ALIBABA CLOUD

Alibaba Cloud

Anti-DDoS

Anti-DDoS Origin User Guide

Document Version: 20220629

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}`

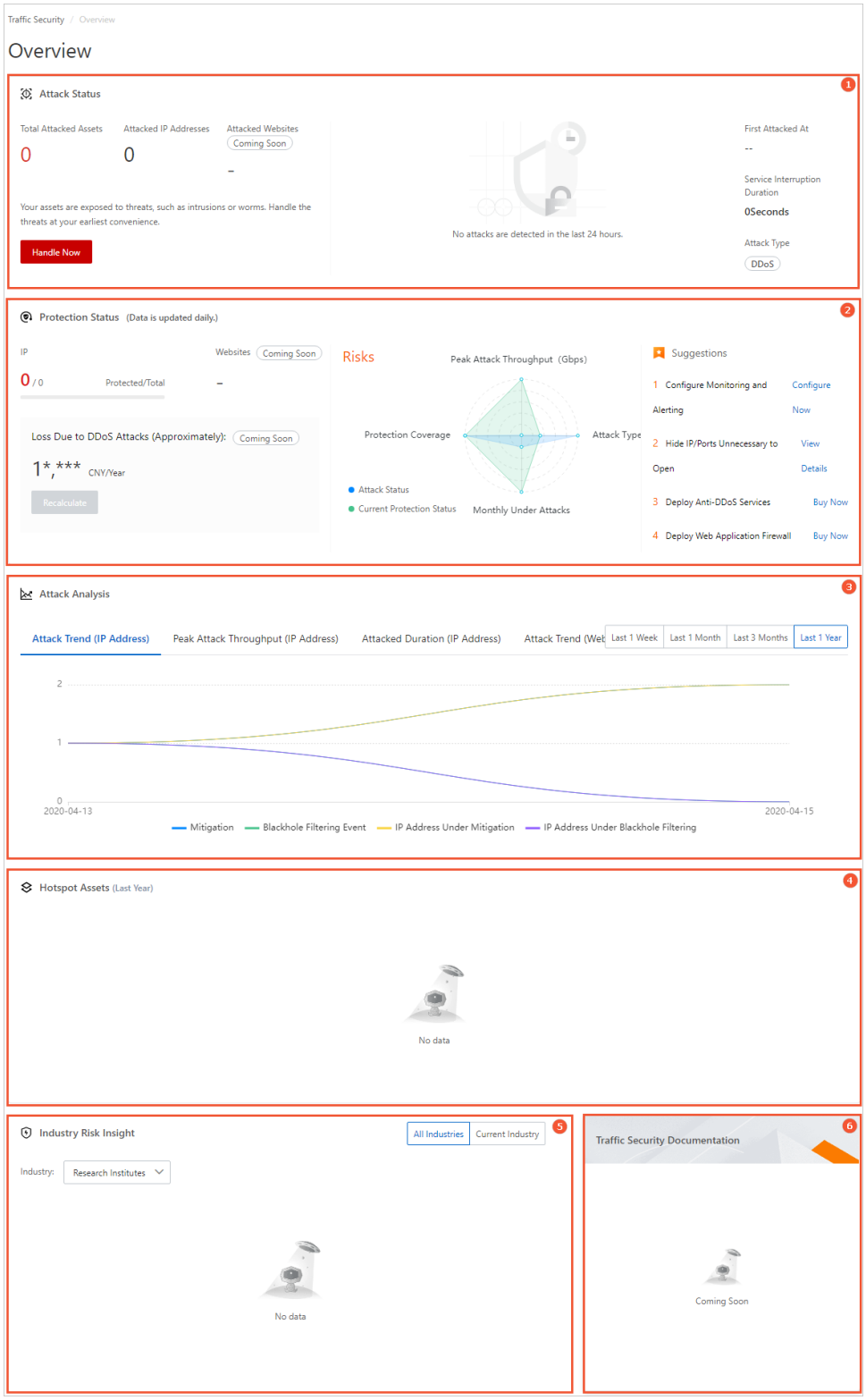
Table of Contents

1.View the Overview page of Traffic Security

The Overview page of Traffic Security provides insight into the network traffic attacks on your network assets, which helps you handle the attacks. The Overview page also enables you to view the protection status and attack trends of assets, evaluate the security status of assets, and view hotspot assets. In this topic, network traffic attacks are referred to as traffic attacks for short. This topic describes how to query data and details about the data on the Overview page of Traffic Security.

Query data on the Overview page of Traffic Security

1.
2. In the left-side navigation pane, click **Overview**.
3. On the **Overview** page, view the overall data of traffic security.

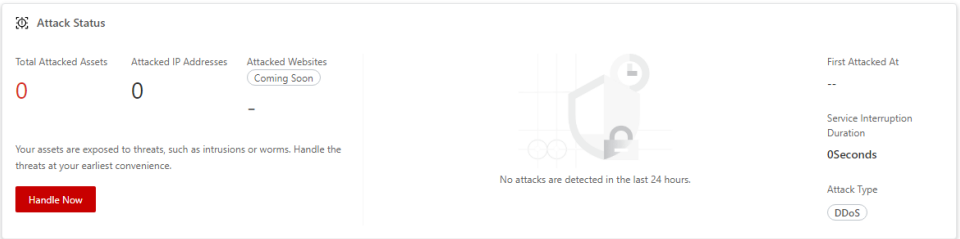


The following table describes the data that you can query on the Overview page of Traffic Security.

Name	Description	Supported operation	Detailed description
Attack Status (Section 1 in the preceding figure)	Provides an overview about the traffic attacks on your network assets and helps you handle attacks that interrupt your service. Traffic Security supports only public IP addresses.	You can click **Handle Now** to view the emergency response operations and mitigation plans that are provided to specific attacked assets.	Detailed description of Attack Status
Protection Status (Section 2 in the preceding figure)	Displays the security status of your network assets and provides security hardening suggestions.	If your network assets have security risks, we recommend that you implement security hardening based on the suggestions to reinforce security.	Detailed description of Protection Status
Attack Analysis (Section 3 in the preceding figure)	Displays the trend of traffic attacks on your network assets over the last year. This helps you evaluate potential risks to your service and what is required to protect your service.	You can switch between the time ranges of data and the types of attack data that you want to query.	Detailed description of Attack Analysis
Hotspot Assets (Section 4 in the preceding figure)	Ranks the most attacked assets over the last year. This helps you identify core assets.	None.	Detailed description of Hotspot Assets
Industry Risk Insight (Section 5 in the preceding figure)	Helps you analyze the trend in the quantity of traffic attacks in the industry of your business over the last six months. This helps you understand the industry-specific security posture.	You can specify the industry of your business to focus on the security risks in the industry.	Detailed description of Industry Risk Insight
Traffic Security Documentation (Section 6 in the preceding figure)	Provides the latest updates in the field of traffic security. This helps you obtain up-to-date information in this field.	You can view the details of the update in which you are interested.	Traffic Security Documentation

Detailed description of Attack Status

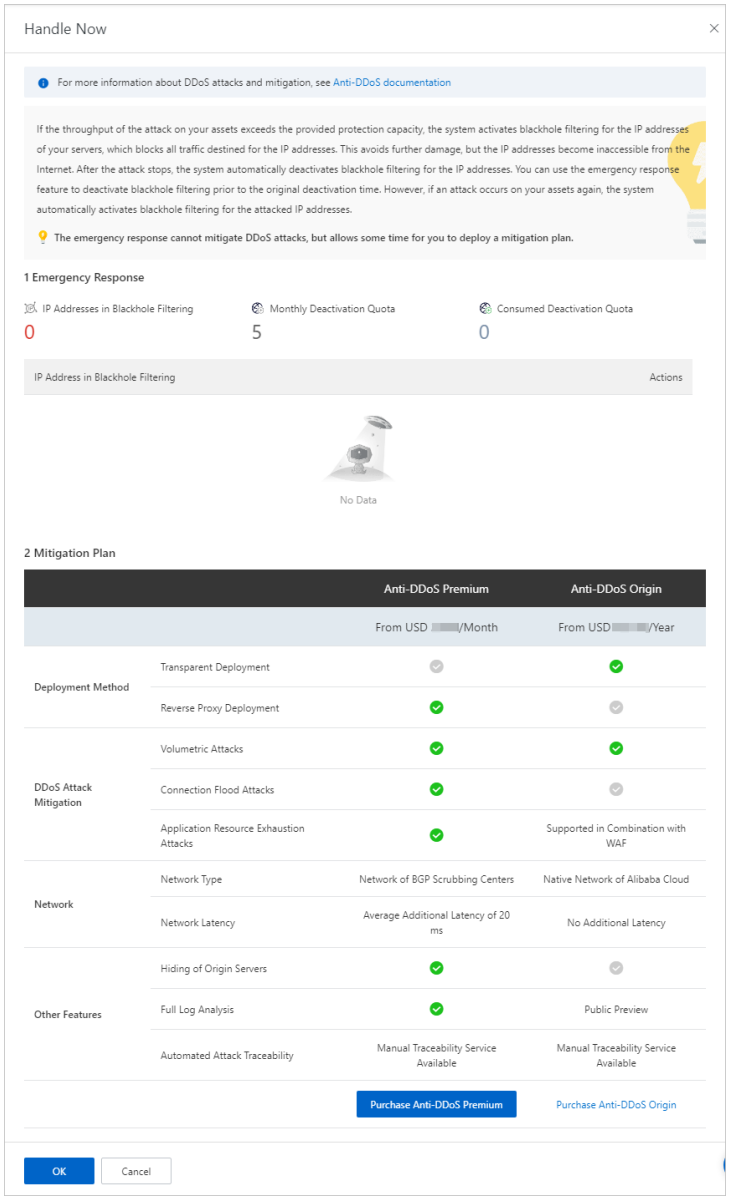
The **Attack Status** section displays an overview of the traffic attacks on your network assets. Traffic Security supports only public IP addresses. The overview includes the following information: **Total Attacked Assets**, **Attacked IP Addresses**, **First Attacked At**, **Service Interruption Duration**, and **Attack Type**.



If this section displays an attack that has interrupted your service, you can click **Handle Now** to query the information, **Emergency Response**, and **Mitigation Plan** for the attack. The following list describes the details:

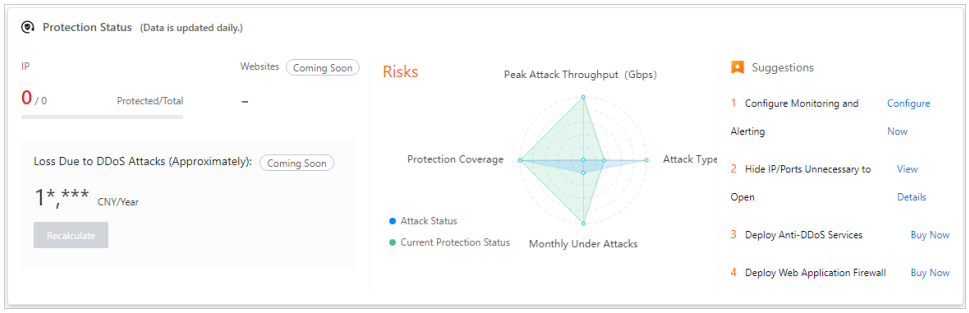
- You can refer to the information in the **Emergency Response** section to restore your service at the earliest opportunity. However, this does not prevent potential attacks on your service. Limits are also imposed on emergency response operations. For example, both the operation quota and the protection capability are limited.
- You can refer to the information in the **Mitigation Plan** section to deploy a service that helps you avoid attacks of the same type. After you deploy a security service, service interruptions caused by the attacks are reduced or no longer occur.

For example, if your service is interrupted due to a distributed denial of service (DDoS) attack, you can use two methods to handle the attack on the **Handle Now** page. First, in the **Emergency Response** section, deactivate black filtering for the IP address that is attacked. If this quota is exhausted, you must deploy a mitigation plan. Second, in the **Mitigation Plan** section, deploy Anti-DDoS Pro or Anti-DDoS Origin to better protect your service against DDoS attacks. For more information about mitigation plans and how to activate the services, see the information on the **Handle Now** page.



Detailed description of Protection Status

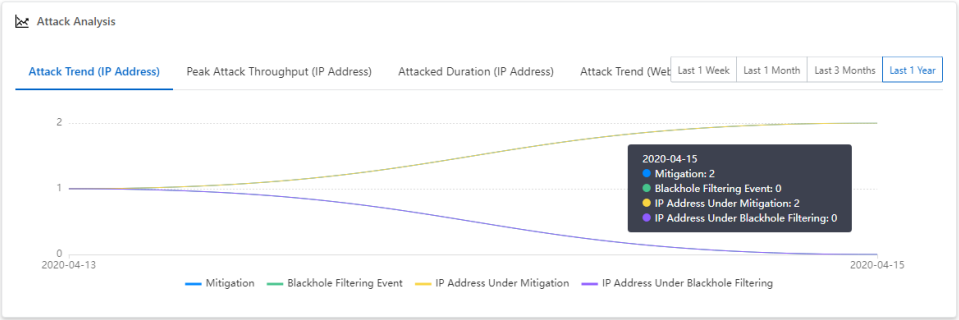
The **Protection Status** section displays the security status of your network assets, such as the proportion of protected assets to all assets and the security evaluation of your service. This section also displays **Suggestions** for security hardening. This helps you understand the network-related weaknesses in your service and offers suggestions to improve protection.



If the security evaluation result for your service is **Risks** as shown in the preceding figure, we recommend that you implement the security hardening measures in the **Suggestions** section. This improves protection for your service.

Detailed description of Attack Analysis

The **Attack Analysis** section displays the trend of traffic attacks on your network assets over the last year. This helps you evaluate potential risks to your service and what is required to protect your service.



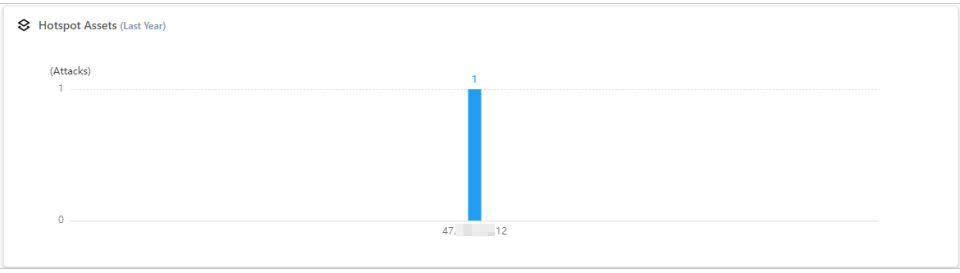
You can query the following data:

- **Attack Trend (IP Address)**: the basic information about the traffic attacks on your IP addresses. The information includes **Mitigation**, **Blackhole Filtering Event**, **IP Address Under Mitigation**, and **IP Address Under Blackhole Filtering**.
- **Peak Attack Throughput (IP Address)**: the trend of peak attack traffic based on IP addresses.
- **Attacked Duration (IP Address)**: the trend of the duration of traffic attacks based on IP addresses.

You can click the buttons in the upper-right corner of the section to switch between time ranges to query. The time ranges are **Last 1 Week**, **Last 1 Month**, **Last 3 Months**, and **Last 1 Year**.

Detailed description of Hotspot Assets

The **Hotspot Assets** section ranks the most attacked assets over the last year. This helps you identify core assets.



We recommend that you deploy a comprehensive security hardening solution for the most attacked assets. For more information, see Best practices for mitigating DDoS attacks.

Detailed description of Industry Risk Insight

The **Industry Risk Insight** section displays the trend in the quantity of traffic attacks in various industries over the last six months. This helps you understand the security posture specific to the industry of your business.

You can click **All Industries** or **Current Industry** in the upper-right corner of the section to query the related data. The following list describes the details:

- After you click **All Industries**, you can select an industry in which you are interested from the **Industry** drop-down list. Then, you can query the quantity of traffic attacks in the industry over the last six months. For example, you can select Research Institutes, Automotive Manufacturing, or Gaming.
- After you click **Current Industry**, you can specify the industry of your business and query the quantity of traffic attacks in the industry over the last six months

Traffic Security Documentation

The **Traffic Security Documentation** section provides links to the latest updates in the field of traffic security. This helps you understand the background of traffic security and obtain up-to-date information in this field.

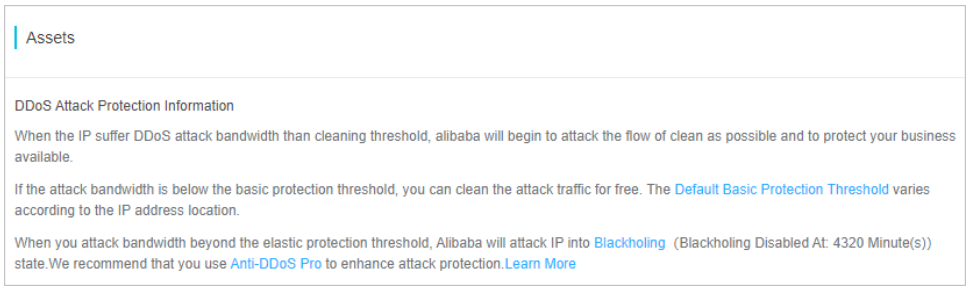
You can click a link to view the details of the update in which you are interested.

2.Assets

Anti-DDoS Origin Basic is enabled by default. It provides a protection capacity of up to 5 Gbit/s for Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and elastic IP addresses (EIPs) under your Alibaba Cloud account. Protection against distributed denial of service (DDoS) attacks for the preceding assets is provided free of charge. The Assets page shows the assets that belong to an Alibaba Cloud account and their protection status along with traffic trends. These assets include ECS instances, SLB instances, and EIPs. The information allows you to obtain an overview of the security risks from DDoS attacks on your assets. You can also use the information to improve protection of your assets.

Procedure

1.
2.
3. On the **Assets** page, view protection information in the **DDoS Attack Protection Information** section.



   In the **DDoS Attack Protection Information** section, you can perform the following operations:

   - Click **Default Basic Protection Threshold** to view default blackhole triggering thresholds for different assets that reside in each region.
   - Click **Blackholing** to view the blackhole filtering policy of Alibaba Cloud.
   - Click **Anti-DDoS Origin** to go to the **Manage Instances** page. You can purchase Anti-DDoS Origin instances as needed. For more information, see Purchase an Anti-DDoS Origin Enterprise instance.

4. Click the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud services that you want to protect.

   > **Note** The **Others** tab shows all the on-demand Anti-DDoS Origin instances under your account. On-demand instances can protect servers in on-premises data centers outside China and cloud assets based on CIDR blocks. You can manually enable or disable protection in the console or by using API operations. For more information, see Enable traffic rerouting to an on-demand instance and ModifyOnDemaondDefenseStatus.

5. In the list of assets, view the protection status of each asset.

   The **Assets** page lists all assets in a region and provides further details about protection against DDoS attacks for each asset. The details include **Status**, **Protection Capacity**, and **Cleaning Trigger Value**.

   - **Status** indicates the security status of an instance. Available states include **Normal**, **Cleaning**, and **Black Hole Activated**.

- If an instance is in the Cleaning state, you can manually cancel traffic scrubbing. For more information, see Cancel traffic cleaning.
- If an instance is in the Black Hole Activated state, you can view the blackhole events. For more information, see View the time when a black hole is enabled for an instance and the reason for enabling the black hole.

- **Protection Capacity** indicates the capacity of an instance to mitigate DDoS attacks. The capacity indicates the maximum bandwidth of DDoS attacks that the instance can mitigate. If the bandwidth consumed by DDoS attacks exceeds the protection capacity of an instance, blackhole filtering is triggered. As a result, all traffic that is destined for the instance is routed to a blackhole. For more information about how to improve the protection capacity of an instance, see Step 6.
- **Cleaning Trigger Value** indicates the minimum bandwidth that must be reached before traffic scrubbing is triggered. The bandwidth is measured in Mbit/s and packets per second (PPS). For more information, see Configure a traffic scrubbing threshold.

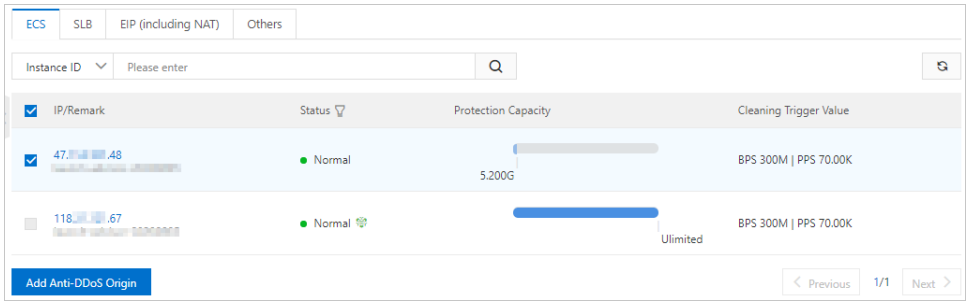
6. Improve the protection capacity of a specific asset.
   - Enable Anti-DDoS Origin

     If you have purchased an Anti-DDoS Origin Enterprise instance in the current region, you can perform the following operations to enable Anti-DDoS Origin for a specific asset.

     Anti-DDoS Origin Enterprise instances provide account-level DDoS mitigation for all your assets and services. This helps mitigate DDoS attack risks on the cloud. Enterprises can protect their large-scale services at controllable costs, without the need to change their service architecture or increase latency. For more information, see What is Anti-DDoS Origin?

     The procedure used to configure Anti-DDoS Origin for different assets, such as ECS, SLB, and EIP assets, is similar. The following procedure describes how to enable Anti-DDoS Origin for an ECS instance. You can use this example as a reference for other types of assets.

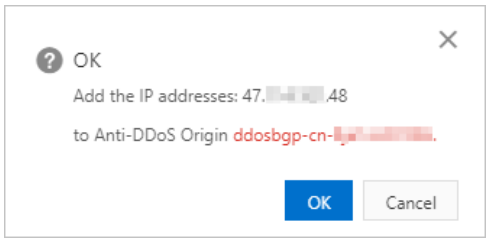
     a. Select the ECS instance for which you want to enable Anti-DDoS Origin from the ECS instance list and click **Add Anti-DDoS Origin**.

     b. In the Anti-DDoS Origin instance list, find the required instance and click **Add** in the Operation column.

c. In the **OK** message, click **OK**.



- Activate Anti-DDoS Pro or Anti-DDoS Premium

  If your services face a high risk of DDoS attacks, we recommend that you activate Anti-DDoS Pro or Anti-DDoS Premium. For example, if your services experience frequent DDoS attacks, volumetric DDoS attacks, or DDoS attacks that severely affect your services, you can activate Anti-DDoS Pro or Anti-DDoS Premium. Anti-DDoS Pro and Anti-DDoS Premium defend against volumetric DDoS attacks. For more information, see What are Anti-DDoS Pro and Anti-DDoS Premium?

