloud Technical Support. We will offer support during your stress test.

Evaluating Impact of Stress Test in Advance

You are recommended to contact Tencent Cloud solution architects or Tencent Cloud Technical Support before you conduct the stress test to evaluate possible consequences and develop risk aversion measures.

FAQ

FAQ about Block

Last updated：2020-05-09 18:03:50

Why is my IP blocked?

Tencent Cloud reduces costs of cloud services by sharing the infrastructure, with one public IP shared by many users. When a high-traffic attack occurs, the entire Tencent Cloud network may be affected, not only the target servers. To protect other users and ensure network stability, the target server IP needs to be blocked.

Why isn't anti-DDoS service always free?

DDoS attacks threaten not only the targets but also the entire cloud network and affect non-attacked Tencent Cloud users as well. In addition, DDoS protection incurs high costs, including cleansing fees and bandwidth fees, among which bandwidth costs the most. Bandwidth fees are calculated based on the total amount of traffic, and there is no difference between fees incurred by normal traffic and attack traffic.
Therefore, Tencent Cloud provides Anti-DDoS Basic service free of charge for all users. However, once the attack traffic exceeds the free protection threshold, we will have to block the attacked IP from all public network access.

Why can't my IP be unblocked immediately?

A DDoS attack usually does not stop immediately after the target IP is blocked and the attack duration varies. Tencent Cloud security team sets the default blocking duration based on big data analysis.
Since IP blocking takes effect in ISP network, Tencent Cloud cannot monitor whether the attack traffic has stopped after the attacked public IP is blocked. If the IP is unblocked but the attack is still going on, the IP will be blocked again. During the gap between the IP being unblocked and blocked again, Tencent Cloud's basic network will be exposed to the attack traffic, which may affect other Tencent Cloud users. In addition, IP blocking is a service purchased from ISPs with restrictions on the total number of times and the frequency of unblocking.

How can I unblock my IP earlier in case of emergency?

- You can upgrade the base protection capacity, so that the blocked IP can be unblocked automatically.
- You have three chances each day to unblock the IP by yourself in case of emergency.

Why is there a limit on the number of chances for self-service unblocking? What are the restrictions?

Tencent Cloud pays ISPs for blocking attacked IPs, and ISPs impose limits on the number of times and frequency of unblocking.
Only **three** chances of self-service unblocking are provided for Anti-DDoS Advanced every day. The system resets the chance counter daily at midnight. Unused chances cannot be accumulated for the next day.

How can I prevent my IP from being blocked?

When purchasing an Anti-DDoS Advanced instance, select an appropriate protection bandwidth based on the historical attack traffic data to ensure that the protection bandwidth is higher than the peak attack traffic.

How can I prevent my IP from being blocked again?

You are recommended to increase the base protection bandwidth or elastic protection bandwidth to improve the protection capability. Enabling elastic protection can help you defend against high-traffic attacks. In addition, elastic protection is pay-as-you-go, which can reduce your security costs.

FAQ about Billing

Last updated：2019-05-07 10:27:12

Does the same billing model apply to the Anti-DDoS Advanced elastic defense services? How is it calculated?

Yes. You will be billed according to your daily elastic protection bandwidth range. See Billing Overview for more billing details.
For example, suppose you bought an Anti-DDoS Advanced instance with 20 Gbps base protection bandwidth and 50 Gbps elastic protection bandwidth. Suppose your instance experienced a DDoS attack on one day with 45-Gbps peak traffic flow, which exceeded the base protection bandwidth limit and therefore activated elastic protection. 45 Gbps falls within the 40 Gbps to 50 Gbps range and your elastic charge for that day will be based on the range.

Should I pay for the attack traffic even after my Anti-DDoS Advanced IP is blocked?

No. According to the billing model mentioned above, and because your IP is automatically blocked when the attack traffic exceeded the elastic protection bandwidth, you only need to pay for the difference between the base protection bandwidth limit and the elastic protection bandwidth limit. The amount of traffic that exceeds the elastic protection bandwidth limit will not be calculated.

I purchased the elastic defense service a month ago and has not experienced any attacks. Do I still have to pay?

No. In such cases, no additional elastic defense service fees will apply.

If I have purchased base protection bandwidth with a speed of 100 Gbps, can I reduce the bandwidth speed to 50 Gbps?

No. You can increase, but not decrease your base protection bandwidth.

Can I increase the elastic protection bandwidth when my application is being attacked?

