Alibaba Cloud
Anti-DDoS Basic

Anti-DDoS Basic Service

Issue: 20181218

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 information, supplementary instructions, and other content that the user must understand.	 **Note:** 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]*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

1 Product Introduction

1.1 What is Anti-DDoS Basic

Anti-DDoS Basic is a free Distributed Denial of Service (DDoS) protection service that safeguards data and applications.

Anti-DDoS Basic prevents and mitigates DDoS attacks by routing traffic away from your infrastructure. This service guarantees availability and performance of your properties on Alibaba Cloud. It also provides enhanced visibility and control over your security. As a global service from Alibaba Cloud Security, Anti-DDoS Basic functions with 5Gbps capacity of DDoS mitigation against common DDoS attacks.

For more information, see the *Anti-DDoS Basic product details* page.

- Security credibility plan

  You can enjoy an extra DDoS mitigation capacity on top of the default offering based on your security credibility score.
- Extensive protection scenarios

  Anti-DDoS Basic defends against various DDoS attacks, including but not limited to ICMP flood, UDP flood, TCP flood, SYN flood, and ACK flood attacks.
- Scalable DDoS mitigation capacity

  By improving your credibility score, you can get more extra DDoS mitigation capacity.
- Shortened black hole duration

  With security credibility, the default black hole duration triggered by extreme attacks can be shortened, bringing your business back to life faster.
- Maintainable security credibility

  You can learn the scoring criteria of the security credibility score and take the initiative to improve it.

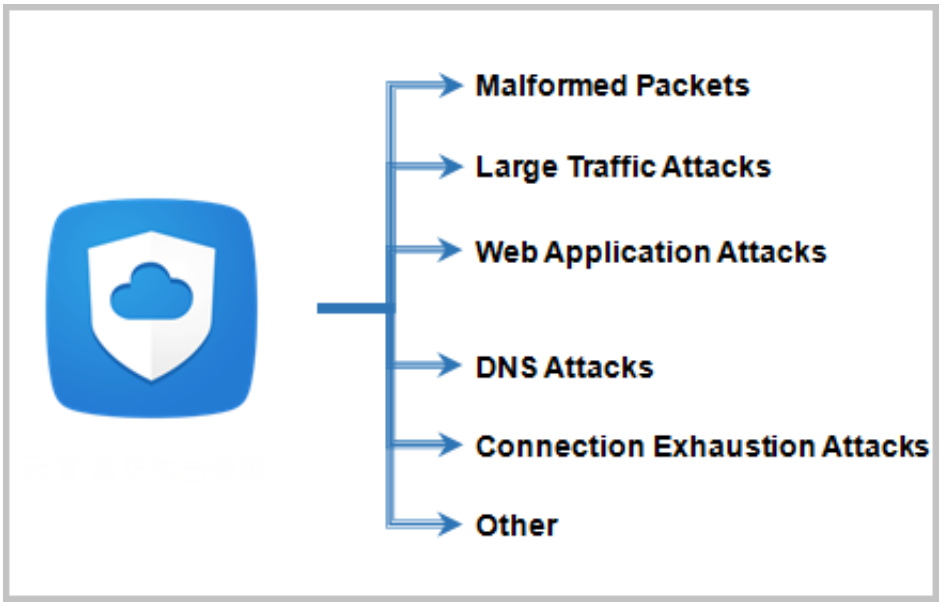
1.2 How Anti-DDoS Basic works

Anti-DDoS Basic currently supports BGP and DNS redirection technologies. Its dominant protection mode is passive cleansing, supplemented by active suppression. The service comprehensively manages DDoS attacks.

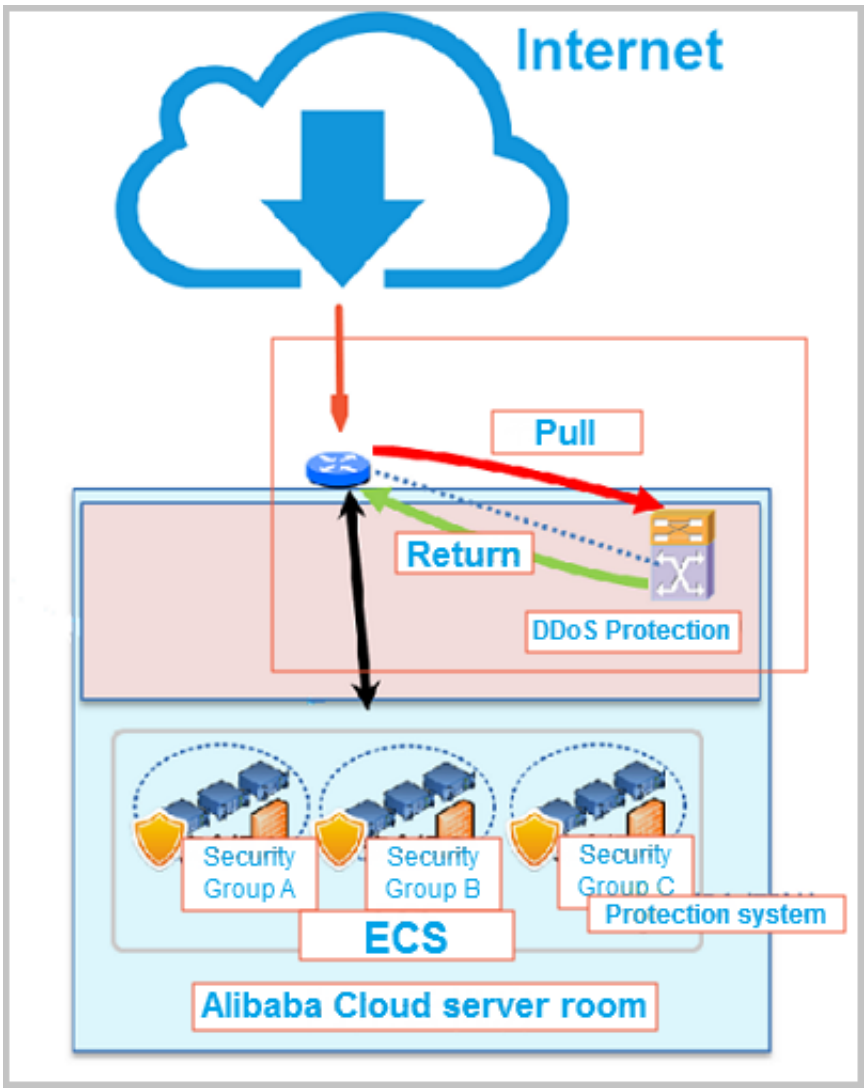
On the basis of conventional technologies, such as proxy, detection, rebound, authentication, black/white lists, and message compliance, Alibaba Cloud Anti-DDoS Basic also integrates web security and filtering, reputation analysis, Layer-7 application analysis, user behavior analysis, feature learning, defense and counter-work, and other technologies. This service can block and filter threats, and guarantees that the protected users are secured even during the attack.

