Anti-DDoS
Practical Tutorial

Copyright Notice

Trademark Notice

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Practical Tutorial How To File a Report With the Network Supervision Department After Being Attacked?

Last updated: 2025-03-19 21:57:31

When your business suffers from DDoS network attacks, it is recommended to adopt Anti-DDoS service to ensure the security and stability of your business. At the same time, it is advised to file a report with the network supervision department.

Filing a Report Process

1. After suffering an attack, file a report with the local cyber supervision department as soon as possible and provide relevant information according to the requirements of the cyber supervision department.
2. The cyber supervision department will judge whether it meets the filing standards and enter the cyber supervision processing procedure.
3. After the formal case filing, Tencent Cloud will cooperate with the contact person of the cyber supervision department to provide attack evidence collection.

> **Note:**
> Specific filing standards can be consulted with the local cyber supervision department.

What Relevant Evidence Can Tencent Cloud Provide?

After your report is filed with the network supervision department, Tencent Cloud will cooperate with the department to provide the following assistance:

- Tencent Cloud will cooperate with the network supervision department and provide the network supervision contact person with your business traffic logs and attack information on the Tencent Cloud platform.

  > **Note:**
  > Since the relevant data will be used as legal evidence, it cannot be provided directly to you. You can view the information related to attack traffic in the Tencent Cloud console by yourself.

- Tencent Cloud cannot analyze the traffic logs and attack information, etc., and directly conclude who the attacker is.

> **Note:**
> Since Tencent Cloud is not a judge and cannot determine who is guilty; nor is it a police officer with law enforcement powers who can conduct filing investigations; Tencent Cloud can only act as a provider of evidence and a witness.

- Tencent Cloud will respond in a timely manner to the network supervision department's request for assistance in the investigation and cooperate in the work.
- It is recommended that you refer to the local network supervision department's filing investigation standards when suffering from security attacks and actively request the public security network police to file an investigation.

Viewing Attack-Related Information

You can view traffic, attack events, Packet Capture Information, etc. in the Anti-DDoS (New Version) Console.

Remote Protection Scheme With Anti-DDoS Pro

Last updated: 2025-03-19 22:03:59

Requirement Background

Affected by objective factors, Anti-DDoS Pro only supports users in Beijing, Shanghai, and Guangzhou regions of Tencent Cloud and promises full protection capabilities. Full protection aims to successfully defend against every DDoS attack, integrating the current local cleaning center capabilities while dynamically adjusting according to the actual network status at that time to fully resist attacks. In addition, high-defense package products have not yet been launched in other regions of the Chinese mainland such as Chengdu and Chongqing. If a user's business origin server is deployed on Tencent Cloud and needs to use the Anti-DDoS Pro protection capability of non-origin server regions of Tencent Cloud, this solution can be referred to.

Protection Solution

This solution mainly consists of Anti-DDoS Pro, Cloud Load Balancer (CLB), and origin server business servers. Deploy CLB in regions with Anti-DDoS Pro resources and bind it with Anti-DDoS Pro. Configure the private network origin-pull rules of CLB to ensure that the business can be accessed through the public IP of CLB.

- Under regular circumstances, the business can resolve to the origin server's public IP address as needed (or directly resolve to the CLB public IP address in a different location), allowing business traffic to access the origin server nearby.
- After an attack occurs, resolve the business to the CLB IP address to clean the DDoS attack traffic. After cleaning is completed, CLB forwards the traffic back to the origin server through the private network dedicated line.

The specific protection solution is shown in the following figure:

Solution Effect

- Break the limitation of regional protection capabilities and have up to 300 Gbps of Anti-DDoS protection capabilities.
- Business traffic is forwarded using Tencent Cloud's private network dedicated line, which has high reliability and low delay.
- Fully enjoy the advantages of Tencent Cloud's Anti-DDoS network. All public IP addresses are BGP IPs with low delay.

Advice and Precautions

- Deploy Anti-DDoS Pro and CLB instances in advance.
- Establish a business availability monitoring mechanism. In the absence of an automatic switching mechanism, intervene in a timely manner when access exceptions to the origin server are detected.
- Conduct verification and drills regularly to understand and be familiar with the details of the solution and solve possible problems.

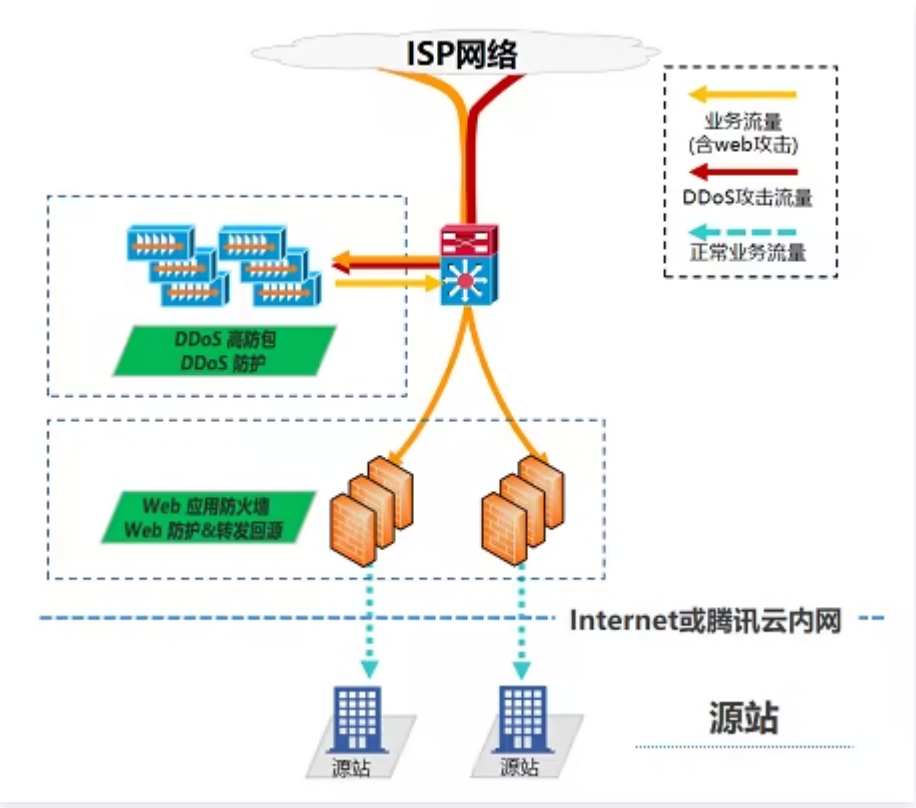
Using Anti-DDoS Pro Together With WAF

Last updated: 2025-03-19 22:04:10

Anti-DDoS Pro can be integrated with Web Application Firewall (WAF) to offer users comprehensive security protection.

- Providing DDoS protection capability of hundreds of Gbps at one click, Anti-DDoS Pro can easily defend against DDoS attacks and ensure the stable operation of your business.
- The WAF offers real-time protection, effectively intercepting web attack behaviors and ensuring the data and information security of user businesses.

Deployment Solution



Configuration Process

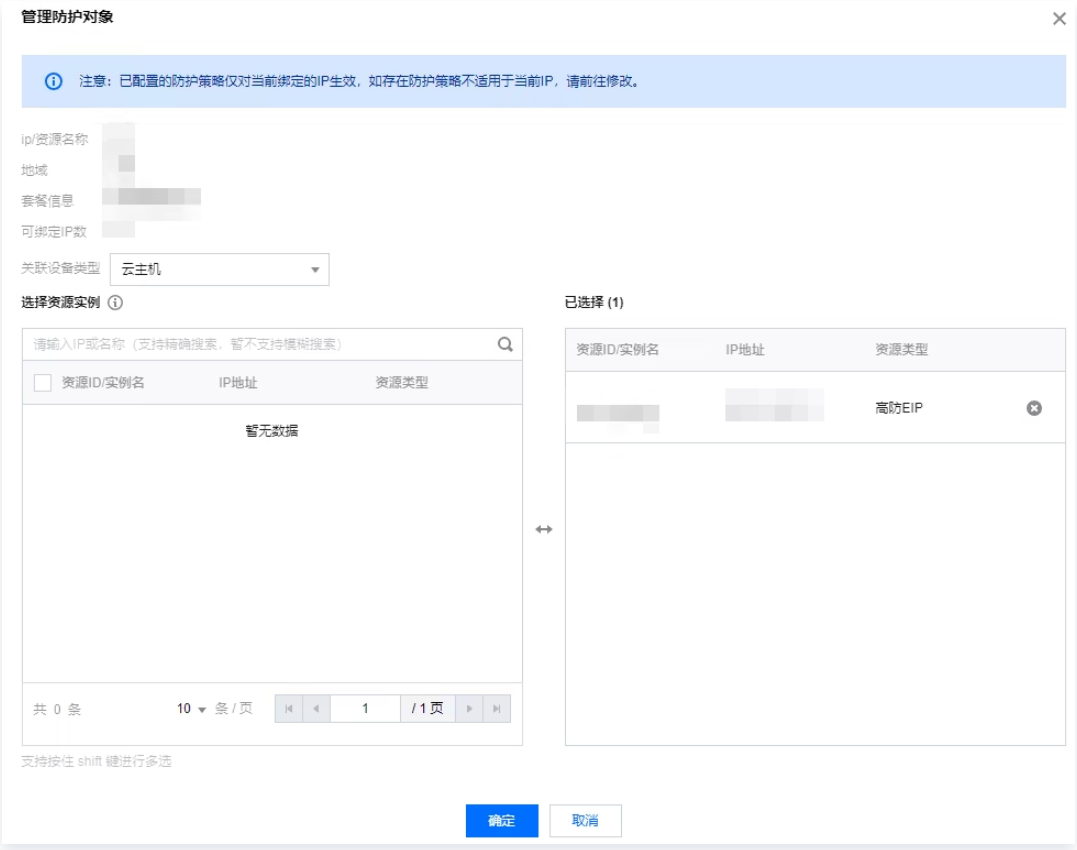
Configure Web Application Firewall

To quickly access the Web Application Firewall, please refer to Web Application Firewall Quick Start.

Configure Anti-DDoS Pro

1. Log in to the Anti-DDoS (New Version) Console, and click on **Anti-DDoS Instances** in the left sidebar.
2. On the Anti-DDoS Instances page, select the target instance, and click on **Manage Protection Object** in the operation column.

3. In the Manage Protection Object window, select "Associated Device Type" and "Resource Instance" according to actual protection needs.
   - Associated device types: Supports Cloud Host, Cloud Load Balancer (CLB), WAF, and other public cloud resources with public IP addresses.
   - Select resource instances: Multi-option selection is allowed, and the number of "selected resource instances" must not exceed the number of bindable IPs.



4. After making selections, click **Confirm**.

Stress Testing Advice For Business Systems

Last updated: 2025-03-19 22:05:47

The stress testing process is somewhat similar to a DDoS attack. To ensure the effectiveness of the stress test, it is advisable for users to refer to this document for applicable suggestions before conducting the stress test and then formulate a suitable implementation scheme.

