

Alibaba Cloud

Anti-DDoS DDoS Protection Guide

Document Version: 20220706

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
 Danger	A danger notice 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.
 Warning	A warning notice 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 restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.Introduction to DDoS attacks	05
2.Best practices for mitigating DDoS attacks	08
3.Blackhole filtering policy of Alibaba Cloud	12
4.View black hole triggering thresholds in Anit-DDoS Origin Basi.....	16
5.Terms	19

1. Introduction to DDoS attacks

A distributed denial of service (DDoS) attack uses multiple computers to launch coordinated attacks against one or more targets through malicious programs. The attack undermines the performance or consumes network bandwidth and makes the target servers unresponsive.

Attack principle

Typically, an attacker installs a DDoS master program on a single computer using an unauthorized account and then installs agent programs on multiple computers. During a specified period, the DDoS master program communicates with a large number of agent programs. When the agents receive the command, they initiate attacks. The master program can initiate hundreds or even thousands of agent programs within seconds.

Risks of DDoS attacks

The attacks may cause the following risks to your business:

- Significant economic loss

Once DDoS attacks occur, your origin server may be unable to provide services and users cannot access your services, resulting in huge economic loss and reputation damage.

For example, when an e-commerce platform suffers from DDoS attacks, websites cannot be accessed or may be temporarily closed. Therefore, legitimate users cannot purchase products.

- Data leak

Attackers may get access to the core data of your business.

- Unfair competition

Competitors may launch DDoS attacks against your service to gain a competitive advantage.

For example, if a game is under DDoS attacks, the number of players reduces, and the game may go offline for a few days.

Common DDoS attack types

Type	Typical attack	Description
Malformed packet attack	Fragment flood, smurf, stream flood, land flood, malformed IP packet, malformed TCP packet, and malformed UDP packet	A malformed packet attack occurs when malformed IP packets are sent to a target system. This may cause the system to stop responding.
Transport layer DDoS attack	SYN flood, Ack flood, UDP flood, ICMP flood, and RST flood	SYN floods are protocol attacks that exploit a vulnerability in the TCP three-way handshake. In a normal handshake process, when a server receives a SYN request, the server saves the connection in a SYN queue. If attackers continuously send SYN requests to the server but do not respond with the expected ACK messages, server resources are consumed. When the SYN queue is full, the server will stop responding to requests from users.

Type	Typical attack	Description
DNS DDoS attack	DNS request flood, DNS response flood, DNS query flood (spoofed request and real requests), authoritative server attacks, and local server attacks	DNS query floods execute real query requests, which is a normal service operation. If multiple zombies initiate a large number of domain name query requests at the same time, the server cannot respond to them. This can result in a denial of service.
Connection-based DDoS attack	Low and slow attack, connection exhaustion attack, Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC), Slowloris, PyLoris, and XOIC	<p>Slowloris attacks can exhaust the concurrent connection resources of a target server. When the number of concurrent connections reaches the upper limit, the server denies additional connection attempts. For example, if the server receives a new HTTP request, the server processes the request, returns a response, and closes the connection. If the connection remains open, the server must establish a new connection when it receives another HTTP request. If all connections remain open, the server stops responding to any new requests.</p> <p>The Slowloris attacks exploit the features of HTTP. An HTTP request starts with <code>\r\n\r\n</code>, indicating the end of the header fields. If the server receives only <code>\r\n</code>, the connection remains open and waits for the subsequent content of the request.</p>

Type	Typical attack	Description
Application layer attack	HTTP GET flood, HTTP POST flood, and HTTP flood attacks	<p>Application layer attacks can simulate user requests. You can hardly tell the attacks and normal requests apart, like search engines and crawlers.</p> <p>Transactions and pages that consume large amounts of resources in web services are vulnerable to HTTP flood attacks in high concurrency scenarios, for example, paging and sharding. If the page size is too large, frequent paging will consume large amounts of resources.</p> <p>The attacks are hybrid attacks. Operations that are performed frequently and have the features of real user operations are identified as HTTP flood attacks. For example, if a website is accessed by ticketing software, the access can be identified as an HTTP flood attack.</p> <p>HTTP flood attacks target the backend services of web applications. In addition to causing a denial of service, HTTP flood attacks directly affect the functionality and performance of web applications, including the response time, database services, and disk read and write operations.</p>

How do I identify a DDoS attack?