The present Anti-DDoS system built by Alibaba Cloud offers T-level defense capacity. Meanwhile, Alibaba Cloud is also expanding its protection nodes in various regions.

Based on independently developed Alibaba Cloud Security, Alibaba Cloud offers anti-DDoS service to defend against Layer-3 to Layer-7 DDoS attacks such as SYN flood, UDP flood, ACK flood, ICMP flood, DNS Query flood, NTP Reply flood, and HTTP flood attacks. The attacks protected against by Anti-DDoS Basic service are listed in the following figure:



Anti-DDoS Basic builds DDoS attack detection and cleansing systems at the egress of Alibaba Cloud data centers and mainly adopts the bypass deployment architecture. The network topology of Anti-DDoS Basic service is illustrated as follows:



1.3 Features

Alibaba Cloud Security Anti-DDoS Basic service provides the following functions.

Type	Feature	Description
Attack protection	Malformed message filtering	Filters frag flood, smurf, stream flood , and land flood attacks.
Attack protection	Malformed message filtering	Filters malformed IP packets, TCP packets and UDP packets.
Attack protection	DDoS attack protection on transport layer	Filters syn flood, ack flood, udp flood , icmp flood, and rstflood attacks.
Management	Attack evidence collection	Captures abnormal traffic packets automatically.

Type	Feature	Description
Management	Attack event management	Supports management statistics about attack events and attack traffics.

1.4 Benefits

Alibaba Cloud Security Anti-DDoS Basic service provides you the following benefits.

Reliable network protection lines

- Stable access speed under DDoS attacks.
- Sufficient bandwidth guarantees no interference from other users.
- High quality bandwidth guarantees service availability and stability.

Precise protection

- Accurate identification of attacks and provides rapid protection.
- Cleaning equipment based on independent research and development algorithms guarantees a low false positive rate.
- No interaction between single point cleaning and multipoint cleaning.

Maintenance-free

- Eliminates the need to purchase expensive cleaning equipment.
- Enabled by default and set up automatically.
- Intelligent business learning and dynamic protection rules configuration.

Free of charge

- Anti-DDoS Basic is a free service.
- Offers more free protection bandwidth based on your security credibility in Alibaba Cloud.

1.5 Scenarios

Alibaba Cloud Anti-DDoS Basic applies to Internet DDoS attack protection.

Scope: Free DDoS attack protection for ECS, SLB, EIP, NAT and WAF services on Alibaba Cloud.

Limit: Scenarios that require no more than 5 GB DDoS attack protection.

2 Quick Start

2.1 Get started with Anti-DDoS Basic

Alibaba Cloud Anti-DDoS Basic is enabled and initialized by default with the creation of ECS, Server Load Balance, or EIP instances. This service provides a 5 Gbps mitigation capacity free of charge.

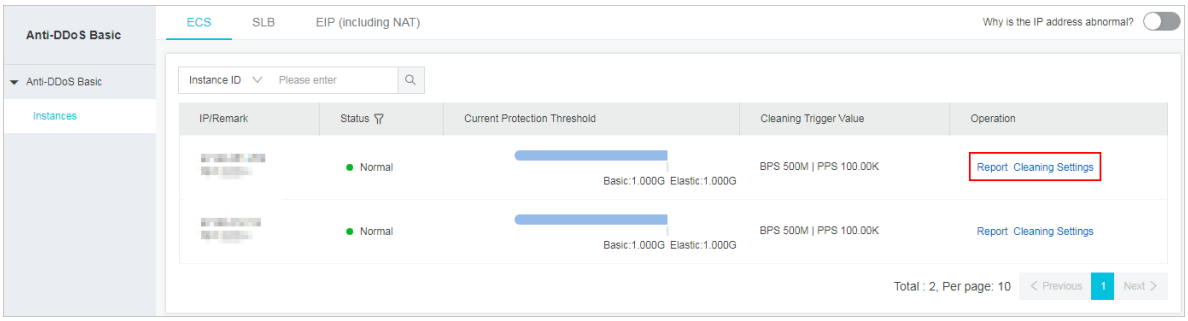
Context

In Alibaba Cloud Security Anti-DDoS Basic console, you can take the following operations:

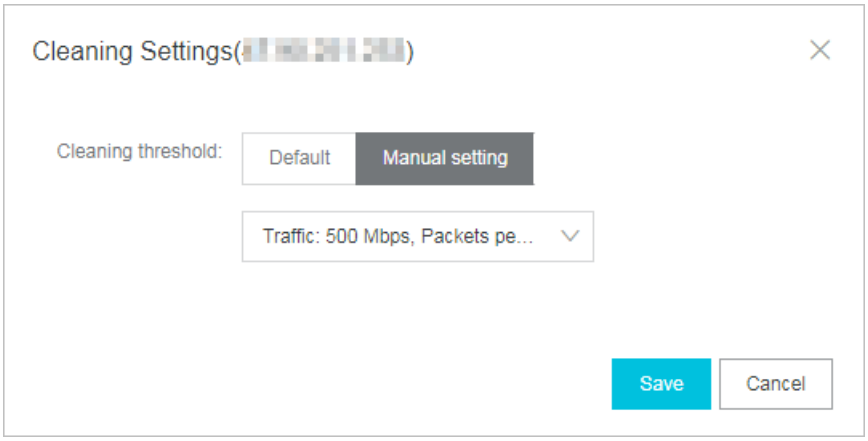
- Set **Cleaning Trigger Value**. When the IP suffers DDoS attack and the attack bandwidth exceeds the cleaning threshold, Alibaba starts to scrub the flow automatically to guarantee your business availability.
- Check **Protection Threshold**. The protection threshold consists of Basic protection threshold and Elastic protection threshold.
  - If the attack bandwidth is below the basic protection threshold, the attack traffic can be scrubbed for free. The *Default Basic Protection Threshold* varies according to the regions of your IP addresses.
  - When the attack bandwidth is between the basic protection threshold and the elastic protection threshold, the available protection traffic that Alibaba Cloud provides for free is consumed. The elastic protection threshold is determined by your IP address, traffic consumption, and security credibility. After all of the free-of-charge protection traffic is consumed, the protection threshold decreases to the basic protection threshold. *Learn more*.

Procedure

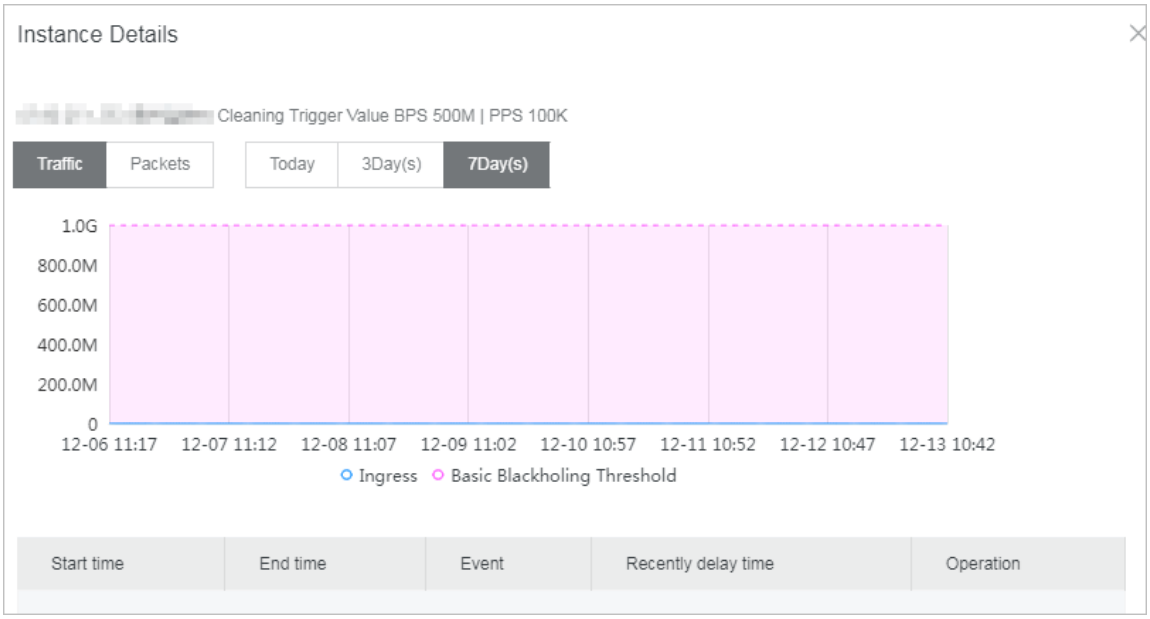
1. Log on to the *Anti-DDoS Basic console*.
2. Select a region.
3. On the **Anti-DDoS Basic** > **Instances**page, select the instance type tab: **ECS**, **SLB**, or **EIP(including NAT)**.
4. Select the instance, check the current Cleaning Trigger Value and Current Protection Threshold.



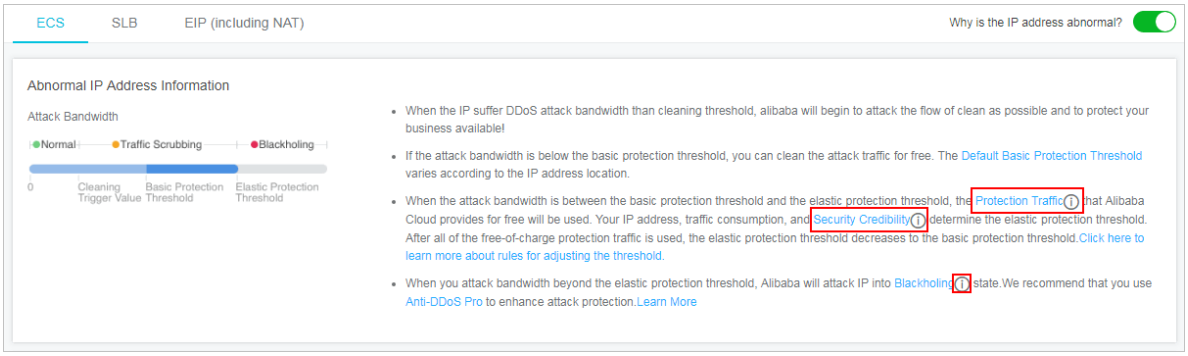
- Click **Cleaning Settings** to change the cleaning threshold mode to Default or Manual setting. For the Default mode, the system dynamically adjusts the cleaning threshold value based on traffic load. For the Manual setting mode, you can select the cleaning threshold value according to your business requirements.