> **Note:**
> The following suggestions are mainly based on the impact of Anti-DDoS on Stress Testing. Other aspects related to Stress Testing, such as network bandwidth, linkage loads, or other basic resource situations, should be considered and supplemented by users based on actual conditions.

Adjust Protection Policy

- It is recommended to disable CC protection policy. If there are some objective reasons that prevent disabling CC protection policy, please adjust the HTTP request count threshold for CC attack protection to above the maximum value of the stress test.
- It is recommended to disable Anti - DDoS protection policy. If there are some objective reasons that prevent disabling Anti - DDoS protection policy, please adjust the threshold clearing for Anti - DDoS protection to above the maximum value of the stress test.

Control Stress Testing Traffic and Request Count

- It is recommended to set the bandwidth of stress test to less than 1 Gbps, otherwise it may trigger attack protection.
- It is recommended to limit the HTTP request count in the stress test to within 20,000 QPS (that is, the HTTP request count does not exceed 20,000 per second), otherwise it may trigger attack protection.
- It is recommended that the number of new connections per second in the stress test be less than 50,000, the maximum connection count be less than 2,000,000, and the number of inbound packets per second be less than 200,000.

> **Note:**
> If the stress test needs to exceed the above limits, please contact Tencent Cloud technical support. The after-sales team will cooperate in conducting the stress test.

Assess Potential Impact Of Stress Testing In Advance

It is recommended that users contact Tencent Cloud architects or Tencent Cloud Technical Support before conducting stress testing to fully assess the potential impact and range of the stress test and develop reasonable risk avoidance measures.

Solution For Origin Server IP Exposure

Last updated: 2026-02-25 10:35:58

Since some attackers record the IPs used by the origin server, there is a possibility of bypassing the high protection and directly attacking the origin server IP after using the BGP high-protection package. If the above situation occurs, it is recommended to replace the origin server IP.
Before replacing the origin server IP, you can refer to this document to check for possible factors that expose the origin server IP to avoid continued exposure of the newly replaced origin server IP.

Check Method

DNS Resolution Record Check

Check all DNS parsing records on the old origin server IP that was attacked, such as subdomain parsing records, mail server MX (Mail Exchanger) records, and NS (Name Server) records, to ensure that all are configured to the high-protection IP, avoiding some parsing records directly resolving to the newly replaced origin server IP.

Information Leakage and Command Execution Vulnerability Check

- Check if there are vulnerabilities of information leakage in the website or business system, such as phpinfo() leakage, GitHub information leakage, etc.
- Check if there are command execution vulnerabilities in the website or business system.

Trojan or Backdoor Check

Check whether there are hidden risks such as Trojans or backdoors on the origin server.

Other Suggestions

- It is recommended not to use an IP of the same or similar IP range as the old origin server as the new origin server IP to avoid attackers guessing and scanning the C segment or similar IP ranges.
- It is recommended to prepare backup links and backup IPs in advance.
- It is recommended to set the origin range to avoid malicious scans by attackers.

Create and Use Guide For Anti-DDoS EIP

Last updated: 2026-03-11 18:07:41

> **Note:**
> Only standard account types support the creation of **high-protection EIP**. If you are unsure about your account type, please refer to Elastic IP - Account Type Explanation.

Step 1: Purchase Anti-DDoS Pro Package Of the Enterprise Edition

Log in to Tencent Cloud Official Website, go to Anti-DDoS Pro Purchase Page to make a purchase. For more information, see Purchase Guide.

Step 2: Create BGP Bandwidth Package

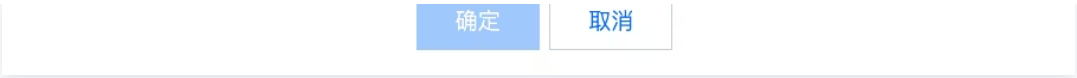
Refer to Create IP Bandwidth Package documentation to create a BGP bandwidth package.

> **Note:**
> If you have already created a Conventional BGP bandwidth package in the region you need to use, you can skip this step and go to Step Three.

Step 3: Create Anti-DDoS EIP

1. Log in to the Cloud Virtual Machine Console, and click on **Public Network IP** in the left sidebar.
2. On the Public Network IP page, select the region and click **Apply**.

3. In the Apply EIP window, configure the relevant parameters and click **Yes** to complete the EIP application.



Parameter	Description
IP Address Type	Select high-protection EIP
Billing mode	No need to select, high-protection EIP only supports Bandwidth Package billing mode
Shared bandwidth package	Select the regular BGP shared bandwidth package to join.
Bandwidth Cap	Set the bandwidth limit as needed and allocate bandwidth resources reasonably.
Anti-DDoS Pro package of the Enterprise Edition	Select the Anti-DDoS Pro package of the Enterprise Edition to bind.
Quantities	Select the number of applications as needed and ensure that the total number of EIPs does not exceed the total product quota. For details, see Quota Configuration - Usage Limitation.
Name	EIP instance name, not required.
Tag	If you need to add tags, you can do so here, and permission management can be done through tags.

Subsequent Operations

If you need to bind cloud resources to EIP, see Binding Elastic IP to Cloud Resources.

Smooth Switching Of Online Business To Anti-DDoS Advanced

Last updated: 2025-03-19 22:06:40

Requirement Background

The launched business may have many specific settings and restriction conditions, and the impact of business interruption is relatively large. Therefore, it is recommended that users refer to the relevant suggestions in this section and adopt appropriate switching methods to avoid possible risks before switching the launched business to this product.

Recommendation

> **Note:**
> The following advice is based on Tencent Cloud's past online business switch experiences. Users need to complete and supplement according to their actual business conditions to ensure that the risks during the switch process are minimized.

Technical Dimension

- Modify the hosts file locally instead of directly modifying the DNS A record. The testers perform business tests locally to verify availability and test latency and other related indicators.
- If the intelligent domain name resolution product has been used, the DNS A record can be modified based on some ISPs or regions. First, divert a small amount of traffic to the high-protection IP for grayscale launch and then gradually complete all business switches.
- Reduce the TTL of DNS so that it can switch back as soon as possible once an issue occurs.
- Prepare a rollback plan in advance and operate orderly according to the rollback plan once an issue occurs.

Business Dimension

- Select backup business, non-important business and non-critical business to migrate first.
- Migrate during periods with less business.

Obtain Client Real IP (Port Access)

Last updated: 2026-03-11 18:04:14

This article will introduce how to obtain the client IP through the TOA module, to replace the incorrect domain access method in the DDoS API documentation and the port access method that lacks installation commands for dependency packages of other release versions' compiling environments.

The TOA module is a high-performance, lightweight tcp connection information collection tool. It can obtain the real IP of the client at the application layer and forward it to the backend server. This article will introduce how to use the TOA module to obtain the client IP under both domain access and port access methods.

Domain Access Method

The following content is configured at the corresponding location of the Nginx reverse proxy to obtain the client IP information:

```
log_format real_ip '$http_x_forwarded_for - $remote_user [$time_local] '
    '"$request" $status $body_bytes_sent '
    '"$http_referer" "$http_user_agent"';

server {
    listen 80;
    server_name yourdomain.com;

    location / {
        proxy_pass http://backend_server;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        access_log /var/log/nginx/access.log real_ip;
    }
}
```

Among them, the `proxy_set_header` configuration item is used to set the HTTP request header and add the real IP of the client to the request header; the `access_log` configuration item is used to set the log format of Nginx, so as to record the real IP of the client in the log.

Port Access Method

The Backend Service Loads the TOA Module

You can load the TOA module in the following three ways:

- Method 1 (Recommended): If it is Tlinux, use modprobe to load the TOA module.
- Method 2: Depending on the Linux version of the origin server, download the corresponding compiled toa.ko file and load it directly.
- Method 3: If you cannot find your current origin server Linux version in Method 1, you can compile and load it yourself by downloading the TOA source file.

Method 1: Load the TOA Module Using Modprobe

The following figure shows that loading the TOA module with modprobe failed. You can refer to processing method to repair it.

```
[root@VM-32-81-tencentos ~]# lsmod | greo -i toa
[root@VM-32-81-tencentos ~]#
```

Handling Method

1. Check the kernel configuration file to see if TOA is supported. It can be seen that TOA is compiled in the form of a module.

```
[root@VM-32-81-tencentos ~]# zcat /proc/config.gz | grep -i toa
CONFIG_TOA=m
[root@VM-32-81-tencentos ~]#
```

2. Load the module through modprobe toa.
3. Check again whether TOA is supported. As shown in the figure below, it represents that it has been supported.

```
[root@VM-32-81-tencentos ~]# modprobe toa
[root@VM-32-81-tencentos ~]# lsmod | grep -i toa
toa                    20480  0
[root@VM-32-81-tencentos ~]#
```

Method 2: Download the Compiled TOA Module and Load It

1. According to the version of Linux on Tencent Cloud, download the corresponding TOA package and decompress it.

- centos
  - CentOS-7.2-x86_64.tar.gz
  - CentOS-7.3-x86_64.tar.gz
  - CentOS-7.4-x86_64.tar.gz
  - CentOS-7.5-x86_64.tar.gz
  - CentOS-7.6-x86_64.tar.gz
  - CentOS-7.7-x86_64.tar.gz
  - CentOS-7.8-x86_64.tar.gz
  - CentOS-7.9-x86_64.tar.gz
  - CentOS-8.0-x86_64.tar.gz
  - CentOS-8.2-x86_64.tar.gz
- debian
  - Debian-11.1-x86_64.tar.gz
  - Debian-10.2-x86_64.tar.gz
  - Debian-9.0-x86_64.tar.gz
- suse linux
  - openSUSE-Leap-15.3-x86_64.tar.gz
- ubuntu
  - Ubuntu-14.04.1-LTS-x86_64.tar.gz
  - Ubuntu-16.04.1-LTS-x86_64.tar.gz
  - Ubuntu-18.04.1-LTS-x86_64.tar.gz
  - Ubuntu-20.04.1-LTS-x86_64.tar.gz

2. After the decompression is completed, execute the cd command to enter the just decompressed folder, and then select any method to load the TOA module.
   - One-click execution of script

```
/bin/bash -c "$(curl -fsSL https://edgeone-document-file-1258344699.cos.ap-guangzhou.myqcloud.com/TOA/install_toa.sh)"
```

   The following will be displayed after loading successfully:

```
[root@VM-0-14-centos toa]# /bin/bash -c "$(curl -fsSL https://eo-toa-1258348367.cos.ap-shanghai.myqcloud.com/install_toa.sh)"
toa.ko install successfully
[root@VM-0-14-centos toa]#
```