You identify a DDoS attack when:

- Your server is suddenly disconnected, the access speed becomes slow, and users are offline but the network and devices are working properly.
- The CPU or memory usage of your server increases significantly.
- The outbound or inbound traffic increases significantly.
- Your business website or application suddenly receives a large number of unsolicited requests.
- The logon to your server fails or becomes too slow.

2. Best practices for mitigating DDoS attacks

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

Common DDoS attack types include:

- Network layer attacks

UDP amplification attacks, such as NTP flood attacks, fall under this category. These attacks send a wave of traffic to a network. This high volume of traffic congests the network, consumes the network bandwidth, and makes the network unresponsive.

- Transport layer attacks

SYN flood attacks and connection flood attacks fall under this category. These attacks consume the connection pool resources of a server to achieve denial-of-service (DoS).

- Session layer attacks

SSL attacks fall under this type of attack. These attacks consume the SSL session resources of a server to achieve DoS.

- Application layer attacks

Typical types of application layer attacks include DNS flood, HTTP flood, and dummy attacks. These attacks occupy application processing resources and consume the processing resources of a server to achieve DoS.

Best practices

You can mitigate attacks against your assets on Alibaba Cloud by using the following methods:

- Reduce your attack surface and isolate resources and irrelevant services.

- Configure a security group.

You can configure security groups to open only the ports that are necessary for your services. This prevents access requests that are irrelevant to the service and protects your system against malicious scanning or unexpected exposure.

For more information about security groups, see [Create a security group](#).

- Use a VPC.

You can use a Virtual Private Cloud (VPC) to implement logical isolation within your network and prevent attacks from zombies.

For more information about VPC, see [Create an IPv4 VPC](#).

- Optimize the service architecture and leverage the public cloud to implement auto scaling and failover for your system.

- Evaluate the performance of the service architecture.

In the early stages of service deployment or during the operations, the technical team must perform a stress test on the service architecture to evaluate its throughput capability and provide detailed technical guidance for DDoS mitigation.

- Use an elastic and redundant architecture.

A single point of failure (SPOF) can be avoided by using load balancing or an active geo-redundancy architecture. If you deploy your services on Alibaba Cloud, you can use Server Load Balancer (SLB) to concurrently process access requests on multiple servers and balance the user access traffic among the servers. This reduces the workload on a single server and improves the throughput capability, which in turn helps mitigate DDoS attacks at the connection layer.

For more information about SLB, see [Overview](#).

- Deploy Auto Scaling.

Auto Scaling automatically scales your computing resources based on your service demands and policies. After you deploy Auto Scaling, the system mitigates session layer and application layer attacks and automatically adds servers when your services are under attack. This improves the processing performance and avoids severe impact on your services.

For more information about Auto Scaling, see [Grant permissions to Auto Scaling](#).

- Optimize DNS resolution.

You can use intelligent DNS resolution to mitigate DNS attacks. In addition, we recommend that you host your services on multiple DNS service providers and optimize DNS resolution in the following ways:

- Do not allow unsolicited DNS responses.
- Drop quick retransmission packets.
- Enable TTL.
- Drop DNS queries and responses that are anomalous.
- Drop unexpected or unsolicited DNS queries.
- Enable authentication for the DNS client.
- Cache responses.
- Use ACLs.
- Use ACLs, BCP38, and IP reputation.

- Over-provision bandwidth.

Test server performance to evaluate the bandwidth and the number of requests that your server can handle in normal business scenarios. Make sure that you buy more bandwidth than you need. This helps avoid any influence on normal users if the attack bandwidth is greater than the normal bandwidth.

- Enhance server security and improve server performance, such as connections.

Harden the OS and software to reduce the attack surface and increase the costs of attacks in the following ways:

- Make sure that system files on the server are up-to-date, and update system patches in a timely manner.
- Check all servers to know the sources of visitors.
- Disable services and ports that you do not need. For example, enable only port 80 for web servers, or set policies on the firewall.
- Limit the number of SYN semi-joins that are enabled at a single time, shorten the timeout for SYN semi-joins, and limit SYN and ICMP traffic.

- Check logs for network devices and server systems. If vulnerabilities are detected on a server or the system time of a server changes, the server may be under attack.
- Restrict file sharing outside the firewall. This reduces the opportunities that hackers intercept system files. If the attackers replace a file with a Trojan, the file transfer function goes down.
- Make full use of network devices to protect network resources. You must consider such policy configurations when you configure a router as traffic control, packet filtering, semi-join timeout, garbage packet discarding, forged source data packet discarding, SYN threshold, disabling ICMP, or UDP broadcasts.
- Restrict new TCP connections and control the transmission rate of suspected malicious IP addresses by using software firewalls such as iptable.

