Alibaba Cloud
Anti-DDoS Pro

DDoS Protection Guide

Issue: 20190801

Legal disclaimer

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

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

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

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

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

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

Legal disclaimer... I
Generic conventions... I
1 Basic Concepts... 1
1.1 Common DDoS attacks... 1
1.2 Alibaba Cloud black hole policies... 1
1.3 Traffic scrubbing and black hole... 4
2 Common DDoS Protection Solutions... 6
2.1 Alibaba Cloud best practices for relieving DDoS attacks... 6

1 Basic Concepts

1.1 Common DDoS attacks

Distributed Denial of Service (DDoS) exploits client/server technology to combine multiple computers and form a platform to initiate an attack against one or more targets, which poses a threat that is orders of magnitude greater than that of a denial of service attack.

Malformed packets

Malformed packets indicate Frag flood, Smurf, Stream flood, Land flood attacks, IP malformed packets, TCP malformed packets, and UDP malformed packets.

Transport-layer DDoS attacks

Transport-layer DDoS attacks indicate SYN flood, Ack flood, UDP flood, ICMP flood, and RST flood attacks.

DNS DDoS attacks

DNS DDoS attacks indicate DNS Request flood, DNS Response flood, valid and invalid source DNS Query flood attacks, and authoritative server and local server attacks.

Connection DDoS attacks

Connection DDoS attacks indicate TCP slow connection attacks, connect exhaustion attacks, Loic, Hoic, Slowloris, Pyloris, and Xoic among other slow attacks.

Web application DDoS attacks

Web application-layer attacks indicate HTTP Get flood, HTTP Post flood, and HTTP flood attacks.

1.2 Alibaba Cloud black hole policies

This topic explains the black hole policy of Alibaba Cloud Security.

What is a black hole?

When the attack traffic to a server exceeds the black hole threshold configured for the server room, the server is thrown into a black hole to block external network access to the server. Once a server is thrown into a black hole, it become unavailable during the black hole duration. After that, the system determines that the attack traffic stops , and the black hole status is automatically lifted.

The black hole is a service that Alibaba Cloud purchases from the operator who imposes strict restrictions on the time and frequency to lift the black hole. The black hole state cannot be manually deactivated. Thus, you must patiently wait for the system to auto unban the server.

Why enact the black hole policy? Why can not help users resist the attack for an unlimited period of time?

DDoS attacks severely impair not only victims, but also the entire cloud network. Besides, DDoS defense costs a lot, the biggest among which is the bandwidth cost.

Alibaba Cloud purchases bandwidth from ISPs. ISPs will not clean out DDoS attack traffic when calculating the bandwidth cost, but will directly charge Alibaba Cloud on the consumed bandwidth.

Alibaba Cloud Security potentially defends against DDoS attacks for Alibaba Cloud users free of charge at a limited cost, but when the attacking traffic exceeds the threshold, Alibaba Cloud will block the traffic to the IP address under attack.

How to view the black hole threshold and duration?

See Anti-DDoS Basic black hole threshold to check the current DDoS mitigation capacity of your ECS, SLB, or EIP instances.

See View the black hole duration to check how long it takes before your IP becomes accessible during a black hole event.

How to improve the black hole threshold?

Join up our Security Credibility plan for free to get an extra DDoS mitigation capacity based on your security credibility score.

See Check security credit details to learn the scoring criteria of the security credibility score and take the initiative to improve it. By improving your credibility score, you can get more extra DDoS mitigation capacity.

What to do if the black hole threshold is not enough?

You can purchase the Anti-DDoS Pro service to easily prevent DDoS attacks and safeguard normal operation of servers. Anti-DDoS Pro is designed to help users defend against DDoS attacks, with clear commitment on the protection capability and defense performance.

What is the difference between the Security Credibility plan and Anti-DDoS Pro?

The Security Credibility plan helps users with good credit records to increase the protection capability against the first attack. The black hole threshold is adjusted as the credibility score changes, with no fixed protection capability warranted.

Anti-DDoS Pro service is designed to help users defend against DDoS attacks, with clear commitment on the protection capability and defense performance.

Black hole triggering thresholds for various regions

The default black hole triggering thresholds offered by basic protection feature of Anti-DDoS Basic in various regions are as follows (Unit: bps):

Note:
The triggering thresholds apply to Alibaba Cloud ECS, Server Load Balancer, VPC, and other products.