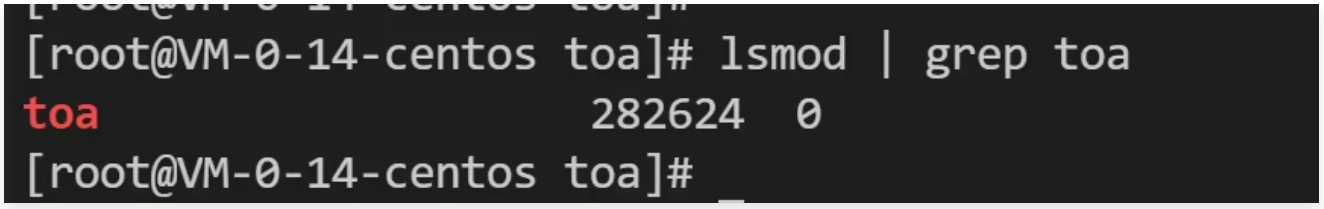
   - Manual configuration loading

```
# Decompress the tar package
tar -zxvf CentOS-7.2-x86_64.tar.gz
# Enter the package directory after decompression
cd CentOS-7.2-x86_64
# Load the toa module
insmod toa.ko
# Copy to the kernel module directory
cp toa.ko /lib/modules/uname -r/kernel/net/netfilter/ipvs/toa.ko
# Set automatic loading of the toa module on system boot
echo "insmod /lib/modules/uname -
r/kernel/net/netfilter/ipvs/toa.ko" >> /etc/rc.local
```

You can confirm whether it has been loaded successfully through the following command:

```
lsmod | grep toa
```

When TOA appears, it means that it has been loaded successfully, as shown in the following figure:



Method 3: Compile and Load the TOA Module By Yourself

1. Install the compiling environment.
   - Check the current kernel version number, confirm that kernel-devel and kernel-headers are installed, and ensure that the version numbers are consistent with the kernel version.
   - Confirm that GCC and Make are installed.
   - If the above environment dependencies are not installed, refer to the following commands for installation:
     - centos

```
yum install -y gcc
yum install -y make
```

```
yum install -y kernel-headers kernel-devel
```

- Ubuntu/Debian

```
apt-get install -y gcc
apt-get install -y make
apt-get install -y linux-headers-$(uname -r)
```

2. After installing the compiling environment, you can choose any method to execute commands to complete the download, compilation and loading of the source code.
   - One-click script compilation and loading

```
/bin/bash -c "$(curl -fsSL https://edgeone-document-file-
1258344699.cos.ap-
guangzhou.myqcloud.com/TOA/compile_install_toa.sh)"
```

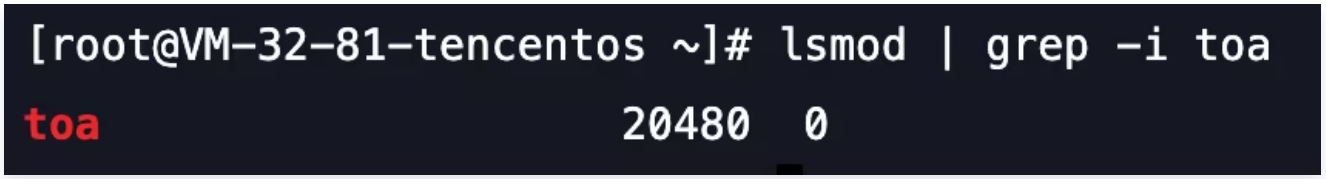
   - Manual compilation and loading

```
# Create and enter the compilation directory
mkdir toa_compile && cd toa_compile
# Download the source code tar package
curl -o toa.tar.gz https://edgeone-document-file-
1258344699.cos.ap-guangzhou.myqcloud.com/TOA/toa.tar.gz
# Decompress the tar package
tar -zxvf toa.tar.gz
# Compile the toa.ko file; after successful compilation, the
toa.ko file will be generated in the current directory
make
# Load the toa module
insmod toa.ko
# Copy to the kernel module directory
cp toa.ko /lib/modules/`uname -r`/kernel/net/netfilter/ipvs/toa.ko
# Set automatic loading of the toa module on system boot
echo "insmod /lib/modules/`uname -
r`/kernel/net/netfilter/ipvs/toa.ko" >> /etc/rc.local
```

3. Execute the following instructions to confirm whether it has been loaded successfully:

```
lsmod | grep toa
```

When toa appears, it means that it has been loaded successfully, as shown in the following figure:



Verification To Obtain Client IP Information

If your current business is one of the following two scenarios and you only need to obtain one type of client address, either IPv4 or IPv6, you can follow the steps below to load the TOA module on the server side to obtain the real IP address of the client.

- The origin server is IPv4, only the IPv4 client address needs to be obtained.
- The origin server is IPv6, only the IPv6 client address needs to be obtained.

You can build a TCP service and simulate client requests with another server for verification.

1. On the current server, you can create an HTTP service through Python to simulate a TCP service, as shown below:

```
# Based on Python 2
python2 -m SimpleHTTPServer 10000

# Based on Python 3
python3 -m http.server 10000
```

2. Use another server as the client, construct the client request, and simulate the TCP request with a Curl request:

```
# Use curl to initiate an HTTP request, where the domain name is the
L4 proxy domain name, and 10000 is the L4 proxy forwarding port
curl -i "http://a8b7f59fc8d7e6c9.example.com.edgeonedy1.com:10000/"
```

Sample Code In C Language

Modify the Origin Server Business Code and Obtain the Real IP Of IPv4/IPv6 Clients At the Same Time

If you need to obtain both IPv4 and IPv6 client addresses at the same time, you need to modify the origin server business code while loading the TOA module.
When the origin server establishes service listening, it can refer to the following two methods:

- Use the IPv4 address structure `struct sockaddr_in` to build the service, which listens to the IPv4 format address.

```
#include <sys/socket.h>
#include <stdio.h>
#include <unistd.h>
#include <netinet/in.h>
#include <memory.h>
#include <arpa/inet.h>


int main(int argc,  char **argv){
    int    l_sockfd;
    // The server address uses the IPv4 structure
    struct sockaddr_in serveraddr;
    // Business modification point: The client address must use the
IPv6 structure
    struct sockaddr_in6 clientAddr;
    int server_port = 10000;


    memset(&serveraddr, 0, sizeof(serveraddr));
    // Create a socket
    l_sockfd = socket(AF_INET, SOCK_STREAM, 0);
    if (l_sockfd == -1){
        printf("Failed to create socket.\n");
        return -1;
    }

    // Initialize server address information
    memset(&serveraddr, 0, sizeof(struct sockaddr_in));
    serveraddr.sin_family = AF_INET;
    serveraddr.sin_port = htons(server_port);
    serveraddr.sin_addr.s_addr = htonl(INADDR_ANY);


    int isReuse = 1;
```

```
    setsockopt(l_sockfd, SOL_SOCKET,SO_REUSEADDR,(const
char*)&isReuse,sizeof(isReuse));

    // Associate socket with server address information
    int nRet = bind(l_sockfd,(struct sockaddr*)&serveraddr,
sizeof(serveraddr));
    if(-1 == nRet)
    {
        printf("bind error\n");
        return -1;
    }
    // Listen on the socket
    listen(l_sockfd, 5);


    int clientAddrLen = sizeof(clientAddr);
    memset(&clientAddr, 0, sizeof(clientAddr));
    // Accept connections from clients
    int linkFd = accept(l_sockfd, (struct sockaddr*)&clientAddr,
&clientAddrLen);
    if(-1 == linkFd)
    {
        printf("accept error\n");
        return -1;
    }
    // Business modification point: Determine whether the client is
IPv4 or IPv6 based on the type of client sin6_family
    //    When it is AF_INET, it means the client is IPv4, convert the
client address pointer to struct sockaddr_in* for retrieval
    // When it is AF_INET6, it means the client is IPv6, use struct
sockaddr_in6* to obtain
    if (clientAddr.sin6_family == AF_INET) {
        printf("AF_INET accept getpeername %s : %d successful\n",
               inet_ntoa(((struct sockaddr_in*)&clientAddr)-
>sin_addr),
               ntohs(((struct sockaddr_in*)&clientAddr)->sin_port));
    }else if (clientAddr.sin6_family == AF_INET6){
        char addr_p[128] = {0};
        inet_ntop(AF_INET6, (void *)&((struct
sockaddr_in6*)&clientAddr)->sin6_addr, addr_p, (socklen_t
```

```
)sizeof(addr_p));
        printf("AF_INET6 accept getpeername %s : %d successful\n",
                addr_p,
                ntohs(((struct sockaddr_in6*)&clientAddr)-
>sin6_port));
    }else{
        printf("unknow sin_family:%d \n", clientAddr.sin6_family);
    }
    close(l_sockfd);
    return 0;
}
```

- Use the IPv6 address structure `struct sockaddr_in6` to build the service, which listens to the IPv6 format address.

```
#include <sys/socket.h>
#include <stdio.h>
#include <unistd.h>
#include <netinet/in.h>
#include <memory.h>
#include <arpa/inet.h>


int main(int argc,  char **argv)
{
    int    l_sockfd;
    // The server address uses the IPv6 structure
    struct sockaddr_in6 serveraddr;
    // The client address uses the IPv6 structure
    struct sockaddr_in6 clientAddr;
    int server_port = 10000;


    memset(&serveraddr, 0, sizeof(serveraddr));

    // Create a socket
    l_sockfd = socket(AF_INET6, SOCK_STREAM, 0);
    if (l_sockfd == -1){
```

```
        printf("Failed to create socket.\n");
        return -1;
    }
    // Set the server address information
    memset(&serveraddr, 0, sizeof(struct sockaddr_in6));
    serveraddr.sin6_family = AF_INET6;
    serveraddr.sin6_port = htons(server_port);
    serveraddr.sin6_addr = in6addr_any;


    int isReuse = 1;
    setsockopt(l_sockfd, SOL_SOCKET,SO_REUSEADDR,(const
char*)&isReuse,sizeof(isReuse));
    // Associate socket with server address information
    int nRet = bind(l_sockfd,(struct sockaddr*)&serveraddr,
sizeof(serveraddr));
    if(-1 == nRet)
    {
        printf("bind error\n");
        return -1;
    }
    // Listen on the socket
    listen(l_sockfd, 5);


    int clientAddrLen = sizeof(clientAddr);
    memset(&clientAddr, 0, sizeof(clientAddr));

    // Accept connection requests from clients
    int linkFd = accept(l_sockfd, (struct sockaddr*)&clientAddr,
&clientAddrLen);
    if(-1 == linkFd)
    {
        printf("accept error\n");
        return -1;
    }

    // The client address information received here is all stored in
the IPv6 structure.
```

```
    // Among them, the client's IPv4 address is also mapped to an IPv6
address, for example: ::ffff:119.29.1.1
    char addr_p[128] = {0};
    inet_ntop(AF_INET6, (void *)&clientAddr.sin6_addr, addr_p,
(socklen_t )sizeof(addr_p));
    printf("accept %s : %d successful\n", addr_p,
ntohs(clientAddr.sin6_port));

    // Modifications to make: Use the system macro definition
IN6_IS_ADDR_V4MAPPED to determine whether an IPv6 address is a mapped
IPv4 address (indicating the client is IPv4).
    if(IN6_IS_ADDR_V4MAPPED(&clientAddr.sin6_addr)) {
        struct sockaddr_in real_v4_sin;
        memset (&real_v4_sin, 0, sizeof (struct sockaddr_in));
        real_v4_sin.sin_family = AF_INET;
        real_v4_sin.sin_port = clientAddr.sin6_port;
        // Reading the last four bytes gives the client's true IPv4
address.
        memcpy (&real_v4_sin.sin_addr, ((char *)&clientAddr.sin6_addr)
+ 12, 4);
        printf("connect %s successful\n",
inet_ntoa(real_v4_sin.sin_addr));
    }

    close(l_sockfd);
    return 0;
}
```

Java Code Example

When the origin server establishes service listening, it can refer to the following two methods:

1. Build the service using the IPv4 address structure; addresses in both IPv4 and IPv6 formats can be monitored.
2. Build the service using the IPv6 address structure; addresses in both IPv4 and IPv6 formats can be monitored.

