ALIBABA CLOUD

Alibaba Cloud

Anti-DDoS

Product Introduction on Alibaba DDoS Protection

Document Version: 20201026

Alibaba Cloud

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**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Overview

Alibaba Cloud provides you with various anti-DDoS solutions. You can select an appropriate solution based on your business needs. This topic describes the anti-DDoS solutions and application scenarios.

The anti-DDoS solutions include Anti-DDoS Origin Basic, Anti-DDoS Origin Enterprise, Anti-DDoS Pro, Anti-DDoS Premium, and GameShield. Anti-DDoS Origin Basic is provided free of charge. The following table describes these solutions.

> **Note** If you want a customized security solution, contact pre-sales customer service to consult Alibaba Cloud security architects.

Solution	Overview	Scenario	Protection capability
Anti-DDoS Origin Basic	Anti-DDoS Origin Basic can defend against up to 5 Gbit/s of DDoS attacks free of charge for public IP addresses of Alibaba Cloud services, such as ECS, SLB, WAF, and EIP.	Business that has basic requirements on security. Anti-DDoS Origin Basic is automatically enabled after you purchase an Alibaba Cloud service. We recommend that you use other security solutions for additional protection if your business requires high security.	The maximum protection capability is 5 Gbit/s. For more information, see Editions.
Anti-DDoS Origin Enterprise	Anti-DDoS Origin Enterprise improves the protection capability for Alibaba Cloud services, such as ECS, SLB, WAF, and EIP. You can apply the protection capability of Anti-DDoS Origin Enterprise to Alibaba Cloud services with a simple configuration.	• Business that is latency-sensitive, such as online videos and live Q&A. • Business whose ports, domain names, and IP addresses are frequently attacked.	Anti-DDoS Origin Enterprise supports unlimited protection. For more information, see unlimited protection.

Solution	Overview	Scenario	Protection capability
Anti-DDoS Pro and Anti-DDoS Premium	Anti-DDoS Pro and Anti-DDoS Premium protect servers on the Internet against volumetric DDoS attacks. These servers may be deployed on Alibaba Cloud or provided by a third party. After the configuration, you can forward your business traffic to Anti-DDoS Pro or Anti-DDoS Premium for scrubbing. Only normal traffic is forwarded to the origin server. This ensures the stability and reliability of the origin server.	• Financial, e-commerce, and portal websites. • Internet egresses of government networks, portals, and open platforms. • Important live streaming and sales promotions. • Business that encounters attacks and blackmailing from competitors. • Mobile apps that encounter spam user registration, brushing, and fraudulent traffic.	• Anti-DDoS Pro supports burstable protection. For more information, see burstable protection. • Anti-DDoS Premium supports advanced protection. For more information, see advanced mitigation.
GameShield	GameShield protects against DDoS and HTTP flood attacks in the gaming industry. The same as Anti-DDoS Pro or Anti-DDoS Premium, GameShield can defend against Tbit/s of DDoS attacks. It can also defend against TCP-based HTTP flood attacks that are specific to the gaming industry.	• Gaming business that encounters heavy-traffic bandwidth suppression. • Gaming business that encounters attacks from a large number of zombies over a long period of time.	GameShield provides Tbit/s of protection capability.

2.Anti-DDoS Origin

2.1. What is Anti-DDoS Origin?

Anti-DDoS Origin is a protection service that improves protection capacity against DDoS attacks for resources. These resources include Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, elastic IP addresses (EIPs), and Web Application Firewall (WAF) instances. Anti-DDoS Origin directly protects cloud services and imposes no limits, which is different from Anti-DDoS Pro and Anti-DDoS Premium. You do not need to change the IP addresses of the resources that you want to protect. You do not need to consider the limits on the number of Layer-4 ports and the number of Layer-7 domain names. Anti-DDoS Origin is easy to deploy. You only need to bind the IP address of a resource that you want to protect with Anti-DDoS Origin. The protection for the resource only requires a few minutes to take effect.

Limits

Anti-DDoS Origin Enterprise instances are available only in mainland China. If you want to purchase an Anti-DDoS Origin Enterprise instance outside mainland China, you must submit a submit a ticket or contact sales personnel. After the request is approved, you can purchase an Anti-DDoS Origin Enterprise instance.