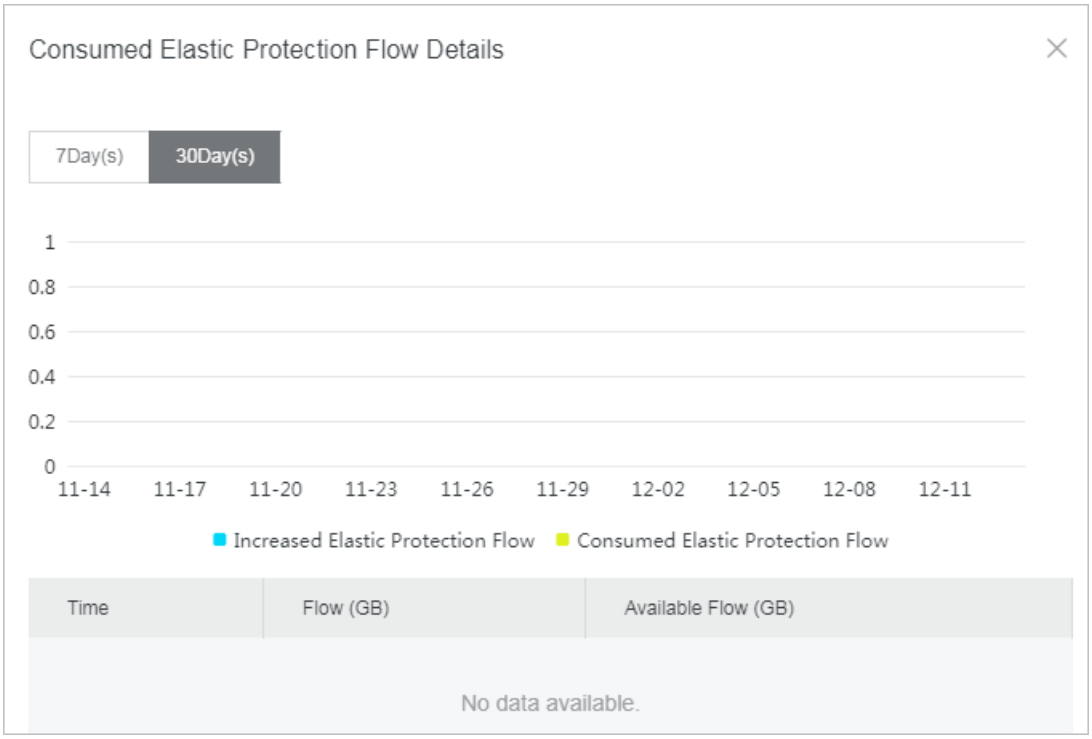
- Click **Report** to view the traffic and packets trend of this instance and the DDoS event details.



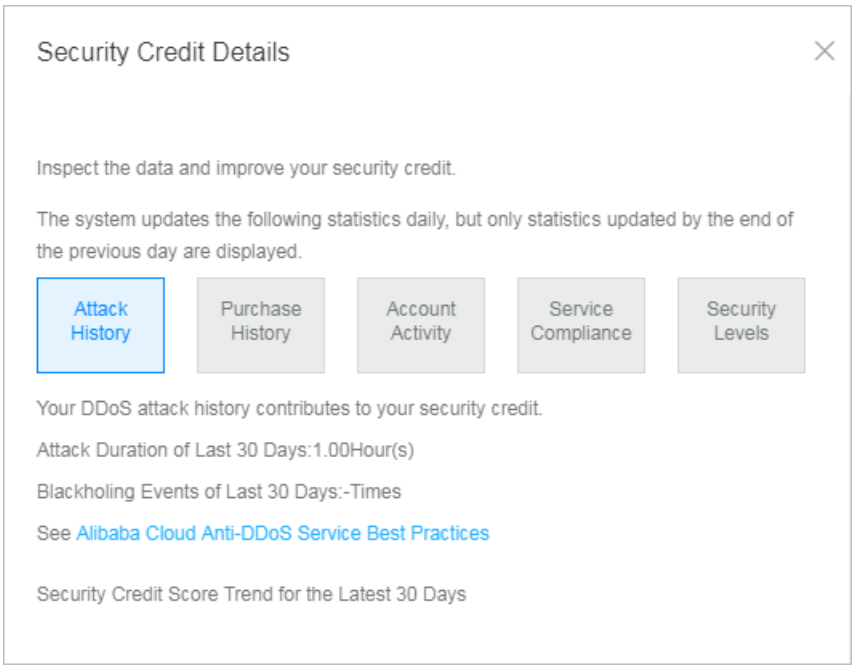
5. View IP exception descriptions When the **Why is the IP address abnormal?** switch is turned on, you can view the information about protection traffic, security credibility score, and automatic blackhole deactivation time.



- Hover your mouse on the **Protection Traffic** icon to check your available protection traffic. Additionally, you can click **Protection Traffic** to see the elastic protection traffic consumption details.



- Hover your mouse on the **Security Credibility** icon to check your security credit score. Additionally, you can click **Security Credibility** to see the security credit details.



With a higher credibility score, you can get more extra DDoS mitigation capacity. We recommend that you learn the credibility score policy and maintain a better credibility score.

- Hover your mouse on the **Blackholing** icon to check your blackhole deactivation time.