Build a Service Using the IPv4 Address Structure

It should be noted that: The sample code uses the IPv4 address structure to build the service. If you need to use the IPv6 address structure to build the service, you need to change `serverS`

`ocket.bind(new InetSocketAddress(InetAddress.getByName(IPV4_HOST), serverPort));` to `serverSocket.bind(new InetSocketAddress(InetAddress.getByName(IPV6_HOST), serverPort));`

```
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.net.InetAddress;
import java.net.InetSocketAddress;
import java.net.ServerSocket;
import java.net.Socket;
import java.net.SocketAddress;

public class ServerDemo {

    /** If you use the IPv4 address structure to build a service, use
IPV4_HOST */
    public static final String IPV4_HOST = "0.0.0.0";

    /** If you use the IPv6 address structure to build a service, use
IPV6_HOST */
    public static final String IPV6_HOST = "::";

    public static void main(String[] args) {
        int serverPort = 10000;
        try (ServerSocket serverSocket = new ServerSocket()) {
            // Enable address reuse
            serverSocket.setReuseAddress(true);
            // Bind server address and port, using IPv4 here
            serverSocket.bind(new
InetSocketAddress(InetAddress.getByName(IPV4_HOST), serverPort));
            System.out.println("Server is listening on port " +
serverPort);

            while (true) {
                // Accept client connections
                Socket clientSocket = serverSocket.accept();
                System.out.println("New client connected: " +
clientSocket.getRemoteSocketAddress());
```

```
                // Handle client requests
                handleClientRequest(clientSocket);
            }
        } catch (IOException e) {
            System.err.println("Failed to create server socket: " +
e.getMessage());
        }
    }

    /**
     * Processing function, specific implementation for specific
business, here is just an example
     * The function of this function is to return the client's input to
the client unchanged
     */
    private static void handleClientRequest(Socket clientSocket) {
        try (InputStream inputStream = clientSocket.getInputStream();
             OutputStream outputStream = clientSocket.getOutputStream())
{

            // Read the data sent by the client
            byte[] buffer = new byte[1024];
            int bytesRead;
            while ((bytesRead = inputStream.read(buffer)) != -1) {
                // Reply to the client with the received data as is
                outputStream.write(buffer, 0, bytesRead);
            }

        } catch (IOException e) {
            // When the client disconnects
            System.err.println("Failed to handle client request: " +
e.getMessage());
        } finally {
            try {
                clientSocket.close();
            } catch (IOException e) {
                System.err.println("Failed to close client socket: " +
e.getMessage());
            }
        }
```

```
    }
}
```

Build a Service Using the IPv6 Address Structure

```
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.net.InetAddress;
import java.net.InetSocketAddress;
import java.net.ServerSocket;
import java.net.Socket;
import java.net.SocketAddress;

public class ServerDemo {

    /** If you use the IPv4 address structure to build a service, use
IPV4_HOST */
    public static final String IPV4_HOST = "0.0.0.0";

    /** If you use the IPv6 address structure to build a service, use
IPV6_HOST */
    public static final String IPV6_HOST = "::";

    public static void main(String[] args) {
        int serverPort = 10000;
        try (ServerSocket serverSocket = new ServerSocket()) {
            // Enable address reuse
            serverSocket.setReuseAddress(true);
            // Bind server address and port, using IPv4 here
            serverSocket.bind(new
InetSocketAddress(InetAddress.getByName(IPV6_HOST), serverPort));
            System.out.println("Server is listening on port " +
serverPort);

            while (true) {
                // Accept client connections
                Socket clientSocket = serverSocket.accept();
```

```
                System.out.println("New client connected: " +
clientSocket.getRemoteSocketAddress());

                // Handle client requests
                handleClientRequest(clientSocket);
            }
        } catch (IOException e) {
            System.err.println("Failed to create server socket: " +
e.getMessage());
        }
    }

    /**
     Processing function, specific business implementation, here is just
an example
     * The function of this function is to return the client's input to
the client unchanged
     */
    private static void handleClientRequest(Socket clientSocket) {
        try (InputStream inputStream = clientSocket.getInputStream();
             OutputStream outputStream = clientSocket.getOutputStream())
{

            // Read the data sent by the client
            byte[] buffer = new byte[1024];
            int bytesRead;
            while ((bytesRead = inputStream.read(buffer)) != -1) {
                // Reply to the client with the received data as is
                outputStream.write(buffer, 0, bytesRead);
            }

        } catch (IOException e) {
            // When the client disconnects
            System.err.println("Failed to handle client request: " +
e.getMessage());
        } finally {
            try {
                clientSocket.close();
            } catch (IOException e) {
```

```
                System.err.println("Failed to close client socket: " +
e.getMessage());
            }
        }
    }
}
```

Output Results At the Console

```
Server is listening on port 10000
New client connected: /127.0.0.1:50680
New client connected: /0:0:0:0:0:0:0:1:51124
New client connected: /127.0.0.1:51136
```

More References

Monitor the Running State Of TOA

To ensure the stability of the TOA kernel module operation, the TOA kernel module also provides a monitoring feature. After inserting the toa.ko kernel module, you can monitor the working status of the TOA module by executing the following commands.

```
cat /proc/net/toa_stats
```

The running status of TOA is as follows:

```
[root@VM-32-81-tencentos ~]# cat /proc/net/toa_stats
                                CPU0       CPU1
syn_recv_sock_toa          :       0          0
syn_recv_sock_no_toa       :    1804       1815
getname_toa_ok             :       0          0
getname_toa_mismatch       :       0          0
getname_toa_bypass         :       0          0
getname_toa_empty          :   22810      22671
vtoa_get                   :       0          0
vtoa_attr_err              :       0          0
vtoa_lookup_err            :       0          0
vtoa_netlink_err           :       0          0
getname_vtoa_ipv4_err      :       0          0
getname_vtoa_ipv6_err      :       0          0
```

The meanings of the main monitoring metrics are shown below:

Metric Name	Description
syn_recv_sock_toa	The number of connections receiving TOA information.
syn_recv_sock_no_toa	The number of connections received without TOA information.
getname_toa_ok	This count increases when getsockopt is called to successfully obtain the source IP, and also when the accept function is called to receive a client request.
getname_toa_mismatch	When getsockopt is called to obtain the source IP, this count increases if the type does not match. For example, if a client connection stores an IPv4 source IP instead of an IPv6 address, this count will increase.
getname_toa_empty	This count increases when the `getsockopt` function is called on a client file descriptor that does not contain TOA.
ip6_address_alloc	When the TOA kernel module obtains the source IP and source Port stored in the TCP data packet, it will allocate space to save the information.
ip6_address_free	When a connection is released, the TOA kernel module releases the memory previously used to store the source IP and source port. When all connections are closed, the sum of this count across all CPUs should equal the count of ip6_address_alloc.

Obtain the Actual Client IP (Domain Name Integration)

Last updated: 2025-03-20 09:44:21

This document will introduce how to obtain the real IP directly through Anti - DDoS, and for Tomcat, Apache, Nginx and IIS servers, introduce corresponding X - Forwarded - For configuration schemes and methods to obtain the real IP.

Background

Usually, when a user accesses a website, the browser may not go directly to the server, and protection services such as CDN and Anti - DDoS are deployed in the middle. For example, the architecture is: "User > CDN/Anti - DDoS > origin server".

If you have used the Anti - DDoS service, you can directly obtain the real IP of the visitor through the Anti - DDoS service, and you can also obtain the real IP of the visitor by configuring the website server. When the Anti - DDoS IP uses the website business forwarding rules, the real IP of the client can be obtained by using the X - Forwarded - For field in the http header.

X - Forwarded - For: It is an extended field of the http header. The purpose is to enable the server to identify the real IP of the client connected through proxy and other means.
The format is: X - Forwarded - For: Client, proxy1, proxy2, proxy3...

When the high - protection IP forwards the user's access request to the real server, it will record the real IP of the requesting user at the beginning of the X - Forwarded - For field. Therefore, the origin server application only needs to obtain the content of the X - Forwarded - For field in the http header.

Obtain the Real IP Through HTTP Header

The Anti - DDoS service provides the feature of obtaining the real IP of the client by default. Below are two recommended ways to obtain the source IP of the client. You can choose either of them according to your needs:

Method 1

The Anti - DDoS service obtains the real IP address of the client by using X - Forwarded - For.

- The real Client IP will be placed in the X-Forwarded-For field of the HTTP header by the advanced anti-DDoS service, with the following format:

```
X-Forwarded-For: real client IP, proxy server 1-IP, proxy server 2-IP,
...
```

> **Note:**
> When using this method to obtain the client's real IP, the first address obtained is the client's real IP.

- The method for obtaining the X-Forwarded-For field by calling the SDK API in various languages is as follows:
  - ASP:

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

  - ASP.NET (C#):

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

  - PHP:

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

  - JSP:

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

Method 2

The Anti - DDoS service supports using the X - Real - IP variable to obtain the source IP of the client (during use, the modification of this variable by multiple reverse proxies passed later is considered).
The ways for various languages to obtain the X - Real - IP field by calling the SDK API are as follows:

- ASP:

```
Request.ServerVariables("HTTP_X_REAL_IP")
```

- ASP.NET (C#):

```
Request.ServerVariables["HTTP_X_REAL_IP"]
```

- PHP:

```
$_SERVER["HTTP_X_REAL_IP"]
```

- JSP:

```
request.getHeader("HTTP_X_REAL_IP")
```

Print the Real IP In Access Logs

How Tomcat Obtains the Real Client'S Ip Address In Access Logs

If your origin server is deployed with a Tomcat server, you can obtain the real IP address of the visitor by enabling the X - Forwarded - For function of Tomcat.