How Anti-DDoS Origin works

Anti-DDoS Origin protects the public IP addresses of Alibaba Cloud resources against Layer 3 and Layer 4 volumetric attacks. These resources include ECS instances, SLB instances, WAF instances, and EIPs. When the traffic exceeds the default scrubbing threshold that is predefined in Anti-DDoS Origin, traffic scrubbing is automatically triggered to mitigate DDoS attacks.

Anti-DDoS Origin adopts passive scrubbing as a major protection policy and active blocking as an auxiliary policy to mitigate DDoS attacks. It employs conventional technologies such as reverse detection, blacklist and whitelist, and packet compliance. These technologies allow protected resources to work normally under continuous attacks. Anti-DDoS Origin deploys a DDoS attack detection and scrubbing system at the egress of an Alibaba Cloud data center. This system is deployed in bypass mode.

Scenarios

Anti-DDoS Origin is suitable for applications that are deployed on Alibaba Cloud. It meets the requirements for you when your service scale is large and you are sensitive to network quality. You have low possibility of exposure to DDoS attacks. However, you may suffer significant economic losses if interruption or compromised response time of services occurs due to DDoS attacks. Anti-DDoS Origin allows you to improve protection capacity against DDoS attacks at a minimum cost. It also reduces the potential risk of DDoS attacks that target your services.

Anti-DDoS Origin is suitable for the following resources:

- Resources that resides on Alibaba Cloud.
- A large number of public IP addresses.
- Services that require high clean bandwidth or queries per second (QPS).
- IPv6-based inbound requests.

Editions

Anti-DDoS Origin provides two editions: Anti-DDoS Origin Basic and Anti-DDoS Origin Enterprise.

- Anti-DDoS Origin Basic provides basic protection against DDoS attacks for public IP addresses of Alibaba Cloud resources free of charge. Anti-DDoS Origin Basic provides protection capacity of no more than 5 Gbit/s. For more information, see View black hole triggering thresholds in Anit-DDoS Origin Basic.
- Anti-DDoS Origin Enterprise provides shared and unlimited protection for public IP addresses of Alibaba Cloud resources after you purchase an instance. Unlimited protection provides defense against DDoS attacks. The unlimited protection capacity is based on the total number of resources that reside in an anti-DDoS cluster. The unlimited protection capacity increases with the increase of the overall network capacity of Alibaba Cloud. The increased protection capacity is free of charge.
  - After you purchase an Anti-DDoS Origin Enterprise instance, the instance protects the public IP addresses of Alibaba Cloud resources. These resources include ECS instances, SLB instances, EIPs, and WAF instances.
  - Anti-DDoS Origin Enterprise mitigates DDoS attacks for servers in on-premises data centers outside China and cloud assets based on Classless Inter-Domain Routing (CIDR) blocks. It also provides on-demand Anti-DDoS Origin instances. You can contact sales personnel to purchase on-demand instances.

  For more information about the billing methods of Anti-DDoS Origin, see Billing methods of Anti-DDoS Origin.

Benefits

Anti-DDoS Origin provides the following benefits:

- Allows you to immediately use the service after you purchase an instance. Supports quick deployment within one minute. Anti-DDoS Origin directly protects your cloud services. This eliminates the need to deploy mitigation plans and switch IP addresses.
- Provides burstable protection capacity. When your assets experience volumetric DDoS attacks, Anti-DDoS Origin uses all resources that reside in a region to provide unlimited protection.
- Adopts Alibaba Cloud Border Gateway Protocol (BGP) bandwidth resources across different Internet Service Providers (ISPs). These ISPs include China Telecom, China Unicom, China Mobile, CERNET, and Great Wall Broadband. You can obtain fast access to the networks of these ISPs by using only one IP address.
- Provides protection bandwidth as required. This can ensure service continuity and security for big promotions, event releases, and important services.
- Supports protection capacity sharing among multiple IP addresses. This enhances protection capacity for multiple IP addresses.
- Protects IPv6 networks in multiple regions. For more information, see View black hole triggering thresholds in Anit-DDoS Origin Basic.

2.2. Scenarios

Anti-DDoS Origin Enterprise protects your resources against Layer 3 and Layer 4 traffic-based attacks. When the traffic exceeds the default scrubbing threshold that is predefined in Anti-DDoS Origin Enterprise, traffic scrubbing is automatically triggered to protect against distributed denial-of-service (DDoS) attacks.