3 User Guide

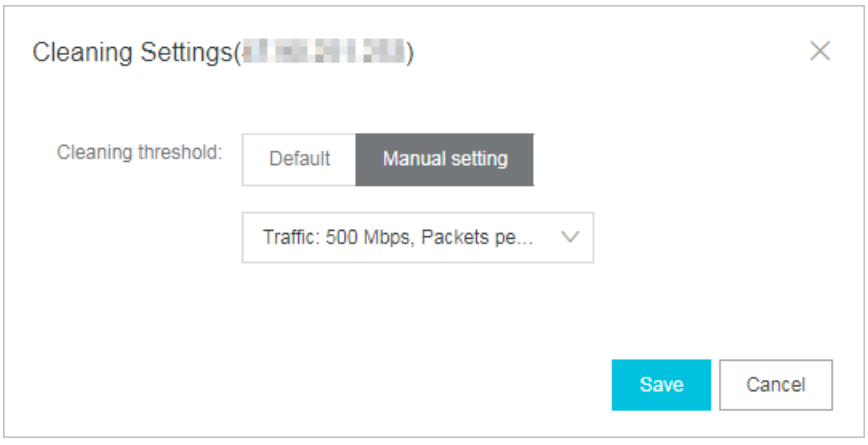
3.1 Set the cleaning trigger value

Alibaba Cloud Security Anti-DDoS Basic mitigates SYN flood, UDP flood, ACK flood, ICMP flood, and DNS flood DDoS attacks. To set the cleaning trigger value in Anti-DDoS Basic, follow these steps:

Procedure

1. Log on to the *Anti-DDoS Basic console*.
2. Select a region.
3. On the **Anti-DDoS Basic** > **Instances**page, select the instance type tab: **ECS**, **SLB**, or **EIP(including NAT)**.
4. Locate to the instance to be operated.

   Note:
   You can search for target instances by **Instance ID**, **Instance Name**, and **Instance IP**.
5. Click **Cleaning Settings** to configure the cleaning threshold value setting for the IP.
6. In the **Cleaning Settings** dialog box, select the cleaning threshold mode: .**Default** or **Manual setting**.



- **Default**: Anti-DDoS Basic service dynamically adjusts the cleaning threshold value based on the traffic load status.
- **Manual setting**: You can select the traffic and packet threshold values manually. When traffic exceeds this threshold value, Anti-DDoS Basic traffic cleaning is triggered. (We recommend that you adjust the cleaning threshold value appropriately when your website has some promotion activities.)

Note:

The cleaning threshold value can be a bit bigger than the actual access traffic value. If the threshold value is too big, it is not effective on DDoS attacks defense; if the threshold value is too small, the normal access can be affected due to the unexpected traffic cleaning.

When traffic to an IP reaches the cleaning threshold value, you can view the cleaning information in the Alibaba Cloud Security Anti-DDoS Basic console. If normal access requests are affected, you can cancel the traffic cleaning and adjust the cleaning threshold value appropriately.

3.2 Disable traffic scrubbing

Alibaba Cloud servers enjoys a free DDoS mitigation capacity by default. When they are targeted by traffic attacks, the traffic scrubbing service is activated automatically. The traffic scrubbing service consists of three units: detecting center, cleaning center, and centralized management center.

Context

The detecting center monitors data traffic flowing into the cloud server, and identifies abnormal traffic in a timely manner, such as DDoS attack. When an abnormity is detected, the management center guides the scrubbing 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 ensures only legitimate traffic can be forwarded to the target system.

You can manually cancel traffic scrubbing for instance IP in the abnormal status.

Note:

One account can manually disable traffic scrubbing for three times in one day.

Procedure

1. Log on to the *Anti-DDoS Basic console*.
2. Select a region.
3. Select ECS, Server Load Balancer, or EIP (including NAT), and locate to the instance IP that is in the cleaning status, and click **View Details**.
4. Click **Cancel Cleaning**.

3.3 Check black hole duration

When your server suffers massive DDoS attacks and the black hole mechanism is triggered, the public IP of the server is banned for a certain time period based on the security credibility of the server.

Context

The default black hole duration is 2.5 hours and the IP 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.

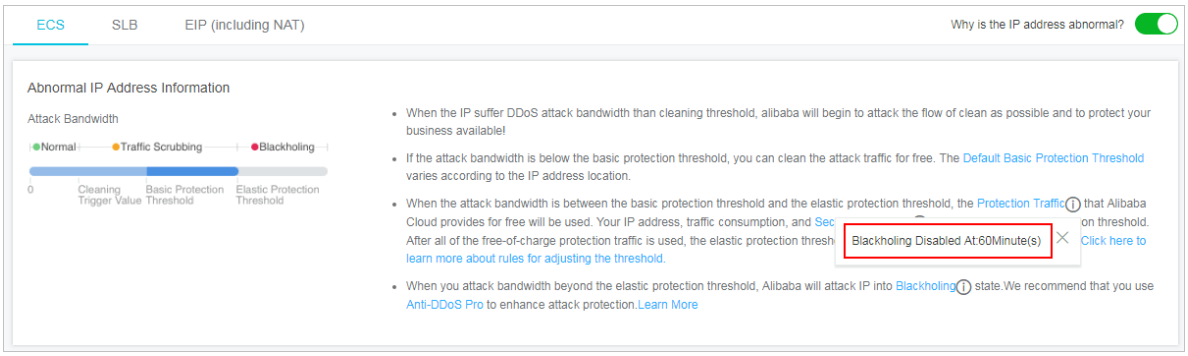
You can log on to the Anti-DDoS Basic console to view the specific black hole threshold and duration.

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.
- Black hole is a service provided by Internet service providers (ISPs) and ISPs have a clear black hole disabled time limit. Thus, in general, the black hole duration is no less than 30 minutes, and the specific black hole duration of your account is automatically adjusted according to the security credibility of your account.

Procedure

1. Log on to the *Anti-DDoS Basic console*.
2. On the **Anti-DDoS Basic** > **Instances** page, make sure that the **Why is the IP address abnormal?** switch in the upper-right corner is turned on.
3. Hover your mouse over the **Blackholing** icon to check the current black hole duration.