Region	1-core CPU classic-network ECS	2-core CPU classic-network ECS	4-core (or later) CPU classic-network ECS	Server Load Balancer and VPC
China East 1	500 M	1G	5 G	5 G
China East 2	500 M	1G	2 G	2 G
China North 1	500 M	1G	5 G	5 G
China North 2	500 M	1G	2 G	2 G
China North 3	500 M	1G	2 G	2 G
China North 5	500 M	1G	2 G	2 G
China South 1	500 M	1G	2 G	2 G
Hong Kong	500 M	500 M	500 M	500 M
US West 1	500 M	1G	2 G	2 G
US East 1	500 M	500 M	500 M	500 M
Tokyo	500 M	500 M	500 M	500 M
Singapore	500 M	500 M	500 M	500 M
Sydney	500 M	500 M	500 M	500 M

Region	1-core CPU classic-network ECS	2-core CPU classic-network ECS	4-core (or later) CPU classic-network ECS	Server Load Balancer and VPC
Kuala Lumpur	500 M	500 M	500 M	500 M
Mumbai	500 M	1G	1G	1G
Frankfurt	500 M	500 M	500 M	500 M
Dubai	500 M	500 M	500 M	500 M

Black hole duration

The default black hole duration is 2.5 hours and the server cannot be unbanned during this period. The actual black hole duration depends on the attack situation and may range from 30 minutes to 24 hours. The duration of the black hole is mainly influenced by the following factors:

- Whether the attack persists. The black hole duration keeps extending, if the attack continues. The black hole duration is re-calculated from the time of extension.
- Whether the attack is frequent. If a user is attacked for the first time, the black hole duration will be automatically shortened. On the contrary, the black hole duration for a user under frequent attacks will be automatically extended as the user is more likely to be attacked again.

Note:

For users suffering overly frequent black holes, Alibaba Cloud reserves the right to extend the black hole duration and reduce the black hole threshold. You can go to the console to view the specific black hole threshold and duration.

1.3 Traffic scrubbing and black hole

By default, Anti-DDoS Basic is activated, once the ECS instance is created. This service includes traffic scrubbing and black hole.

Traffic scrubbing

The traffic scrubbing service consists of three units: detecting center, cleaning center , and centralized management center. The detecting center monitors data traffic flowing into the ECS instance, and identifies abnormal traffic in a timely manner, such as DDoS attack. When an abnormity is detected, the management center guides the cleaning center to clean suspicious traffic based on the traffic diversion policy . Malicious traffic is removed, while legitimate traffic is returned to the original instance. This guarantees that only the legitimate traffic is forwarded to the target system.

Black hole

When the attack traffic exceeds the default traffic threshold, the black hole triggering service automatically triggers a black hole. The threshold varies from regions and CPU configurations. For more information about default settings of different regions, see Anti-DDoS Basic black hole threshold.

The black hole causes traffic to be restricted for a period of time (2.5 hours by default), depending on attack status.

Meanwhile, the traffic scrubbing service comes into effect. The black hole duration keeps extending, if the attack continues. In addition, the black hole state cannot be manually deactivated. You must patiently wait for the system to auto unban the server .

To meet your urgent requirements for service recovery, you can use Alibaba Cloud Anti-DDoS Pro.

Anti-DDoS Pro is a value-added, paid service, applicable when services are unavailable after a heavy DDoS attack. You can redirect attack traffic to the Anti-DDoS Pro IP address to guarantee stability and reliability of the source instance.

2 Common DDoS Protection Solutions

2.1 Alibaba Cloud best practices for relieving DDoS attacks

Distributed Denial of Service Attack (DDoS Attack) is a malicious cyber-attack on a target system. It usually makes the victim’ s services unable to be normally accessed, i.e., the denial of service.

Common DDoS attacks include:

- Network layer attack

  The typical network layer attack is a UDP reflection attack. It mainly congests the network bandwidth of the victim using heavy traffic, causing the victim’ s services not to respond to customer access normally.
- Transport layer attack

  The typical transport layer attack includes an SYN flood attack, a connection s attack, etc. It occupies connection pool resources of a server to achieve the purpose of denying the service.
- Session layer attack

  The typical session layer attack is an SSL connection attack. It occupies SSL session resources of a server to achieve the purpose of denying the service.
- Application layer attack

  The typical application layer attack includes a DNS flood attack, an HTTP flood attack, a dummy attack, etc. It occupies application processing resources of a server and significantly consumes the processing performance of the server to achieve the purpose of denying the service.

Best practices for relieving DDoS attacks

It is recommended that Alibaba Cloud users relieve DDoS attacks through the following methods:

- Reduce surface exposure and isolate resources and irrelevant services to reduce the risk of being attacked.
  - Configure a security group

    Avoid exposing ports which are not required for the service on the public network as much as possible so as to avoid requests and accesses irrelevant to the service. Configuring a security group can effectively prevent the system from being scanned or exposed accidentally.

    For more information, see Security Group User Guide.
  - Use Virtual Private Cloud (VPC)

    The logic isolation within the network is implemented through VPC to prevent attacks from Intranet zombie computers.

    For more informatioin, see VPC User Guide.
- Optimize the business architecture and design auto scaling and failover based on features of the public cloud.
  - Deploy Server Load Balancer

    Transport layer DDoS attacks within a certain amount of traffic can be effectively relieved by deploying Server Load Balancer (SLB) instances to balance loads across multiple servers. Meanwhile, after the SLB is deployed, the user access traffic can be allocated to servers uniformly to reduce the burden of a single server and increase the access speed.