- Monitor your services and prepare an emergency response plan.

- Focus on Anti-DDoS Basic monitoring.

If your services suffer from DDoS attacks, Anti-DDoS Basic sends alert information by using SMS or email. If the services suffer from heavy traffic attacks, it notifies you of alerts by means of phone calls. We recommend that you handle the alert immediately.

For more information about how to configure alert message recipients and voice alert methods, see [Configure alert notifications for DDoS attack events](#).

- Use Cloud Monitor.

Cloud Monitor can be used to collect and obtain monitoring metrics or custom monitoring metrics for Alibaba Cloud resources. These metrics are then used to test the availability of services and configure alerts.

For more information about Cloud Monitor, see [What is CloudMonitor?](#).

- Develop an emergency response plan.

Develop an emergency response plan in advance based on your technical service architecture and human resources. If necessary, conduct technical drills in advance to test the response plan.

- Select an optimal commercial security solution. Alibaba Cloud provides both free Anti-DDoS Basic and paid security solutions.

- Web Application Firewall (WAF)

WAF protects against transport layer attacks, session layer attacks, and application layer attacks for web applications, such as HTTP flood attacks.

For more information, see [What is WAF?](#).

- Anti-DDoS Origin

Anti-DDoS Origin provides shared full protection against DDoS attacks for cloud services that use public IP addresses. Anti-DDoS Origin takes effect immediately after you purchase it.

For more information about Anti-DDoS Origin, see [What is Anti-DDoS Origin?](#).

- Anti-DDoS Pro and Anti-DDoS Premium

We recommend that you use Anti-DDoS Pro or Anti-DDoS Premium to protect against volumetric DDoS attacks.

For more information about Anti-DDoS Pro and Anti-DDoS Premium, see [What are Anti-DDoS Pro and Anti-DDoS Premium?](#).

- Game Shield

Game Shield is an industry solution proposed for the common DDoS attacks and HTTP flood attacks that occur in the gaming industry. Compared with Anti-DDoS Pro and Anti-DDoS Premium, Game Shield provides better protection at a lower cost.

For more information about Game Shield, see [What is Game Shield](#).

Cautions

DDoS attacks have become a major concern due to their wide-range of impacts. DDoS attacks on Internet Service Providers (ISPs) can impact downstream customers.

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

- Do not establish a DDoS mitigation platform by using Alibaba Cloud services.
- Do not release instances for which blackhole filtering is triggered.
- Do not continuously replace, unbind, or add IP addresses, such as SLB IP addresses, Elastic IP addresses, or NAT gateway addresses to servers for which blackhole filtering is triggered.
- Do not establish an IP address pool or allocate attack traffic over a large number of IP addresses to defend against attacks.
- Do not use non-dedicated security services, such as CDN and OSS, to protect servers that are vulnerable to attacks.
- Do not bypass the security rules by using multiple accounts.

3. Blackhole filtering policy of Alibaba Cloud

If DDoS attacks occur on an Alibaba Cloud asset that uses a public IP address and the volume of the DDoS attacks exceeds the mitigation capability provided for the asset, blackhole filtering is triggered. Blackhole filtering is used to block all inbound Internet traffic that is destined for the public IP address and protects the asset against subsequent attacks. This topic describes the blackhole filtering policy of Alibaba Cloud and how to handle and prevent blackhole filtering.

What is blackhole filtering?

If volumetric DDoS attacks occur on an Alibaba Cloud asset that uses a public IP address and the peak attack bandwidth exceeds the mitigation capability provided for the asset, blackhole filtering is triggered for the IP address. The peak attack bandwidth is measured in bit/s.

If blackhole filtering is triggered, all inbound Internet traffic that is destined for the IP address is temporarily blocked. The IP address cannot be accessed over the Internet. Blackhole filtering protects the asset against subsequent attacks and prevents other assets from being affected by the attacked IP address. During blackhole filtering, Alibaba Cloud continuously monitors the status of DDoS attacks. A period of time after the DDoS attacks stop, Alibaba Cloud automatically deactivates blackhole filtering for the asset. Then, the asset can be accessed over the Internet. You can manually deactivate blackhole filtering before the DDoS attacks stop.

Why is blackhole filtering required?