Overview

Anti-DDoS Origin Enterprise is suitable for applications that are deployed on Alibaba Cloud. It meets the requirements for you when your business size is big and you are sensitive to network quality. You have low possibility of exposure to DDoS attacks. However, you may suffer significant economic losses if disruption or compromised response time of services occurs due to DDoS attacks. Anti-DDoS Origin Enterprise allows you to improve protection capacity against DDoS attacks at a minimum cost. It also reduces the potential risk of DDoS attacks that target your services. Anti-DDoS Origin Enterprise is suitable for the following resources:

- Resources that reside in Alibaba Cloud.
- A large number of public IP addresses.
- Services that require high business bandwidth or queries per second (QPS).
- IPv6-based incoming requests.

Evaluate applicability based on the attack type

The following table provides a list of DDoS attack types and indicates whether Anti-DDoS Origin Enterprise is suitable for each type.

Attack type	Applicable	Security specification (recommended)
Reflection attacks such as Simple Service Discovery Protocol (SSDP), Network Time Protocol (NTP), and Memcached attacks.	Yes	We recommend that you include a deployment method that integrates **Anti-DDoS Origin Enterprise, Server Load Balancer (SLB), and Elastic Compute Service (ECS)**. To obtain effective protection, you can use Server Load Balancer to drop inbound traffic from a port on which you do not configure a listener.
UDP flood attacks	Yes	
SYN flood attacks (large packets)	Yes	
SYN flood attacks (small packets)	Yes, but the protection is limited	We recommend that you use Anti-DDoS Pro and Anti-DDoS Premium.
Connection flood attacks	No	We recommend that you use Anti-DDoS Pro and Anti-DDoS Premium or GameShield.
HTTP flood attacks	No	While you are using Anti-DDoS Origin Enterprise to defend against traffic-based attacks, we recommend that you integrate **Anti-DDoS Origin Enterprise with Web Application Firewall (WAF)**. To obtain effective protection, you can use WAF to defend against HTTP flood attacks.
Web attacks	No	

Evaluate applicability based on the business type

The following table provides a list of business types and indicates whether Anti-DDoS Origin Enterprise is suitable for each business type.

Service type	Applicable	Security specification (recommended)
Websites	Yes	• If your websites may encounter DDoS attacks: We recommend that you include a deployment method that integrates **Anti-DDoS Origin Enterprise, Server Load Balancer (SLB), and Elastic Compute Service (ECS)**. To obtain effective protection, you can use Server Load Balancer to drop inbound traffic from a port on which you do not configure a listener. • If your websites may encounter DDoS attacks, HTTP flood attacks, or web attacks: While you are using Anti-DDoS Origin Enterprise to defend against traffic-based attacks, we recommend that you integrate **Anti-DDoS Origin Enterprise with Web Application Firewall (WAF)**. To obtain effective protection, you can use WAF to defend against HTTP flood attacks.
Games	No	We recommend that you use GameShield.
UDP-based services	No	We recommend that you use Anti-DDoS Pro and Anti-DDoS Premium or GameShield.
Apps	Yes	We recommend that you include a deployment method that integrates **Anti-DDoS Origin Enterprise, Server Load Balancer (SLB), and Elastic Compute Service (ECS)**. To obtain effective protection, you can use Server Load Balancer to drop inbound traffic from a port on which you do not configure a listener.

3.What are Anti-DDoS Pro and Anti-DDoS Premium?

Anti-DDoS Pro and Anti-DDoS Premium are proxy-based mitigation services provided by Alibaba Cloud to mitigate DDoS attacks. These services can be used to protect network servers against volumetric DDoS attacks. To protect servers against volumetric and resource exhaustion DDoS attacks, Anti-DDoS Pro and Anti-DDoS Premium forward traffic to the Alibaba Cloud anti-DDoS network by using DNS resolution.

How Anti-DDoS Pro and Anti-DDoS Premium work

You can connect your services to Anti-DDoS Pro or Anti-DDoS Premium by using domain names or ports. The domain names or service IP addresses are mapped to the IP or CNAME addresses of Anti-DDoS Pro or Anti-DDoS Premium instances based on the forwarding rules that you configured. This way, traffic is rerouted to the instances.