    For more information, see SLB User Guide.
  - Deploy Auto Scaling

    Auto Scaling is a management service that automatically adjusts elastic computing resources according to your business needs and policies in an economical manner. By deploying Auto Scaling, the system can effectively relieve session layer and application layer attacks, and automatically adds servers when being attacked, which improves the processing performance and avoids severe impact to the service.

For more information, see Auto Scaling User Guide.

- Deploy smart DNS resolution Optimize DNS resolution by using the smart resolution to effectively avoid risks caused by DNS traffic attacks. Meanwhile, we recommend that you host the service on multiple DNS service providers.
  - Shield unrequested DNS response information
  - Discard the fast retransmit data packet
  - Enable TTL
  - Discard the unknown DNS query request and response data
  - Discard unrequested or sudden DNS requests
  - Enable DNS client verification
  - Cache response information
  - Use the ACL permission
  - Use ACL, BCP38, and IP reputation
- Prepare the remaining bandwidth

  Run a server performance test to assess bandwidth and the number of requests that the normal business environment can withstand. Make sure that a certain remaining bandwidth is available when purchasing the bandwidth, thus avoiding the influence on normal users when the bandwidth is greater than the normal bandwidth usage while being attacked.

- Strengthen the server security and improve performances of the server such as connections.

  Strengthen the server security, reduce attacked items, and increase the attack cost of the attacker.

  - Make sure that system files on the server are up-to-date, and promptly update system patches.
  - Check the host of all servers to know the source of visitors.
  - Filter unnecessary services and ports. For example, only enable port 80 for WWW servers, and disable all other ports, or set block policies on the firewall.
  - Limit the number of SYN semi-joins that are open at the same time, shorten the timeout for SYN semi-joins, and limit SYN/ICMP traffic.
  - Check logs for network devices and server systems carefully. As long as vulnerabilities or changes in time appear, this server may be attacked.
  - Restrict file sharing with network files outside the firewall. Reduce the opportunity that hackers intercept system files. If the hackers replace it with a Trojan, file transfer functions are undoubtedly paralyzed.
  - Make full use of network devices to protect network resources. The following strategy configurations must be considered when configuring the router: traffic control, packet filtering, semi-join timeout, garbage packet discarding , counterfeit source data packet discarding from the source, SYN threshold, disabling ICMP and UDP broadcasts.
  - Restrict new TCP connections, connections, and the transmission rate of suspected malicious IPs via software firewalls such as iptable.
- Carry out business monitoring and emergency response.

  - Focus on Anti-DDoS Basic monitoring

    When your services are suffering from DDoS attacks, Anti-DDoS Basic sends alert information through SMS or mail. It also supports alarming by phone when the services are suffering from heavy traffic attacks. It is recommended that you perform emergency response processing immediately when receiving the alert.

For more information about configuring the alert message recipient and voice alert method, see Anti-DDoS Basic Message Recipient Setting.

- CloudMonitor

  CloudMonitor can be used to collect and obtain monitoring metrics for Alibaba Cloud resources or monitoring metrics customized by users, to test the availability of services, and to set alarms for these metrics.

  For more information, see CloudMonitor User Guide.

- Select an appropriate commercial security solution. Alibaba Cloud provides free Anti-DDoS Basic and commercial security solutions such as Anti-DDoS Pro IP and Game Shield. You can also select security solutions from other manufacturers.

  - Web Application Firewall (WAF)

    WAF can provide effective safeguard on transport layer attacks, session layer attacks, and application layer attacks for web applications.

    For more information, see WAF User Guide.

  - Anti-DDoS Pro IP

    It is recommended that you use Alibaba Cloud Anti-DDoS Pro IP for heavy traffic DDoS attacks.

    For more information, see Anti-DDoS Pro IP User Guide.

  - Game Shield

    Game Shield is an industry solution proposed for common DDoS attacks and HTTP flood attacks in the game industry. Compared with Anti-DDoS Pro IP, Game Shield provides more pertinence, better defense effects, and a lower cost.

Cautions

DDoS attacks are the recognized public enemy industry-wide. It not only affects the victims, but also affects the service providers’ network stability, thus causing service losses to other users within the same network.

Computer networks are shared environments. The stability must be maintained by each party. Some behaviors may affect the whole network and the network of other tenants. So you need to pay attention to the following items:

- Do not establish the DDoS protection platform using Alibaba Cloud product mechanism
- Do not release instances which are in black hole status
- Do not continuously replace, unbind, and add IP products such as SLB IP, Elastic IP , and NAT Gateway to servers which are in black hole status
- Do not defend by establishing an IP pool or allocating the attack traffic to a large variety of IPs
- Do not prepose Alibaba Cloud non-network security defense products (including but not limited to CDN and OSS) that are vulnerable to attack
- Do not get around the rules by using multiple accounts