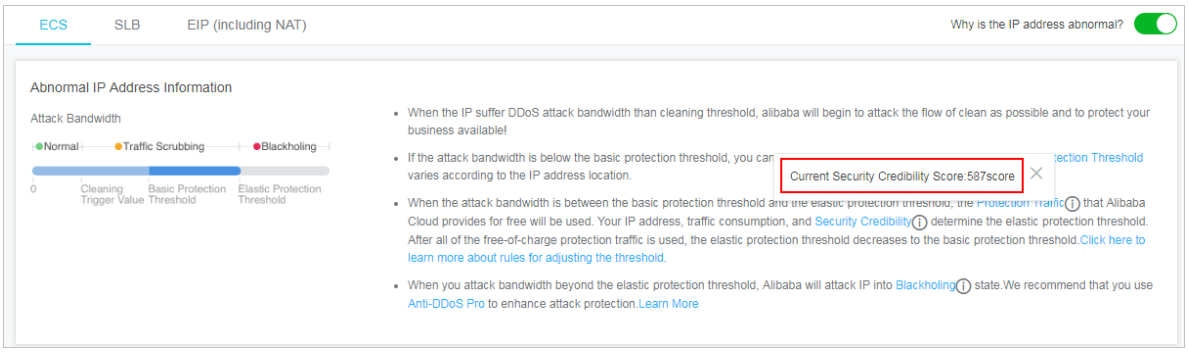
3.4 Check security credit details

To check your current security credibility score and details in the Alibaba Cloud Anti-DDoS Basic console, follow these steps:

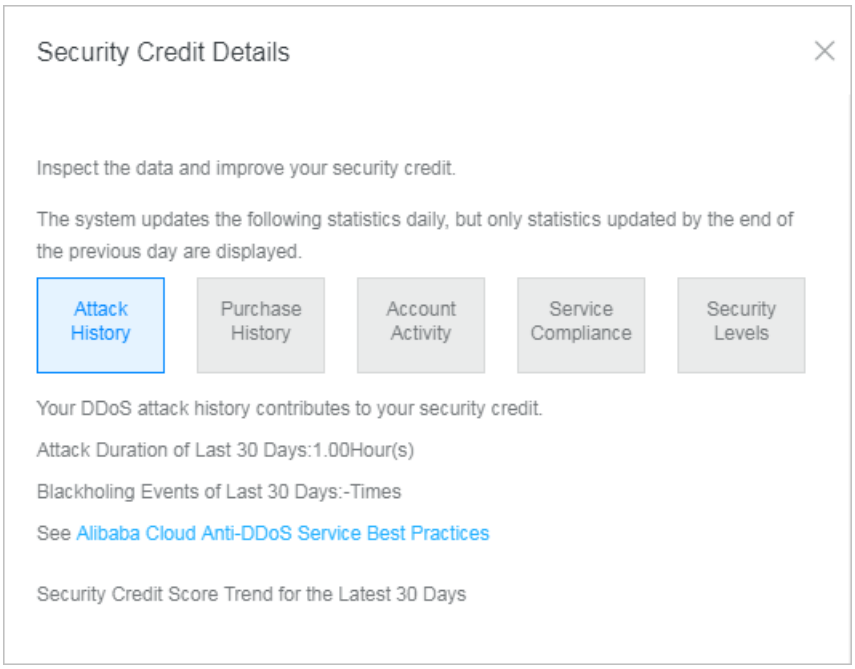
Context

Procedure

1. Log on to the *Alibaba Cloud Anti-DDoS Basic console*.
2. On the **Anti-DDoS Basic** > **Instances** page, make sure that the **Why is the IP address abnormal?** switch in the upper-right corner is turned on.
3. Hover your mouse over the **Security Credibility** icon to check the current security credibility score.



4. Click **Security Credibility** to check the security score details.



We recommend that you maintain your security credibility score based on the security credit rating criteria to obtain more free elastic DDoS protection capacity.

3.5 Configure DDoS Protection notification settings

Alibaba Cloud provides DDoS Protection notifications. When a server under your account suffers DDoS attacks, triggers traffic scrubbing or the blackhole mechanism, the system sends notifications by specified methods to specified receivers.

Manage message recipients

To configure the notification methods (Internal Messages, Email, and Text message) and recipients for Security Notice, follow these steps:

1. Log on to the *Message Center console*.
2. Click **Message Settings** and locate to **Security Notice**.
3. Click **Modify** and select the message recipient.

> **Note:**
> To add a new message recipient, click **Add Receiver**.

3.6 Connect to a server whose IP address is thrown into the black hole

If your server suffers from a heavy traffic attack and its IP address is thrown into the black hole, then all external traffic to the server is discarded. However, you can still access this server from Alibaba Cloud services within the same region as that of this server.

Note:
During the black hole period, external access requests sent to this server are blocked.

You can use an Alibaba Cloud ECS instance to connect to your server, even when its IP address is thrown into the black hole.

1. Connect to an Alibaba Cloud ECS instance that can be normally accessed and is within the same region as this server.

   Note:
   This ECS instance must be connectable to the server under black hole status. They must belong to the same VPC environment, and the connection is not blocked by any security group access control rules.

2. Use a tool or command line to connect from the ECS instance to the server under black hole status.

After successfully connecting to the server from the ECS instance, you can transfer files from the server to the ECS instance and modify the configuration files on this server.

3.7 Anti-DDoS Basic black hole threshold

Anti-DDoS Basic may actively trigger a black hole to lock network access to the instance if the data transfer rate exceeds the default black hole threshold (unit: bps). Once in a black hole, the instance under attack cannot be unblocked. See the following table for the default threshold settings for different regions.