  In the left-side navigation pane, click **Anti-DDoS Services**. Then, click **Anti-DDoS Pro** or **Anti-DDoS Premium** to go to the related console.

  - Anti-DDoS Pro is ideal for services that are deployed in mainland China.
  - Anti-DDoS Premium is ideal for services that are deployed outside mainland China.

3.Use Traffic Security Manager

Traffic Security Manager displays the architecture of the traffic protection solution that is provided by Alibaba Cloud and the protection status of your network assets. This way, you can analyze the pain points in the traffic protection capability of your service and view the solutions to reinforce security. This topic describes how to use Traffic Security Manager.

Context

You can view the total number of network assets that belong to the current Alibaba Cloud account. The network assets can belong to Elastic Compute Service (ECS), Server Load Balancer (SLB), Elastic IP Address (EIP), NAT Gateway (NAT), or Virtual Private Cloud (VPC). You can also view the total number of attacked network assets and check whether each security service of Alibaba Cloud is activated for the account.

Procedure

1.
2.
3. In the upper-right corner of the **Traffic Security Manager** page, click **Start** to experience the demo of Traffic Security Manager.

   The demo provides a walkthrough that allows you to view the following information: **Asset Security Overview**, **Traffic Type Overview**, **Attacked Assets**, **Attack Sources**, and **Attack Events**.

   > **Notice** The data in the demo is for reference only.

4. Join invitational preview.

   If you want to view your actual traffic data by using Traffic Security Manager, submit a .

   After Alibaba Cloud engineers receive your application to join invitational preview, they contact you by using the contact information that you submit and confirm information that is related to your application.

   After your application is approved, you can view the actual traffic data on the **Traffic Security Manager** page.

4.Purchase an Anti-DDoS Origin Enterprise instance

If you want to improve the DDoS mitigation capabilities for the public IP addresses of Alibaba Cloud resources, you can purchase an Anti-DDoS Origin Enterprise instance. The public IP addresses include public IP addresses of Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and Application Load Balancer (ALB) instances, elastic IP addresses (EIPs), IP addresses of Network Address Translation (NAT) gateways, and IP addresses of Web Application Firewall (WAF) instances.

Prerequisites

- The real-name verification is completed for your Alibaba Cloud account.
- The public IP addresses that you want to protect are public IP addresses of Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and Application Load Balancer (ALB) instances, elastic IP addresses (EIPs), IP addresses of Network Address Translation (NAT) gateways, and IP addresses of Web Application Firewall (WAF) instances.

Context

Anti-DDoS Origin is offered in two editions: Anti-DDoS Origin Basic and Anti-DDoS Origin Enterprise.

- By default, Anti-DDoS Origin Basic is activated. Anti-DDoS Origin Basic provides a basic protection capacity of up to 5 Gbit/s against DDoS attacks free of charge for the public IP addresses of Alibaba Cloud resources.
- Anti-DDoS Origin Enterprise is a paid service that protects the public IP addresses of Alibaba Cloud resources. Anti-DDoS Origin Enterprise provides shared and unlimited protection capacities. You do not need to change your service IP address.

  Unlimited protection defends against DDoS attacks based on the total network capacity of Alibaba Cloud. The unlimited protection capacity increases with the increase of the overall network capacity of Alibaba Cloud. You do not need to pay extra fees for the increase in capacity.

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

Procedure

1. Access the Anti-DDoS Origin buy page by using your Alibaba Cloud account.
2. On the **Anti-DDoS Origin** buy page, set **Product Type** to **Anti-DDoS Origin** and configure the following parameters.

Parameter	Description
Mitigation Plan	The mitigation plan of the Anti-DDoS Origin instance. Default value: **Enterprise**. You cannot change the value of this parameter.
Mitigation Times	The mitigation sessions. Default value: **Unlimited**. You cannot change the value of this parameter.
IP Version	The version of the IP protocol. Valid values: **IPV4** and **IPV6**.

Parameter	Description
Region	The region where the Anti-DDoS Origin Enterprise instance resides. **Notice** ◦ The Anti-DDoS Origin Enterprise instance must reside in the same region as the assets whose public IP addresses you want to protect. The public IP addresses include public IP addresses of Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and Application Load Balancer (ALB) instances, elastic IP addresses (EIPs), IP addresses of Network Address Translation (NAT) gateways, and IP addresses of Web Application Firewall (WAF) instances. ◦ Anti-DDoS Origin Enterprise instances are available only in the Chinese mainland. If you want to purchase an Anti-DDoS Origin Enterprise instance outside the Chinese mainland, submit a or contact the sales personnel.
Business Scale	The average network bandwidth of the business that you want to protect. For more information about how to estimate the business scale, see Instance specifications of Anti-DDoS Origin Enterprise. The subscription fee of an Anti-DDoS Origin Enterprise instance increases with the business scale. For more information, see Billing methods of Anti-DDoS Origin.
IP Addresses	The total number of public IP addresses that you want to protect. The minimum value that you can specify for this parameter is **100**. If you want to protect more public IP addresses, you can increase the value. The subscription fee of an Anti-DDoS Origin Enterprise instance increases with the number of public IP addresses. For more information, see Billing methods of Anti-DDoS Origin.
Resource Group	A resource group is a group of resources that belong to an Alibaba Cloud account. You can manage members, permissions, and resources in a resource group. You can select an existing resource group or create a resource group. For more information, see Create a resource group.
Quantity	The number of Anti-DDoS Origin Enterprise instances that you want to purchase.
Duration	The validity period of the Anti-DDoS Origin Enterprise instance. You can select **Auto-renewal** based on your business requirements.

3. Click **Buy Now**.
4. Confirm the order and complete the payment.

Result

After you purchase the Anti-DDoS Origin Enterprise instance, you can view the instance on the Manage Instances page in the Anti-DDoS Origin console. You can add specific public IP addresses that you want to protect to the Anti-DDoS Origin Enterprise instance. For more information, see Add a cloud service to Anti-DDoS Origin Enterprise for protection.

5.Use the service monitoring feature

The Service Monitoring page shows the protection data of the Anti-DDoS Origin instance to help you understand the security posture of your service. The protection data includes the traffic trends of protected assets and the DDoS attack events. This topic describes the monitoring data and how to query service monitoring data.

Prerequisites

An Anti-DDoS Origin instance is purchased, and your assets are protected by the instance.

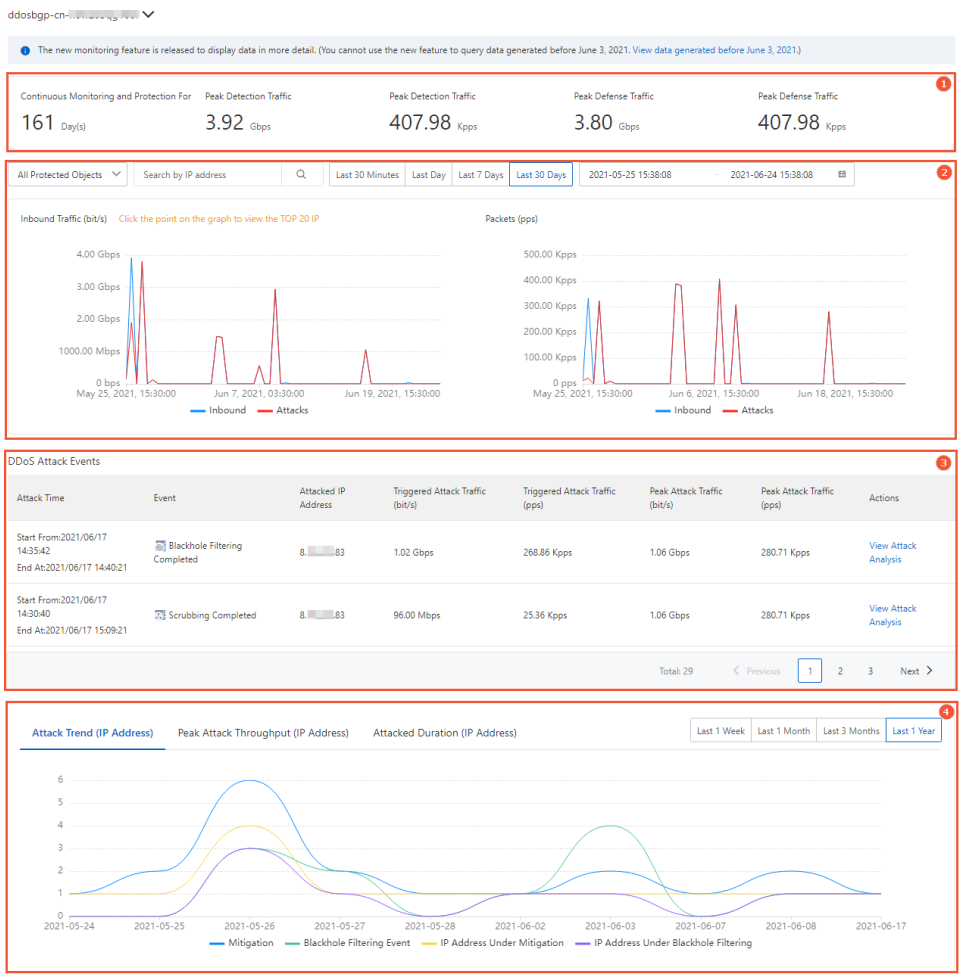
For more information, see Purchase an Anti-DDoS Origin Enterprise instance and Add a cloud service to Anti-DDoS Origin Enterprise for protection.

Context

On the Service Monitoring page, you can query data generated on and after June 3, 2021. If you want to query data that is generated before June 3, 2021, perform operations described in View security reports.

Query service monitoring data

1.
2.
3.
4. In the upper-left corner of the page that appears, select the Anti-DDoS Origin instance that you want to query.
5. View the service monitoring data of the Anti-DDoS Origin instance.



The following table describes the data that you can view on the Service Monitoring page.

Section	Purpose	Supported operation	Description
Service statistics (Section 1)	The statistics help you understand the historical peak traffic of attacks that are detected by the Anti-DDoS Origin instance. The statistics include Continuous Monitoring and Protection For, Peak Detection Traffic (in bit/s), Peak Detection Traffic (in pps), Peak Defense Traffic (in bit/s), and Peak Defense Traffic (in pps).	None.	Description of service statistics
Traffic trend charts (Section 2)	The charts help you understand the trends of inbound traffic destined for the public IP addresses that are protected by the Anti-DDoS Origin instance. The charts include the Inbound Traffic (bit/s) and Packets (pps) charts.	You can specify a protected object and a time range to query related data.	Description of traffic trend charts

Section	Purpose	Supported operation	Description
DDoS attack events (Section 3)	The event list and charts allow you to view details about attack events detected by the Anti-DDoS Origin instance. The events include traffic scrubbing and blackhole filtering events. You can analyze and handle attack events based on the details.	◦ You can specify a protected object and a time range to query related data. ◦ You can view attack analysis results, manually cancel traffic scrubbing, and download packet capture files for a specific DDoS attack event.	Description of DDoS attack events
Attack trend charts (Section 4)	The charts help you understand the trends of network attacks detected by the Anti-DDoS Origin instance over the last year. This helps you evaluate potential risks to your service and what is required to protect your service.	You can specify a time range to query related data.	Description of attack trend charts

Description of service statistics

Section 1 displays the following data:

- **Continuous Monitoring and Protection For**: indicates the number of days that the Anti-DDoS Origin instance protects your assets.
- **Peak Detection Traffic**: indicates the peak traffic of your service that is detected by the Anti-DDoS Origin instance. The peak traffic is measured by both bandwidth in bit/s and packet forwarding rate in pps.
- **Peak Defense Traffic**: indicates the peak traffic of attacks that are detected by the Anti-DDoS Origin instance. The peak traffic is measured by both bandwidth in bit/s and packet forwarding rate in pps.

Description of traffic trend charts

Section 2 provides the following charts:

- **Inbound Traffic (bit/s)**: shows the trends of inbound traffic for protected IP addresses. Unit: bit/s. This chart shows the total traffic and attack traffic.
- **Packets (pps)**: shows the trends of packet forwarding rate in the inbound direction for protected IP addresses. Unit: pps. This chart shows the forwarding rates of all packets and attack packets.

In this section, you can configure the following items to query related data:

- Protected object: You can select **All Protected Objects** from the drop-down list or enter an IP address that is protected in the search box to query related data.

  If you select **All Protected Objects**, you can click a point on a trend chart to query the top 20 IP addresses that are protected in descending order by traffic volume at that point in time.
- Time range: You can select **Last 30 Minutes**, **Last Day**, **Last 7 Days**, or **Last 30 Days**. You can also customize a time range to query related data.

  A custom time range must be within the last 30 days.

Description of DDoS attack events

List of attack events: shows all the attack events that are detected by the Anti-DDoS Origin instance. Each attack event record contains the following information: **Attack Time**, **Event**, **Attacked IP Address**, **Triggered Attack Traffic (bit/s)**, **Peak Attack Traffic (bit/s)**, and **Peak Attack Traffic (pps)**.

You can perform the following operations on an attack event:

- **Cancel Scrubbing**: You can perform this operation only on in-progress traffic scrubbing events. If you confirm that a traffic surge is not caused by attacks, you can manually cancel traffic scrubbing. For example, a traffic surge may be caused by promotional events.
- **Download**: You can perform this operation to download the packet capture files for the attack event. You can use the downloaded files as evidence to report to network supervisors.
- **View Attack Analysis**: You can perform this operation to view analysis details about the attack event. For more information, see View information on the Attack Analysis page.

You can specify a protected object and a time range in the traffic trend charts section to filter attack events.

Description of attack trend charts

Section 4 displays the trends of network attacks detected by the Anti-DDoS Origin instance over the last year. This section provides the following charts:

- **Attack Trend (IP Address)**: displays the trends of the number of attacks detected by the Anti-DDoS Origin instance. You can view the following information: **Mitigation**, **Blackhole Filtering Event**, **IP Address Under Mitigation**, and **IP Address Under Blackhole Filtering**.
- **Peak Attack Throughput (IP Address)**: displays the trends of peak traffic of attacks detected by the Anti-DDoS Origin instance.
- **Attacked Duration (IP)**: displays the trends of attacks by duration. The durations include **Less Than 10 Minutes**, **10-30 Minutes**, **30-120 Minutes**, **2-10 Hours**, and **More Than 10 Hours**.

In the upper-right corner above a chart, you can specify a time range to query related data. You can select **Last 1 Week**, **Last 1 Month**, **Last 3 Months**, or **Last 1 Year** to query related data.

6.View information on the Attack Analysis page

After you add your public IP address in the cloud to an Anti-DDoS Origin Enterprise instance, you can query the DDoS attack events that occur on the asset and the event details on the Attack Analysis page. This way, you can view the details of the attack mitigation process. This topic describes how to view information on the Attack Analysis page.

Prerequisites

- An Anti-DDoS Origin Enterprise instance is purchased.

  For more information, see Purchase an Anti-DDoS Origin Enterprise instance.
- The public IP addresses that you want to protect are added to the Anti-DDoS Origin Enterprise instance.

  For more information, see Add a cloud service to Anti-DDoS Origin Enterprise for protection.

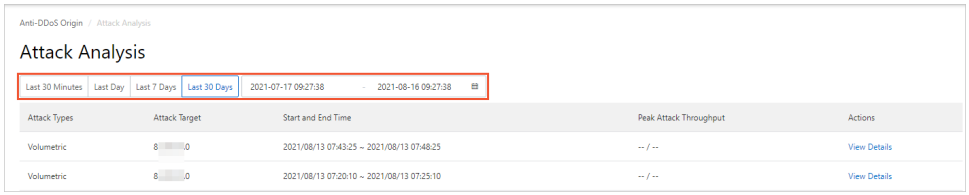
Context

The **Attack Analysis** page displays the events of volumetric DDoS attacks and the event details. On the **Attack Analysis** page, you can view the information about an attack event, such as the attack target, start time, end time, and peak attack traffic. You can also view the event details on the **Attack Analysis**. The details include the source IP addresses, attack types, and source locations. This allows you to view the attack mitigation process in a visualized manner. User experience is improved.

Procedure

1.
2.
3. On the **Attack Analysis** page, select a time range to query attack events.

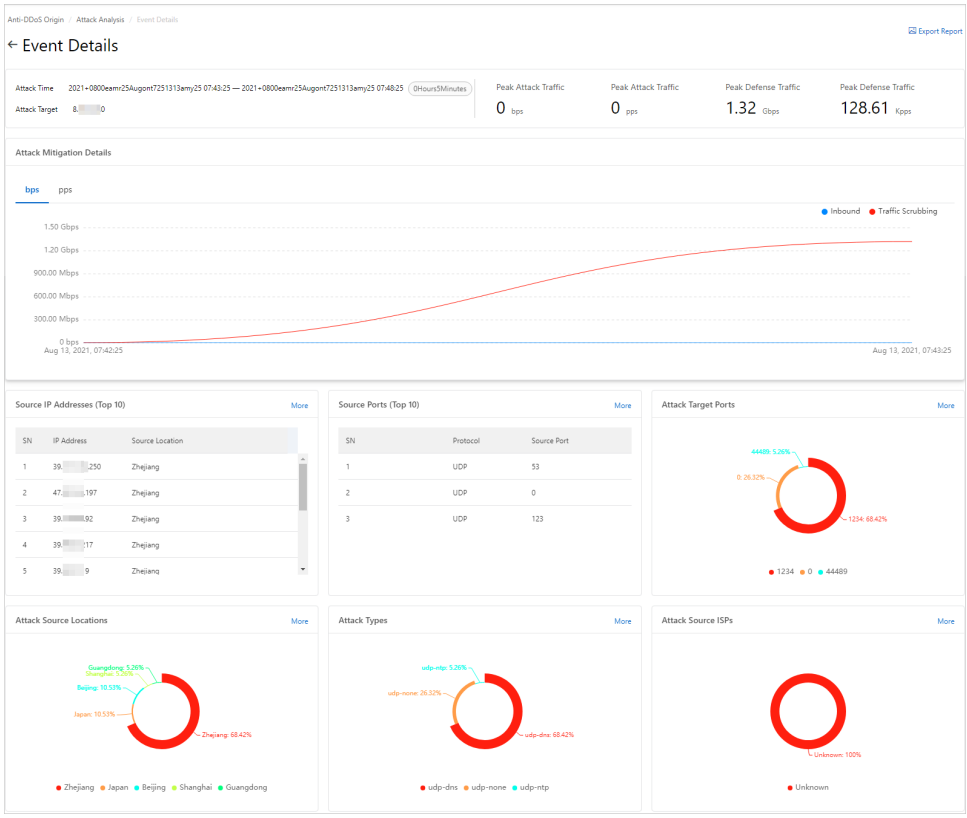
   You can select **Last 30 Minutes**, **Last Day**, **Last 7 Days**, or **Last 30 Days**. You can also specify a custom time range. A custom time range must be within the last 30 days.

   The **Attack Analysis** page displays the volumetric DDoS attack events that occur on your public IP addresses that are protected by the Anti-DDoS Origin Enterprise instance. The IP addresses may be from different regions. Each attack event contains the following information:

   - **Attack Types**: Only **Volumetric** is supported.
   - **Attack Target**: the public IP address that is attacked.
   - **Start and End Time**: the start time and end time of the attack.
   - **Peak Attack Throughput**: the peak attack bandwidth in bit/s and the peak forwarding rate of attack packets in pps.
4. View event details.

You can click **View Details** in the Actions column of an attack event to go to the **Event Details** page. On this page, you can view the event details and perform the required operations.



The **Event Details** page displays the following information:

- **Attack Time**, **Attack Target**, **Peak Attack Traffic**, and **Peak Defense Traffic**, which are in the upper part of the page.

  Peak Attack Traffic: displays the peak attack bandwidth and the peak forwarding rate of the attack packets that are detected by the Anti-DDoS Origin Enterprise instance. **Peak Defense Traffic**: displays the peak attack bandwidth that is scrubbed by the Anti-DDoS Origin Enterprise instance and the peak forwarding rate of the attack packets. The peak attack bandwidth is in bit/s and the peak forwarding rate is in pps.

- **Attack Mitigation Details**: displays the trends of bandwidth changes to the inbound traffic and the scrubbed traffic, and the trends of forwarding rate changes to the inbound packets and the traffic scrubbing packets. The bandwidths of the inbound traffic and the scrubbed traffic are in bit/s and the forwarding rates of the inbound packets and the traffic scrubbing packets are in pps.

- **Source IP Addresses (Top 10)**: displays the source locations and IP addresses of requests. The list displays the top 10 IP addresses from which the most requests are initiated. You can click **More** to view the top 100 IP addresses.

  > **Note** The requests include attack requests and normal service requests.

- **Source Ports (Top 10)**: displays the source ports and protocols of the requests. The list displays the top 10 ports from which the most requests are initiated. You can click **More** to view the top 100 ports.

> **Note** The requests include attack requests and normal service requests.

- **Attack Target Ports**: displays the distribution of destination ports. You can click **More** to view the distribution of requests destined for different destination ports.

  > **Note** The requests include attack requests and normal service requests.

- **Attack Source Locations**: displays the distribution of locations from which attack traffic is originated. You can click **More** to view the distribution of requests originated from different locations.
- **Attack Types**: displays the distribution of attack types. You can click **More** to view the distribution of different attack types.
- **Attack Source ISPs**: displays the distribution of Internet service providers (ISPs) from which attack traffic is originated. You can click **More** to view the distribution of requests originated from different ISP networks.

7.On-demand protection

7.1. Enable traffic rerouting to an on-demand instance

After you purchase an on-demand Anti-DDoS Origin instance, you can manually enable traffic rerouting to the instance if DDoS attacks are detected on a server in a data center. Then, traffic is rerouted to the traffic scrubbing centers of Alibaba Cloud around the world for traffic scrubbing. After the attacks stop, you can manually disable traffic rerouting to the on-demand instance to prevent a latency increase for your services. This topic describes how to enable and disable traffic rerouting to an on-demand instance for a server in a data center.

Scenarios

You can use on-demand instances to protect servers in data centers outside the Chinese mainland without the need to change IP addresses and network architecture for your services.

Prerequisites

An on-demand Anti-DDoS Origin instance is purchased.

> Note

Procedure

1.
2.
3.
4.
5. Find the on-demand instance for which you want to enable traffic rerouting and click **Start Redirection** in the Operation column. In the message that appears, click **OK**.
   After you enable traffic rerouting to the on-demand instance, the instance enters the **Redirecting** state. This indicates that the system is rerouting the traffic destined for protected assets to mitigate DDoS attacks.

   If you want to stop traffic rerouting to the on-demand instance, click **Pause Redirection** in the Operation column.