Inbound traffic passes through the anti-DDoS data center. In the traffic scrubbing center, malicious network traffic is filtered out, and normal network traffic is forwarded back to the origin server by using forwarding ports. This ensures stable access to the origin servers.

Anti-DDoS Pro and Anti-DDoS Premium

Alibaba Cloud provides the following two services based on the region where your servers are deployed:

- Anti-DDoS Pro: applies to scenarios in which your servers are deployed in **mainland China**. It uses eight Border Gateway Protocol (BGP) lines at the Tbit/s level to protect servers against volumetric DDoS attacks.
- Anti-DDoS Premium: applies to scenarios in which your servers are deployed **outside mainland China**. Backed by the world-leading distributed near-origin traffic scrubbing capabilities, Anti-DDoS Premium mitigates unlimited DDoS attacks.

For more information, see Differences between the features of Anti-DDoS Pro and Anti-DDoS Premium.

Benefits

Anti-DDoS Pro and Anti-DDoS Premium are more stable and easier to deploy than traditional DDoS mitigation solutions. These services rely on high-quality BGP networks and intelligent protection technologies to provide strong and precise protection with high availability.

- Easy deployment

  You can connect your services to Anti-DDoS Pro or Anti-DDoS Premium by using domain names or ports. The process requires up to five minutes. You do not need to install hardware or software or configure routers.

- Massive protection bandwidth

  Anti-DDoS Pro and Anti-DDoS Premium each can mitigate a minimum of 8 Tbit/s of DDoS attacks in mainland China, and a minimum of 2 Tbit/s outside mainland China. These services protect servers against DDoS attacks at the network layer, transport layer, and application layer.

- Precise protection

Anti-DDoS Pro and Anti-DDoS Premium provide precise protection against various attacks on transactions, encryption, Layer 7 applications, smart terminals, and online services.

- Intelligent protection

  Anti-DDoS Pro and Anti-DDoS Premium automatically optimize protection algorithms and learn service traffic baselines from the protection analysis of volumetric and resource exhaustion DDoS attacks. This enables the services to identify malicious IP addresses, and then scrub and filter out attack traffic.

- Burstable protection

  Anti-DDoS Pro and Anti-DDoS Premium support burstable protection. You can configure this feature in the Anti-DDoS Pro or Anti-DDoS Premium console. The settings take effect within seconds, and you do not need to install additional devices. Your services are not interrupted during the process. Therefore, you do not need to make any adjustments to your services.

- Origin server security ensured

  Anti-DDoS Pro and Anti-DDoS Premium hide the IP addresses of origin servers. This way, attackers cannot identify the address of your origin server. This increases the security of your origin server.

- Protection against volumetric DDoS attacks

  Volumetric DDoS attacks at the transport layer congest networks, leave data centers unavailable, and interrupt or paralyze your services. Based on technologies such as proxy, detection, rebound, authentication, blacklist and whitelist, and packet compliance, Anti-DDoS Pro and Anti-DDoS Premium employ IP reputation investigation, near-origin traffic scrubbing, and in-depth packet analysis of network fingerprints, user behavior, and content characteristics. These technologies block and filter out threats based on custom rules. This enables the protected services to provide external services even under sustained attacks.

- Protection against resource exhaustion DDoS attacks (HTTP flood attacks)

  Anti-DDoS Pro and Anti-DDoS Premium integrate intelligent protection engines to protect against resource exhaustion DDoS attacks when application-layer services are interrupted under attacks. These services also support URL-level threat filtering at custom frequencies to improve the protection success rate, protection efficiency, and work efficiency of O&M personnel. Intelligent protection engines provide effective protection by:

  - Learning your traffic to obtain traffic characteristics.
  - Dynamically generating normal service baselines.
  - Quickly discovering exceptions of traffic and characteristics.
  - Automatically participating in the analysis of attack characteristics.
  - Automatically generating a combination of multi-dimensional policies.
  - Dynamically executing or canceling protection policy instructions.

- Stability and high availability
  - Anti-DDoS Pro and Anti-DDoS Premium use high-availability network protection clusters to prevent single-point failure and redundancy. The processing capabilities of Anti-DDoS Pro and Anti-DDoS Premium can be scaled up. They also offer automated detection and attack policy matching to provide real-time protection and a scrubbing service availability of up to 99.99%.