1. Open the server.xml file ("tomcat/conf/server.xml"), and the content of the AccessLogValve logging feature is as follows:

```
<Host name="localhost"  appBase="webapps" unpackWARs="true"
autoDeploy="true">
    <Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
           prefix="localhost_access_log." suffix=".txt"
            pattern="%h %l %u %t "%r" %s %b" />
```

2. Add "%{X-Forwarded-IP}i" to the pattern, and the modified server.xml is:

```
<Host name="localhost"  appBase="webapps" unpackWARs="true"
autoDeploy="true">
     <Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
            prefix="localhost_access_log." suffix=".txt"
            pattern="%{X-Forwarded-For}i %h %l %u %t "%r" %s %b" />
</Host>
```

3. View the localhost_access_log log file to obtain the real IP address of the visitor corresponding to X-Forwarded-For.

How Apache Obtains the Real Client'S Ip Address In Access Logs

If your origin server is deployed with an Apache server, you can obtain the client IP address by running a command to install the third - party module mod_remoteip of Apache and modifying the http.conf file.

1. Open the httpd.conf configuration file and modify the file content as follows:
   Apache maps xff to remote_addr. For details, see Installing mod_remoteip.
2. Define the log format.

```
LogFormat "%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\"
\"%{User-Agent}i\"" common
```

3. Restart Apache to make the configuration take effect.

```
Restart Apache by executing /[apache_directory]/httpd/bin/apachectl
restart
```

4. View the access.log log file to obtain the real IP address of the visitor corresponding to X-Forwarded-For.

How Nginx Obtains the Real Client'S Ip Address In Access Logs

If your origin server is deployed with an Nginx reverse proxy, you can configure the Location information in the Nginx reverse proxy so that the backend web server can obtain the real IP address of the client through a similar function.

1. According to the configuration of the origin server Nginx reverse proxy, configure the following content in the corresponding location of the Nginx reverse proxy to obtain the customer IP information.

```
log_format main '$remote_addr [$http_x_forwarded_for]- $remote_user
[$time_local] '
                '"$request" $status $body_bytes_sent '
                '"$http_referer" "$http_user_agent"';
```

2. Restart nginx.

Map the Client'S Real IP Through a Plug-In

Tomcat Configuration Scheme

Configure Tomcat to map xff to remote_addr. For details, see Tomcat Configuration Documentation.
The configuration example is as follows:

```
<Valve className="org.apache.catalina.valves.RemoteIpValve"
 remoteIpHeader="x-forwarded-for"
 proxiesHeader="x-forwarded-by"
 internalProxies="192\.168\.0\.10|192\.168\.0\.11"
 trustedProxies="62\.234\.227\.\d{1,3}|212\.64\.62\.\d{1,3}"
 />
```

Apache Configuration Solution

Map xff to remote_addr in Apache. You need to install mod_remoteip to operate.
The configuration example is as follows:

```
RemoteIPHeader X-Forwarded-For
RemoteIPTrustedProxyList x.x.x.x/24
```

IIS 6 Configuration Scheme

If your origin server is deployed with an IIS 6 server, you can obtain the real IP address of the visitor from the access log recorded by the IIS 6 server by installing the F5XForwardedFor.dll plug - in.

1. Download and install F5XForwardedFor module.
2. Copy the F5XForwardedFor.dll file from the x86\Release or x64\Release directory to a specified directory (such as C:\ISAPIFilters) based on your server's operating system version, and ensure that the IIS process has read access to that directory.
3. Open IIS Manager, find the currently open website, right-click on it and select **Attribute** to open the "Attribute" page.
4. On the "Attribute" page, switch to ISAPI Filter, click **Add**, and configure the following information in the pop-up window:
   - **Filter Name**: F5XForwardedFor.
   - **Executable File**: The full path of F5XForwardedFor.dll, for example: C:\ISAPIFilters\F5XForwardedFor.dll.
5. Click **Yes** and restart the IIS 6 server.
6. View the access log recorded by the IIS 6 server (the default log path is: C:\WINDOWS\system32\LogFiles\, and the file name of IIS logs ends with .log) to obtain the real IP address of the visitor corresponding to X-Forwarded-For.

IIS 7 Configuration Scheme

If your origin server is deployed with an IIS 7 server, you can obtain the real IP address of the visitor from the access log recorded by the IIS 7 server by installing the F5XForwardedFor module.

1. Download and install F5XForwardedFor module.
2. Copy the F5XFFHttpModule.dll and F5XFFHttpModule.ini files from the x86\Release (or x64\Release) directory to a specified directory (such as C:\x_forwarded_for\x86 or C:\x_forwarded_for\x64) based on your server's operating system version, and ensure that the IIS process has read access to that directory.
3. In the selection of IIS server, double-click **Module** to enter the "Module" interface.
4. Click **Configure Native Module**, in the pop-up dialog box, click **Register**, and select the operating system to register the downloaded DLL file.
   - x86 OS: Registration module x_forwarded_for_x86
     - Name: x_forwarded_for_x86
     - Path: C:\x_forwarded_for\x86\F5XFFHttpModule.dll
   - x64 OS: Registration module x_forwarded_for_x64
     - Name: x_forwarded_for_x64
     - Path: C:\x_forwarded_for\x64\F5XFFHttpModule.dll
5. After registration, check the newly registered module (x_forwarded_for_x86 or x_forwarded_for_x64) and click **Yes**.
6. In ISAPI and CGI restrictions, add the registered DLL file according to the operating system, and change its "Restriction" to "Allow".
   - x86 Operating System:
     - ISAPI or CGI Path: C:\x_forwarded_for\x86\F5XFFHttpModule.dll
     - Description: x86
   - x64 Operating System:
     - ISAPI or CGI Path: "C:\x_forwarded_for\x64\F5XFFHttpModule.dll"
     - Description: x64
7. Restart the IIS 7 server and wait for the configuration to take effect.
8. View the access log recorded by the IIS 7 server (the default log path is: C:\WINDOWS\system32\LogFiles\, and the file name of IIS logs ends with .log) to obtain the real IP address of the visitor corresponding to X-Forwarded-For.

Protection Scheduling Solution Combined With the Origin Server

Last updated: 2025-03-20 09:44:33

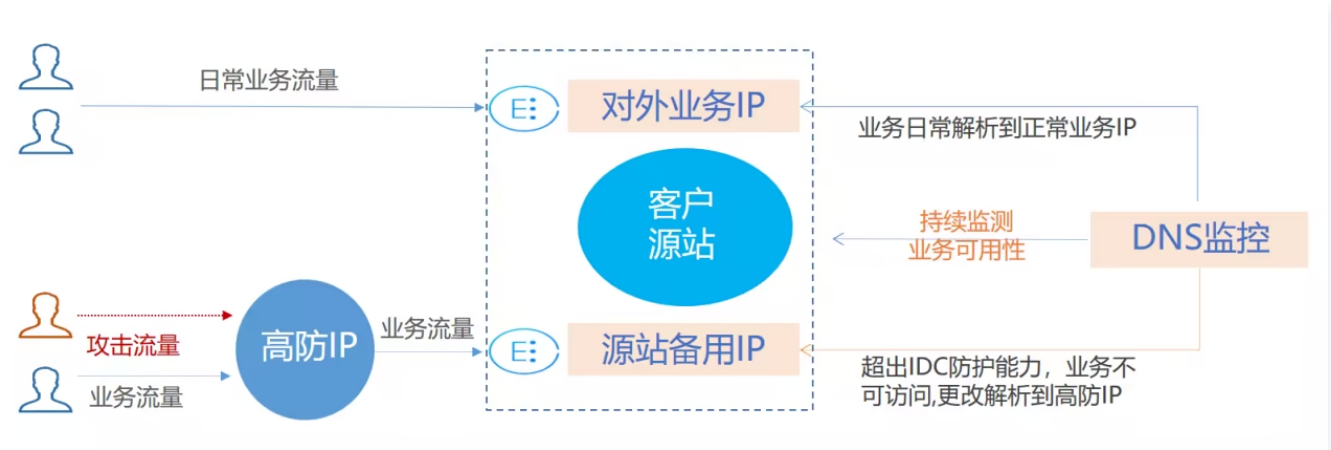
Requirement Background

Some users' businesses have strict requirements for delay, or are limited by business requirements to directly access the origin server under normal circumstances. In this case, you can consider combining the protection scheduling solution of the origin server.
This solution can meet the requirement of directly accessing the origin server under normal traffic conditions, but can quickly have protection capabilities after being attacked.

Protection Solution

The protection scheduling solution combined with the origin server is shown in the following figure:

> **Note:**
> This solution relies on DNS service provider and requires monitoring and smart switch features.



Solution Description

This solution mainly consists of a high-protection IP, DNS monitoring, the customer's origin server's external business IP, and the origin server's backup IP.

- Under regular circumstances, the business domain is resolved to the normal external business IP, and the business traffic directly accesses the origin server. DNS monitoring monitors in real-time whether the origin server's business can be accessed normally.

- When DNS monitoring detects that the normal external business IP cannot be accessed, according to the settings of the smart switch, it quickly resolves the business domain to the high-protection IP. The high-protection IP cleans the attack traffic and forwards the clean business traffic to the secondary IP of the origin server, thereby ensuring business availability.

> ⚠ **Note:**
> To avoid false switching caused by factors such as network jitter and ensure the monitoring effect, manual switching is recommended.

Solution Effect

- Meet the needs of directly accessing the origin server under regular circumstances.
- Suitable for businesses with very strict requirements for delay.
- After being attacked beyond the protection capacity of the origin server, it can automatically switch to the high-protection IP for protection.

Advice and Precautions

- It is necessary to complete the configuration of the origin server's secondary IP and high-protection IP forwarding rules in advance.
- It is recommended to distribute the origin server's secondary IP and normal business IP across different physical lines to achieve better protection effectiveness.
- It is recommended to regularly perform verification and drills, familiarize with the details of the solution, and address any potential issues.