If DDoS attacks occur on an asset that uses a public IP address, you can use blackhole filtering to protect the asset against subsequent attacks. DDoS attacks exhaust the resources of the attacked asset and affect other assets. You can use blackhole filtering to protect the asset against subsequent attacks.

What do I do if blackhole filtering is triggered?

If blackhole filtering is triggered for your asset, it indicates that your asset cannot defend against the current DDoS attacks. To resolve this issue, we recommend that you use one of the following methods:

- (Recommended) Improve the DDoS mitigation capability for your asset

You can purchase an [Anti-DDoS](#) instance to improve the traffic scrubbing capability and deploy the Anti-DDoS instance at the edge of the Alibaba Cloud network to protect your asset. The Alibaba Cloud network is the networking infrastructure of Alibaba Cloud. For more information, see [How do I prevent blackhole filtering from being triggered?](#).

- Wait for Alibaba Cloud to automatically deactivate blackhole filtering

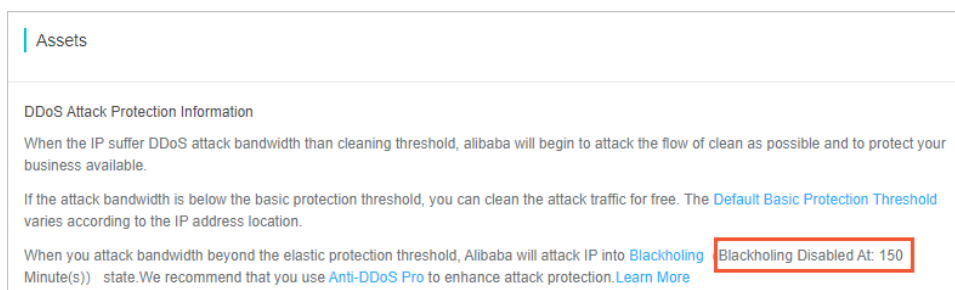
Alibaba Cloud monitors the status of DDoS attacks on your asset and automatically deactivates blackhole filtering for your asset a period of time after the DDoS attacks stop. Then, the asset can be accessed over the Internet. By default, Alibaba Cloud automatically deactivates blackhole filtering 2.5 hours after the DDoS attacks stop. In actual scenarios, Alibaba Cloud automatically deactivates blackhole filtering 30 minutes to 24 hours after the DDoS attacks stop. The period of time varies based on the frequency at which your asset is attacked. In rare cases, the period of time exceeds 24 hours. The duration of blackhole filtering varies based on the following factors:

- The duration of attacks. If attacks continue for a long time, the duration of blackhole filtering is extended.

- The frequency of attacks. If an asset experiences attacks for the first time, the duration of blackhole filtering automatically decreases. If an asset experiences frequent attacks, the asset has a high probability to encounter continuous attacks, and the duration of blackhole filtering is automatically extended.

Note If blackhole filtering is frequently triggered for an asset, Alibaba Cloud reserves the right to further extend the duration of blackhole filtering and lower the threshold to trigger blackhole filtering for the asset. You can view the actual duration and threshold of blackhole filtering in the console.

You can view the time when blackhole filtering is automatically deactivated for your asset, such as an Elastic Compute Service (ECS) instance, a Server Load Balancer (SLB) instance, an elastic IP address (EIP), or a simple application server, on the **Assets** page of the . For more information, see [View the duration of blackhole filtering](#).



● Manually deactivate blackhole filtering

If you want to recover your service during blackhole filtering, you can manually deactivate blackhole filtering. If you deactivate blackhole filtering, you can deploy a mitigation plan within a specific period of time. However, DDoS attacks cannot be mitigated. After you manually deactivate blackhole filtering, blackhole filtering may be triggered again if the DDoS attacks do not stop.

The following table describes the methods to deactivate blackhole filtering in different Anti-DDoS services.

Anti-DDoS service	Method to deactivate blackhole filtering	Limit
Anti-DDoS Origin Basic (Anti-DDoS instances are not purchased.)	<p>On the Overview page of the , click Handle Now in the Real-time Attack Detection section to deactivate blackhole filtering for the IP addresses that are attacked.</p> <p>Note If blackhole filtering is triggered for your ECS instance, you can change the public IP address of your ECS instance or resolve the domain name of your website service to an SLB instance. For more information, see Change the public IP address of an instance.</p>	You can deactivate blackhole filtering for your asset that is protected by an Anti-DDoS Origin Basic instance for a specific number of times per month. For more information, see the information that is displayed in the Handle Now panel.