  - Anti-DDoS Pro and Anti-DDoS Premium monitor the CPU and memory resources of all servers and the inbound traffic that is forwarded to the traffic scrubbing center. This ensures the availability of the data center. They also monitor the availability of server engines and have automatic offline and recovery mechanisms.
  - Anti-DDoS Pro and Anti-DDoS Premium monitor the availability of back-to-origin links and automatically switch to secondary links when primary links are unstable, which ensures link availability.
  - Anti-DDoS Pro and Anti-DDoS Premium perform health checks on protected origin servers. If an origin server is not running at optimal capacity, the service traffic is forwarded to another origin server. They also monitor the HTTP status codes of origin servers and initiate back-to-origin or switchover operations when errors are detected.

- Traffic rerouting

  Anti-DDoS Pro and Anti-DDoS Premium forward traffic based on cloud service-specific security events and DNS resolution. They enable DDoS mitigation for vulnerable cloud services by connecting these cloud services to themselves and disable DDoS mitigation for secure cloud services. You can customize the forwarding templates of Anti-DDoS Pro and Anti-DDoS Premium to automatically schedule DDoS mitigation based on the status of cloud services.

Scenarios

Anti-DDoS Pro and Anti-DDoS Premium are suitable for finance websites, e-commerce websites, portal websites, Internet egresses of government networks, portals, and open platforms. They provide DDoS mitigation for important live streaming and sales promotions. Anti-DDoS Pro and Anti-DDoS Premium protect against malicious attacks and ransom-driven attacks, and prevent mobile applications from spam user registration, brushing, and fraudulent traffic.

We recommend that you use Anti-DDoS Pro and Anti-DDoS Premium in the following scenarios when security risks occur in the preceding industries:

- Ransom-driven DDoS attacks occur.
- DDoS attacks make your services inaccessible, and urgent protection is required to recover your services.
- DDoS attacks frequently occur. Continuous protection against DDoS attacks is required to ensure service stability.

Differences between the features of Anti-DDoS Pro and Anti-DDoS Premium

The following table describes the features that are supported by Anti-DDoS Pro and Anti-DDoS Premium. The features that are not listed in the table are supported by both Anti-DDoS Pro and Anti-DDoS Premium.

> **Notice** The table allows you to distinguish between Anti-DDoS Pro and Anti-DDoS Premium. We recommend that you choose Anti-DDoS Pro for servers deployed in mainland China and Anti-DDoS Premium for servers deployed outside mainland China.

A check sign (√) indicates that the feature is supported and a cross sign (×) indicates that the feature is not supported.

Feature	Description	Anti-DDoS Pro	Anti-DDoS Premium	References
Instances - Mainland China Acceleration (MCA)	MCA must be used with Anti-DDoS Premium Insurance or Unlimited Plan. If your server is deployed outside mainland China, you can purchase an MCA instance to accelerate your services for users in mainland China.	×	√	Mainland China Acceleration billing methods Configure Anti-DDoS Premium MCA
Instances - Secured Mainland China Acceleration (Sec-MCA)	Anti-DDoS Premium supports Sec-MCA. This allows you to accelerate access from users in mainland China to services in regions outside mainland China.	×	√	Sec-MCA billing methods Configure Anti-DDoS Premium Sec-MCA
Instances - Global Advanced Mitigation	Global advanced mitigation must be used with Anti-DDoS Premium Insurance Plan that provides two advanced mitigation sessions. If the two advanced mitigation sessions are exhausted, you can purchase more global advanced mitigation sessions.	×	√	Billing methods for global advanced mitigation Purchase global advanced mitigation
Website Config - Enable HTTP/2	In the **Enter Site Information** step, you can add a domain name and turn on **Enable HTTP/2**.	√	×	Add a website
Website Config - Cname Reuse	In the **Enter Site Information** step, you can turn on **CNAME Reuse**.	×	√	CNAME reuse
Sec-traffic manager - Network Acceleration	You can select **Network Acceleration** when you add a rule on the **General** tab in the console.	×	√	Overview
Sec-Traffic Manager - Sec-MCA	You can select **Sec-MCA** when you add a rule on the **General** tab in the console.	×	√	Overview
Protection for Infrastructure - Diversion from Origin Server	The Diversion from Origin Server policy blocks network traffic transmitted from regions outside mainland China over China Telecom or China Unicom lines.	√	×	Configure diversion from the origin server