Yes. You can increase and decrease elastic protection bandwidth on the Anti-DDoS Advanced Basic Info page. The available options vary by region. For details, please see Product Overview.

> If you have already been billed for attack traffic when you made the adjustment, you will be billed based on the new plan starting the next day.

If a protected IP suffers more than one attack during a day, will I be billed repeatedly for those attacks?

The Anti-DDoS Advanced service is billed based on the peak attacking traffic during the day and for once only.

If I have purchased two Anti-DDoS Advanced instances, and the base protection bandwidth limits of both Anti-DDoS Advanced instances are exceeded, how do I pay for the elastic protection?

You need to pay for the instances separately if both of them have exceeded their base protection bandwidth limits.

FAQ about Feature

Last updated：2020-08-21 14:05:51

Is Anti-DDoS Advanced available for non-Tencent Cloud users?

Yes. Anti-DDoS Advanced can protect all types of servers on the internet, including but not limited to those in Tencent Cloud, other clouds, and customer IDCs.

> ICP filing issued by MIIT is required for all domain names connected to Anti-DDoS Advanced in Mainland China.

Does Anti-DDoS Advanced support wildcard domain names?

Yes. You can protect wildcard domain names by configuring website traffic forwarding rules.
Wildcard domain name resolution involves using wildcards (*) as secondary domain names to allow all secondary domain names to point to the same IP. For example, you can configure *.tencent.com.

Does Anti-DDoS Advanced automatically add intermediate IPs to the security group?

No. You need to manually add the intermediate IP range to the CVM security group. If you have deployed firewall or other server security protection software on the real server, you also need to add the intermediate IP range to the allowlist to prevent business traffic from being affected due to blocking or speed limiting.

Can I set a private IP as the real server IP in Anti-DDoS Advanced?

No. Anti-DDoS Advanced forwards traffic over the public network. Therefore, you cannot use a private IP.

How long does it take for a real server IP update to take effect?

Changes to the real server IP protected by Anti-DDoS Advanced take effect in seconds.

How long does it take for configuration modifications in the Anti-DDoS Advanced Console to take effect?

Changes to the Anti-DDoS Advanced service configuration take effect in seconds.

Does Anti-DDoS Advanced support IPv6 protocol for traffic forwarding?

Currently, the IPv6 protocol is not supported.

Does Anti-DDoS Advanced support HTTPS mutual authentication?

- For website applications, HTTPS mutual authentication is not supported.

- For non-website applications over TCP, HTTPS mutual authentication is supported.

Does Anti-DDoS Advanced have packet capture files?

Anti-DDoS Advanced supports downloading packet capture files. For detailed directions, please see Viewing Statistics Report .

How does Anti-DDoS Advanced deal with load balancing if multiple real server IPs are configured?

- Load balancing based on source IP hash is used for website applications.
- For non-website applications, load balancing based on weighted round robin is used to forward traffic to real server IPs in turn.

How many forwarding ports and domain names are supported by one Anti-DDoS Advanced instance?

- Forwarding ports: 60 forwarding rules for TCP/UDP protocol are provided free of charge by default. The quantity can be increased.
- Domain names: 60 forwarding rules for HTTP/HTTPS protocol are provided free of charge by default. The quantity can be increased.

What is business bandwidth? What will happen if this value is exceeded?

The business bandwidth purchased is for the entire Anti-DDoS Advanced instance. It refers to the inbound and outbound traffic of all normal businesses in the instance.
If your business traffic exceeds the free tier, it will trigger traffic speed limit, which may result in random packet loss. If this problem persists, please upgrade the business bandwidth in time.

> 100 Mbps forwarding bandwidth is available free of charge for each Anti-DDoS Advanced instance.

Does Anti-DDoS Advanced support session persistence?

Anti-DDoS Advanced support session persistence, which is not enabled by default. For non-website businesses, you can configure this feature in the consoles as instructed in Configuring Session Persistence.

Does Anti-DDoS Advanced support health check?

Health check is enabled for non-website businesses, which is recommended. You can modify this feature as instructed in Configuring Health Check.

WS is not enabled on my real server. After I bind my business to Anti-DDoS Advanced, why is the access to the real server slow?

Anti-DDoS servers have Window Scaling (WS) enabled by default. If this is not enabled on the real server, a delay will occur when the sliding window is filled up while receiving slightly larger files. You are recommended to enable WS for your real server.