CC Protection Policy Configuration Process and Precautions

Last updated: 2026-03-11 17:58:03

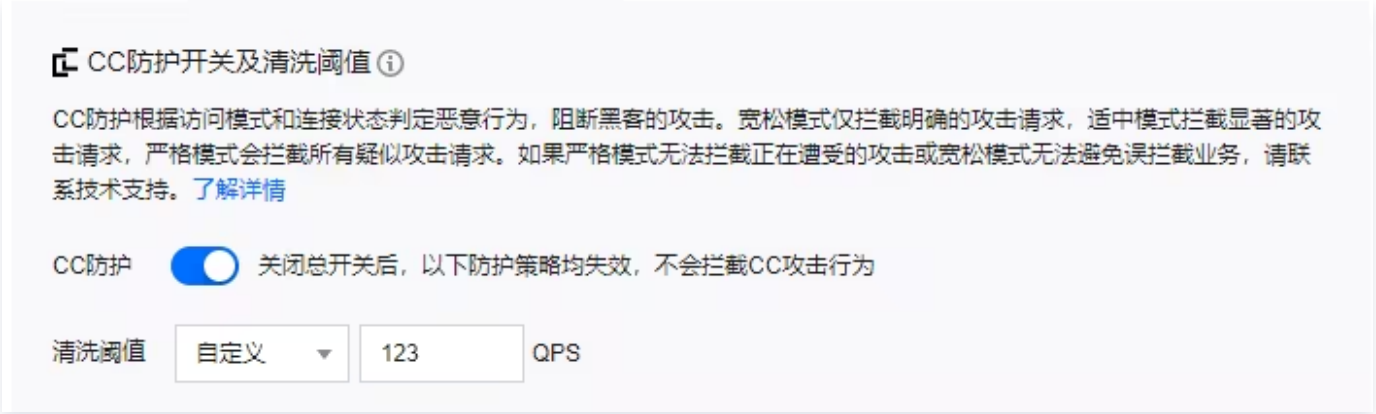
Anti-DDoS Advanced provides CC attack protection. The protection policy includes protection level, threshold clearing, precise protection, and CC frequency limit, etc. After your business is integrated, you can refer to the CC attack protection policy configuration process introduced in this document to make relevant configurations to better protect your business.

Configuration Steps

1. Log in to the Anti-DDoS (New Version) console. In the left sidebar, click **Protection Policy** > **CC Protection**.
2. In the left list, select the domain name under the ID of the high-protection IP, such as **212.64.xx.xx bgpip-000002je** > **http:80** > **www.xxx.com&quot**.

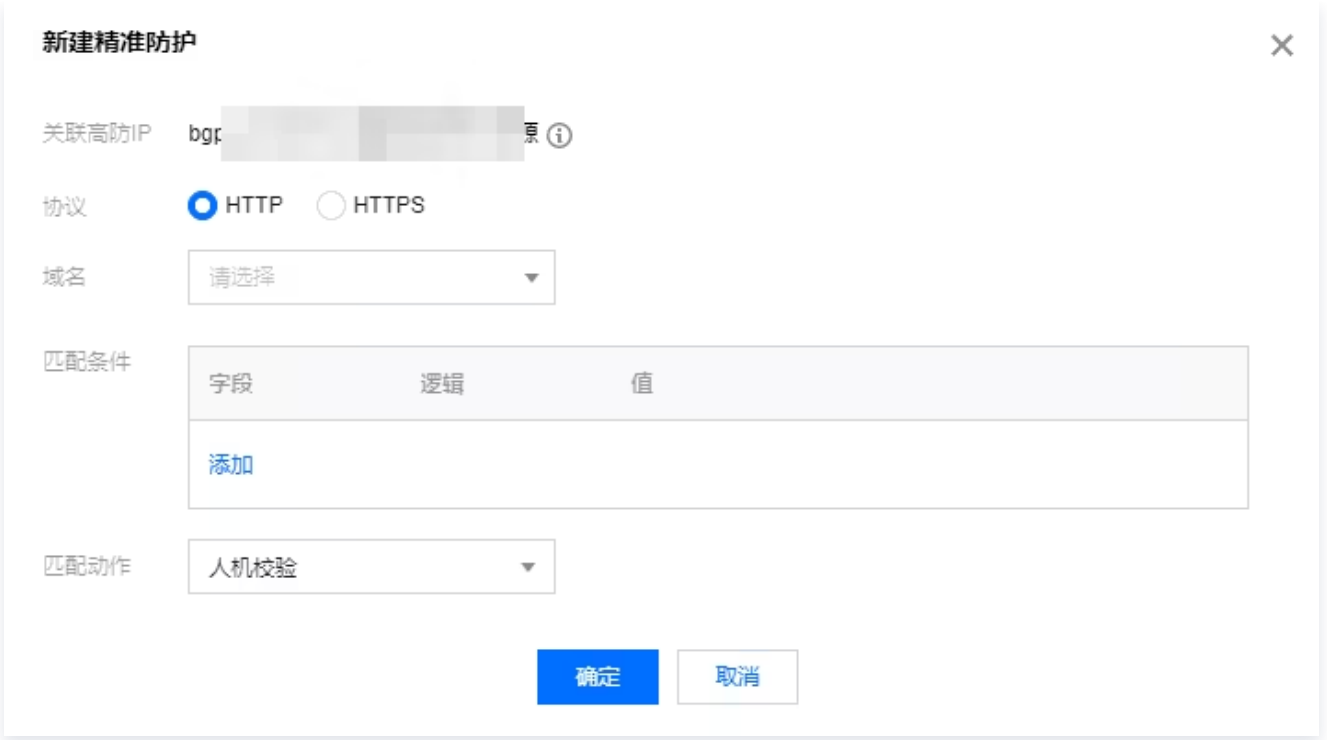
3. **CC Protection Switch and Threshold-clearing**. On the right side, select the CC protection switch and threshold-clearing card, click  to turn on the switch, and set the CC protection threshold-clearing.

> **Note:**
> - The threshold clearing is the CC protection switch of DDoS high defense. The specific threshold can be set to 1.5 times the peak value of normal business.
> - If no specific threshold is set, the high-protection IP will not trigger the cleansing action, that is, the CC protection is in a closed state. When there is a CC attack, the protection level, precise protection, and CC frequency limit related policies configured on the console will not take effect. For detailed information, see CC Protection Switch and Threshold Clearing.



4. **Precise Protection Policy Configuration.**
   When an attack occurs, it is recommended to obtain specific information about the attack request through network packet capture, middleware access logs, other protection devices, etc., and determine the attack feature combined with the business to complete the configuration of the precise protection policy.
   After enabling precise access control, you can combine common HTTP fields (such as URI, UA, Cookie, Referer and Accept, etc.) as conditional protection policies to filter access requests, and set human-machine verification or discard policy actions for requests that hit the conditions.
   4.1 In the precise protection card, click **Settings** to enter the frequency limit rule list.
   4.2 Click **Create New** to create a precise protection rule, fill in the relevant fields, and after completion, click **Yes**. For detailed configuration instructions, see Precise Protection.

> ⚠ **Note:**
> - If there are multiple HTTP fields in the same policy, all conditions must be met to match this policy.
> - DDoS high-protection IP can support precise protection configuration for HTTPS business.



Field	Field Description
uri	The URI address of the access request.
ua	The client browser flag and other related information that initiates the access request.
cookie	The Cookie information carried in the access request.
referer	The source website of the access request, that is, which page jump generates this access request.
accept	The data type that the client initiating the access request hopes to receive.
Matching condition	• Discard: Do not perform CAPTCHA and drop directly. • Human-machine verification: Perform human-machine identification using algorithms.

5. **CC Frequency Limit**

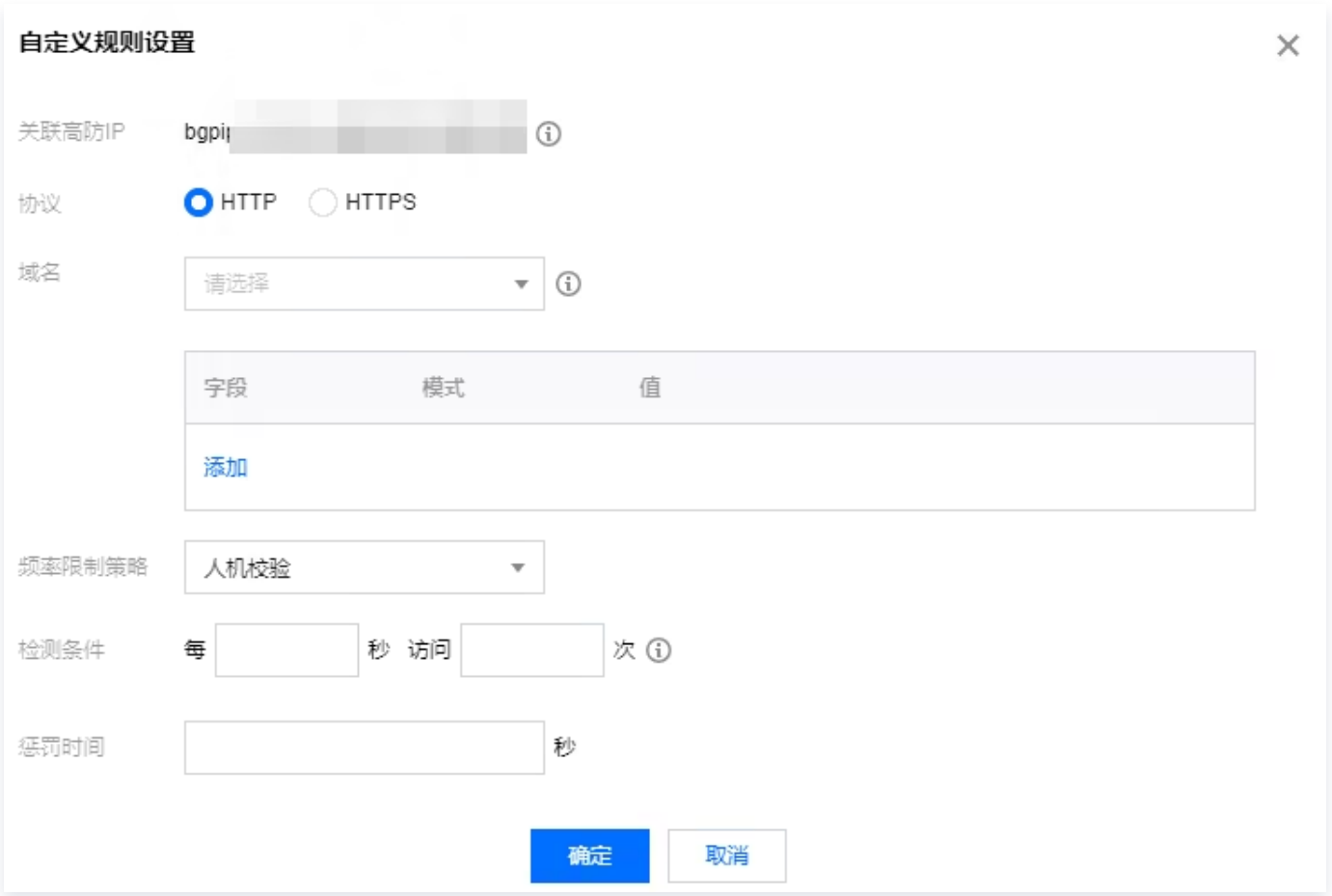
   DDoS high defense provides frequency control protection policies for websites that have been connected to protection, supporting the limitation of the access frequency of the source IP. You can customize the frequency control rules. When it is detected that a single source IP accesses a certain page abnormally frequently in a short term, human-machine verification will be set or discarding policy will be adopted.

   5.1 In the CC frequency limit card, click **Settings** to enter the precise protection rule list.

5.2 Click **Add Rule** to create a frequency control rule, fill in the relevant fields, and click OK. For detailed configuration instructions, please refer to CC Frequency Limit.