Note:

- The default threshold settings apply to ECS, SLB, and EIP.
- The actual black hole threshold of your ECS, SLB, or EIP instance also indicates the type and network bandwidth of the instance, and is subject to the threshold in the Alibaba Cloud console. For more information, see *How to check the black hole threshold of your instance?*

Region	Solo-Core CPU ECS	Duo-Core CPU ECS	Quad-Core or higher CPU ECS	SLB and EIP
East China 1	500 M	1 G	5 G	5 G
East China 2	500 M	1 G	2 G	2 G
North China 1	500 M	1 G	5 G	5 G
North China 2	500 M	1 G	2 G	2 G
North China 3	500 M	1 G	2 G	2 G
South China 1	500 M	1 G	2 G	2 G
Hong Kong	500 M	500 M	500 M	500 M
US East 1	500 M	1 G	2 G	2 G
US West 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
Kuala Lumpur	500 M	500 M	500 M	500 M
Mumbai	500 M	1 G	1 G	1 G
Frankfurt	500 M	500 M	500 M	500 M
Dubai	500 M	500 M	500 M	500 M

The black hole duration is the amount of time the triggered black hole lasts, 2.5 hours by default. The actual black hole duration varies from 30 minutes to 24 hours, depending on attack intensity. Additionally, the following factors are considered:

- Attack Continuity. The black hole duration is extended, if the attack continues.
- Attack Frequency. The black hole duration is shortened automatically when the ECS instance is attacked for the first time, but can be prolonged accordingly, if under frequent attacks.

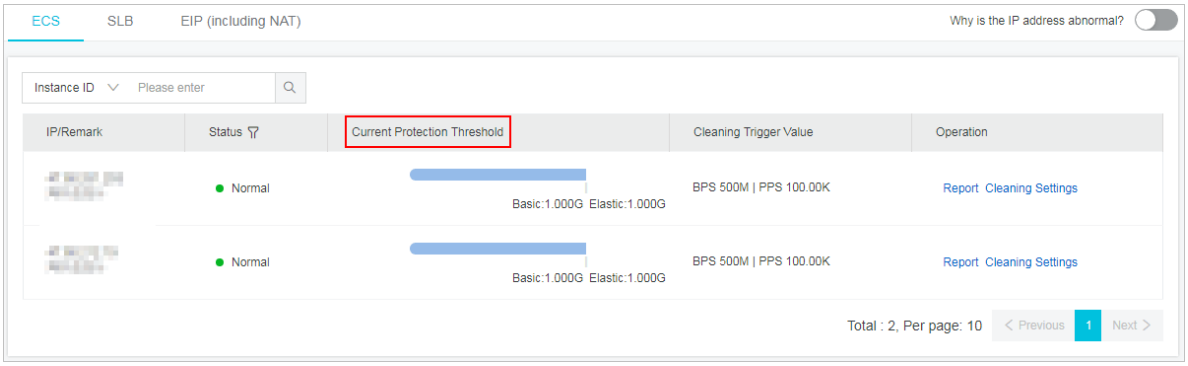
Note:

If an ECS instance triggers too many black holes, Alibaba Cloud Security reserves the right to extend the black hole duration and lower its threshold. You can check the actual duration and threshold information in Alibaba Cloud Anti-DDoS Basic console.

How to check the black hole threshold of your instance?

To check the actual black hole threshold of your ECS, SLB, or EIP instance, follow these steps:

1. Log on to *Alibaba Cloud Anti-DDoS Basic console*.
2. Select the region.
3. On the **Anti-DDoS Basic** > **Instances** page, select the instance type tab: **ECS**, **SLB**, or **EIP (including NAT)**.
4. Locate the instance, and check the actual black hole threshold of the instance in the **Current Protection Threshold** column.



3.8 Anti-DDoS Basic black hole threshold for web hosting

The default black hole threshold for web hosting is as follows (unit: bps).

Note:

For shared web hosting, the specific black hole threshold cannot be defined as multiple web hosting may share one IP address. Additionally, the actual threshold must be lower than the default threshold value. When a shared web hosting server triggers the black hole, all the other servers that share IP address with this server becomes inaccessible. We strongly recommend that you buy ECS instance if you give utmost importance to the security.

Region	Web hosting threshold
China (Hangzhou)	5 G
China (Qingdao)	5 G
China (Shenzhen)	2 G
China (Beijing)	2 G
China (Shanghai)	2 G
Hong kong	500 M
US West	500 M
Singapore	500 M

The black hole duration is the amount of time the triggered back hole lasts, 2.5 hours by default. The actual black hole duration varies from 30 minutes to 24 hours, depending on attack intensity. Additionally, the following factors are considered:

- Attack Continuity. The black hole duration is extended, if the attack continues.
- Attack Frequency. The black hole duration is shortened automatically when the ECS instance is attacked for the first time, but can be prolonged accordingly, if under frequent attacks.

Note:
If an ECS instance triggers too many black holes, Alibaba Cloud Security reserves the right to extend the black hole duration and lower its threshold. You can check the actual duration and threshold information in Alibaba Cloud Anti-DDoS Basic console.

To get more powerful DDoS mitigation capacities, see *Alibaba Cloud Anti-DDoS Pro*.

3.9 ECS stress test guide

Alibaba Cloud Security Anti-DDoS Basic provides defense against DDoS attacks. By default, when the public traffic exceeds 180 MB per second, 30,000 messages per second, or 480 HTTP requests per second on an ECS server, Anti-DDoS Basic automatially starts traffic scrubbing to protect the ECS server.

Therefore, before you start the stress testing on an ECS server, you have to adjust the cleaning trigger value to an appropriate value in the *Alibaba Cloud Anti-DDoS Basic console*. For more information, view *Set the cleaning trigger value*.

Note:
We recommend that you do not set the increasing pace per minute to exceed 100 times during the stress test.