Anti-DDoS service	Method to deactivate blackhole filtering	Limit
Anti-DDoS Origin Enterprise	<ul style="list-style-type: none"> In the console, choose Network Security > Anti-DDoS Origin > Manage Instances. On the page that appears, find the attacked IP address and click Deactivate Black Hole in the Actions column. The IP address must be protected by an Anti-DDoS Origin Enterprise instance. For more information, see Deactivate blackhole filtering. Call the DeleteBlackhole operation of the Anti-DDoS Origin API to deactivate blackhole filtering. For more information, see Make API requests. 	You can deactivate blackhole filtering for your asset that is protected by an Anti-DDoS Origin Enterprise instance for a specific number of times per month. The number of times is greater than or equal to the number of the IP addresses that can be protected by the instance.
Anti-DDoS Pro	<ul style="list-style-type: none"> In the console, choose Mitigation Settings > General Policies. On the page that appears, use the Deactivate Blackhole Status feature that is displayed on the Protection for Infrastructure tab to manually deactivate blackhole filtering. For more information, see Deactivate blackhole filtering. Call the ModifyBlackholeStatus operation of the Anti-DDoS Pro API to deactivate blackhole filtering. For more information, see Make API requests. 	<ul style="list-style-type: none"> After blackhole filtering is triggered, you must wait for at least 2 minutes before you can deactivate the blackhole filtering. You can deactivate blackhole filtering for your asset that is protected by an Anti-DDoS Pro instance up to five times per day.
Anti-DDoS Premium	You cannot manually deactivate blackhole filtering for your asset that is protected by an Anti-DDoS Premium instance.	None.

How do I prevent blackhole filtering from being triggered?

If the peak attack bandwidth of the DDoS attacks exceeds the mitigation capability provided for your asset, blackhole filtering is triggered. A higher mitigation capability lowers the possibility of blackhole filtering. To prevent blackhole filtering from being triggered, you must improve the mitigation capability (blackhole filtering threshold) for your asset.

You can use one of the following methods to improve the mitigation capability for your asset:

- Use Anti-DDoS Origin Basic free of charge

Anti-DDoS Origin Basic provides a basic mitigation capability of up to 5 Gbit/s against DDoS attacks for Alibaba Cloud assets free of charge. In this case, the assets refer to the assets that use public IP addresses. The basic mitigation capability for assets varies based on the specifications of the assets and the regions to which the assets belong. For more information, see [View black hole triggering thresholds in Anti-DDoS Origin Basic](#).

Alibaba Cloud can also increase your blackhole filtering threshold based on your security credit score. The security credit score is calculated by Security Credibility. The security credit score is not fixed. You can improve your security credit score to obtain a higher mitigation capability free of charge. To improve your security credit score, you can control the exposure of your asset.

Security Credibility determines the blackhole filtering threshold based on multiple factors. Security Credibility improves the mitigation capability against the first DDoS attack for users who have a qualified security credit score. The blackhole filtering threshold is adjusted as the security credit score changes. Security Credibility does not guarantee a fixed mitigation capability. For more information, see [Security Credibility](#).

- Deploy an Anti-DDoS instance of a paid edition
 - Purchase an [Anti-DDoS Origin Enterprise](#) instance to enable [best effort protection](#) without the need to change your service IP address.
 - Purchase an [Anti-DDoS Pro](#) or [Anti-DDoS Premium](#) instance and switch your service traffic to the IP address of the instance. This way, you can obtain up to Tbit/s of mitigation capabilities. Anti-DDoS Pro and Anti-DDoS Premium guarantee a committed mitigation capability and defense effect.

For more information about scenario-specific anti-DDoS solutions, see [Scenario-specific anti-DDoS solutions](#).

Can I use ACLs to mitigate DDoS attacks and prevent blackhole filtering from being triggered?

No, you cannot use access control lists (ACLs) to mitigate DDoS attacks and prevent blackhole filtering from being triggered. ACLs take effect only when attacks reach the edge of the Alibaba Cloud network in which your server resides. ACLs cannot mitigate DDoS attacks that are initiated from multiple botnets and destined for your server. When the DDoS attacks reach the edge of the Alibaba Cloud network in which your server resides, the volume of attacks far exceeds the mitigation capability of the ACLs. To mitigate the DDoS attacks, you must deploy mitigation policies at the edge of an Internet service provider (ISP) backbone network.