   > **Note** After you click Pause Redirection, the system no longer reroutes the traffic destined for protected assets to your on-demand instance and does not mitigate DDoS attacks for your assets.

What to do next

You can also enable the Automatic (NetFlow) mode to automatically reroute traffic to an on-demand instance. You can enable or disable traffic rerouting to an on-demand instance based on the NetFlow information about your servers in data centers and rules that you specified. For more information about how to enable the Automatic (NetFlow) mode, see Enable the Automatic (NetFlow) mode.

Related operations

- ModifyOnDemaondDefenseStatus

7.2. Enable the Automatic (NetFlow) mode

After you purchase an on-demand Anti-DDoS Origin instance, you can configure the start mode for the instance. If you use the default start mode and DDoS attacks are detected on your server in a data center, you must manually enable traffic rerouting to the instance. You can also enable the Automatic (NetFlow) mode. If the inbound bandwidth or packets consecutively exceed a threshold for the specified number of times, the Automatic (NetFlow) mode allows the system to automatically reroute traffic to the instance.

Prerequisites

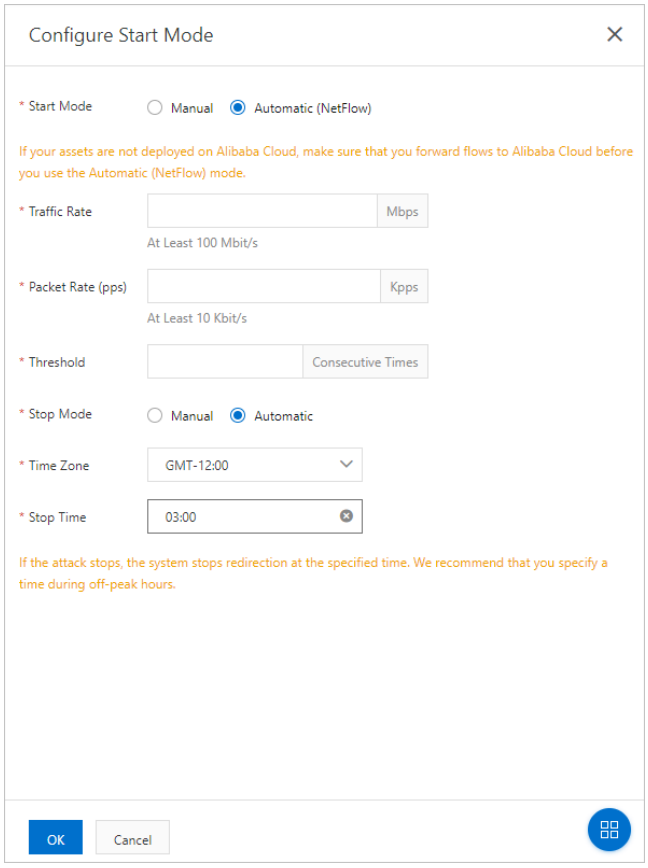
- An on-demand Anti-DDoS Origin instance is purchased.

  Note

- To protect the assets that are not deployed on Alibaba Cloud, such as servers in data centers, you must provide the NetFlow information of these servers for Alibaba Cloud. For more information, submit a or use a DingTalk group to submit the application.

Procedure

1.
2.
3.
4. Find the on-demand instance for which you want to enable the Automatic (NetFlow) mode and choose **More > Configure Start Mode** in the Operation column.
5. In the **Configure Start Mode** panel, configure the parameters.



Parameter	Description
Start Mode	The mode used to enable traffic rerouting to the on-demand instance. Valid values: ○ **Manual**: If DDoS attacks are detected on your server in a data center, you must manually enable traffic rerouting to the on-demand instance. After the attacks stop, you must manually disable traffic rerouting to the on-demand instance. This is the default value. If you select this option, you do not need to configure other parameters. ○ **Automatic (NetFlow)**: If the inbound bandwidth or packets consecutively exceed the threshold for the specified number of times, the system automatically reroutes traffic to the on-demand instance. If you select this option, you must configure other parameters, including Stop Mode. **Notice** Before you enable the **Automatic (NetFlow)** mode, make sure that you have provided the NetFlow information of your server for Alibaba Cloud.
Traffic Rate	The threshold of inbound bandwidth. Unit: Mbit/s. Minimum value: 100.
Packet Rate (pps)	The threshold of inbound packets. Unit: Kpps. Minimum value: 10.

Parameter	Description
Threshold	If the inbound bandwidth or packets consecutively exceed the threshold for the specified number of times, the system automatically reroutes traffic to the on-demand instance. The specified number of times is the value of this parameter.
Stop Mode	The mode used to stop traffic rerouting to the on-demand instance. Valid values: ○ **Manual**: If the DDoS attacks stop, you must manually disable traffic rerouting to the on-demand instance. This is the default value. ○ **Automatic**: If the DDoS attacks stop, the system no longer reroutes traffic to the on-demand instance from the time you specified. If you select this option, you must configure the following parameters: ■ **Time Zone**: the time zone of your server. The time zone must be in the `GMT-hh:mm` format. For example, the value `GMT-08:00` indicates that the time zone is UTC+8. ■ **Stop Time**: the time from which the system no longer reroutes traffic to the on-demand instance. The time must be in the 24-hour clock and in the `hh:mm` format. We recommend that you set this parameter to a value that is defined as off-peak hours. If the system detects that DDoS attacks stop, the system no longer reroutes traffic to the on-demand instance from the time you specified.

6. Click **OK**.
   After the Automatic (NetFlow) mode is enabled, if the inbound bandwidth or packets consecutively exceed the threshold for the specified number of times, the system automatically reroutes traffic to the on-demand instance. You can view the protection status of the on-demand instance on the **Others** tab of the **Assets** page. For more information, see Enable traffic rerouting to an on-demand instance.

References

- SetInstanceModeOnDemand: specifies the scheduling mode for an on-demand instance.
- CreateSchedruleOnDemand: creates a scheduling rule for an on-demand instance.
- QuerySchedruleOnDemand: queries the scheduling rule of an on-demand instance.
- ConfigSchedruleOnDemand: modifies the scheduling rule of an on-demand instance.
- DeleteSchedruleOnDemand: deletes the scheduling rule of an on-demand instance.

8.Cleaning settings

8.1. Configure a traffic scrubbing threshold

By default, Anti-DDoS Origin provides free basic protection for your assets that are deployed on Alibaba Cloud. The assets include the public IP addresses of Elastic Compute Service (ECS) instances, public IP addresses of Server Load Balancer (SLB) instances, and elastic IP addresses (EIPs). Basic protection can be used to mitigate DDoS attacks of up to 5 Gbit/s. If the service traffic of an asset exceeds the normal service traffic, Anti-DDoS Origin scrubs the attack traffic to ensure service availability. This topic describes how to configure a traffic scrubbing threshold.

Context

Anti-DDoS Origin uses artificial intelligence (AI) to analyze and scrub attack traffic. You can configure a traffic scrubbing threshold based on your normal service traffic. Then, Anti-DDoS Origin uses the big data capabilities provided by Alibaba Cloud to learn the normal service traffic and uses algorithms to identify DDoS attacks.

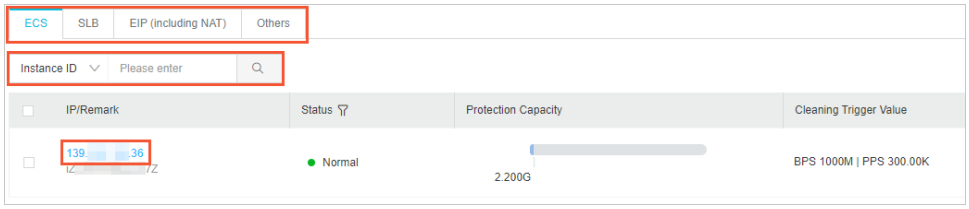
Anti-DDoS Origin scrubs attack traffic only when Anti-DDoS Origin identifies DDoS attacks and the attack traffic reaches the traffic scrubbing threshold that you configure. This prevents traffic scrubbing by mistake due to a fixed traffic scrubbing threshold. For example, if your normal service traffic fluctuates and exceeds the fixed traffic scrubbing threshold, traffic scrubbing may be triggered by mistake.

Procedure

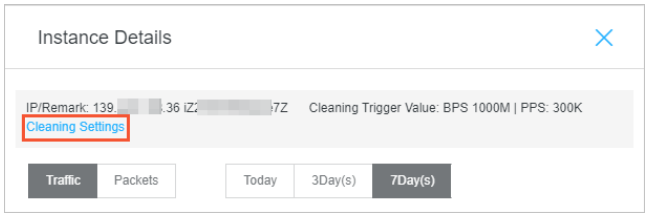
1.
2.
3.
4. Click the **ECS**, **SLB**, or **EIP (including NAT)** tab and select an asset for which you want to configure a traffic scrubbing threshold.

   > **Note** On the **Others** tab, you can configure on-demand Anti-DDoS Origin instances. You cannot configure traffic scrubbing on this tab. For more information about on-demand Anti-DDoS Origin instances, see Enable traffic rerouting to an on-demand instance.

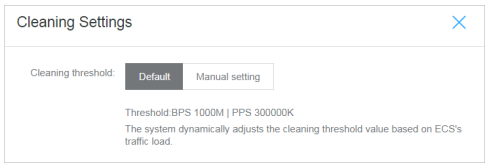
5. In the IP address list, click the IP address for which you want to configure a traffic scrubbing threshold in the **IP/Remark** column.



6. In the **Instance Details** panel, click **Cleaning Settings**.



7. In the **Cleaning Settings** panel, specify **Cleaning threshold** for the IP address.



You can set Cleaning threshold to one of the following values to configure a traffic scrubbing threshold:

- **Default**: Anti-DDoS Origin adjusts the traffic scrubbing threshold based on the throughput of your ECS instance.
- **Manual setting**: You can select a specific threshold that includes **Traffic** and **Packets per Second**.

  > **Note** If DDoS attacks are detected, or the throughput or the packets per second (pps) reaches the selected threshold, traffic scrubbing is triggered.

  If you select Manual setting, take note of the following items:

  - Configure a traffic scrubbing threshold that is slightly greater than the actual throughput and pps. If the threshold is significantly greater than the actual throughput or pps, the protection effect is compromised. If the threshold is significantly less than the actual throughput or pps, normal traffic may be scrubbed.
  - If normal traffic is scrubbed, we recommend that you increase the traffic scrubbing threshold.
  - During large promotions or activities for a website, we recommend that you increase the traffic scrubbing threshold.

8. Click **OK**.

8.2. Cancel traffic cleaning

Anti-DDoS Basic provides default protection against distributed denial of service (DDoS) attacks for Alibaba Cloud instances. Anti-DDoS Basic automatically detects attacks and cleans excessively high traffic for instances that experience flood attacks. You can cancel traffic cleaning for IP-bound assets that are in an abnormal state such as cleaning.

Context

Cleaning refers to real-time monitoring that Anti-DDoS Basic performs on incoming data traffic of instances. Based on the monitoring result, Anti-DDoS identifies suspicious traffic such as DDoS attacks. On the premises of business continuity, Anti-DDoS Basic cleans excessively high traffic and redirects suspicious traffic from original routes to a cleaning module. Then, the cleaning module identifies and strips malicious content from suspicious traffic. After the filtering process, legitimate traffic is returned to the original routes and then forwarded to target systems.

> **Note** You can cancel cleaning a maximum of three times a day for each account.

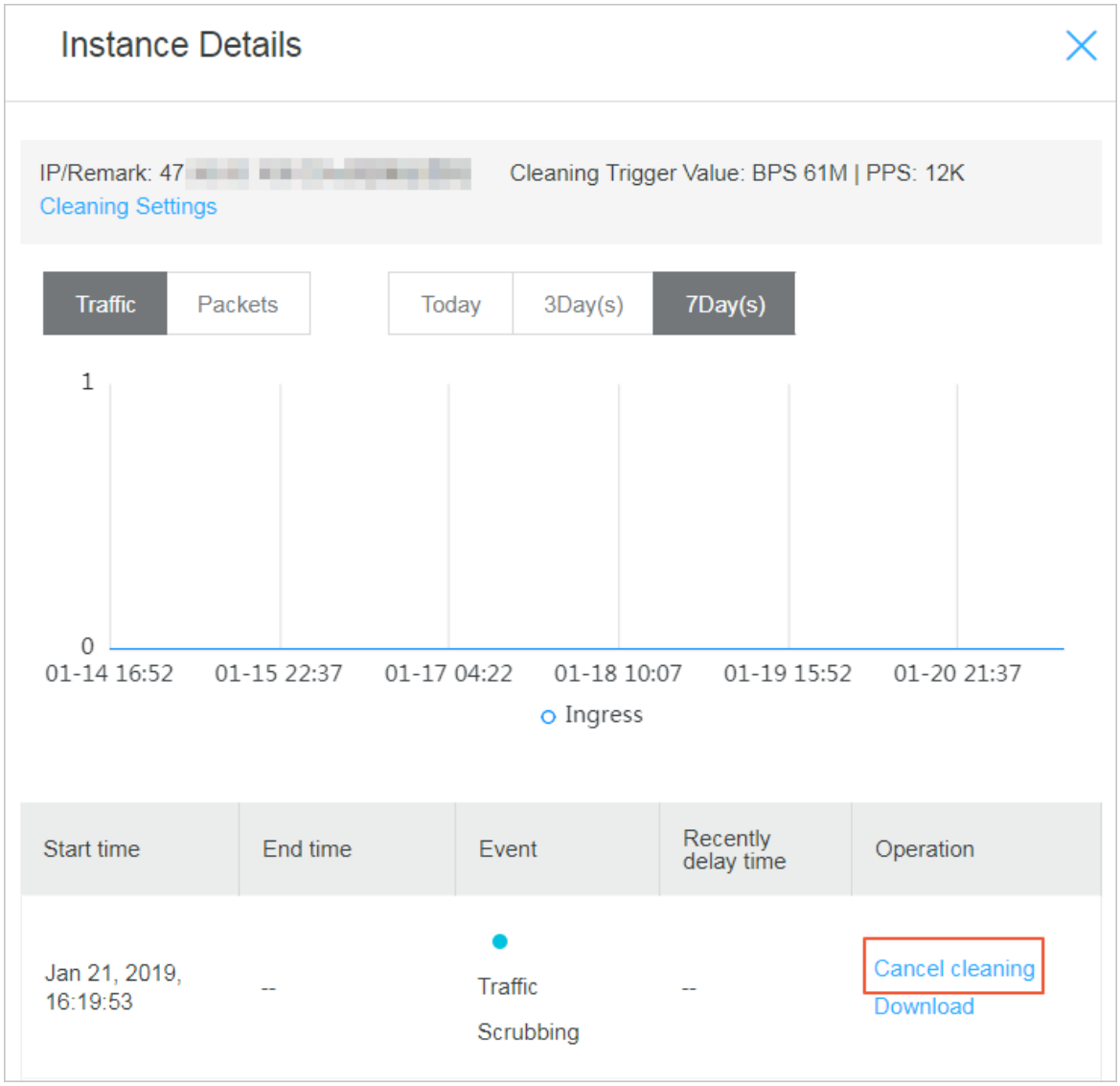
Procedure

1.
2.
3. Click the **ECS**, **SLB**, or **EIP (including NAT)** tab and select an asset for which you want to configure a traffic scrubbing threshold.

   > **Note** On the **Others** tab, you can configure on-demand Anti-DDoS Origin instances. You cannot configure traffic scrubbing on this tab. For more information about on-demand Anti-DDoS Origin instances, see Enable traffic rerouting to an on-demand instance.

4. In a list of instances, find an instance of which the **Status** is **Cleaning**, and click the **IP** of the instance.
5. On the **Instance Details** page, find an entry of which the **Event** is **Traffic Scrubbing** and the **End Time** is empty and click **Cancel cleaning** in the Operation column.

   > **Note** If no traffic scrubbing event exists, the **cancel cleaning** operation is unavailable.



Result

The traffic cleaning operation is canceled.

What's next

After you cancel traffic cleaning, we recommend that you increase cleaning thresholds in specific scenarios, such as scenarios with a sharp increase in traffic during large activities or promotions. This action avoids triggering traffic cleaning again. For more information, see Configure a traffic scrubbing threshold.

> **Note** The maximum cleaning threshold for each instance of a cloud service changes based on the instance type. If the maximum cleaning threshold that you can configure cannot meet your requirements, we recommend that you upgrade the specified instance type of the cloud service.

8.3. Cloud service specification and

cleaning trigger value

Alibaba Cloud provides basic DDoS protection capabilities to help mitigate DDoS attacks on cloud products open to the public network. When the network traffic of the public IP address of the cloud product exceeds the specified cleaning threshold, the traffic to this IP is automatically scrubbed to protect your normal service from DDoS attacks.

For more information about traffic scrubbing, see Traffic scrubbing, black hole, and threshold value.

The maximum cleaning threshold supported for each Alibaba cloud service depends on the specifications of the instance. When you create or change an ECS or SLB instance, the system automatically adjusts the maximum cleaning threshold based on the current instance specification.

> **Note** The actual black hole threshold for each instance IP is calculated based on factors such as maximum cleaning threshold and security credibility score.

- For the specific calculation method of the maximum cleaning threshold of ECS instances, see Basic DDoS Protection for ECS.
- For the specific calculation method of the maximum cleaning threshold of SLB instances, see Basic DDoS Protection for SLB.

8.4. Perform a stress test on an ECS instance

Anti-DDoS Origin Basic provides protection against DDoS attacks for Elastic Compute Service (ECS) instances free of charge. By default, if the network bandwidth of an ECS instance exceeds 180 Mbit/s, the number of packets exceeds 30,000 per second, or the number of HTTP requests exceeds 480 per second, Anti-DDoS Origin Basic automatically scrubs traffic. The preceding values may vary based on instance types.

Before you perform a stress test on an ECS instance, you must log on to the Anti-DDoS console to change the protection threshold for the ECS instance. For more information, see Configure a traffic scrubbing threshold.

> **Note** We recommend that you do not increase the request volume more than 100 times per minute during the stress test.

9.Instances

9.1. Add a cloud service to Anti-DDoS Origin Enterprise for protection

After you purchase an Anti-DDoS Origin Enterprise instance, you can add the IP addresses of your Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, Web Application Firewall (WAF) instances, or your elastic IP addresses (EIPs) to Anti-DDoS Origin Enterprise for protection.

Prerequisites

An Anti-DDoS Origin Enterprise instance is purchased. For more information, see Purchase an Anti-DDoS Origin Enterprise instance.

> Note

Procedure

1.
2.
3.
4. On the **Manage Instances** page, find the purchased Anti-DDoS Origin Enterprise instance. In the Actions column, click **Add Protected Asset**.

   > Note **Add Protected Asset** appears only if no IP addresses of cloud services are added to the instance. If the IP address of a cloud service is added to the instance, you can click **Manage** in the Actions column. On the **Instances** page, click **Add Protected Asset**.

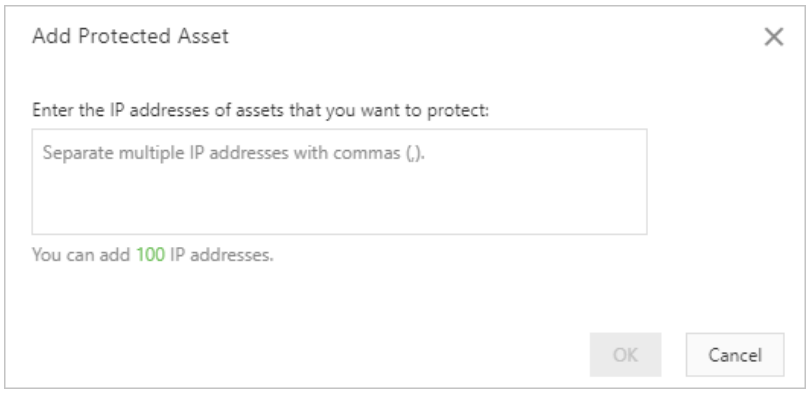
   

5. (Optional)Authorize Anti-DDoS Origin Enterprise to access other cloud services.
   - If you use Anti-DDoS Origin Enterprise for the first time, you must follow the instructions that are provided on the page to complete the authorization for the cloud services under your account.

     > Note The authorization prompt appears only if you use the Anti-DDoS Origin Enterprise instance for the first time. If authorization is complete, no prompt appears.

   - If you have already completed the authorization, skip this step.
6. In the **Add Protection Target** dialog box, add the IP address of a cloud service that you want to protect, and click **OK**.

> **Note**
>
> - You must enter the IP addresses of ECS, SLB, and WAF instances, and EIPs under your Alibaba Cloud account. These instances and EIPs must be in the same region as the Anti-DDoS Origin Enterprise instance.
> - You must separate multiple IP addresses with commas (,).



After the configuration is complete, Anti-DDoS Origin Enterprise protects the IP address that you added.

FAQ:

- When I add the IP address of a service, the system prompts that the number of IP addresses reaches the upper limit. What do I do?
- What do I do if the error message "The IP address does not belong to your account" is displayed when I add an IP address to Anti-DDoS Origin?

References

- View security reports
- Deactivate blackhole filtering

9.2. View security reports

After you add an IP address to an Anti-DDoS Origin instance for protection, you can view security reports in the Anti-DDoS Origin console. The security reports include the traffic overview of the instance, traffic information about each IP address, and DDoS attack events.

Procedure

1.
2.
3.
4. On the **Manage Instances** page, find the instance whose security reports you want to view and click **View Monitoring Details** in the **Actions** column. The **Monitoring** page appears.
5. On the **Monitoring** page, select a protected object and a time range. The console shows the trend of network traffic and DDoS attack events. The network traffic metric includes the inbound traffic and number of received data packets.

> **Note** You can query security reports of the last 30 days.

9.3. View operation logs

This topic describes how to view the operation logs of Anti-DDoS Origin instances. In the Anti-DDoS Origin console, you can trace configuration changes of each instance.

Procedure

1.
2.
3.
4. On the **Manage Instances** page, find the instance whose operation logs you want to view and click **Operation Log** in the **Actions** column.
5. On the **Operation Log** page, view the configuration change logs of the instance.

   You can specify a time range and query operation logs that are generated within the time range. Each operation log includes the operation time and details.

> **Note** You can view operation logs of the last 30 days.

9.4. Upgrade an Anti-DDoS Origin Enterprise instance

If the clean bandwidth and the protected IP addresses of your Anti-DDoS Origin Enterprise instance do not meet your business requirements, you can upgrade the instance. This topic describes how to upgrade your Anti-DDoS Origin Enterprise instance.

Prerequisites

An Anti-DDoS Origin Enterprise instance is purchased. For more information, see Purchase an Anti-DDoS Origin Enterprise instance.