3.10 Avoid Anti-DDoS Basic false positives by using a whitelist

In some situations, you may find that some normal traffic is blocked by Anti-DDoS Basic (such as normal website service access).

Context

For example, in an NAT network environment (hosts in the LAN share an Internet IP address for Internet access), some hosts in the LAN infected by a virus or suffering intrusion may attack an

ECS server. In this situation, once Alibaba Cloud Security acknowledges the attacks, it blocks the shared Internet IP address of the NAT, resulting to an access failure.

However, you can set a whitelist in the Alibaba Cloud Security Control platform to avoid such false positives.

Procedure

1. Log on to the *Alibaba Cloud Security Control console*.

   Note:
   You can also hover your mouse on the account icon in the upper-right corner of Alibaba Cloud console and click **Security Control** to open it.

2. Go to **Whitelist** > **Access Whitelist**, click **Add**.
3. Select the Object Type, and enter the Source IP (not the IP belongs to your current Alibaba Cloud account). Then, select object IPs of your current account from the list on the left side (for example, select a public IP of your ECS instance), click the right arrow button to add the selected IPs to the list on the right side, and click **OK**. Thus, the specified source IP is added to the access whitelist of the selected object IPs, and all accesses from the source IP to the object IPs are not restricted by Alibaba Cloud Security Control platform.

   Note:
   To allow accesses from all IPs to the object IP, enter 0.0.0.0 in the **Source IP** field.

   After setting the whitelist, all accesses to the target host asset from the source IP in the access whitelist are not restricted by any Alibaba Cloud security controls, even if the access may be risky. Therefore, set the access whitelist carefully.

   Note:
   After the source IP is added to the access whitelist, it takes effect within 10 minutes.

4 FAQ

4.1 Apply for adding IP addresses to the global whitelist of Alibaba Cloud Security

Alibaba Cloud provides a secured cloud environment, where suspicious actions are monitored and blocked in real time. In cases where you use a third party CDN or security vendor's product to forward requests or perform security scan, Alibaba Cloud Security may regard these behaviors as suspicious. Consequently, access exceptions may result from attack behaviors that contain source IP address in the forwarded requests or unpermitted operations from security scan.

Considering the necessity of such products, Alibaba Cloud allows CDN and security vendors (applicant) to apply for permissions to add the IP addresses of their products to the global whitelist of Alibaba Cloud Security basic protection. The relevant procedure is as follows.

Note:
If you only want to configure a whitelist for all of your ECS instances, see *Configure an access whitelist in Security Control*.

To make an application, the applicant must write an official letter that contains the following information:

- A list of the IP addresses to be added to the whitelist. In case of numerous IP addresses, an official link to these IP addresses can be provided and sent as an email attachment.
- Usage descriptions of these IP addresses.
- Commitment of adherence to relevant laws, regulations, and Alibaba Cloud's relevant regulations. The applicant must commit to not mounting any type of attack against Alibaba Cloud's users. If the added IP addresses are deemed as security threats to Alibaba Cloud's users or are allegedly used to commit law violations and patent infringements, the applicant is fully liable for the resulting impact. The applicant stands liable to compensate Alibaba Cloud for any losses.
- Contact information (telephone number is recommended).
- The applicant's corporate seal.

The applicant, on behalf of the vendor's company, must send the electronic copy of the company's business license and the official letter through email to the following addresses:

- To: dachao.xdc@alibaba-inc.com

- Cc: yemin.ym@alibaba-inc.com

Authorization

Upon receiving an application, Alibaba Cloud sends an initial, non-automatic reply to the applicant within two working days for review purposes. Alibaba Cloud has the right to request the applicant to clarify any doubts in regard to the application materials during the application review process. The review may take several working days. When the review is completed, Alibaba Cloud notifies the applicant of the result.

The applicant accepts that Alibaba Cloud can clean the whitelist periodically in accordance with the specified policy. The applicant is required to notify Alibaba Cloud of any adjustments or changes to the IP addresses of relevant products. If Alibaba Cloud determines that the added IP addresses cause security threats to Alibaba Cloud users, Alibaba Cloud will remove these IP addresses permanently and reserves the right to hold the applicant legally accountable.

4.2 Anti-DDoS Basic FAQ

Currently, every ECS instance has Anti-DDoS Basic enabled by default. When the web traffic of an ECS instance exceeds the specified DDoS threshold, the Anti-DDoS cleansing device starts to clean the traffic.

What is the role of Anti-DDoS Basic port whitelist?

Anti-DDoS Basic helps you detect ports in service. If you authorize to activate a port, you can add the port to the port whitelist so that Anti-DDoS Basic service does not issue alarms for this port.

Does Anti-DDoS Basic defend against SYN flood attacks?

Yes, Anti-DDoS Basic can defend against SYN flood attacks.

Can I select a time period for viewing the Anti-DDoS protection results?

Yes. Alibaba Cloud Security Anti-DDoS Basic console supports queries of DDoS attack events in the last 24 hours.

Why did not Alibaba Cloud Security Anti-DDoS Basic defend against the 20 MB attack that my ECS server suffered?

Alibaba Cloud Security Anti-DDoS Basic is a public anti-DDoS service. It won't block low-traffic attacks (lower than 100 MB). We recommend that you optimize your server performance or install Cloud Lock or other host firewalls to handle the attacks of the traffic lower than 100 MB.

What is the AliVulfix process on the ECS server?

The AliVulfix process is a program in Alibaba Cloud Security for detecting vulnerabilities on ECS.

Why can not a black hole be canceled immediately?

Black holes last for 30 minutes to 24 hours for a vast majority of users. If a user is under frequent attacks, Alibaba Cloud may impose penalties by increasing black hole frequency.

Black hole is a service that Alibaba Cloud purchases from operators who have explicit restrictions on black hole removal time. That is why black hole cannot typically be canceled immediately.