Note:

- When configuring the CC frequency limit policy for URI, you need to first configure the frequency limit of the "/" directory, and the match mode must be set to equal. After configuring the "/" directory, you can set the URI access frequency limit of other directories.
- The specific effect of configuring the frequency limit of the "/" directory is that if the frequency of a single source IP requesting the "/" directory of this domain name exceeds the threshold within a unit time, the corresponding policy action (human-machine verification or drop) is triggered.
- After each domain name configures the frequency limit policy of the "/" directory, the detection time of other directories must be consistent.
- When there is an unfixed string in the requested URI, it can be solved by configuring the match mode to include, that is, to match the same prefix in the URI.



Field	Field Description
Cookie	The Cookie information carried in the access request.
User-Agent	The client browser flag and other related information that initiates the access request.
Uri	The URI address of the access request.
Frequency limit policy	• Discard: Do not perform CAPTCHA and drop directly. • Human-machine verification: Perform human-machine identification using algorithms.
Check condition	Set the access frequency according to business conditions. It is recommended to enter 2 – 3 times the normal number of accesses. For example, if the average number of visits to the website is 20 times/minute, it can be configured to 40 – 60 times/minute, which can be adjusted according to the severity of the attack.
Penalty duration	It is at most one day.

Quickly Synchronize Forwarding Rules To a New High-Defense IP

Last updated: 2025-03-20 09:48:38

After a user purchases a new Anti-DDoS Advanced instance, when there are many instances or when configuring a triple-network Anti-DDoS Advanced instance, if a convenient method is required to quickly synchronize the forwarding rules, please refer to this document for configuration.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Management Console, and in the left directory, click **Business Access** > **Port Access**.
2. On the Port Access page, click **Batch Export**.
3. In the IP input field, search for and display the configured forwarding rules, select the forwarding rules to be exported, and click **Copy**.

4. On the Port Access page, click **Batch Import**.
5. Enter the newly purchased Anti-DDoS IP (without configured forwarding rules) into the corresponding input field, then in the input field below, paste the content you just copied, and click **Confirm**.

6. In the port access list, you can see the successfully imported forwarding rules.

Achieving Triple-Network Traffic Scheduling through Intelligent Scheduling

Last updated: 2026-03-11 17:41:01

this document guides you how to pass intelligent scheduling to achieve triple-network traffic scheduling.

Overview

After purchasing Anti-DDoS IPs for the triple-network, a common method of business traffic scheduling is forwarding based on the ISP source of DNS requests. That is, traffic from China Telecom is scheduled to the protective IP of China Telecom, traffic from China Unicom is scheduled to the protective IP of China Unicom, traffic from China Mobile is scheduled to the mobile protective IP, and traffic from other ISPs is scheduled to the Anti-DDoS line with the highest priority. You can configure intelligent scheduling to achieve the above scenario.

Prerequisites

- Before enabling intelligent scheduling, please connect the business that needs protection to the anti-DDoS instance for protection.

  > **Note:**
  > - If you need to add the IP of the cloud product under protection to the purchased high-defense package instance, please refer to Anti-DDoS quick start.
  > - If you need to add layer-4 or layer-7 business to the purchased Anti-DDoS high-defense IP instance, please refer to Anti-DDoS port access or domain name access.

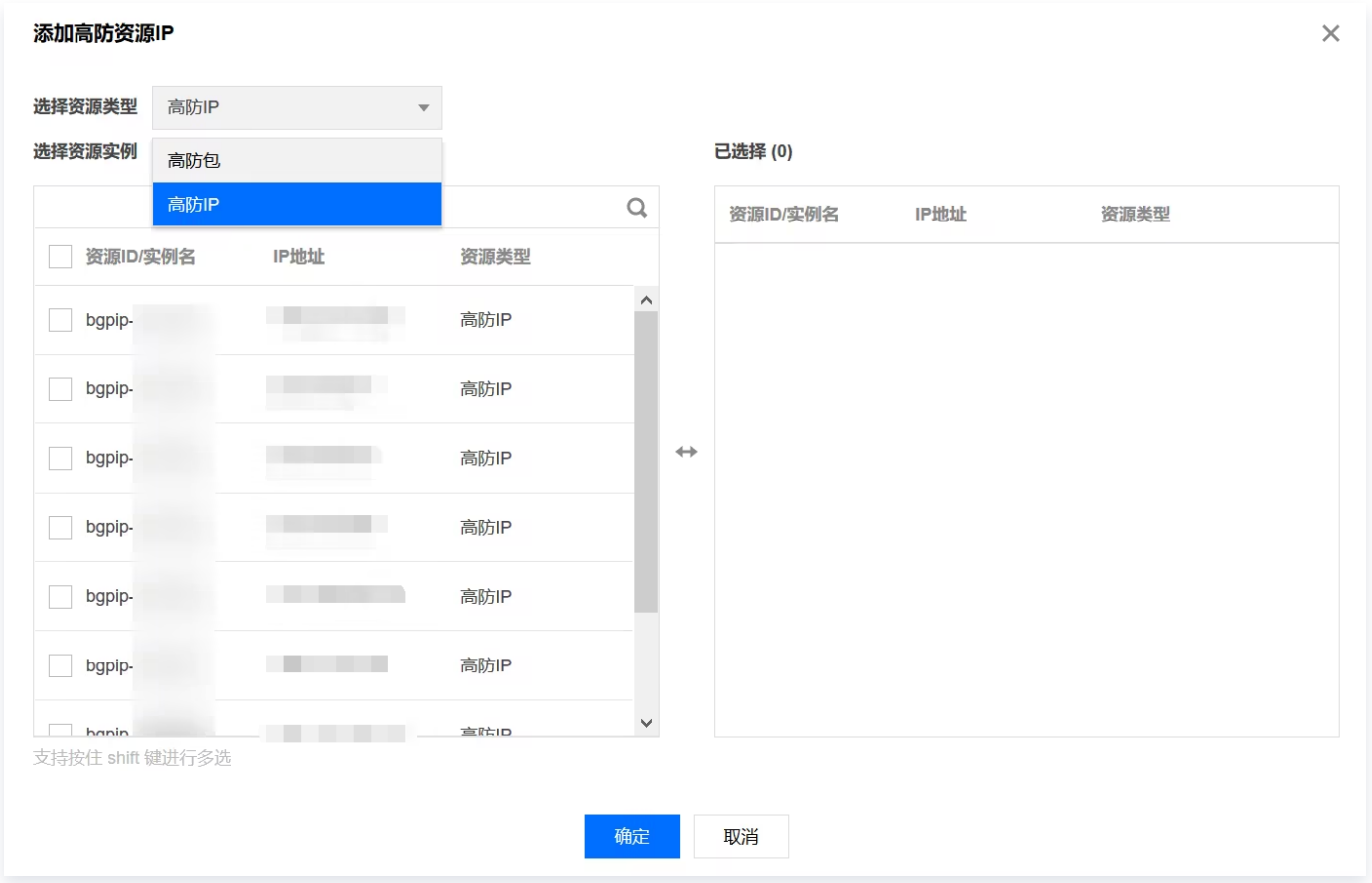
- Before modifying DNS resolution, you need to successfully purchase a DNS product, such as Tencent Cloud's DNS.

Operation Steps

1. Log in to the Anti-DDoS (New Version) Console. In the left sidebar, click **Intelligent Scheduling**.
2. On the Intelligent Scheduling page, click **Create Scheduling Policy**. The system will automatically generate a CNAME record.

3. Create an intelligent scheduling page. The TTL value defaults to 60 seconds. The value range is 1 (second) – 3600 (seconds). The scheduling method is default priority.

4. click **Add High Defense Resource IP**, select the anti-DDoS instances and IPs that require setting intelligent scheduling, and click **Confirm**.



5. After selecting an anti-DDoS instance, the Anti-DDoS line of the instance enables DNS resolution by default, and then sets its priority.

> **Note:**
> - The priority configurations of the three ISP lines should be identical, ensuring responses are made according to the ISP source of the DNS request.
> - About the configuration of intelligent scheduling, see Intelligent Scheduling.

Quickly Restore Business after CVM Enters Blocking

Last updated: 2025-03-20 09:49:41

A DDoS attack refers to the act of controlling a large number of computers or network bots to simultaneously access a target server, causing congestion and excessive load on the target server, thereby preventing legitimate users from accessing the server normally. This type of attack can seriously affect the availability of websites or services and bring significant losses to the victims.

You can choose an appropriate solution to restore your business based on your business situation.

Solution One: Wait For Automatic Unblocking Upon Expiration To Restore Business

If your network service has been attacked by DDoS and blocked, you can wait for the system to automatically unblock it. Under the default setting of Anti-DDoS Basic, blocking will be automatically lifted after 2 to 24 hours (the specific blocking duration is subject to the actual blocking duration). You can log in to the Anti-DDoS (New Version) Console, select the **Unblocking Service** page in the left sidebar, and view the remaining self-service unblocking attempts.
You can also check the estimated unblocking time through Internal Message, Short Message Service (SMS), or mailbox, and then evaluate whether to wait for automatic unblocking based on the business delivery situation.

Solution Two: Manually Unblock Using Anti - DDoS To Restore Business

If your business has been integrated with Anti-DDoS, you can manually lift the black hole. For specific operations, please refer to Self-service Unlocking.

Note:

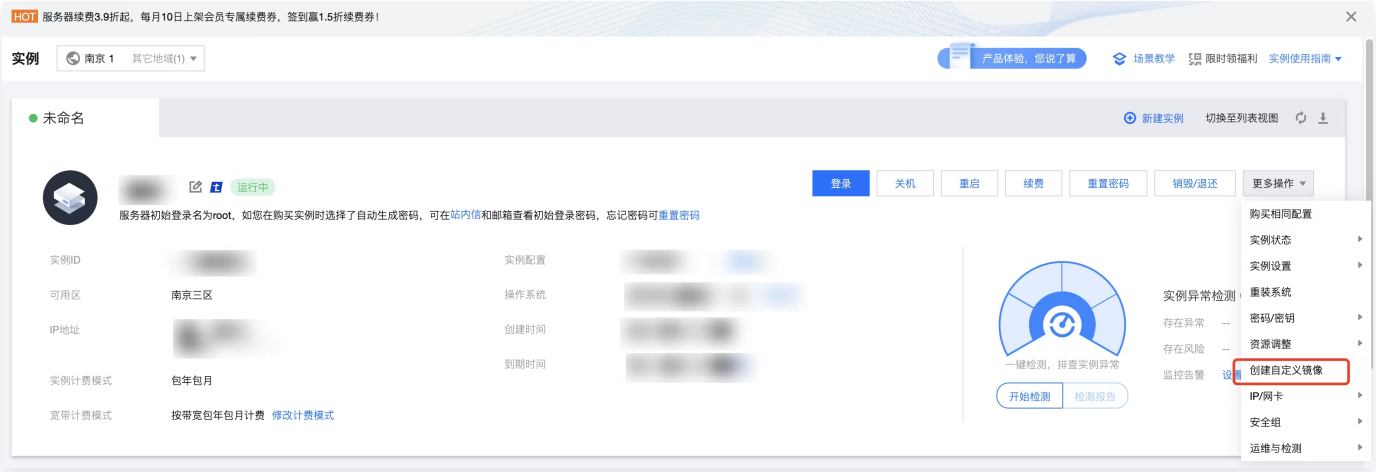
- Users of Anti-DDoS Pro (excluding the lightweight and inclusive versions) and Anti-DDoS IP will have three chances of self-service unlocking per day. No unlocking operations can be performed after exceeding three times a day.
- Unblocking may fail (unblocking failure will not deduct your remaining unlocking times). Please wait patiently for a while and try again.