Feature	Description	Anti-DDoS Pro	Anti-DDoS Premium	References
Protection for infrastructure - Deactivate Blackhole Status	You can manually deactivate blackhole filtering in the console to recover services.	√	×	Deactivate blackhole filtering
Investigation - Operation Logs	You can view the logs of the last 30 days on the Operation Logs page.	√	×	Operation logs
Investigation - Adv. Mitigation Logs	You can view the logs of the last 30 days on the Adv. Mitigation Logs page.	×	√	Query advanced mitigation logs

DDoS cost protection

Anti-DDoS Pro and Anti-DDoS Premium support **DDoS cost protection**. These services safeguard against costs incurred due to the usage spikes on the protected Elastic Compute Service (ECS) or Server Load Balancer (SLB) instances caused by DDoS attacks. If the costs of any protected resources increase due to DDoS attacks, you can submit aticket to obtain a voucher.

4.Scenario-specific anti-DDoS solutions

Alibaba Cloud integrates advanced security technologies and years of experience in DDoS mitigation into a variety of commercial anti-DDoS solutions. You can select an anti-DDoS solution based on your service requirements. This topic describes how to select anti-DDoS solutions for different scenarios.

Scenarios

Scenario	Applicable scope	Description	Mitigation plan
High-risk DDoS attacks (Anti-DDoS Pro or Anti-DDoS Premium is recommended.)	• DDoS attacks occur on websites, Internet egresses of government networks, portals and open platforms, important live streaming activities, and sales promotions. These websites refer to financial, e-commerce, and portal websites. • Ransom-driven DDoS attacks occur. • DDoS attacks freeze your services and you want to recover your services at the earliest opportunity. • DDoS attacks frequently occur. Continuous protection against DDoS attacks is required to ensure service stability. • Mobile applications encounter spam user registration, brushing, and fraudulent traffic.	Anti-DDoS Pro and Anti-DDoS Premium can protect Alibaba Cloud Elastic Compute Service (ECS) instances and servers that are not deployed on Alibaba Cloud from volumetric DDoS attacks. They can route network traffic to the Alibaba Cloud global anti-DDoS network by using DNS resolution, scrub volumetric and resource exhaustion attack traffic, and hide the IP addresses of origin servers.	Select a mitigation plan for Anti-DDoS Pro or Anti-DDoS Premium based on the following descriptions: • Anti-DDoS Pro Profession: applies to scenarios in which your servers are deployed in mainland China and your services are provided to users who are located in mainland China. • Anti-DDoS Premium Insurance or Unlimited: applies to scenarios in which your servers are deployed outside mainland China and your services are provided to users who are located outside mainland China. • Anti-DDoS Premium MCA or Anti-DDoS Premium Sec-MCA: applies to scenarios in which your servers are deployed outside mainland China and your services are provided to users who are located in mainland China.

Scenario	Applicable scope	Description	Mitigation plan
Low-risk DDoS attacks on large-scale services (Anti-DDoS Origin is recommended.)	• Service resources are deployed on Alibaba Cloud. • Large-scale services are running. For example, the clean bandwidth is greater than 1 Gbit/s, and the queries per second (QPS) over HTTP and HTTPS is greater than 5,000. • A large number of public IP addresses need to be protected. • DDoS attacks occasionally occur. • IPv6-based inbound requests exist.	Anti-DDoS Origin improves the DDoS mitigation capabilities of Alibaba Cloud services. These services include ECS, Server Load Balancer (SLB), Web Application Firewall (WAF), and Elastic IP Address (EIP). Anti-DDoS Origin uses the native protection network of Alibaba Cloud to mitigate volumetric DDoS attacks without changing the IP addresses of origin servers.	Select a mitigation plan for Anti-DDoS Origin based on the following descriptions: • Anti-DDoS Origin Basic is activated by default. • Anti-DDoS Origin Basic mitigates DDoS attacks of up to 5 Gbit/s. If this mitigation capability is insufficient to meet your service requirements, we recommend that you use Anti-DDoS Origin Enterprise. ◦ Anti-DDoS Origin Enterprise and SLB: applies to scenarios in which you want to mitigate only DDoS attacks. In these scenarios, you can use SLB to discard traffic whose protocol and port are not specified in the SLB listener to improve protection capabilities. ◦ Anti-DDoS Origin Enterprise and WAF: applies to scenarios in which you want to mitigate DDoS attacks, web attacks, and HTTP flood attacks. In these scenarios, you can use WAF to mitigate HTTP flood attacks and Anti-DDoS Origin Enterprise to mitigate volumetric DDoS attacks to improve protection capabilities.