Context

You can increase the values of **Business Scale** and **IP Addresses** of the purchased Anti-DDoS Origin Enterprise instance. For more information about instance specifications, see Purchase an Anti-DDoS Origin Enterprise instance.

> **Note** You cannot upgrade an Anti-DDoS Origin Basic instance. If you use an Anti-DDoS Origin Basic instance and the default 5 Gbit/s protection bandwidth does not meet your business requirements, you can purchase an Anti-DDoS Origin Enterprise instance. For more information, see Purchase an Anti-DDoS Origin Enterprise instance.

Procedure

1.

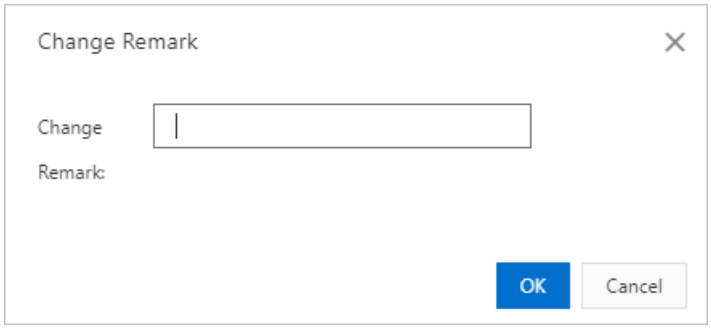
2.
3.
4. On the **Manage Instances** page, find the instance that you want to upgrade. In the **Actions** column, click the **More** icon and select **Upgrade**.
5. On the **Upgrade/Downgrade** page, upgrade the instance.
6. Read and select **Anti-DDoS Origin Terms of Service** and click **Buy Now**.
7. Complete the payment.

9.5. Specify an alias for an Anti-DDoS Origin instance

You can specify an alias for an Anti-DDoS Origin instance. If you have multiple Anti-DDoS Origin instances, you can specify an alias for each instance based on the characteristics of the instances. The characteristics include the applicable object, usage scenario, and object scope. You can use aliases to differentiate instances to simplify identification and management of your instances.

Procedure

1.
2.
3.
4. On the **Manage Instances** page, find the instance for which you want to specify an alias and click the Edit icon to the right of **Remark**.
5. In the **Change Remark** dialog box, enter an alias and click **OK**.



Result

After you specify the alias, the alias is displayed below the ID of the instance. You can repeat the preceding steps to change the alias of an Anti-DDoS Origin instance at any time based on your business requirements.

10.Mitigation settings (public preview)

10.1. Configure cross-border traffic blocking

After you add the IP address of your cloud asset to Anti-DDoS Origin Enterprise, you can enable the cross-border traffic blocking feature to block cross-border traffic. This improves DDoS mitigation effects. This feature is applicable to scenarios where your service does not involve cross-border traffic.

Prerequisites

- An Anti-DDoS Origin Enterprise instance is purchased.

  For more information, see Purchase an Anti-DDoS Origin Enterprise instance.

  > **Note** The mitigation settings feature is now public preview. If you have purchased an Anti-DDoS Origin Enterprise instance, you can submit a to enable this feature.

- The IP address of your cloud asset is added to Anti-DDoS Origin Enterprise.

  For more information, see Add a cloud service to Anti-DDoS Origin Enterprise for protection.

Context

The cross-border traffic blocking feature blocks cross-border traffic within a specific blocking period

- Cross-border traffic:
  - If your cloud asset resides in mainland China, the feature blocks traffic that originates from outside mainland China.
  - If your cloud asset resides outside mainland China, this feature blocks traffic that originates from mainland China.
- Blocking period: 30 minutes to 1 day.
- Limits: By default, you can enable this feature 10 times per month for each Anti-DDoS Origin Enterprise instance.

  If your quota is exhausted, you can submit a to request technical support.

You can manually disable this feature at any time during the blocking period.

Enable cross-border traffic blocking

1.
2.
3. On the **Cross-Border Traffic Blocking** tab, select the region where the Anti-DDoS Origin Enterprise instance resides and the instance that you want to manage.
4. In the protected asset list, find the IP address that you want to manage and enable the feature.

   You can use one of the following methods to enable the feature:

- For an IP address: Find the IP address and turn on **Region Blocking**.
- For multiple IP addresses: Select the IP addresses and click **Batch Enable**.

5. In the **Configure Blocking Period** dialog box, select a duration and click **OK**.

   Valid values: 30 minutes to 1 day.

   > **Note** The blocking period cannot be modified after it is applied. If you need to modify the blocking period, you must disable the cross-border traffic blocking feature and configure the blocking period again.

   After the preceding settings are completed, **Region Blocking** for the IP address is turned on, and the feature takes effect immediately. In the protected asset list, you can view the **Start Time** and **End Time** of the blocking period.

   After the blocking period ends, the feature no longer blocks cross-border traffic, and **Region Blocking** for the IP address is turned off.

Manually disable cross-border traffic blocking

You can manually disable the cross-border traffic blocking feature during the blocking period.

> **Note** If this feature is enabled for an IP address, you cannot remove the IP address from the Anti-DDoS Origin Enterprise instance during the blocking period. To remove the IP address, you must disable the feature.

1.
2.
3. On the **Cross-Border Traffic Blocking** tab, select the region where the Anti-DDoS Origin Enterprise instance resides and the instance that you want to manage.
4. In the protected asset list, find the IP address that you want to manage and disable the feature.

   You can use one of the following methods to disable the feature:

   - For an IP address: Find the IP address and turn off **Region Blocking**.
   - For multiple IP addresses: Select the IP addresses and click **Batch Disable**.

5. In the dialog box that appears, click **OK**.
   After the preceding settings are completed, **Region Blocking** for the IP address is turned off, and the feature no longer blocks cross-border traffic.

10.2. Configure policies

After you add the IP addresses of your cloud services to your Anti-DDoS Origin Enterprise instance, you can configure policies based on your business requirements to allow or deny requests that have specific characteristics. This better protects your cloud services against distributed denial-of-service (DDoS) attacks.

Prerequisites

- An Anti-DDoS Origin Enterprise instance is purchased. For more information, see Purchase an Anti-DDoS Origin Enterprise instance.

> **Note** The Mitigation Settings feature that provides policy configuration is in public preview and is free of charge. This feature is available only if an Anti-DDoS Origin Enterprise instance is purchased. If you want to enable this feature, submit a .

- The IP addresses of your cloud services are added to the Anti-DDoS Origin Enterprise instance. For more information, see Add a cloud service to Anti-DDoS Origin Enterprise for protection.

Procedure overview

If this is the first time you use the policy configuration feature, perform the following steps:

1. Create a policy template. For more information, see Select or create a policy template.
2. Add cloud services to the policy template. The policy template is applied to the added cloud services. For more information, see Add cloud services to the policy template.
3. Configure specific policies in the template. After you configure the policies, the policies take effect on the cloud services that you added in the preceding step.

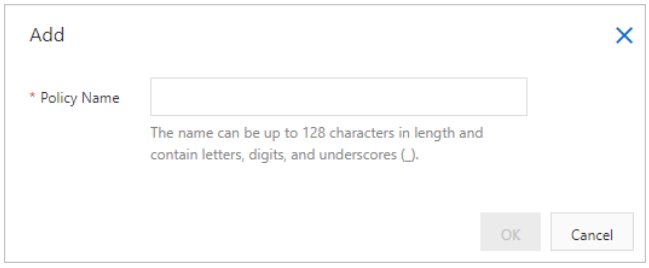
   The following table describes the supported policies.

Policy	Description	Configuration
ICMP Blocking	Denies Internet Control Message Protocol (ICMP) requests during traffic scrubbing. This protects the origin server against scans and helps mitigate ICMP flood attacks.	Turn on or off **Status** of **ICMP Blocking**. After you enable this policy, ICMP requests are denied. **Note** This policy takes effect on the IP addresses in the whitelist. ICMP requests from the IP addresses are also denied. For more information, see Configure the ICMP Blocking policy.
Source Port Blocking	Denies User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) requests over the source or destination ports to mitigate UDP reflection attacks.	Specify the protocols and ports to deny requests. After you enable this policy, requests are denied based on the specified protocol and ports. For more information, see Configure the Source Port Blocking policy.
Blacklist and Whitelist	Denies or allows requests from specific source IP addresses.	Configure the IP address blacklist and whitelist. After you enable this policy, requests from the IP addresses that are included in the blacklist are denied, and requests from the IP addresses that are included in the whitelist are allowed. For more information, see Configure the Blacklist and Whitelist policy.

Policy	Description	Configuration
Byte-Match Filter	Matches bytes for the content of specific packets to deny, allow, or limit the rates of requests when the instance is scrubbing traffic.	Specify Byte-Match Filter rules to match the required bytes. If requests contain the matching bytes, the requests are denied, allowed, or limited based on the policy. For more information, see Configure the Byte-Match Filter policy.

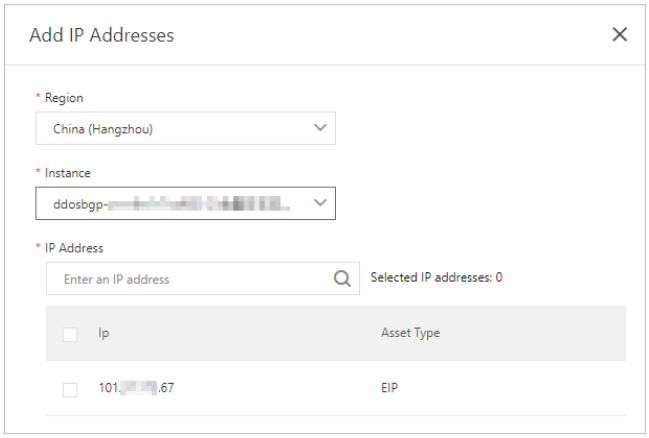
Procedure

1.
2.
3. Click the **Policy Configuration** tab.
4. Select or create a policy template.
   - If you have created policy templates, click the required policy template below **Policy Template**.
   - If you have not created policy templates, perform the following steps to create a policy template:
     a. Click **Create Policy** next to **Policy Template**.
     b. In the **Add** dialog box, specify **Policy Name** and click **OK**.



     After you create the policy template, the template is automatically selected.
5. Add cloud services to the policy template.
   i. In the **Target assets** section on the right, click **Add IP Addresses**.

ii. In the **Add IP Addresses** dialog box, select the IP addresses of the required cloud service to apply the policy template.



Parameter	Description
Region	The region of the cloud service whose IP addresses you want to add to the Anti-DDoS Origin Enterprise instance.
Instance	The Anti-DDoS Origin Enterprise instance to which you want to add the IP addresses.
IP Address	The IP addresses of the cloud service. **Note** An IP address can be added to only one policy template. You cannot select an IP address that is added to a different policy template.

iii. Click **OK**.

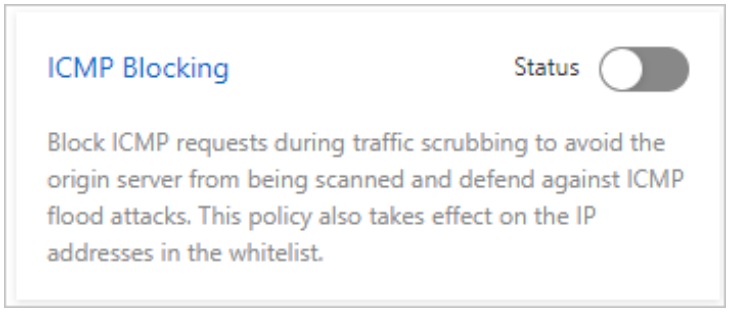
After you add the IP addresses, requests to the IP addresses are processed based on the policies in this template. By default, no policies are enabled in the newly created policy template. You must configure specific policies to deny or allow specific requests.

You can click **Remove** to remove the IP addresses of cloud services from the **Target assets** section.

6. (Optional)Configure the **ICMP Blocking** policy.

To enable or disable the **ICMP Blocking** policy, perform the following steps:

i. On the Policy Configuration tab, turn on or off **Status** for the **ICMP Blocking** option.

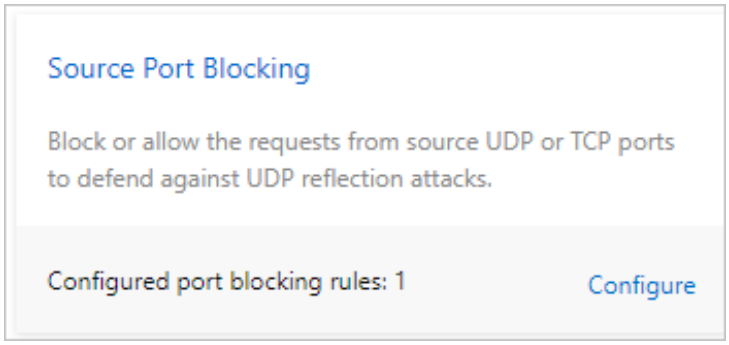


ii. In the **Ok** dialog box, click **OK**.

7. (Optional)Configure the **Source Port Blocking** policy.

   To configure the Source Port Blocking policy, perform the following steps:

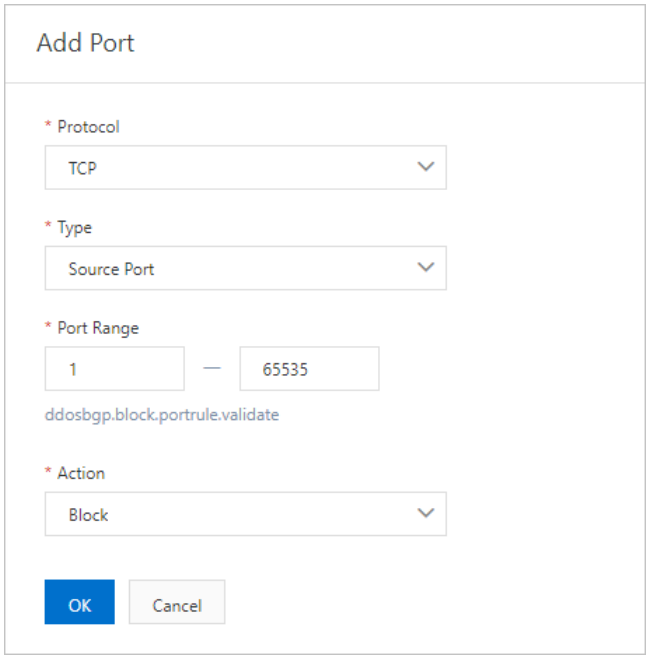
   i. On the Policy Configuration tab, click **Configure** for the **Source Port Blocking** option.



   ii. In the **Configure Source Port Blocking** panel, click **Add**.

> **Note** You can add a maximum of eight port blocking rules.

iii. In the **Add Port** dialog box, configure the following parameters.



Parameter	Description
Protocol	The protocol of the requests that you want to block. Valid values: **TCP** and **UDP**.
Type	The type of port used by the requests that you want to block. Valid values: **Source Port** and **Destination Port**.
Port Range	The range of ports used by the requests that you want to block. Valid values: 1 to 65535. **Note** Make sure that the port ranges of two port blocking rules that have the same protocol and port type do not overlap.
Action	The action that is triggered by requests that use the specified protocol and ports. The value is fixed as **Block**.

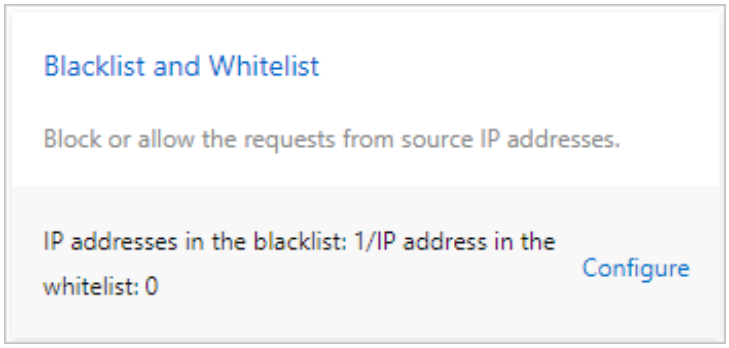
For more information about the recommended configurations of the Source Port Blocking policy, see Recommended configurations for the Source Port Blocking policy.

iv. Click **OK**.
After you add a port blocking rule, the rule automatically takes effect. Requests that use the specified protocol and ports are denied. You can manage configured port blocking rules in the **Configure Source Port Blocking** panel. For example, you can click **Edit** or **Delete** to edit or delete a port blocking rule.

8. (Optional)Configure the Blacklist and Whitelist policy.

To configure the Blacklist and Whitelist policy, perform the following steps:

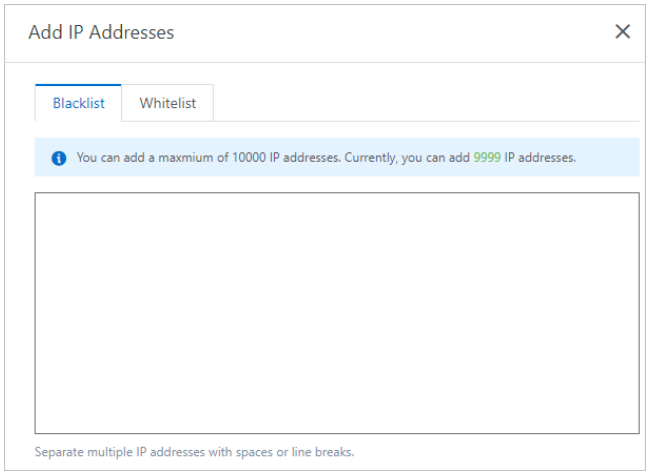
i. On the Policy Configuration tab, click **Configure** for the **Blacklist and Whitelist** option.



ii. In the **Blacklist and Whitelist** panel, click **Add IP Addresses**.

iii. In the **Add IP Addresses** dialog box, configure the blacklist and whitelist.

You can add a maximum of 10,000 IP addresses to the blacklist and a maximum of 10,000 IP addresses to the whitelist. You must separate multiple IP addresses with spaces or line feeds.

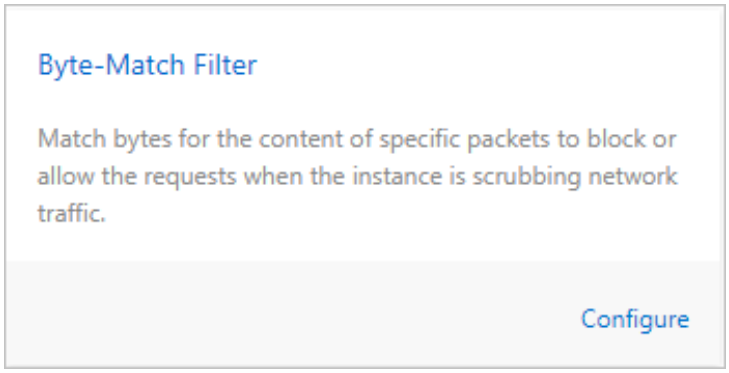


iv. Click **OK**.
After you configure the Blacklist and Whitelist policy, the policy immediately takes effect. Requests from the IP addresses that are included in the blacklist are denied, and requests from the IP addresses that are included in the whitelist are allowed. You can manage the configured blacklist and whitelist in the **Blacklist and Whitelist** panel. For example, you can click **Delete** to delete an IP address or click **Clear** to clear the blacklist or whitelist.

9. (Optional)Configure the Byte-Match Filter policy.

To configure the Byte-Match Filter policy, perform the following steps:

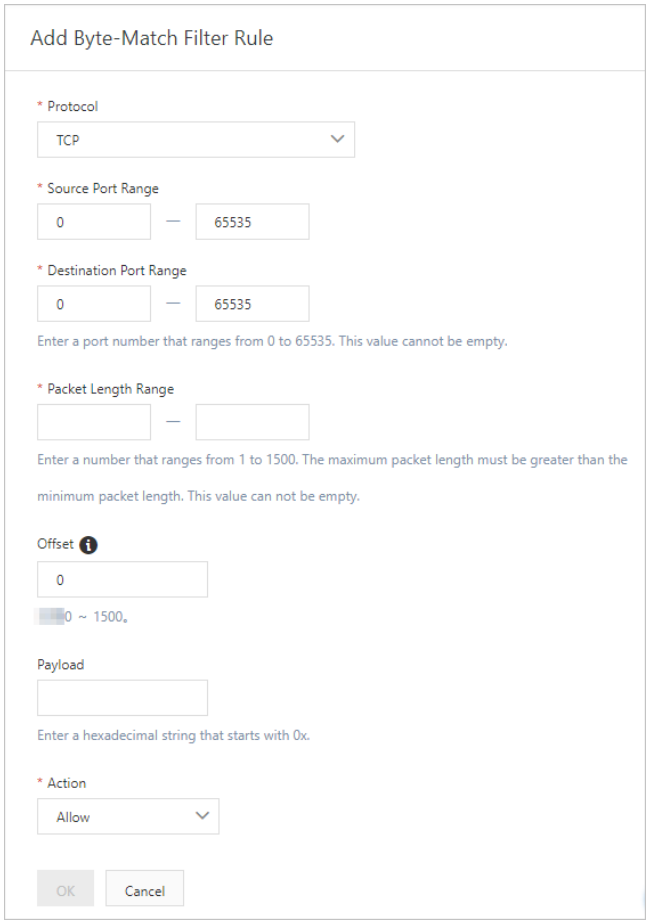
i. On the Policy Configuration tab, click **Configure** for the **Byte-Match Filter** option.



ii. In the **Configure Byte-Match Filter** panel, click **Add**.

> **Note** You can add a maximum of eight Byte-Match Filter rules.

iii. In the **Add Byte-Match Filter Rule** dialog box, configure the following parameters.



Parameter	Description
Protocol	The type of the protocol. Valid values: **TCP** and **UDP**.
Source Port Range	The range of source ports. Valid values: 1 to 65535.
Destination Port Range	The range of destination ports. Valid values: 1 to 65535.
Packet Length Range	The range of packet lengths. Valid values: 1 to 1500. Unit: bytes.
Offset	The offset of bytes in UDP or TCP packets. Valid values: 0 to 1500. Unit: bytes. If you set the offset to 0, the system starts matching from the first byte.
Payload	The matching payload of UDP or TCP packets. You must enter a hexadecimal string that starts with 0x.

Parameter	Description
Action	The action that is triggered by the matching requests. Valid values: **Allow**, **Block**, **Limit Bandwidth of Source IP Address**, and **Limit Bandwidth of Session**. If you select **Limit Bandwidth of Source IP Address** or **Limit Bandwidth of Session**, you must specify **Bandwidth**. Valid values of **Bandwidth**: 1 to 100000.

iv. Click **OK**.
After you configure the Byte-Match Filter policy, the policy automatically takes effect. Requests that meet the rules are denied, allowed, or limited based on the policy. You can manage the configured Byte-Match Filter rules in the **Configure Byte-Match Filter** panel. For example, you can click **Edit**, **Delete**, Move Down, or Move Up to manage the rules.