You can use traffic analysis and filtering methods together with sufficient network bandwidth to scrub attack traffic. If you want to expand the network bandwidth of your server to the bandwidth of the attack traffic and deploy a scrubbing center to scrub the attack traffic, the costs generated by bandwidth expansion and the servers used for traffic scrubbing can be excessively high. If each user deploys a scrubbing center, the overall mitigation costs significantly increase.

In this case, a cost-effective DDoS mitigation plan is provided. Cloud service providers offer large network bandwidths and deploy scrubbing centers at their ISP backbone networks. DDoS attacks are scrubbed in the scrubbing center closest to the location where the attacks are initiated. The cloud service providers offer the Software-as-a-Service (SaaS)-based anti-DDoS services for users to purchase. This way, the scrubbing centers can be repeatedly used, and the costs for each user are reduced.

4. View black hole triggering thresholds in Anti-DDoS Origin Basic

The following table lists the default thresholds at which Anti-DDoS Origin Basic automatically triggers black holes in each region. These thresholds are measured in bit/s.

Note


- Anti-DDoS Origin Basic automatically trigger black holes for Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, elastic IP addresses (EIPs), and Web Application Firewall (WAF) instances. This feature is available for IPv4 networks in all regions and for IPv6 networks only in specific regions. In the following table, a check sign (✓) in the Support IPv6 column indicates that the automatic black hole triggering feature is supported for IPv6 traffic in the region and the thresholds are applicable to both IPv4 and IPv6 networks. A cross sign (×) indicates that the feature is not supported for IPv6 traffic in the region and the thresholds are applicable only to IPv4 networks.
- In practice, black hole triggering thresholds for ECS instances, SLB instances, and EIPs vary based on the instance type and bandwidth that you purchase. For more information, go to the [Assets](#) page of the Anti-DDoS console for more details. For more information, see [Assets](#).
- In each region, the same threshold to trigger black holes is applied to WAF instances, SLB instances, and EIPs.

Region	Support IPv4	Support IPv6	ECS instance with one vCPU	ECS instance with two vCPUs	ECS instance with more than four vCPUs	SLB instance, EIP (includes public IP addresses of NAT gateways), and WAF instance
China (Hangzhou)	✓	✓	500 MB	1 GB	5 GB	5 GB
China (Shanghai)	✓	✓	500 MB	1 GB	2 GB	2 GB
China (Qingdao)	✓	×	500 MB	1 GB	5 GB	5 GB
China (Beijing)	✓	✓	500 MB	1 GB	2 GB	2 GB
China (Zhangjiakou-Beijing Winter Olympics)	✓	✓	500 MB	1 GB	2 GB	2 GB
China (Hohhot)	✓	✓	500 MB	1 GB	2 GB	2 GB

Region	Support IPv4	Support IPv6	ECS instance with one vCPU	ECS instance with two vCPUs	ECS instance with more than four vCPUs	SLB instance, EIP (includes public IP addresses of NAT gateways), and WAF instance
China (Shenzhen)	√	√	500 MB	1 GB	2 GB	2 GB
China (Heyuan)	√	√	500 MB	1 GB	2 GB	2 GB
China (Chengdu)	√	×	500 MB	1 GB	2 GB	2 GB
China (Hong Kong)	√	√	500 MB	500 MB	500 MB	500 MB
Singapore (Singapore)	√	×	500 MB	500 MB	500 MB	500 MB
Australia (Sydney)	√	×	500 MB	500 MB	500 MB	500 MB
Malaysia (Kuala Lumpur)	√	×	500 MB	500 MB	500 MB	500 MB
Indonesia (Jakarta)	√	×	500 MB	500 MB	500 MB	500 MB
Japan (Tokyo)	√	×	500 MB	500 MB	500 MB	500 MB
Germany (Frankfurt)	√	×	500 MB	500 MB	500 MB	500 MB
UK (London)	√	×	500 MB	500 MB	500 MB	500 MB
US (Silicon Valley)	√	×	500 MB	1 GB	2 GB	2 GB
US (Virginia)	√	×	500 MB	500 MB	500 MB	500 MB
India (Mumbai)	√	×	500 MB	1 GB	1 GB	1 GB
UAE (Dubai)	√	×	500 MB	500 MB	500 MB	500 MB

The default black hole duration is 2.5 hours. During this period, blackholing is enabled and cannot be disabled. The actual black hole duration changes based on the type of attack, ranging from 30 minutes to 24 hours. The duration of a black hole changes based on the following factors:

- The duration of attacks. If attacks continue, the black hole duration is extended. The next black hole duration is set to zero and starts at the time when the last black hole duration is extended.
- The frequency of attacks. If an asset experiences attacks for the first time, the black hole duration automatically decreases. Otherwise, assets that experience frequent attacks have a high probability to encounter continuous attacks. In such cases, the black hole duration is automatically extended.