Scenario	Applicable scope	Description	Mitigation plan
DDoS attacks on mobile applications (GameShield is recommended.)	• Mobile gaming services are the main scenarios. • Services can integrate Alibaba Cloud SDKs. • Services require fine-grained protection for real-time data that is transmitted over custom transport protocols. • Services require accelerated network transmission. • Services require encrypted network transmission. • The sources of DDoS attacks need to be traced.	GameShield can mitigate volumetric DDoS attacks and HTTP flood attacks in the gaming industry. GameShield integrates the lightweight Alibaba Cloud Security SDKs to eliminate DDoS attacks, HTTP flood attacks, and TCP flood attacks that are specific to the gaming industry faced by mobile applications.	None.

Service types

Service type	Anti-DDoS Pro and Anti-DDoS Premium	Anti-DDoS Origin	GameShield
Websites	√	√	×
UDP-based services	√	×	√
Applications	√	√	×
Games	√	×	√ (Recommended)

DDoS attack types

Symbol description:

- √: indicates that mitigation is supported
- x: indicates that mitigation is not supported

Attack type	Anti-DDoS Pro and Anti-DDoS Premium	Anti-DDoS Origin	GameShield
Malformed packet attacks	√	√	√

Attack type	Anti-DDoS Pro and Anti-DDoS Premium	Anti-DDoS Origin	GameShield
Transport layer DDoS attacks	√	√ Anti-DDoS Origin can mitigate SYN flood attacks (packet fragment attacks), but the mitigation capability is limited. In this case, we recommend that you use Anti-DDoS Pro or Anti-DDoS Premium.	√
DNS DDoS attacks	√	× We recommend that you use WAF and Anti-DDoS Origin Enterprise.	×
Connection-based DDoS attacks	√	× We recommend that you use WAF and Anti-DDoS Origin Enterprise.	√
Application-layer attacks	√	× We recommend that you use WAF and Anti-DDoS Origin Enterprise.	×

5.Pre-sales FAQ

This topic provides answers to some commonly asked questions about pre-sales of Alibaba Cloud Anti-DDoS.

Does Alibaba Cloud Anti-DDoS provide free services?

Yes, Alibaba Cloud Anti-DDoS provides free services. Anti-DDoS Origin Basic is activated for every Alibaba Cloud user. Anti-DDoS Origin Basic mitigates DDoS attacks of up to 5 Gbit/s free of charge. You do not need to purchase, activate, or configure this service. For more information, see What is Anti-DDoS Origin?.

Alibaba Cloud does not provide unlimited protection free of charge. Bandwidth resources are essential to DDoS attack mitigation. Bandwidth usage takes the highest proportion in mitigation service billing. Alibaba Cloud pays for bandwidth resources provided by Internet Service Providers (ISPs), such as China Telecom, China Unicom, and China Mobile. The bandwidth costs include bandwidth charges incurred from mitigating DDoS attacks. Anti-DDoS Origin Basic mitigates DDoS attacks of up to 5 Gbit/s free of charge. When the volume of the DDoS attacks exceeds 5 Gbit/s, Anti-DDoS Origin Basic blocks all traffic to the victim to avoid additional mitigation fees.

Can Anti-DDoS Pro and Anti-DDoS Premium be billed only when they mitigate DDoS attacks?

No, Anti-DDoS Pro and Anti-DDoS Premium are still billed when they are not working. Anti-DDoS Pro and Anti-DDoS Premium are billed on a subscription basis. You must purchase Anti-DDoS Pro or Anti-DDoS Premium instances and complete the payment before you can use the instances to mitigate DDoS attacks. The protection takes effect for the duration of your subscription.

Does Anti-DDoS have trial mitigation plans?

- Anti-DDoS Origin: Anti-DDoS Origin Basic is a free mitigation plan and provides up to 5 Gbit/s protection for public IP addresses of Alibaba Cloud resources. Anti-DDoS Origin Enterprise is a paid mitigation plan and no free trial is provided.