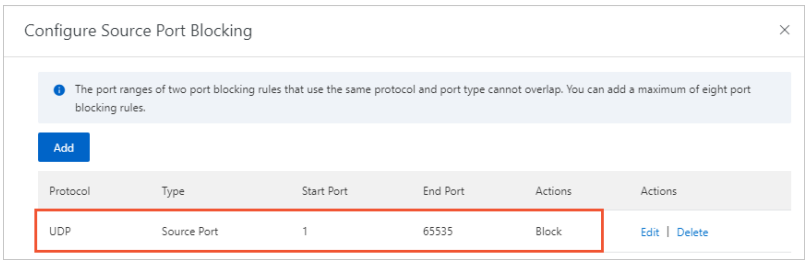
> **Note** You can adjust the order of rules for better management. The adjustment does not affect the rules.

Recommended configurations for the Source Port Blocking policy

We recommend that you configure the Source Port Blocking policy based on the following description and your business requirements. For more information, see Configure the Source Port Blocking policy.

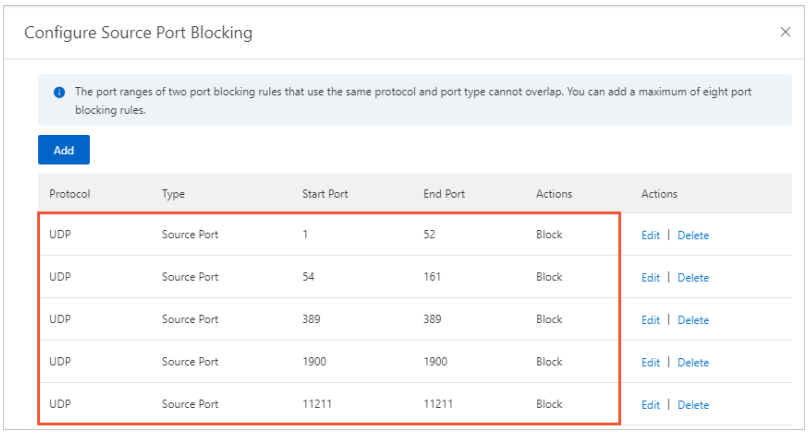
- If your cloud services that are protected by Anti-DDoS Origin Enterprise do not provide UDP services, we recommend that you block all source UDP ports.

  The following figure shows the port configuration.



- If your cloud services that are protected by Anti-DDoS Origin Enterprise provide UDP services, we recommend that you block the common source ports that are exploited by UDP reflection attacks. The ports include ports 1 to 52, ports 54 to 161, port 389, port 1900, and port 11211.

The following figure shows the port configuration.



11.Mitigation analysis (public preview)

11.1. Enable mitigation analysis

Anti-DDoS Origin Enterprise provides the mitigation analysis feature. The feature is free of charge and under public preview. You can use this feature to query and analyze mitigation logs and view mitigation reports. This topic describes how to enable the mitigation analysis feature of an Anti-DDoS Origin Enterprise instance.

Prerequisites

An Anti-DDoS Origin Enterprise instance in mainland China is purchased.

For more information, see Purchase an Anti-DDoS Origin Enterprise instance.

Procedure

1.
2.
3.
4. (Optional)If you use the feature for the first time, you must complete RAM authorization. If you have already completed RAM authorization, skip this step.
   i. Click **Authorize Now**.
   ii. On the **Cloud Resource Access Authorization** page, click **Confirm Authorization Policy**.
   iii. After the authorization is completed, go back to the **Mitigation Analysis (Beta)** page and refresh the page.
5. On the **Mitigation Analysis (Beta)** page, select an Anti-DDoS Origin Enterprise instance and click **Upgrade Now**.
6. On the **Upgrade/Downgrade** page, select On for **Mitigation Analysis (Beta)**.
7. Read and select **Anti-DDoS Origin Terms of Service**, and click **Buy Now**.
8. Complete the payment.

   > **Note** The mitigation analysis feature is free of charge and under public preview.

   After you complete the payment, you must manually enable this feature to start analysis.
9. On the **Mitigation Analysis (Beta)** page, click **Enable Now**.
   After the feature is enabled, the Anti-DDoS Origin Enterprise instance collects mitigation log data, which is stored in Log Service. This way, you can query and analyze mitigation logs and view mitigation reports. To enable or disable the feature, you can turn on or off Status.

What's next

- Query mitigation logs
- View mitigation reports

11.2. Query mitigation logs

After you enable the mitigation analysis feature, you can query and analyze mitigation logs that record the events of an Anti-DDoS Origin Enterprise instance. The events cover traffic scrubbing, blackhole filtering, and traffic rerouting.

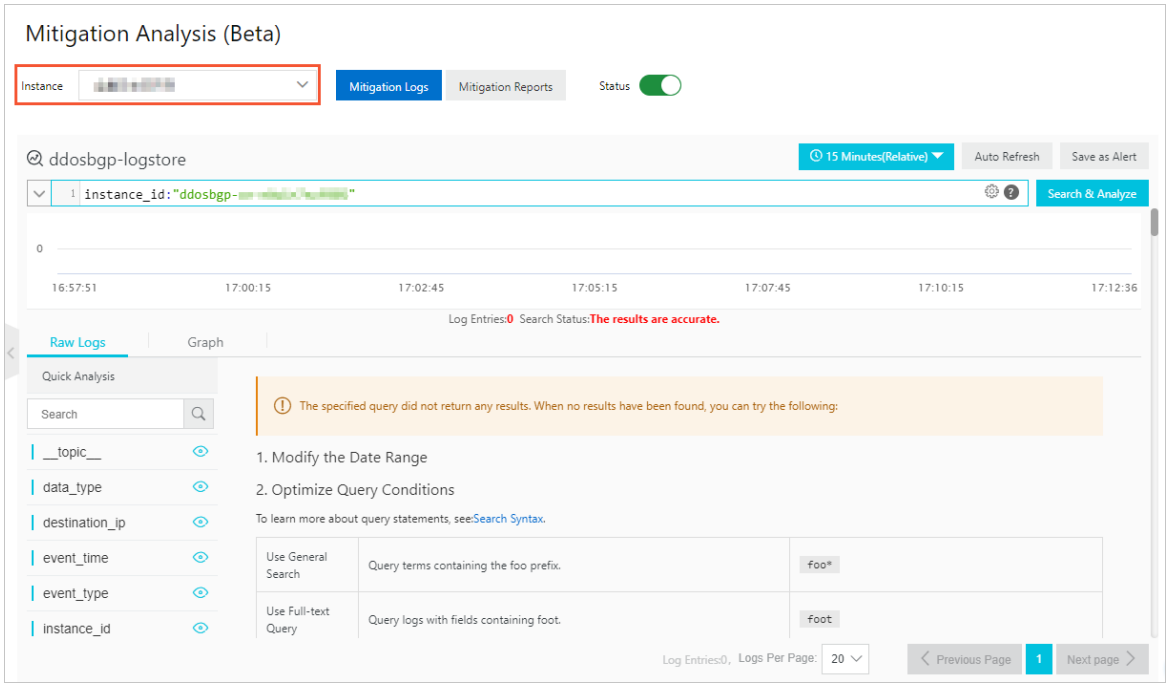
Prerequisites

The mitigation analysis feature is enabled. For more information, see Enable mitigation analysis.

Query and analyze mitigation logs

1.
2.
3.
4. On the **Mitigation Analysis (Beta)** page, select an Anti-DDoS Origin Enterprise instance.

   > **Note** To query the mitigation logs, you must turn on **Status** for the mitigation analysis feature. For more information about how to enable the feature, see Enable mitigation analysis.



5. Enter a query statement in the input field.

   A query statement consists of a search statement and an analytic statement in the format of Search statement|Analytic statement. For more information, see Search syntax and SQL syntax.

6. In the upper-right corner of the page, click **Please Select** and set a time range for the query.

   You can specify a relative time range, time frame, or custom time range.

   > **Note** The query results contain logs that are generated 1 minute earlier or later than the specified time range.

7. Click **Search & Analyze** to view the query and analysis results.

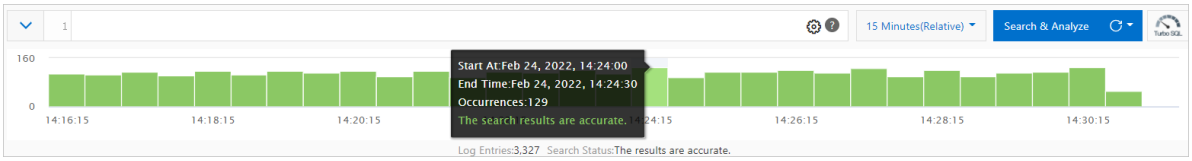
Manage query and analysis results

Log Service displays query and analysis results in a log distribution histogram, on the Raw Logs tab, and on the Graph tab. Log Service allows you to perform operations on the results. For example, you can configure alerts and create saved searches.

> **Note** When you execute a query statement, only 100 lines of data is returned by default. You can use a LIMIT clause to specify the number of lines that can be returned. For more information, see LIMIT clause.

- Log distribution histogram

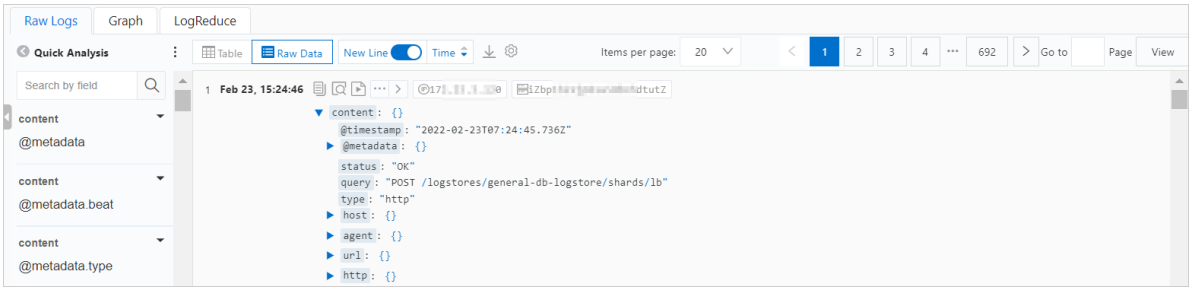
  The log distribution histogram shows the distribution of returned logs in different periods of time.



  - When you move the pointer over a green rectangle, you can view the period of time that is represented by the rectangle and the number of returned logs within the period.
  - If you click a green rectangle, you can view log distribution at a finer-grained level. In addition, you can view the returned logs within the period of time on the **Raw Logs** tab.

- Raw Logs tab

  The **Raw Logs** tab displays the logs that are queried. You can click the **Table** or **Raw Data** tab to view the logs and perform the following operations:



  - Quick Analysis: You can analyze the distribution of a field within a period of time. For more information, see Quick analysis.

    You can click the ⋮ icon to specify whether to show the names or aliases of fields. You can create aliases when you configure indexes. For example, if the alias of host_name is host, host is displayed in the Quick Analysis list after you select Show Field Aliases.

    > **Note** If a field does not have an alias, the name of the field is displayed in the Quick Analysis list even if you select Show Field Aliases.

- Context query: On the **Raw Data** tab, you can find a log and click the icon to query the context information about the log in the raw log file. For more information, see Context query.

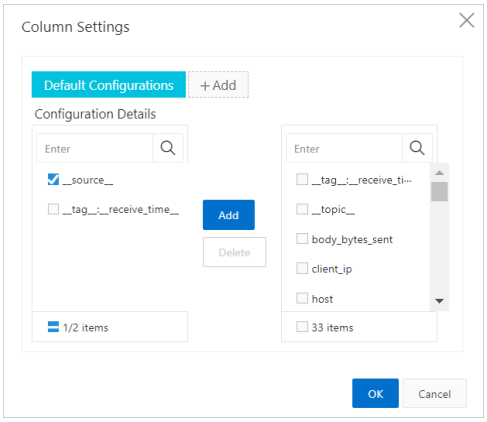
  > **Note** You can perform context query only on the logs that are collected by Logtail.

- LiveTail: On the **Raw Data** tab, you can find a log and click the icon to monitor logs in real time and extract important information from the logs. For more information, see LiveTail.

  > **Note** You can use LiveTail only on the logs that are collected by Logtail.

- Tag Configurations: On the **Raw Data** tab, you can click the icon and select **Tag Configurations** to hide less important fields.

- Column Settings: On the **Table** tab, you can click the icon and select **Column Settings** to specify the columns that you want to display in the table. The column names are field names, and the column content is field values.



- JSON Configurations: On the **Table** or **Raw Data** tab, you can click the icon and select **JSON Configurations** to specify the level for JSON expansion.
- Event Settings: On the **Table** or **Raw Data** tab, you can click the icon and select **Event Settings** to configure events for raw logs. For more information, see Configure events.
- Log Download: On the **Table** or **Raw Data** tab, you can click the icon to download logs. You can specify the tool that is used to download logs and the range of logs to download. For more information, see 下载日志.

- Graph tab

  After you execute a query statement, you can view the query and analysis results on the **Graph** tab.

- View query and analysis results: Log Service renders the results of the query statement to charts. Log Service provides various types of charts, such as tables, line charts, and column charts. For more information, see Chart overview.
- Add a chart to a dashboard: Log Service provides dashboards on which you can analyze data in real time. You can click **Add to New Dashboard** to save the query and analysis results as a chart to a dashboard. For more information, see 可视化概述.
- Configure interactive events: Interactive events are important for data analysis. You can use interactive events to switch between the levels of data dimensions and the analysis granularities to obtain more detailed information. Interactive events include events to open a Logstore, open quick analysis, open a dashboard, open trace analysis, open trace details, and customize an HTTP link. For more information, see Drill-down events.

- LogReduce tab

  On the **LogReduce** tab, you can click **Enable LogReduce** to cluster similar logs during log collection. For more information, see LogReduce.

- Alerting

  On the query and analysis page, you can choose **Save as Alert > New Alert** to configure alerts based on the query and analysis results. For more information, see Configure an alert monitoring rule in Log Service.

- Saved search

  On the query and analysis page, you can click **Save Search** to save a query statement as a saved search. For more information, see Saved search.

11.3. View mitigation reports

After you enable the mitigation analysis feature, you can view mitigation reports on the DDoS BGP Mitigation Report and DDoS BGP Events Report tabs.

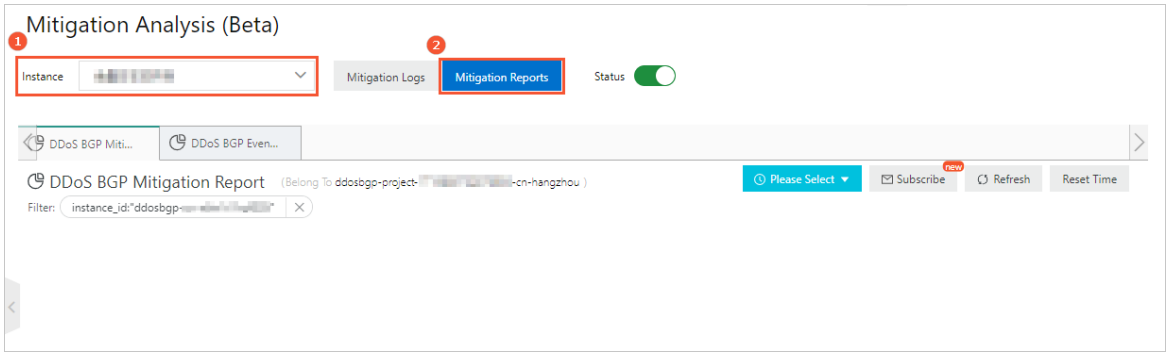
Prerequisites

The mitigation analysis feature is enabled. For more information, see Enable mitigation analysis.

Procedure

1.
2.
3.
4. On the **Mitigation Analysis (Beta)** page, select an Anti-DDoS Origin Enterprise instance and click **Mitigation Reports**.

   > **Note** To view the mitigation reports, you must turn on **Status** for the mitigation analysis feature. For more information about how to enable the feature, see Enable mitigation analysis.



5. Click the tab for a report that you want to view. The tabs include:
   - **DDoS BGP Mitigation Report**: records Inbound Traffic Monitor, Inbound Traffic Monitor (sort by scrubbing centers), Inbound Traffic Monitor (sort by flow types), PktChk, syn cookie, SrcChk, FDR, DipRate, SrcRate, L7 Filter, L4 Filter, DFPDR, DnsChk, IpDR, AntiTcp, AntiUdp, and AntiOtherTcp.
   - **DDoS BGP Events Report**: records statistics on DDoS events.
6. In the upper-right corner of the page, click **Please Select** and set a time range for query.

   You can specify a relative time range, time frame, or custom time range.

   > **Note** The query results contain reports that are generated 1 minute earlier or later than the specified time range.

7. View the mitigation reports.

11.4. Fields in logs

This topic describes all fields in the logs of Anti-DDoS Origin.

The fields are classified into the following types:

- Event fields: record information about the events that occur on the protected assets. The events include traffic scrubbing, blackhole filtering, and on-demand protection. The information includes the time at which the events occurred and the status of the events.
- Traffic detection fields: record information about the traffic that is generated on the protected assets. The information includes the transmission rate of inbound traffic and the packet forwarding rates of different types of data packets.
- Traffic scrubbing fields: record information about the traffic that is denied or allowed by different mitigation policies during traffic scrubbing.

Event fields

Field	Description	Example value

Field	Description	Example value
data_type	The data type. Valid values: • Global_SC_Detection: indicates data about the traffic that is forwarded by the traffic scrubbing center of Anti-DDoS. The traffic is protected by an on-demand instance. • Global_SC_Mitigation: indicates data about the traffic that is scrubbed by the scrubbing center of Anti-DDoS. The traffic is protected by an on-demand instance. • Regional_SC_Detection: indicates data about the inbound traffic of the region in which Alibaba Cloud assets reside. • Regional_SC_Mitigation: indicates data about the scrubbed traffic of the region in which Alibaba Cloud assets reside. • event: indicates data about attack events.	Regional_SC_Mitigation
event_time	The time at which an event occurred. This value is a UNIX timestamp. Unit: seconds.	1624434027
event_type	The type of an event. Valid values: • mitigation_begin: A traffic scrubbing event begins. • mitigation_ended: A traffic scrubbing event ends. • blackhole_begin: A blackhole filtering event begins. • blackhole_ended: A blackhole filtering event ends.	mitigation_begin
instance_id	The ID of the Anti-DDoS Origin instance.	ddosbgp-cn-n6w203qg****
ip	The IP address of an asset that is protected by the Anti-DDoS Origin instance.	39.XX.XX.23
kbps_in	The bandwidth of inbound traffic. Unit: Kbit/s.	1000
new_con	The number of new connections.	1000
pps_in	The packet forwarding rate of inbound traffic. Unit: packets per second.	1000
qps	The number of queries per second (QPS). Unit: QPS.	1000

Field	Description	Example value
scrubbing_center	The region where the traffic scrubbing center resides. Valid values: • us_west: US (Virginia) • us_east: US (Silicon Valley) • frankfurt: Germany (Frankfurt) • hk: China (Hong Kong) • singapore: Singapore (Singapore) • malaysia: Malaysia (Kuala Lumpur) • uk: UK (London) • japan: Japan (Tokyo) • total_summary: all regions • assets_base_region: the region where the asset resides	us_west
subnet	The CIDR block for on-demand protection.	1.XX.XX.1/24
user_id	The ID of an Alibaba Cloud account.	170457416359****

Traffic detection fields

Field	Description	Example value
Ip	The source IP address.	1.XX.XX.1
Time	The point in time at which the log entry about traffic detection was generated. This value is a UNIX timestamp. Unit: seconds.	1624434027
KbpsIn	The bandwidth of inbound traffic at the point in time. Unit: Kbit/s.	1000
KbpsOut	The bandwidth of outbound traffic at the point in time. Unit: Kbit/s.	1000
PpsIn	The forwarding rate of all inbound packets at the point in time. Unit: packets per second.	1000
PpsOut	The forwarding rate of all outbound packets at the point in time. Unit: packets per second.	1000
PpsInSyn	The forwarding rate of inbound SYN packets at the point in time. Unit: packets per second.	1000
PpsInSynack	The forwarding rate of inbound SYN-ACK packets at the point in time. Unit: packets per second.	1000
PpsInFin	The forwarding rate of inbound FIN or RST packets at the point in time. Unit: packets per second.	1000

Field	Description	Example value
PpsInHttpReq	The forwarding rate of inbound TCP packets at the point in time. Unit: packets per second. The TCP packets must meet all the following conditions: • The TCP packets are not SYN, SYN-ACK, FIN, or RST packets. • The destination port is 80, 3128, 8080, or 8088. • The TCP packets contain payloads. The first four bytes of the payloads in HTTP packets are GET, PUT, HEAD, or POST.	1000
PpsInHttpResp	The forwarding rate of inbound TCP packets at the point in time. Unit: packets per second. The TCP packets must meet all the following conditions: • The TCP packets are not SYN, SYN-ACK, FIN, or RST packets. • The destination port is 80, 3128, 8080, or 8088. • The TCP packets contain payloads. The first four bytes of the payloads in HTTP packets are HTTP.	1000
PpsInHttpFlags	The forwarding rate of inbound TCP-ACK packets at the point in time. Unit: packets per second. The TCP-ACK packets are not SYN, SYN-ACK, FIN, or RST packets.	1000
PpsInIcmp	The forwarding rate of inbound ICMP packets at the point in time. Unit: packets per second.	1000
PpsInDns	The forwarding rate of inbound DNS packets at the point in time. Unit: packets per second. The DNS packets are forwarded over UDP, and the source or destination port of the packets is 53.	1000
PpsInUdprisk	The forwarding rate of packets that use a vulnerable source UDP port at the point in time. Unit: packets per second.	1000
PpsInUdpunknown	The forwarding rate of inbound UDP packets at the point in time. Unit: packets per second. The forwarding rate of the UDP packets indicated by this field does not include that indicated by the PpsInDns field. The UDP packets are forwarded over UDP, but the source or destination port of the packets is not 53.	1000

Traffic scrubbing fields

Field	Description	Example value
instance_id	The ID of the Anti-DDoS Origin instance.	ddosbgp-cn-v641is26****
time	The point in time at which the log entry about traffic scrubbing was generated. This value is a UNIX timestamp. Unit: seconds.	1624434027
destination_ip	The destination IP address.	123.XX.XX.169