 **Note** If an asset triggers black holes too often, Alibaba Cloud reserves the right to extend the black hole duration and decrease the black hole threshold for the asset. The actual black hole triggering threshold and black hole duration are displayed in the Anti-DDoS console.

5. Terms

Anti-DDoS Origin Basic provides basic protection against DDoS attacks. By default, Anti-DDoS Origin Basic is enabled for Alibaba Cloud resources that support Internet access, such as Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and elastic IP addresses (EIPs), regardless of whether they are deployed in the classic network or virtual private clouds (VPCs). If the volume of Internet traffic destined for an IP address exceeds the specified scrubbing threshold, Anti-DDoS starts to scrub the traffic to ensure the availability of your service. If the traffic volume exceeds the maximum protection threshold, blackhole filtering is triggered. All Internet traffic to the IP address is temporarily blocked.


traffic scrubbing

Anti-DDoS redirects traffic to a scrubbing device. The scrubbing device checks whether the traffic from specific IP addresses is normal and denies abnormal traffic. In addition, Anti-DDoS limits the volume of traffic destined for your server to mitigate damages. However, this may bring adverse impacts on normal traffic.

blackhole filtering

If an ECS instance suffers from volumetric attacks and the traffic exceeds the maximum protection threshold of Anti-DDoS Origin Basic, blackhole filtering is triggered. When blackhole filtering is triggered for an ECS instance, all Internet traffic to the instance is blocked for a specific period of time. This period varies based on the attack status. The maximum protection threshold varies based on the region and vCPU configuration of the ECS instance. For more information, see [View black hole triggering thresholds in Anti-DDoS Origin Basic](#). The following content describes basic information about blackhole filtering:

- Condition to trigger blackhole filtering: The attack traffic on an ECS instance exceeds the maximum protection threshold of Anti-DDoS Origin Basic.
- Duration: 30 minutes to 24 hours. The duration varies based on the attack status and the region where the protected resource resides.

 **Note** The blackhole filtering duration and blackhole triggering threshold are automatically adjusted based on the security credibility level of your Alibaba Cloud account. A higher security credibility level indicates a shorter blackhole filtering duration and a higher blackhole triggering threshold.

After blackhole filtering stops, Anti-DDoS automatically starts traffic scrubbing to check whether the attacks still continue. If yes, blackhole filtering is triggered again. If no, the Internet access is restored. If the traffic of attacks is overwhelmingly large, it may affect the network stability of Alibaba Cloud data centers. Blackhole filtering cannot be manually stopped in Anti-DDoS Origin Basic.

If you want to immediately restore the Internet access, we recommend that you purchase an [Anti-DDoS Pro](#) or [Anti-DDoS Premium](#) instance.

Anti-DDoS Pro and Anti-DDoS Premium are value-added security services. They protect resources on Alibaba Cloud against volumetric DDoS attacks. You can redirect attack traffic to the IP address that you purchase for Anti-DDoS Pro or Anti-DDoS Premium. This ensures stability and reliability of your origin server.

unlimited protection

Unlimited protection is provided by Anti-DDoS Origin Enterprise. The feature provides best-effort protection against DDoS attacks based on the network configuration and resource usage of the local anti-DDoS scrubbing center. The capability of unlimited protection is upgraded as the overall network capacity of Alibaba Cloud increases. You do not need to pay additional fees. For more information, see [Billing methods of Anti-DDoS Origin](#).

burstable protection

Burstable protection is provided by Anti-DDoS Pro of the Professional plan. You can configure the burstable protection bandwidth to defend against extra attack traffic that exceeds the basic protection bandwidth. If the volume of DDoS attacks exceeds the basic protection bandwidth but is smaller than the burstable protection bandwidth, burstable protection is triggered. You are charged additional fees on the day when burstable protection is triggered. For more information, see [Billing methods of Anti-DDoS Pro](#).