> **Note** We recommend that you use Anti-DDoS Origin Basic to test the mitigation capability of Anti-DDoS Origin and then upgrade your service to Anti-DDoS Origin Enterprise. The upgrade process is completely transparent and does not affect your network and connections.

- Anti-DDoS Pro and Anti-DDoS Premium: Anti-DDoS Pro and Anti-DDoS Premium rely on dedicated data centers to provide traffic scrubbing services. This incurs high costs. No free trial is provided.

Can Anti-DDoS Pro and Anti-DDoS Premium protect servers that are not deployed on Alibaba Cloud?

Yes, Anti-DDoS Pro and Anti-DDoS Premium can protect servers that are not deployed on Alibaba Cloud and Alibaba Cloud Elastic Compute Service (ECS) instances from DDoS attacks. Anti-DDoS Pro and Anti-DDoS Premium instances redirect requests to origin servers over the Internet. Therefore, Anti-DDoS Pro and Anti-DDoS Premium instances can protect servers that are accessible over the Internet, such as servers deployed on Alibaba Cloud, servers that are deployed on third-party cloud platforms, and on-premises servers. For more information, see What are Anti-DDoS Pro and Anti-DDoS Premium?.

Can Anti-DDoS Pro and Anti-DDoS Premium protect servers that are not deployed on Alibaba Cloud but have domains registered with Alibaba Cloud?

Yes, Anti-DDoS Pro and Anti-DDoS Premium can protect servers that are not deployed on Alibaba Cloud but have domains registered with Alibaba Cloud. Both Anti-DDoS Pro and Anti-DDoS Premium provide DDoS mitigation for Alibaba Cloud ECS instances or servers that are not deployed on Alibaba Cloud. Anti-DDoS Pro and Anti-DDoS Premium also provide DDoS mitigation for domains that are registered by using Alibaba Cloud Domains or a third-party domain service.

Do I need to complete ICP filing for a domain before I can use Anti-DDoS Pro or Anti-DDoS Premium?

If you use Anti-DDoS Pro, you must complete Internet Content Provider (ICP) filing for the domain. If you use Anti-DDoS Premium, ICP filing is not required.

What are the regions supported by Anti-DDoS Pro and Anti-DDoS Premium?

- Anti-DDoS Pro: protects servers deployed in mainland China.
- Anti-DDoS Premium: protects servers deployed outside mainland China, including China (Hong Kong).

Do Anti-DDoS Pro and Anti-DDoS Premium have limits on the number of protected domains?

Yes, Anti-DDoS Pro and Anti-DDoS Premium have limits on the number of protected domains.

- By default, each Anti-DDoS Pro instance supports a maximum of 50 domains, only 5 of which can be second-level domains.
- By default, each Anti-DDoS Premium instance supports a maximum of 10 domains, only 1 of

which can be second-level domains.

> **Note** You can increase the number of domains when you purchase an Anti-DDoS Pro or Anti-DDoS Premium instance. Each Anti-DDoS Pro or Anti-DDoS Premium instance supports a maximum of 200 domains. For more information, see Purchase mitigation plans for Anti-DDoS Pro and Anti-DDoS Premium.

Do Anti-DDoS Pro and Anti-DDoS Premium support wildcard domains?

Yes, Anti-DDoS Pro and Anti-DDoS Premium support wildcard domains. You can add wildcard domains on the **Website Config** page. For more information, see Add a website.

A wildcard DNS record is specified by using an asterisk (*) as the leftmost part of a domain name. The record resolves all matching subdomains to the domain. For example, when you specify *.taobao.com as a DNS record, all subdomains that match *.taobao.com are resolved to www.taobao.com.

What are the prerequisites for activating Anti-DDoS Premium?

If you want to use Anti-DDoS Premium to protect a website, you must add the domain of the website to Anti-DDoS Premium. If you want to use Anti-DDoS Premium to protect a non-website service, you only need to add the service port to your Anti-DDoS Premium instance.

Does the basic protection bandwidth provided by Anti-DDoS Pro apply to all traffic or only attack traffic?

The basic protection bandwidth provided by an Anti-DDoS Pro instance is the guaranteed bandwidth for handling both normal and attack traffic of the workloads protected by the instance. All traffic must first pass through the Anti-DDoS traffic scrubbing centers. Attack traffic is filtered out, and only normal traffic is forwarded to the origin server.