Field	Description	Example value
port	The destination port. Valid values: • all (default): indicates the data of all ports • Specific port: indicates the data of a specific port, such as port 80	80
total_traffic_in_bps	The total number of bytes in all types of packets that are scrubbed. Unit: byte per second.	8000
total_traffic_drop_bps	The total number of bytes of all types of packets that are scrubbed and discarded. Unit: byte per second.	800
total_traffic_in_pps	The forwarding rate of all types of inbound packets. Unit: packets per second.	1000
total_traffic_drop_pps	The forwarding rate of all types of packets that are discarded. Unit: packets per second.	1000
pps_types_in_tcp_pps	The forwarding rate of inbound TCP packets. Unit: packets per second.	100
pps_types_in_udp_pps	The forwarding rate of inbound UDP packets. Unit: packets per second.	1000
pps_types_in_icmp_pps	The forwarding rate of inbound ICMP packets. Unit: packets per second.	1000
pps_types_in_syn_pps	The forwarding rate of inbound SYN packets. Unit: packets per second.	1000
pps_types_in_ack_pps	The forwarding rate of inbound ACK packets. Unit: packets per second.	1000
pps_types_in_synack_pps	The forwarding rate of inbound SYN-ACK packets. Unit: packets per second.	1000
pps_types_in_finrst_pps	The forwarding rate of inbound FIN or RST packets. Unit: packets per second.	1000
pps_types_in_dns_pps	The forwarding rate of inbound DNS packets. Unit: packets per second.	1000
pps_types_drop_tcp_pps	The forwarding rate of the TCP packets that are discarded. Unit: packets per second.	1000
pps_types_drop_udp_pps	The forwarding rate of the UDP packets that are discarded. Unit: packets per second.	1000
pps_types_drop_icmp_pps	The forwarding rate of the ICMP packets that are discarded. Unit: packets per second.	1100

Field	Description	Example value
pps_types_drop_syn_pps	The forwarding rate of the SYN packets that are discarded. Unit: packets per second.	1000
pps_types_drop_ack_pps	The forwarding rate of the ACK packets that are discarded. Unit: packets per second.	1000
pps_types_drop_synack_pps	The forwarding rate of the SYN-ACK packets that are discarded. Unit: packets per second.	1000
pps_types_finrst	The forwarding rate of the FIN or RST packets that are discarded. Unit: packets per second.	1000
pps_types_dns	The forwarding rate of the DNS packets that are discarded. Unit: packets per second.	1000
policy_packet_checking_acct_pps	The forwarding rate of the packets that are allowed by the default packet checking policy. Unit: packets per second.	1000
policy_packet_checking_drop_pps	The forwarding rate of the packets that are denied by the default packet checking policy. Unit: packets per second.	1000
policy_dns_retransmission_authentication_drop_pps	The forwarding rate of the packets that are denied by the default first-packet-dropping policy of a domain name. Unit: packets per second.	1000
policy_dns_retransmission_authentication_acct_pps	The forwarding rate of the packets that are allowed by the default first-packet-dropping policy of a domain name. Unit: packets per second.	100
policy_source_ip_authentication_succeed_pps	The forwarding rate of the packets that pass the check by the default source IP address-based authentication policy. Unit: packets per second.	1000
policy_source_ip_authentication_checked_pps	The forwarding rate of the packets that are being checked by the default source IP address-based authentication policy Unit: packets per second.	1000
policy_source_ip_authentication_acct_pps	The forwarding rate of the packets that are allowed by the default source IP address-based authentication policy. Unit: packets per second.	1000
policy_source_ip_authentication_drop_pps	The forwarding rate of the packets that are denied by the default source IP address-based authentication policy. Unit: packets per second.	1000
policy_source_ip_rate_limitation_drop_syn_pps	The forwarding rate of the SYN packets that are denied by the default source IP address-based throttling policy. Unit: packets per second.	1000

Field	Description	Example value
policy_source_ip_rate_limitation_drop_con_max_pps	The forwarding rate of the packets that are denied by the default source IP address-based throttling policy for concurrent connections. The packets are denied because the number of concurrent connections initiated from the source IP addresses exceeds the maximum number of concurrent connections allowed in the policy. Unit: packets per second.	1000
policy_source_ip_rate_limitation_drop_con_rate_pps	The forwarding rate of the packets that are denied by the default source IP address-based throttling policy for concurrent connections. The packets are denied because the connection rate of concurrent connections initiated from the source IP addresses exceeds the maximum connection rate allowed in the policy. Unit: packets per second.	1000
policy_source_ip_rate_limitation_drop_udp_rate_pps	The forwarding rate of the packets that are denied by the default source IP address-based throttling policy for UDP packets. Unit: packets per second.	1000
policy_source_ip_rate_limitation_drop_tcpack_rate_pps	The forwarding rate of the packets that are denied by the default source IP address-based throttling policy for ACK packets. Unit: packets per second.	1000
policy_source_ip_rate_limitation_drop_tcpsynack_rate_pps	The forwarding rate of the packets that are denied by the default source IP address-based throttling policy for SYN-ACK packets. Unit: packets per second.	1000
policy_destination_ip_rate_limitation_drop_syn_rate	The forwarding rate of the SYN packets that are denied by the default source IP address-based throttling policy Unit: packets per second.	1000
policy_destination_ip_rate_limitation_drop_udp_rate	The bandwidth of the UDP packets that are denied by the default destination IP address-based throttling policy. Unit: packets per second.	1000
policy_destination_ip_rate_limitation_drop_ack_rate	The bandwidth of the ACK packets that are denied by the default destination IP address-based throttling policy. Unit: packets per second.	1000
policy_destination_ip_rate_limitation_drop_icmp_rate	The bandwidth of the ICMP packets that are denied by the default destination IP address-based throttling policy. Unit: packets per second.	1000
policy_destination_ip_rate_limitation_drop_other_rate	The forwarding rate of the packets that are denied by the default destination IP address-based throttling policy. Unit: packets per second. The packets exclude UDP, ICMP, TCP-SYN, TCP-SYN-ACK, and TCP-ACK packets.	1000
policy_destination_ip_rate_limitation_drop_synack_rate	The forwarding rate of the SYN-ACK packets that are denied by the default destination IP address-based throttling policy. Unit: packets per second.	1000

Field	Description	Example value
policy_layer_4_filter_l4_filiter_drop_pps	The forwarding rate of the packets that are denied by all fingerprint filtering policies. Unit: packets per second. You can customize the fingerprint filtering policies in Mitigation Settings.	1000
policy_layer_4_filter_l4_filiter_acct_num	The forwarding rate of the packets that are allowed by all the policies in the module of fingerprint filtering policies. Unit: packets per second. You can customize the module of fingerprint filtering policies in Mitigation Settings.	1000
policy_layer_4_filter_l4_filite_drop_rule_1_pps	The forwarding rate of the packets that are denied by the first fingerprint filtering policy in the module of fingerprint filtering policies. Unit: packets per second. You can customize the fingerprint filtering policy in Mitigation Settings.	1000
policy_layer_4_filter_l4_filite_drop_rule_2_pps	The forwarding rate of the packets that are denied by the second fingerprint filtering policy in the module of fingerprint filtering policies. Unit: packets per second. You can customize the fingerprint filtering policy in Mitigation Settings.	1000
policy_layer_4_filter_l4_filite_drop_rule_3_pps	The forwarding rate of the packets that are denied by the third fingerprint filtering policy in the module of fingerprint filtering policies. Unit: packets per second. You can customize the fingerprint filtering policy in Mitigation Settings.	1000
policy_layer_4_filter_l4_filite_drop_rule_4_pps	The forwarding rate of the packets that are denied by the fourth fingerprint filtering policy in the module of fingerprint filtering policies. Unit: packets per second. You can customize the fingerprint filtering policy in Mitigation Settings.	1000
policy_layer_4_filter_l4_filite_drop_rule_5_pps	The forwarding rate of the packets that are denied by the fifth fingerprint filtering policy in the module of fingerprint filtering policies. Unit: packets per second. You can customize the fingerprint filtering policy in Mitigation Settings.	1000
policy_layer_4_filter_l4_filite_drop_rule_6_pps	The forwarding rate of the packets that are denied by the sixth fingerprint filtering policy in the module of fingerprint filtering policies. Unit: packets per second. You can customize the fingerprint filtering policy in Mitigation Settings.	1000
policy_layer_4_filter_l4_filite_drop_rule_7_pps	The forwarding rate of the packets that are denied by the seventh fingerprint filtering policy in the module of fingerprint filtering policies. Unit: packets per second. You can customize the fingerprint filtering policy in Mitigation Settings.	1000
policy_layer_4_filter_l4_filite_drop_rule_8_pps	The forwarding rate of the packets that are denied by the eighth fingerprint filtering policy in the module of fingerprint filtering policies. Unit: packets per second. You can customize the fingerprint filtering policy in Mitigation Settings.	1000
policy_dns_domain_authentication_succ_domain_pps	The forwarding rate of the packets that pass the check based on the default domain-based authentication policy. Unit: packets per second.	1000

Field	Description	Example value
policy_dns_domain_authentication_fail_domain_pps	The forwarding rate of the packets that fail the check based on the default domain-based authentication policy. Unit: packets per second.	1000
policy_dns_domain_authentication_drop_pps	The forwarding rate of the packets that are denied by the default domain-based authentication policy. Unit: packets per second.	1000
policy_dns_domain_authentication_acct_pps	The forwarding rate of the packets that are allowed by the default domain-based authentication policy. Unit: packets per second.	1000
policy_syn_cookie_succ_check_pps	The forwarding rate of the packets that pass the check based on the default SYN cookie-based policy. Unit: packets per second.	1000
policy_syn_cookie_fail_check_pps	The forwarding rate of the packets that fail the check based on the default SYN cookie-based policy. Unit: packets per second.	1000
policy_syn_cookie_drop_pps	The forwarding rate of the packets that are denied by the default SYN cookie-based policy. Unit: packets per second.	1000
policy_syn_cookie_rebound_check_pps	The forwarding rate of the packets that are reversely verified by the default SYN cookie-based policy. Unit: packets per second.	1000
policy_syn_cookie_acct_pps	The forwarding rate of the packets that are allowed by the default SYN cookie-based policy. Unit: packets per second.	1000
policy_udp_defense_drop_pps	The forwarding rate of the packets that are denied by the default UDP protection policy. Unit: packets per second.	1000
policy_antiothertcp_drop_pps	The forwarding rate of the packets that are denied by other default TCP protection policies. Unit: packets per second.	1000
policy_antiothertcp_acct_pps	The forwarding rate of the packets that are allowed by other default TCP protection policies. Unit: packets per second.	1000
policy_antitcp_drop_tcp_pps	The forwarding rate of all TCP packets that are denied by the default TCP protection policy. Unit: packets per second.	1000
policy_antitcp_drop_ack_pps	The forwarding rate of all ACK packets that are denied by the default TCP protection policy. Unit: packets per second.	1000
policy_retransmission_authentication_acct_pps	The forwarding rate of the packets that are allowed by the default first-packet-dropping policy. Unit: packets per second.	1000
policy_retransmission_authentication_drop_pps	The forwarding rate of the packets that are denied by the default first-packet-dropping policy. Unit: packets per second.	1000

12.Black hole policies

12.1. View the duration of blackhole filtering

If blackhole filtering is triggered on a server that encounters distributed denial of service (DDoS) attacks, access to the public IP address of the server is blocked for a specific duration and resumes after the duration expires. The default duration of blackhole filtering varies based on the region where an asset resides. The actual duration varies based on the severity of attacks that the asset encounters. You can view the actual duration for your asset in the Anti-DDoS console.

Context

The default duration of blackhole filtering is 2.5 hours. The actual duration varies from 30 minutes to 24 hours based on the attack severity. The duration for blackhole filtering changes based on the following factors:

- The duration of attacks. If an attack lasts for a long time, the duration of blackhole filtering is extended.
- The frequency of attacks. The first time an asset encounters an attack, the duration of blackhole filtering is shortened. If the asset is frequently attacked, it may suffer from continuous attacks. In this case, the duration of blackhole filtering is extended.

The actual duration and blackhole triggering threshold in the Anti-DDoS console shall prevail. To view the information, perform the operations in this topic.

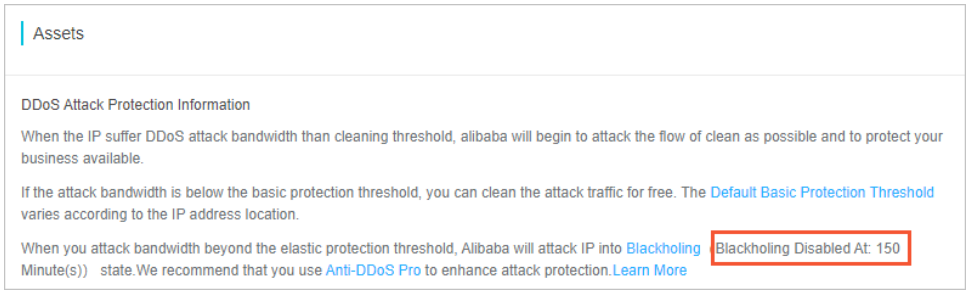
> **Note**
>
> - If an asset triggers blackhole filtering too frequently, Alibaba Cloud may further extend the duration of blackhole filtering and lower the threshold to trigger blackhole filtering for the asset.
> - Blackhole filtering is a service that Internet service providers (ISPs) provide for Alibaba Cloud. ISPs have strict limits on the time to deactivate blackhole filtering. In most cases, the duration of blackhole filtering is greater than or equal to 30 minutes. In addition, the duration is automatically adjusted as the security credit score of your account changes.

For more information about the blackhole filtering policy of Alibaba Cloud, see Blackhole filtering policy of Alibaba Cloud.

Procedure

1.
2.
3. On the **Assets** page, view the protection descriptions in the **DDoS Attack Protection Information** section.

   The time that follows **Blackholing Disabled At** in the **DDoS Attack Protection Information** section indicates the duration of blackhole filtering for assets in the current region.



12.2. View the time when a black hole is enabled for an instance and the reason for enabling the black hole

In the Anti-DDoS Pro console, you can view a list of black hole events for all assets that belong to an account. For example, you can view the time point when a black hole is enabled for an asset and a list of IP addresses from which attacks originate.

Context

The public IP address of an Elastic Compute Service (ECS) or Server Load Balancer (SLB) instance may experience a large number of distributed denial of service (DDoS) attacks. If the throughput of these attacks exceeds the predefined black hole triggering threshold, all traffic to the public IP address is routed to a black hole. Your businesses are no longer accessible by clients because all exterior traffic is dropped.

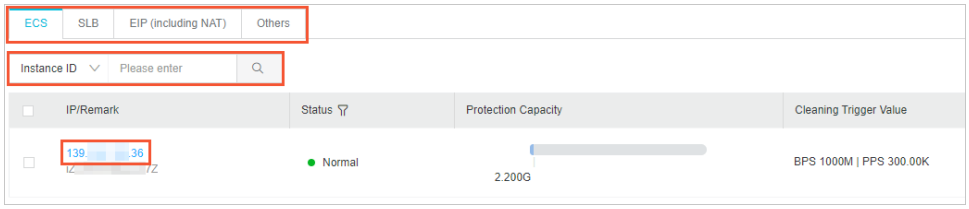
The black hole triggering threshold for an instance changes based on the region where the instance resides. For more information about black holes, see Blackhole filtering policy of Alibaba Cloud.

Procedure

1.
2.
3. Click the **ECS**, **SLB**, or **EIP (including NAT)** tab and select an asset for which you want to configure a traffic scrubbing threshold.

   > **Note** On the **Others** tab, you can configure on-demand Anti-DDoS Origin instances. You cannot configure traffic scrubbing on this tab. For more information about on-demand Anti-DDoS Origin instances, see Enable traffic rerouting to an on-demand instance.

4. In the IP address list, click the IP address for which you want to configure a traffic scrubbing threshold in the **IP/Remark** column.



5. On the **Instance Details** page, view a list of historical black hole events where the **Event** is **Black**

Hole and view the peak traffic for each attack.

The **Start time** and **End time** of a black hole event are displayed.

> **Note** If no black hole or scrubbing event for an asset exists, no result is displayed in the event list.

6. (Optional)In the Operation column of the target event, click **Download**. You can use the downloaded packet file for the attack event as evidence of criminal activity. You can send the evidence to the Internet Crime Reporting Center.

12.3. Connect to an ECS instance for which blackhole filtering is triggered

This topic describes how to connect to an ECS instance for which blackhole filtering is triggered from another ECS instance that resides in the same region.

Context

If your ECS instance encounters a volumetric attack that triggers blackhole filtering, all Internet traffic to the ECS instance is blocked. However, you can still access the ECS instance from Alibaba Cloud services that are in the same region as this ECS instance.

Therefore, after blackhole filtering is triggered for an ECS instance, you can connect to it from another ECS instance in the same region.

Procedure

1. Log on to a normal ECS instance that is in the same region as the ECS instance for which blackhole filtering is triggered.

   > **Note** These two ECS instances must be in the same VPC and be able to communicate with each other. Make sure that communication is not blocked by security group rules. For more information, see Overview.

2. Use a tool or the command line interface to connect to the ECS instance for which blackhole filtering is triggered.
   After the connection is successful, you can modify configuration files on this ECS instance or transfer files to the normal ECS instance to which you log on.

12.4. 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
China (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.

12.5. Deactivate blackhole filtering

This topic describes how to deactivate blackhole filtering that has been triggered for an IP address that is protected by Anti-DDoS Origin Enterprise.

Context

After you purchase an Anti-DDoS Origin Enterprise instance, you can deactivate blackhole filtering 100 times per month free of charge. In the validity period of your Anti-DDoS Origin Enterprise instance, the number of times to deactivate blackhole filtering is automatically reset to 100 at the beginning of each month.

> **Note** If the number of times in a month is not used up, the system clears it by the end of the month and does not add it to the number in the next month.

Before you manually deactivate blackhole filtering, check the time of automatic deactivation in the Anti-DDoS Origin console. If the time is acceptable, we recommend that you wait for blackhole filtering to be automatically deactivated. For more information, see View the duration of blackhole filtering.

Procedure

1.
2.
3. In the left-side navigation pane, choose **Anti-DDoS Origin > Manage Instances**.
4. On the **Manage Instances** page, find the required instance and click **Deactivate Black Hole** in the Actions column.

   > **Note** You can **deactivate blackhole filtering** only when blackhole filtering is triggered for **IP addresses** protected by the instance. If blackhole filtering is not triggered, the **Deactivate Black Hole** operation is not available in the console.

5. On the **Protection Target** tab, find a protected IP address that is in the **Blackholing** state and click **Deactivate Black Hole** in the Actions column.
6. In the **Deactivate Black Hole** dialog box, view the remaining times that you can deactivate blackhole filtering and click **OK**.

   > **Note** Blackhole filtering is a risk management policy used by the backend servers of Alibaba Cloud. If your request to deactivate blackhole filtering fails, your deactivation times for the day are not deducted.

Result

If an error message appears, the deactivation fails. You can wait and try again later. If no error message appears, blackhole filtering is deactivated.

Related information

- DeleteBlackhole

13.Best Practices

13.1. Configure alert notifications for DDoS attack events

This topic describes how to configure alert notifications for blackhole filtering events and traffic scrubbing events that occur on an Anti-DDoS Origin instance. After alert notifications are configured, Alibaba Cloud notifies you of the latest DDoS attack events that occur on your Anti-DDoS Origin instance. This allows you to handle exceptions and restore workloads at the earliest opportunity.

Description of alert notification channels

Anti-DDoS Origin supports the following alert notification channels:

- Message Center

  Message Center is a message notification service that is provided for Alibaba Cloud accounts. You can use Message Center to configure different types of notifications for Alibaba Cloud services. You can enable **Security Notice** in Message Center. If security events are detected on your assets, Alibaba Cloud sends alert notificationsto the specified contacts by using methods, such as internal messages and emails.

- CloudMonitor

  CloudMonitor monitors Internet applications and Alibaba Cloud resources. You can use CloudMonitor to monitor DDoS attack events that occur on Anti-DDoS Origin instances. The DDoS attack events include the following types of events:

  - Blackhole filtering events: If the peak bandwidth of DDoS attacks exceeds the blackhole filtering threshold specified for your asset, blackhole filtering is triggered on your asset.
  - Traffic scrubbing events: If the traffic volume of DDoS attacks exceeds the traffic scrubbing threshold, traffic scrubbing is triggered.

  You can configure event alert rules for Anti-DDoS Origin. If CloudMonitor detects that DDoS attack events occur on Anti-DDoS Origin instances, CloudMonitor sends alert notifications to the specified contacts by using methods, such as emails and DingTalk. This way, you are notified of the latest attack events and can handle exceptions at the earliest opportunity. For more information, see Configure alert rules in CloudMonitor.

- Log Service

  Anti-DDoS Origin Enterprise supports mitigation analysis based on traffic logs. After you enable mitigation analysis for an Anti-DDoS Origin Enterprise instance, the instance collects the service traffic and mitigation logs of the protected assets. You can view and analyze the logs. In addition, you can create custom alert rules for specific service metrics based on the analysis results. If the service metrics for the Anti-DDoS Origin Enterprise instance are abnormal, Log Service sends alert notifications at the earliest opportunity.

  For more information about how to configure alert rules in Log Service, see Configure an alert monitoring rule in Log Service.

The following table compares the alert notification methods from different dimensions. You can choose an alert notification method based on your business requirements.

Item	Message Center	CloudMonitor	Log Service
Supported editions of Anti-DDoS Origin instances	Anti-DDoS Origin Enterprise instances and Anti-DDoS Origin Basic instances	Anti-DDoS Origin Enterprise instances	Anti-DDoS Origin Enterprise instances that have the mitigation analysis feature enabled
Scenarios	General alerting scenarios in which you need only to be notified of attacks	General alerting scenarios in which you can use simple filter conditions to receive alert notifications of important events	Enterprise-level alerting scenarios in which you can configure items such as service metrics, alert policies, notification methods, and content and generate statistical reports based on different combinations of the items
Configuration complexity	Low	Medium	High
Flexibility	Low Alerts can be reported at the beginning and end of an event.	Medium Alerts can be reported at the beginning and end of an event at this time.	High Alerts can be reported at the beginning and end of an event based on traffic thresholds or based on a combination of conditions.
Notification method	• Internal messages • Emails	• Emails • Webhook	• Emails • Webhook
Reliability and timeliness	The reliability is extremely high, and an alert notification is sent within 5 minutes after the alert is generated.	The reliability is high, and an alert notification is sent 5 to 10 minutes after the alert is generated.	The reliability is high, and an alert notification is sent 5 to 10 minutes after the alert is generated.