advanced mitigation

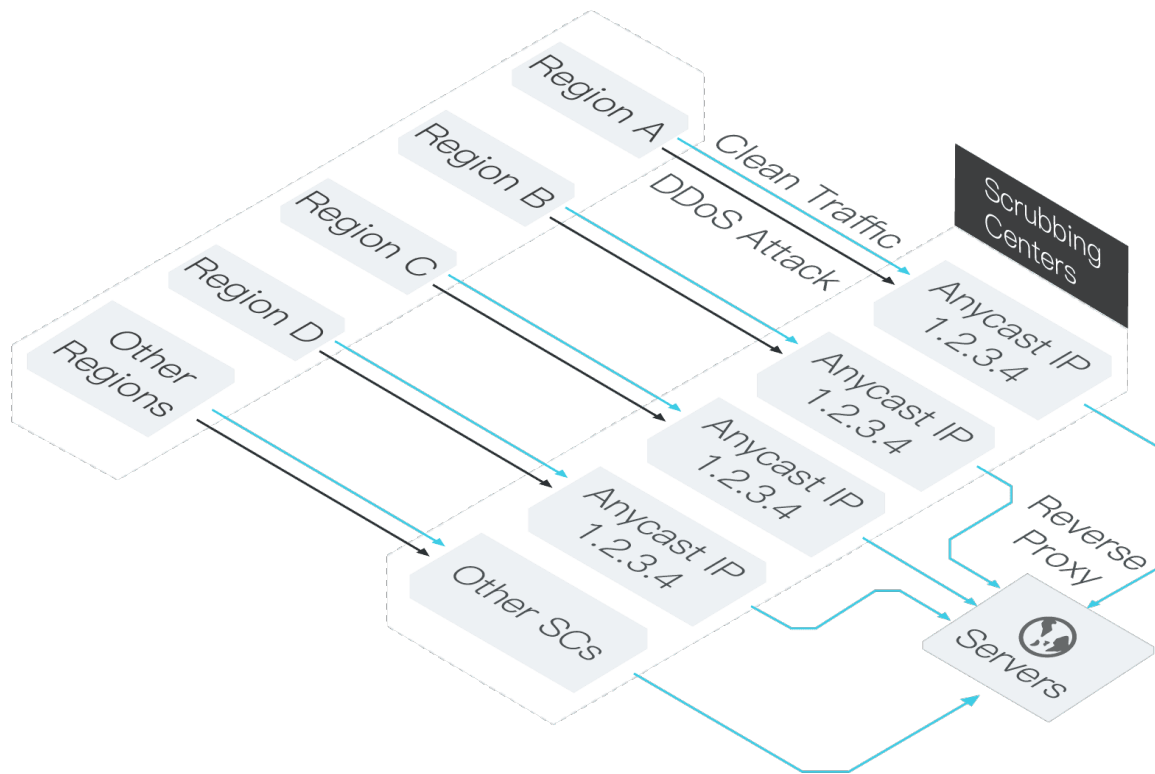
Advanced mitigation is provided by Anti-DDoS Premium of the Insurance or Unlimited mitigation plan. Advanced mitigation leverages anti-DDoS scrubbing centers of Alibaba Cloud outside mainland China to protect your resources against DDoS attacks. For more information, see [Billing methods of the Insurance and Unlimited mitigation plans](#).

anycast

Anti-DDoS Premium uses the anycast method to forward DDoS attack traffic to the nearest anti-DDoS scrubbing centers of Alibaba Cloud around the world.

Anycast is a network addressing and routing method. Packets that are destined for an anycast IP address can be routed to a specific group of hosts identified by the anycast IP address.

Anti-DDoS Premium uses the anycast method to route access traffic to the nearest anti-DDoS scrubbing center that has protection capabilities. This way, Anti-DDoS Premium can provide efficient traffic scrubbing and burstable protection even if requests are highly concurrent and the network is congested.



Traffic that reaches the anycast IP address can be routed to multiple data centers. When access traffic arrives at the anycast IP address, the traffic is forwarded to different data centers based on configured traffic forwarding rules. In most cases, the access traffic is forwarded to the data center nearest to the traffic source.

Assume that the anycast IP address of an Anti-DDoS Premium instance is 170.x.x.x. All anti-DDoS scrubbing centers of Alibaba Cloud outside China advertise routes to this IP address. When data packets are sent to this IP address, the data packets are forwarded to the anti-DDoS scrubbing center through a route with the least hops. When a server in an anti-DDoS scrubbing center becomes unavailable, all scrubbing centers immediately advertise that this IP address is unavailable, and data packets are routed to the nearest anti-DDoS scrubbing center excluding this one.

By default, traffic from Hong Kong (China) is routed to the anti-DDoS scrubbing center of Alibaba Cloud in Hong Kong (China).