- Before performing the unblocking operation, it is recommended that you first check the estimated unblocking time, which may be postponed.
- If the self-service unblocking quota for the day is 0, it is recommended to improve the base protection capability or elastic protection capability to defend against large-scale traffic attacks and avoid being continuously blocked.

By following the above steps, you should be able to successfully manually unblock and recover your business, or you can choose to directly purchase a high-defense product for recovery. For small-traffic attack scenarios, you can select Anti-DDoS Basic (Enhanced Edition). If you have higher protection requirements, you can choose DDoS Protection Pack or DDoS Protective IP.

Solution Three: Create a CVM Instance With the Same Configuration Using a Mirror and Replace the Business Server

1. Select the CVM that enters the black hole, and then create a custom image. For details, see Create Custom Image.



> **Note:**
> Besides using the public images and service market images provided by Tencent Cloud, you can also create custom images. After creating a custom image, you can quickly create a Tencent Cloud CVM instance with the same configuration as the image in the Tencent Cloud Console.

2. Use the custom image created in Step 1 to quickly create a CVM instance with the same configuration. For details, see Create Instance from Custom Image.
3. After the image is created, select the image you created in the image list, and click **Create Instance** on the right side of its row to purchase a server with the same image as before.

Solution Four: Change the Public IP Address Of the CVM Instance

1. Apply for a new Elastic IP in the Public IP Address Console. For details, see Apply for EIP.

2. Unbind the Elastic IP bound to the CVM instance. For details, see Unbind EIP.

> **Note:**
> Traditional account types can check **Allocate a regular public IP address for free after unbinding** when unbinding. After unbinding, a new regular public IP address will be allocated. Each account can re-allocate a regular public IP address for free up to 10 times per day.

3. Bind a new Elastic IP to the CVM instance. For details, see Binding EIP to Cloud Resources.

> **Note:**
> - If a standard account type of cvm instance already has an ordinary public IP, you need to release the ordinary public IP before you can bind an EIP.
> - If a traditional account type of cvm instance already has an ordinary public IP, the ordinary public IP of the current cvm instance will be released after an EIP is bound.
> - The number of cvm instances that can be bound to an EIP varies depending on the CPU configuration of the cvm instance. See Use Limits.

Quick Business Restoration After the Lightweight Application Server Lighthouse Is Blocked

Last updated: 2025-03-20 09:51:34

If Lighthouse suddenly suffers a DDoS attack, the lightweight Cloud Virtual Machine provides a default protection of 2Gbps. However, given the current common attack patterns, once attacked, the server is very likely to crash immediately. The DDoS protection mechanism is as follows: Once attacked and the attack traffic exceeds 2Gbps, the system will isolate the host's IP address, making it inaccessible from the public network, which is similar to being placed in a "small black room". When the attack stops, the server provides self-service unlocking three times. If the server is attacked and the number of temporary isolations exceeds three times, the server will enter a 24-hour isolation state.

You can choose an appropriate solution according to your business situation to restore your business.

Solution One: Wait For Automatic Unblocking Upon Expiration To Restore Business

The lightweight application server may be blocked and isolated due to a DDoS attack, and the isolated lightweight application server is displayed as "BANNING" status in the console.
If your network service suffers a DDoS attack and is blocked, you can wait for the system to automatically unlock. By default, Anti-DDoS Basic will automatically unlock after blocking for 2 to 24 hours (the specific blocking duration is subject to the actual blocking duration). You can check the operation steps of automatic unlocking below.

1. Check the estimated unblocking time through Message Center, Short Message Service (SMS), and mailbox, then evaluate whether to wait for automatic unblocking based on business delivery situation.
2. You can log in to the Anti-DDoS (New Version) Console, select **Unblocking Service** page in the left sidebar, and check the remaining times of self-service unlocking.

> **Note:**
> If the self-service unlocking count is exceeded, self-service unlocking will no longer be supported.

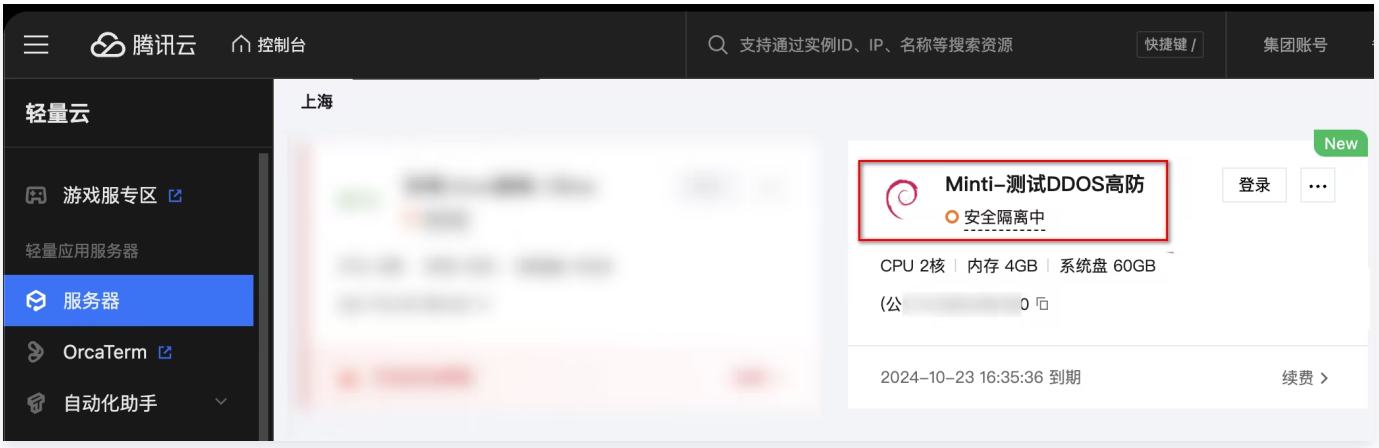
Solution Two: Manually Unblock Using Anti-DDoS To Restore Business

If your host IP is banned and you want to unlock it immediately, you can use the manual unlocking feature. When using this feature, you need to have successfully purchased Anti-DDoS Pro (Lightweight Edition).

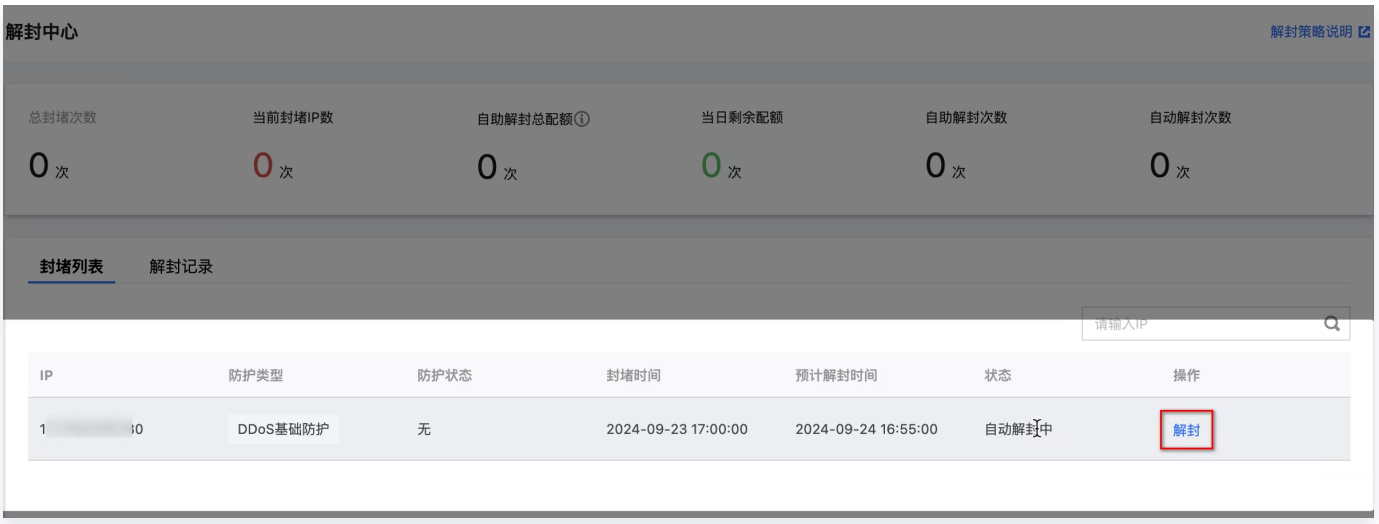
Note:

- Anti-DDoS Pro (lightweight version) is only applicable to Lighthouse.
- The product specification of Anti-DDoS Pro (lightweight version) is 1 IP + up to 10 Gbps protection + 1 year (this is the only specification).
- Since February 27, 2023, the purchased Anti-DDoS Pro (lightweight version) provides self-service unlocking capability 3 times a month. The self-service unlocking capability can only be used to unlock lightweight server resources. For specific operations, please refer to Self-service Unlocking Operation.

1. Log in to Lighthouse, and click on **Server** in the left operation bar.
2. On the server page, view the servers in security isolation.



3. Go to the Unblocking Service page of the Anti-DDoS console, and click **Unblock** in the operation column of the directory IP in the blocking list.



Solution 3: Create an LH Server With Identical Configuration Using a Mirror and Activate a New Lightweight Instance

After a Tencent Cloud lightweight server is attacked, although its public network IP is blocked, the private network remains valid and the host is still usable, but it cannot be accessed from the Internet. In this case, you can use the image feature of the lightweight server to restore it, but this requires newly opening a lightweight server.
The principle is: the old lightweight creates image A > select image A when the new lightweight is activated and the system is installed > the new lightweight is activated > domain resolution is directed to the new lightweight.

1. Select the isolated server, click **Create an Image** to create the old lightweight image A. For detailed instructions, see Creating Custom Image.

2. On the Create Custom Image page, select **Custom Image A**, enter the image name and image description, and click **Start Production**.

3. After completing the creation of the custom image, all data and configurations of the new lightweight are exactly the same as the original, except for the IP address difference.