Configure alert notifications in CloudMonitor (available only for Anti-DDoS Origin Enterprise)

If you have purchased an Anti-DDoS Origin Enterprise instance, you can perform the following steps to configure alert notifications for DDoS attack events in the CloudMonitor console. If you use an Anti-DDoS Origin Basic instance, we recommend that you use Message Center to configure alert notifications. You cannot configure alert notifications for an Anti-DDoS Origin Basic instance in the CloudMonitor console.

1. Log on to the CloudMonitor console.
2. (Optional)Create an alert contact. If you have created a contact, skip this step.
   i. In the left-side navigation pane, choose **Alerts > Alert Contacts**.
   ii. On the **Alert Contacts** tab, click **Create Alert Contact**.

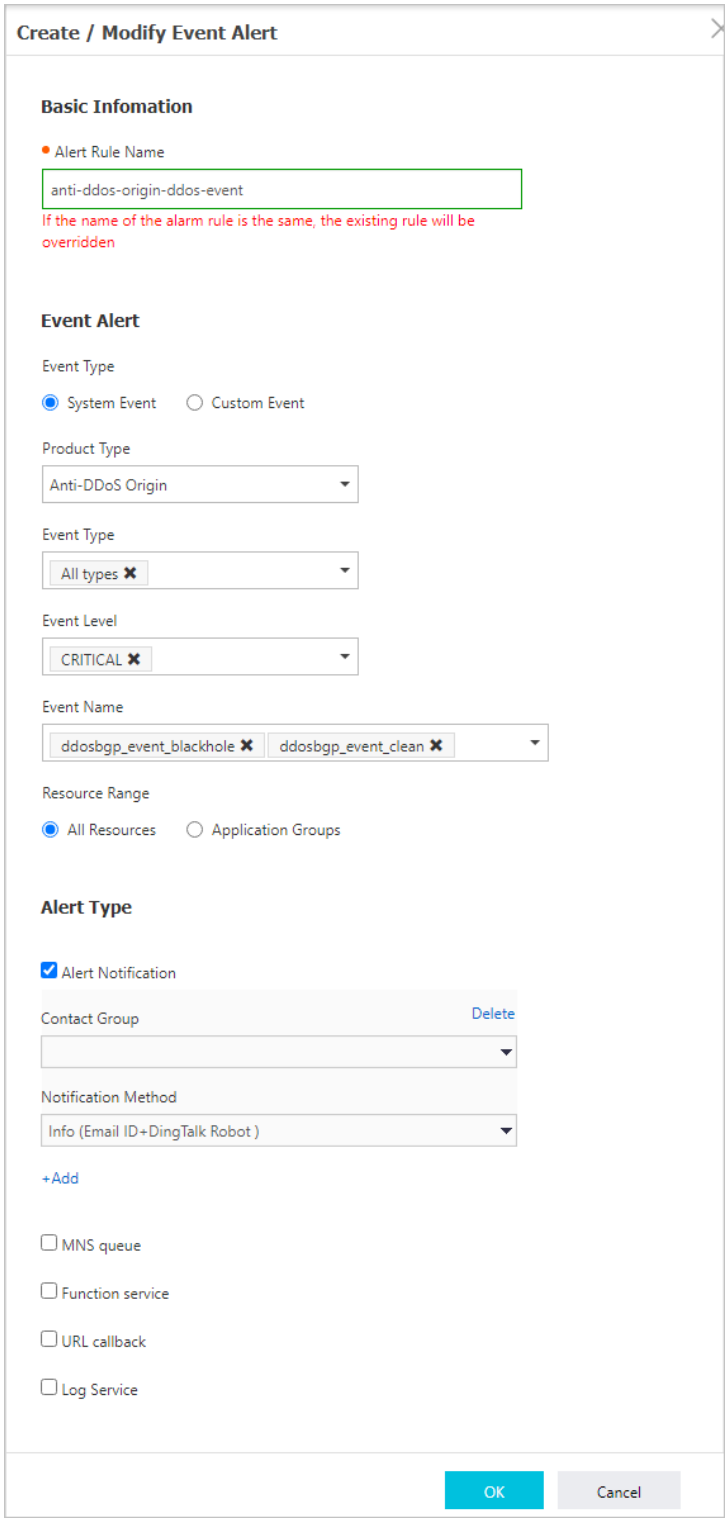
iii. In the **Set Alert Contact** panel, configure the parameters, drag the slider to complete verification, and then click **OK**.

3. (Optional)Create an alert group. If you have created an alert group, skip this step.

> **Note** CloudMonitor sends alert notifications only to an alert group. You can add one or more alert contacts to an alert group.

   i. In the left-side navigation pane, choose **Alerts > Alert Contacts**.
   ii. On the **Alert Contact Group** tab, click **Create Alert Contact Group**.
   iii. In the **Create Alert Contact Group** panel, enter a group name in the **Group Name** field. Select the alert contact that you create from the **Existing Contacts** section and add the contact to the Selected Contacts section. Then, click **Confirm**.

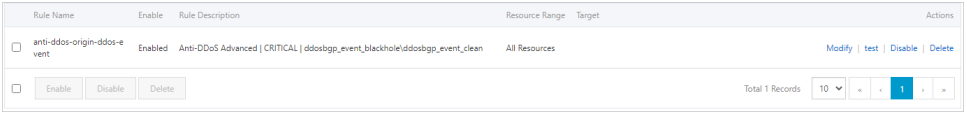
4. In the left-side navigation pane, choose **Alerts > Alert Rules**.
5. On the page that appears, click the **Event Alert** tab. On the Event Alert tab, click **Create Event Alert**.
6. In the **Create / Modify Event Alert** panel, configure the parameters and click **OK**.



Section	Parameter	Description
Basic Information	**Alert Rule Name**	Enter a name for the alert rule.
	Event Type	Select **System Event**.

Section	Parameter	Description
Event Alert	Product Type	Select **Anti-DDoS Origin**, which indicates Anti-DDoS Origin Enterprise instances.
	Event Type	Select the type of event for which you want to receive alert notifications. Valid value: **DDoS attacks**.
	Event Level	Select the level of events for which you want to receive alert notifications. Valid values: **CRITICAL**, **WARN**, and **INFO**. **Notice** You can select multiple levels. If you select multiple levels, you must select **CRITICAL** for all events.
	Event Name	Select the event for which you want to receive alert notifications. Valid values: **ddosbgp_event_blackhole** and **ddosbgp_event_clean**.
	Resource Range	Select **All Resources**.
Alert Type	Alert Notification	Select **Alert Notification** and configure **Contact Group** and **Notification Method**. ○ Contact Group: Select an existing contact group. ○ Notification Method:Set the value to **Info (Email ID+DingTalk Robot)**. Only this option is supported. You can click **Add** to add more contact groups and notification methods.
	MNS queue	You do not need to specify this parameter.
	Function service	You do not need to specify this parameter.
	URL callback	You do not need to specify this parameter.
	Log Service	You do not need to specify this parameter.

After an alert rule is created, you can view the rule in the rule list. The new alert rule is enabled by default. If DDoS attack events occur on an Anti-DDoS Origin Enterprise instance, Alibaba Cloud sends alert notifications to the contacts in the selected contact group. Supported DDoS attack events are blackhole filtering events and traffic scrubbing events.



Configure alert notifications in Message Center (available for Anti-DDoS Origin Basic and Anti-DDoS Origin Enterprise)

You can perform the following steps to configure alert notifications in Message Center.

1. Log on to the Message Center console.
2. In the left-side navigation pane, choose **Message Settings > Common Settings**.
3. On the **Common Settings** page, select **Security Notice**. Then, select the notification methods based on your business requirements.

   The following notification methods are supported:

   - **Internal Messages**: If you select this option, Alibaba Cloud sends alert notifications by using internal messages. You can view the internal messages by clicking the

     icon in the upper-right corner of the Alibaba Cloud Management Console.
   - **Email**: If you select this option, Alibaba Cloud sends alert notifications by using emails. The alert notifications are sent to the email addresses of the contacts that you specify.
4. Click **Add Message Recipient**.
5. In the **Modify Contact** dialog box, select or configure contacts. Then, click **Save**.

After you complete the configurations, Alibaba Cloud sends alert notifications to the specified contacts when DDoS attack events occur on an Anti-DDoS Origin instance.

13.2. Activate Anti-DDoS Origin to protect IP addresses from DDoS attacks

By default, Alibaba Cloud provides basic protection capacity for resources that have public IP addresses configured. These resources include Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, Elastic IP (EIP) instances, and Web Application Firewall (WAF) assets. If the throughput of a DDoS attack is more than the default protection capacity of the resource, we recommend that you purchase Anti-DDoS Origin Enterprise instance. Anti-DDoS Origin Enterprise uses all protection capacity of a region where the public IP address resides to defense against the attacks. This ensures business continuity.

Context

Anti-DDoS Origin Enterprise provides unlimited protection. When DDoS attacks are detected, Anti-DDoS Origin Enterprise automatically uses all the protection capacity of a region where an instance resides to defend against the DDoS attacks.

Prerequisites

Before activating Anti-DDoS Origin Enterprise, you need to confirm the following information:

- The IP address that you want to protect.
- The region where the IP address resides.

> **Note** Anti-DDoS Origin is not available in all regions. Before you activate Anti-DDoS Origin, ensure that Anti-DDoS Origin is available in the region where an IP address that you want to protect resides. For more information about supported regions where you can activate Anti-DDoS Origin Enterprise, see What is Anti-DDoS Origin?.

Procedure

1. For more information about how to purchase an Anti-DDoS Origin Enterprise instance, see Purchase an Anti-DDoS Origin Enterprise instance.

   > **Note** Ensure that the region where an Anti-DDoS Origin instance resides is the same as the region where resources that are protected by the instance reside. The resources include Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and Elastic IP (EIP) instances.

2. Log on to the Anti-DDoS Basic console.
3. On the **Anti-DDoS Origin** page, find the target instance, and click Add a cloud service to Anti-DDoS Origin Enterprise for protection to add the addresses that you want to protect to the instance.

Result

After you add an IP address to an Anti-DDoS Origin instance, the protection capacity of the instance applies to the IP address. On the **Assets** page, you can find that the protection capacity of the IP address increases to the protection capacity of the instance.

13.3. Upgrade Anti-DDoS Origin Enterprise to Anti-DDoS Pro or Anti-DDoS Premium

This topic describes how to upgrade Anti-DDoS Origin Enterprise to Anti-DDoS Pro or Anti-DDoS Premium to enhance protection for your assets. If the protection capability of Anti-DDoS Origin Enterprise cannot meet your business requirements, we recommend that you upgrade Anti-DDoS Origin Enterprise to Anti-DDoS Pro or Anti-DDoS Premium.

Context

For more information about the scenarios for which Anti-DDoS Origin Enterprise is suitable, see Scenarios.

If one of the following issues occurs when you use Anti-DDoS Origin Enterprise, we recommend that you upgrade Anti-DDoS Origin Enterprise to Anti-DDoS Pro or Anti-DDoS Premium:

- Volumetric DDoS attacks exist for a long period of time.
- HTTP flood attacks that cannot be mitigated by Anti-DDoS Origin Enterprise occur.
- Other specific issues.

> **Notice** If you upgrade Anti-DDoS Origin Enterprise to Anti-DDoS Pro or Anti-DDoS Premium, Alibaba Cloud refunds you for the remaining subscription period of the Anti-DDoS Origin Enterprise instance.

If Anti-DDoS Origin Enterprise, Anti-DDoS Pro, or Anti-DDoS Premium cannot meet your business requirements, we recommend that you use Anti-DDoS Origin Enterprise together with Anti-DDoS Pro or Anti-DDoS Premium. For more information, see Use Anti-DDoS Origin Enterprise and Anti-DDoS Pro.

Procedure

1. Contact customer service in the DingTalk group.

   If you are not in the DingTalk group, search for the DingTalk group ID 31182544 to join the DingTalk group.
2. Alibaba Cloud technical support engineers evaluate your business scenario and determine whether all upgrade conditions are met.
3. If all conditions are met, Alibaba Cloud refunds you for the remaining subscription period of Anti-DDoS Origin Enterprise. The refund is calculated based on the specifications and remaining subscription period of the Anti-DDoS Origin Enterprise instance.
4. Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

   For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.
5. Add your services to Anti-DDoS Pro or Anti-DDoS Premium for protection.

   For more information about how to add website services, see Step 1: Add forwarding rules.

   For more information about how to add non-website services, see Step 1: Create a port forwarding rule.

13.4. Best practices for automatic deactivation of blackhole filtering

If your service IP address encounters volumetric DDoS attacks after your service IP address is added to Anti-DDoS Origin Enterprise, blackhole filtering may still be triggered. To avoid extended periods of service disruption, you must deactivate blackhole filtering at the earliest opportunity. Anti-DDoS Origin Enterprise provides a solution to configure alerts and automatically deactivate blackhole filtering.

Prerequisites

This solution requires you to call an API operation of Anti-DDoS Origin Enterprise. Therefore, this solution is available only for Anti-DDoS Origin Enterprise instances. Before you use this solution, make sure that your service IP address is added to an Anti-DDoS Origin Enterprise instance. For more information, see Add a cloud service to Anti-DDoS Origin Enterprise for protection.

Context

You can manually deactivate blackhole filtering for Anti-DDoS Origin Enterprise instances in the Anti-DDoS Basic console. For more information, see Deactivate blackhole filtering. However, manual deactivation may result in delays and unexpected errors. If your service requires a high level of stability and continuity, use the following method to configure alerts and automatically deactivate blackhole filtering:

1. Create an alert rule in the Cloud Monitor console to monitor blackhole filtering that is triggered on an Anti-DDoS Origin Enterprise instance.

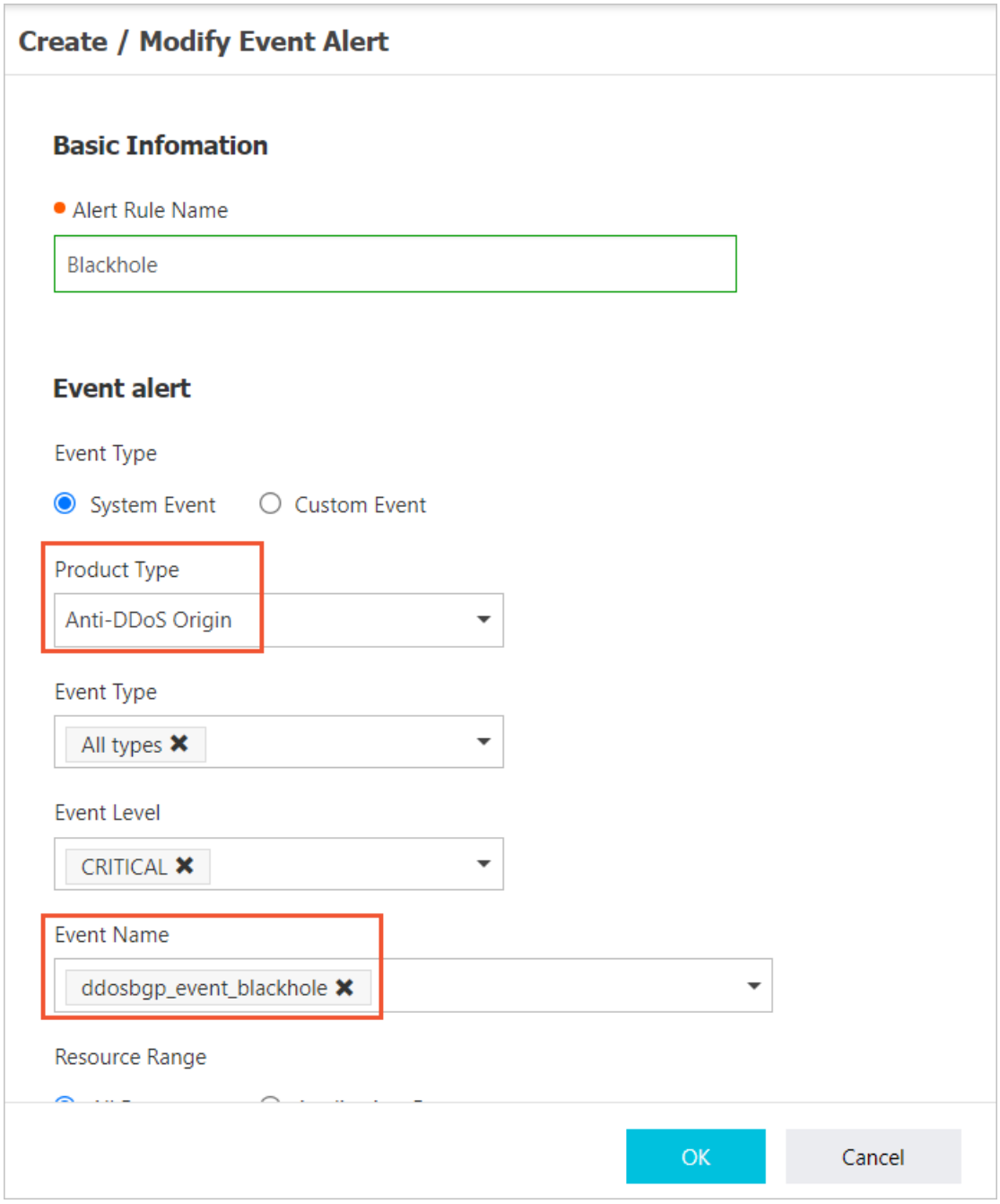
> **Note** If blackhole filtering is triggered and detected on the IP addresses that are added to Anti-DDoS Origin Enterprise, Cloud Monitor sends messages about blackhole filtering. In other scenarios, no messages about blackhole filtering are sent.

2. Create an alert rule to automatically deactivate blackhole filtering on Anti-DDoS Origin Enterprise by calling the DeleteBlackhole operation. For more information, see DeleteBlackhole.

Similarly, you can create rules to automatically call an API operation of Alibaba Cloud DNS. The operation resolves your domain name to the IP address of an Anti-DDoS Pro or Anti-DDoS Premium instance during DDoS attacks.

Procedure

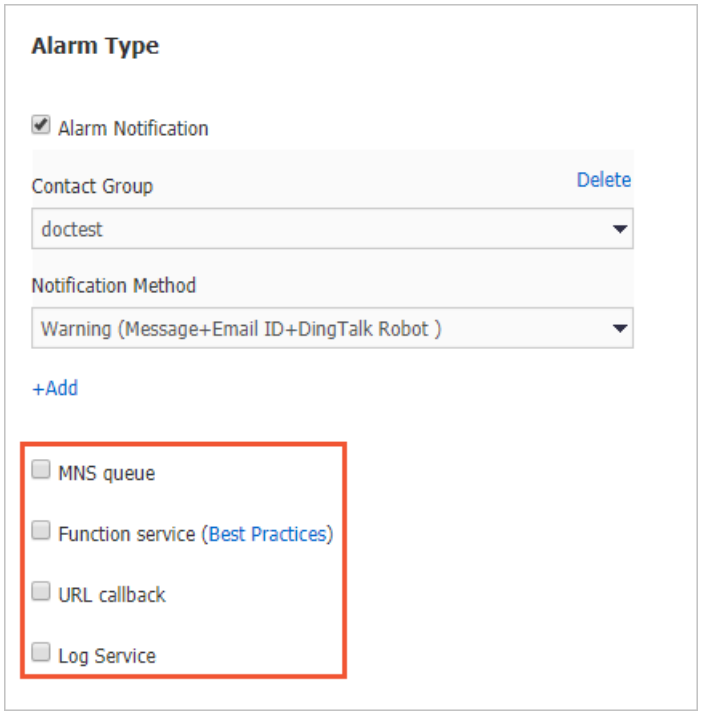
1. Log on to the Cloud Monitor console.
2. In the left-side navigation pane, choose **Alerts > Alert Rules**.
3. On the **Alert Rules** page, click the **Event Alert** tab.
4. Click **Create Event Alert** to create a rule for blackhole filtering.
   - In the panel that appears, set **Product Type** to **Anti-DDoS Origin**.
   - In the **Event Name** drop-down list, select **ddosbgp_event_blackhole**.



5. Select the channel to push alert notifications based your service requirements and click **OK**.

   Cloud Monitor supports the following channels:

   - **MNS queue**
   - **Function service**
   - **URL callback**
   - **Log Service**



The event alert is created. When Cloud Monitor detects that blackhole filtering is triggered on an IP address that is added to Anti-DDoS Origin Enterprise, Cloud Monitor generates an alert and pushes the following message through the specified channel.

Sample alert message:

```
{
    "action": "add", //The event status. The value add indicates that the event begins, and the value del indicates that the event ends.
    "bps": 0, //The throughput when the event is triggered. Unit: Mbit/s.
    "pps": 0, //The packet rate when the event is triggered. Unit: packets per second (PPS).
    "instanceId": "ddosbgp-cn-78v17******", //The ID of the Anti-DDoS Origin Enterprise instance.
    "ip": "47. *. *. *", //The IP address on which the event is triggered.
    "regionId": "cn-hangzhou", //The ID of the region where the Anti-DDoS Origin Enterprise instance resides.
    "time": 1564104493000, //The time when the event begins. The value is a timestamp. Unit: milliseconds.
    "type": "blackhole"  //The event type. The value defense indicates a traffic scrubbing event and the value blackhole indicates a blackhole filtering event.
}
```

6. Specify an alert action that calls the DeleteBlackhole operation to automatically deactivate blackhole filtering. For more information, see DeleteBlackhole.

13.5. Use Anti-DDoS Origin Enterprise and Anti-DDoS Pro

This topic describes how to use Anti-DDoS Origin Enterprise and Anti-DDoS Pro. This solution provides effective protection for your services against distributed denial of service (DDoS) attacks without compromising service continuity. To use Anti-DDoS Origin Enterprise and Anti-DDoS Pro, you can create a scheduling rule for Sec-Traffic Manager of Anti-DDoS Pro to achieve tiered protection.

Background information

Anti-DDoS Origin Enterprise provides protection against DDoS attacks for specific Alibaba Cloud 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 Enterprise directly protects Alibaba Cloud resources. You do not need to change the IP addresses of resources that you want to protect. You also do not need to limit the number of Layer 4 ports and the number of Layer 7 domain names. Anti-DDoS Origin Enterprise provides out-of-the-box features and elastic protection. If your services encounter volumetric DDoS attacks, Anti-DDoS Origin Enterprise uses all resources that reside in a region to provide unlimited protection. Anti-DDoS Origin Enterprise provides unlimited protection, such as protection against DDoS attacks peaked up to hundreds of Gbit/s.

Anti-DDoS Pro provides a maximum of 1.5 Tbit/s bandwidth to implement BGP-based DDoS mitigation with a support for 8 lines. The BGP-based DDoS mitigation with a support for 8 lines can be implemented only in regions inside mainland China. Anti-DDoS Pro protects your services from volumetric DDoS attacks peaked up to Tbit/s. Anti-DDoS Pro forwards DDoS attack traffic to scrubbing centers based on DNS records. Anti-DDoS Pro provides high-quality BGP bandwidth resources for China Telecom, China Unicom, China Mobile, China Education and Research Network (CERNET), and other Internet service providers (ISPs) in mainland China. The average latency is about 20 ms.

To enable interaction between Anti-DDoS Origin Enterprise and Anti-DDoS Pro, you can create a scheduling rule for Sec-Traffic Manager of Anti-DDoS Pro. This rule allows you to use Anti-DDoS Origin Enterprise for daily protection against common DDoS attacks. This rule triggers a switchover from Anti-DDoS Origin Enterprise to Anti-DDoS Pro when volumetric DDoS attacks occur.

Solution overview

This solution allows you to use both Anti-DDoS Origin Enterprise and Anti-DDoS Pro. This solution supports protection for all assets, transparent deployment without extra latencies, and protection against volumetric DDoS attacks. It also helps control costs.

If you want to use this solution, purchase an Anti-DDoS Origin Enterprise instance to protect a maximum of 255 IP addresses of a specific region and enable unlimited protection. Anti-DDoS Origin Enterprise provides a protection bandwidth that ranges from 100 Gbit/s to 300 Gbit/s based on regions. You must also purchase an Anti-DDoS Pro instance as a backup to defend against DDoS attacks of greater than 300 Gbit/s. After you create a scheduling rule, all cloud resources are added to Sec-Traffic Manager for centralized management. If blackhole filtering is triggered by Anti-DDoS Origin Enterprise, Sec-Traffic Manager automatically switches traffic over to Anti-DDoS Pro.

This solution provides the following features:

- Anti-DDoS Origin Enterprise provides multi-region account-level protection without extra latencies. You do not need to change the IP addresses of cloud resources and business structures.
- Anti-DDoS Origin Enterprise provides protection bandwidth that ranges from 100 Gbit/s to 300 Gbit/s based on regions. Anti-DDoS Pro is used to defend against DDoS attacks of greater than 300 Gbit/s.
- If blackhole filtering is triggered, a switchover is automatically performed from Anti-DDoS Origin Enterprise to Anti-DDoS Pro based on DNS records. A switchover requires 1 to 3 minutes or 5 to 10 minutes to complete based on the deployment region of local DNS servers.
- Express Connect circuits are provided for back-to-origin traffic. This eliminates the effect of

blackhole filtering.

After you use Anti-DDoS Origin Enterprise and Anti-DDoS Pro, SLB, ECS, or WAF instances are under the protection of Anti-DDoS Origin Enterprise without extra latencies. If volumetric attacks occur, blackhole filtering is triggered by Anti-DDoS Origin Enterprise. In this case, Sec-Traffic Manager switches traffic from Anti-DDoS Origin Enterprise to Anti-DDoS Pro, which forwards inbound traffic to a scrubbing center but has a latency of about 20 ms. If the attack stops, inbound traffic is forwarded back to SLB, ECS, or WAF instances, and Anti-DDoS Origin Enterprise starts to provide protection.

- If the local DNS servers are deployed in mainland China, the switchover requires 5 to 10 minutes.

  > **Note** If the local DNS servers are deployed outside mainland China, the switchover requires 1 to 3 minutes.

- If protection is switched over to Anti-DDoS Pro, the blackhole filtering threshold is limited to the maximum protection bandwidth of Anti-DDoS Pro. Anti-DDoS Pro provides basic protection of up to 30 Gbit/s and elastic protection of up to 300 Gbit/s. You can also submit a to upgrade the protection bandwidth to 1 Tbit/s or higher.
- After the attack stops, Anti-DDoS Pro is not immediately switched back to Anti-DDoS Origin Enterprise. You can configure the intervals at which Sec-Traffic Manager performs switchovers. The default interval is 120 minutes (two hours). This configuration allows you to avoid frequent switchovers due to continuous attacks and ensures service continuity.

Activate and configure Anti-DDoS Origin Enterprise

Create an Anti-DDoS Origin Enterprise instance and add Alibaba Cloud resources to the instance for protection. Make sure that these resources and the instance are located in the same region. These resources include ECS, SLB, and WAF instances, and EIPs.

> **Notice**
>
> - If the public IP addresses of resources are used to provide services, make sure that the network specifications and specified scrubbing threshold that is related to each resource meet your business requirements. You can view the scrubbing threshold for each resource in the Anti-DDoS Origin console.
> - Before sales promotions, you must estimate the peak bandwidth and inform Alibaba Cloud technical support. This allows you to avoid traffic scrubbing or throttling by mistake and reduces the impact on your business.

1. Create an Anti-DDoS Origin Enterprise instance.

   For more information, see Purchase an Anti-DDoS Origin Enterprise instance.
2. Add the IP address of your origin server to the Anti-DDoS Origin Enterprise instance for protection.

   For more information, see Add a cloud service to Anti-DDoS Origin Enterprise for protection.

Configure Anti-DDoS Pro and Sec-Traffic Manager

Create an Anti-DDoS Pro instance of the Professional plan, add a forwarding rule, and create a scheduling rule for Sec-Traffic Manager. After the configuration is complete, inbound traffic is forwarded to the address pointed by the Canonical Name (CNAME) record of Sec-Traffic Manager.

1. Create an Anti-DDoS Pro instance of the Professional plan.

   For more information, see Purchase an Anti-DDoS Pro or Anti-DDoS Premium instance.

2. Add a domain to the Anti-DDoS Pro instance of the Professional plan.

   For more information, see Add a website.

   > **Note** After you add the forwarding rule for a domain, you do not need to modify the DNS record.

3. Create a scheduling rule for Sec-Traffic Manager to achieve **tiered protection**.

   For more information, see Create a tiered protection rule.

   After you create the rule, you can obtain a CNAME record of Sec-Traffic Manager in the **General** rule list.

4. Update the DNS record of your domain. Visit the website of your DNS provider to change the DNS record so that traffic is forwarded to the CNAME record of Sec-Traffic Manager.

13.6. Use Anti-DDoS Origin and WAF

This topic describes how to use Anti-DDoS Origin and Web Application Firewall (WAF) to provide protection. This solution protects your website against Layer 4 distributed denial of service (DDoS) attacks, Layer 7 web attacks, and HTTP flood attacks.

Prerequisites

- An Elastic Compute Service (ECS) instance is created and has web applications installed. The ECS instance has a public IP address, and your website has a domain name.

  > **Note** If your website provides services in mainland China, the domain name of your website must have an Internet Content Provider (ICP) license. Otherwise, you cannot add the domain name to WAF instances in mainland China to protect your website.

- An Anti-DDoS Origin Enterprise instance is purchased. For more information, see Purchase an Anti-DDoS Origin Enterprise instance.

  > **Note** When you purchase an Anti-DDoS Origin Enterprise instance, you must select a region. Make sure that the Anti-DDoS Origin Enterprise instance and the ECS instance reside in the same region.

- A WAF instance is purchased. For more information, see Purchase a WAF instance.

Context

You can use Anti-DDoS Origin Enterprise to mitigate DDoS attacks for your website. If your website encounters web attacks and HTTP flood attacks, we recommend that you use WAF to protect your website. For more information about WAF, see What is WAF?.

If you use Anti-DDoS Origin Enterprise and WAF to protect your website, you must add your website to WAF and then add the IP address of the WAF instance to Anti-DDoS Origin Enterprise for protection. In this case, all service traffic is first scrubbed by WAF, and only normal traffic is forwarded to the origin server. Attack traffic, such as DDoS attacks, web attacks, and HTTP flood attacks, is blocked.

Procedure

1. Add your website to WAF.

i. Log on to the WAF console.

ii. In the top navigation bar, select the **Mainland China** or **International** region.

WAF automatically determines the specific region based on the location of the origin server.

iii. In the left-side navigation pane, choose **Asset Center > Website Access**.

iv. Click **Add Domain Name**.

You can add your website in two modes: CNAME and transparent proxy. In CNAME mode, the website can be automatically or manually added. In transparent proxy mode, only origin servers that are deployed in the China (Beijing) region are supported.

This topic describes how to add a website in CNAME mode.

v. (Optional)On the **Add Domain Name** page, click **Manually Add Other Websites**. If the **Add Domain Name** page does not appear, skip this step.

vi. Complete the configurations in the **Enter your website information** step of the **Add Domain Name** wizard and click **Next**.

You must specify the following website parameters:

- **Domain Name**: Enter the domain name of the website.
- **Protocol Type**: Select the protocol supported by the website. If your website supports **HTTPS**, select HTTPS and upload the certificate after you add the website. For more information, see Upload an HTTPS certificate.
- **Destination Server (IP Address)**: Select **IP** and enter the public IP address of the ECS instance.
- **Destination Server Port**: After you specify Protocol Type, the server port is automatically matched. You can also specify a non-standard server port. For more information, see View the allowed port range.
- **Does a layer 7 proxy (DDoS Protection/CDN, etc.) exist in front of WAF**: Select **No**.

  If you configure a Layer 7 proxy such as Anti-DDoS Pro, Anti-DDoS Premium, or Content Delivery Network (CDN) before WAF, the requests from a client are forwarded to the Layer 7 proxy before they reach WAF. Anti-DDoS Origin Enterprise is not a Layer 7 proxy. In this case, select No.

For more information about the website parameters, see Add domain names.

vii. Click **Completed. Return to the website list**.
A CNAME record is created for the added website. You can obtain the CNAME record of WAF from the website list.

viii. Run the `ping the CNAME record of WAF` command on your computer to obtain the IP address of the WAF instance.

2. Configure your origin server to allow the back-to-origin Classless Inter-Domain Routing (CIDR) blocks of WAF.

   For more information, see Allow access from back-to-origin CIDR blocks of WAF.

3. Change the DNS settings to resolve the domain name of the website to the CNAME record of WAF that you obtain in Step 1.

   For more information, see Change a DNS record.

   After you change the DNS settings, all requests sent to your website are forwarded to WAF for

traffic scrubbing. WAF blocks web attacks and HTTP flood attacks and only forwards normal traffic to the origin server.

The WAF instance cannot mitigate volumetric DDoS attacks. If your service encounters volumetric DDoS attacks, the performance of the WAF instance deteriorates, which affects service forwarding. Therefore, you must use an Anti-DDoS Origin Enterprise with the WAF instance to protect your service from DDoS attacks.

4. Add the IP address of the WAF instance to your Anti-DDoS Origin Enterprise instance for protection.

   For more information, see Add a cloud service to Anti-DDoS Origin Enterprise for protection.

   After you add the IP address of the WAF instance, the Anti-DDoS Origin Enterprise instance provides unlimited protection. The Anti-DDoS Origin Enterprise instance automatically scrubs service traffic to mitigate DDoS attacks.

13.7. Use Anti-DDoS Origin and SLB

This topic describes how to configure Server Load Balancer (SLB) and Anti-DDoS Origin to protect a website that is hosted on an Elastic Compute Service (ECS) instance. This combination provides better protection than Anti-DDoS Origin Enterprise alone.

Prerequisites

- An ECS instance is created and has web applications installed. For more information, see Overview.
- An Anti-DDoS Origin Enterprise instance is purchased. For more information, see Purchase an Anti-DDoS Origin Enterprise instance.

Context

To use Anti-DDoS Origin Enterprise to protect your website, we recommend that you deploy an SLB instance for the ECS instance where your website is hosted. Then, add the IP address of the SLB instance to Anti-DDoS Origin Enterprise for protection. The SLB instance can discard traffic whose protocol and port are not specified in the SLB listener. This helps mitigate distributed denial of service (DDoS) attacks. The preceding solution defends against different types of DDoS attacks, such as reflection attacks, User Datagram Protocol (UDP) flood attacks, and SYN flood attacks (large packets). The reflection attacks include Simple Service Discovery Protocol (SSDP), Network Time Protocol (NTP), and Memcached attacks.

The following procedure describes how to implement this combination solution.

> **Note** If your origin server is deployed with SLB, you only need to add the IP address of the SLB instance to Anti-DDoS Origin Enterprise for protection. For more information, see Add a cloud service to Anti-DDoS Origin Enterprise for protection.

Procedure

1. Create an Internet-facing SLB instance.

   For more information, see Create a CLB instance.

   When you create an Internet-facing SLB instance, note the following points:

   - SLB does not support cross-region deployment. Make sure that the ECS instance and the SLB instance are in the same region.
   - Anti-DDoS Origin provides protection only for Alibaba Cloud services that have public IP

addresses. Therefore, you must create an Internet-facing SLB instance.

For more information, see Preparations.

After an Internet-facing SLB instance is created, you can obtain the **IP Address** of the SLB instance on the **Instances** page in the SLB console.

2. Configure the Internet-facing SLB instance.

   For more information, see Configure a CLB instance.

   When you configure the Internet-facing SLB instance, note the following points:

   - In the **Protocol and Listener** step, specify only the listening protocol and ports that are required. You can select **TCP**, **UDP**, **HTTP**, or **HTTPS**. Traffic whose protocol and port are not specified in the SLB listener is discarded and not forwarded to the backend ECS instance.
   - In the **Backend Servers** step, select the instance where your website is hosted.

     > **Note** The Internet-facing SLB instance communicates with the backend ECS instance over the internal network. Therefore, we recommend that you disable Internet access to the backend ECS instance after you configure the SLB instance. Make sure that the SLB instance functions properly.

   After the SLB instance is configured, the SLB instance forwards requests from a client to the backend ECS instance based on the existing configurations.

3. Change the DNS settings.

   - If your website is accessed by using its IP address, you can add the IP address of the Internet-facing SLB instance obtained in Step 1 as the IP address of your website. In this case, you do not need to change the DNS settings.
   - If your website is accessed by using its domain name, you must resolve the domain name to the IP address of the SLB instance obtained in Step 1. For more information, see Use an A record to resolve a domain name to an IP address.

4. Add the IP address of the SLB instance to the Anti-DDoS Origin Enterprise instance for protection.

   For more information, see Add a cloud service to Anti-DDoS Origin Enterprise for protection.

   After you add the IP address of the SLB instance, the Anti-DDoS Origin Enterprise instance provides unlimited protection. The Anti-DDoS Origin Enterprise instance automatically scrubs service traffic to mitigate DDoS attacks.

13.8. Use an on-demand Anti-DDoS Origin instance to enable automatic protection for your assets

This topic describes the best practices to use an on-demand Anti-DDoS Origin instance to automatically protect your assets against heavy DDoS attacks. If an attack occurs, you can call API operations to enable automatic protection.

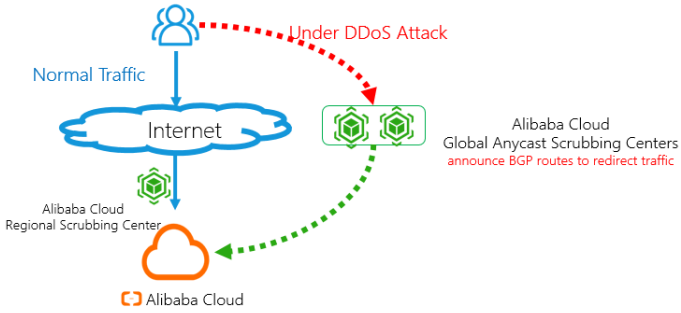
Prerequisites

- An Anti-DDoS Origin Enterprise instance is purchased. For more information, see Purchase an Anti-DDoS Origin Enterprise instance.

- An on-demand Anti-DDoS Origin instance is enabled. To do so, you must contact the sales personnel.
- Alert contacts and alert groups are created in Cloud Monitor. For more information, see Create an alert contact or alert contact group.

Context

An on-demand Anti-DDoS Origin instance can provide protection against DDoS attacks for on-premises data centers, small carriers, customers outside mainland China, and customers who have their own BGP networks. You do not need to change your service IP addresses or network architecture. The following figure shows the protection mechanism of the on-demand Anti-DDoS Origin instance.



Description:

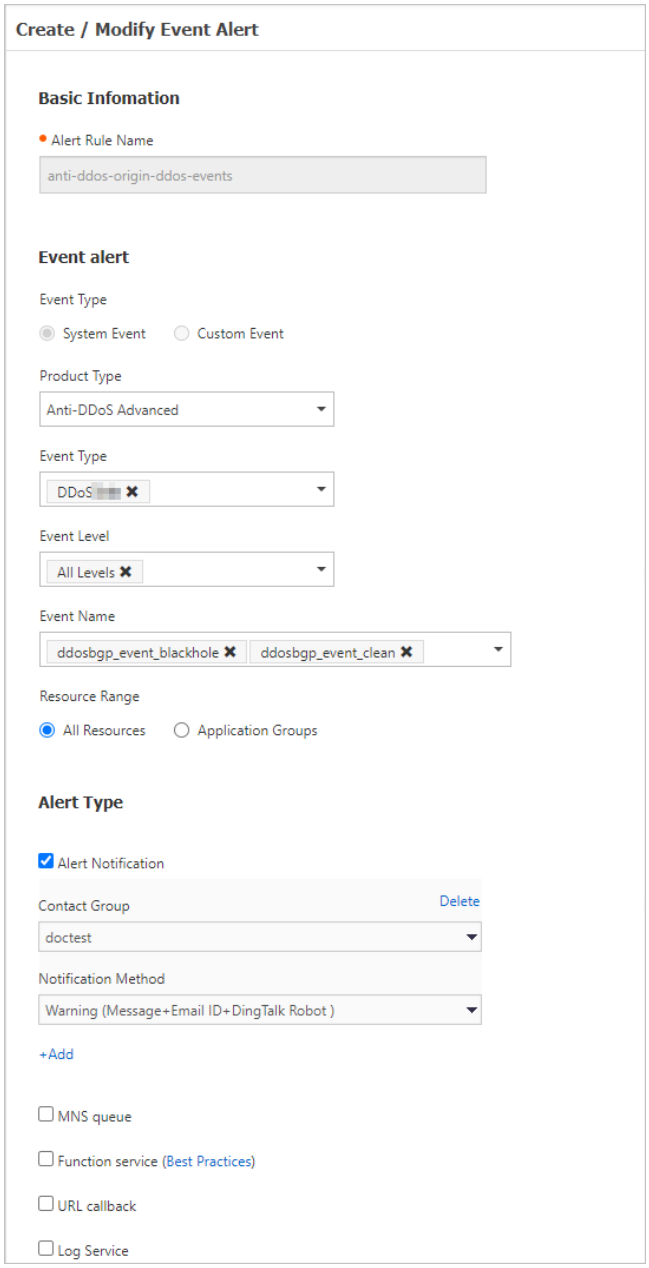
- The service traffic is normal, or a small-scale attack occurs: The traffic is forwarded to the local scrubbing center of Anti-DDoS Origin. The service latency does not increase.
- A DDoS attack occurs: The scrubbing centers distributed across the world declare routes to forward and scrub the traffic. The service latency slightly increases, but the protection capability can reach a Tbit/s level.

You can configure alert rules in Cloud Monitor to monitor DDoS attacks in the local scrubbing center of Anti-DDoS Origin. If an attack occurs, you can call API operations to enable traffic redirection of the on-demand Anti-DDoS Origin instance and disable traffic redirection after the attack stops.

> **Note** In this topic, API request parameters are described in the `<Parameter description>` format. For example, specify the ID of the on-demand Anti-DDoS Origin instance in `instanceId=<yourOnDemandInstanceId>`.
>
> You must replace `<Parameter description>` with the actual parameter value. For example, contact the sales personnel to obtain the ID of your on-demand Anti-DDoS Origin instance and replace `<yourOnDemandInstanceId>` with the ID.

Procedure

1. Configure an alert rule in Cloud Monitor to monitor blackhole filtering and traffic scrubbing events in the local scrubbing center of Anti-DDoS Origin.
   i. Log on to the Cloud Monitor console.
   ii. In the left-side navigation pane, choose **Alarms > Alarm Rules**.
   iii. Click the **Event Alarm** tab.
   iv. On the Event Alarm tab, click **Create Event Alert**.
   v. In the **Create / Modify Event Alert** pane, configure the following alert parameters.

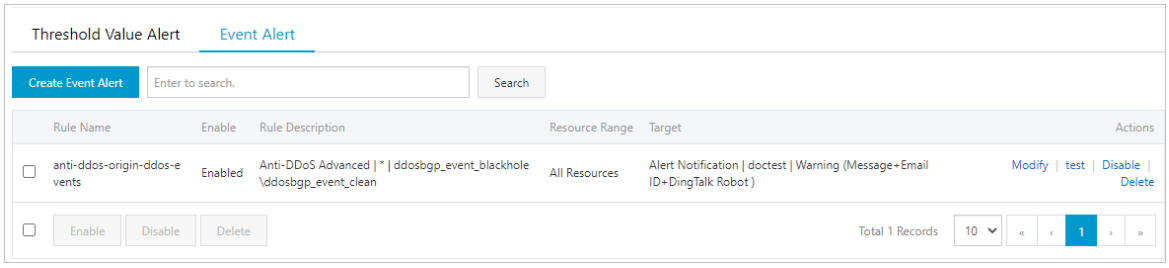


Parameter	Description
Alarm Rule Name	Enter the name of the alert rule. For example, enter Alert for DDoS attacks of Anti-DDoS Origin.
Event Type	Select **System Event**.
Product Type	Select **Anti-DDoS Advanced**.
Event Level	Select **All Levels**.
Event Name	Select **ddosbgp_event_blackhole** and **ddosbgp_event_clean**.
Resource Range	Select **All Resources**.

Parameter	Description
Alarm Notification	Select **Alarm Notification**. Then, specify **Contact Group** and **Notification Method**.

vi. Click **OK**.

The created alert rule automatically takes effect. If the Anti-DDoS Origin instance detects a DDoS attack, contacts in the alert group receive a notification. You can view and manage **event alert rules** in the list. For more information, see Create an alert rule.



2. If a DDoS attack occurs, the contacts receive a notification of the blackhole filtering or traffic scrubbing event. In this case, call the ModifyOnDemaondDefenseStatus API operation to redirect traffic to the global anycast scrubbing centers of Alibaba Cloud.

   You must specify the following request parameters:

   ```
   ? Action=ModifyOnDemaondDefenseStatus
   &DdosRegionId=<yourInstanceRegionId>
   &DefenseStatus=Defense
   &InstanceId=<yourOnDemandInstanceId>
   ```

3. (Optional)Disable blackhole filtering in the on-demand Anti-DDoS Origin instance.
   - If blackhole filtering is not triggered, skip this step.
   - If blackhole filtering is triggered, call the DeleteBlackhole API operation to disable it 10 seconds after you enable traffic redirection.

     You must specify the following request parameters:

     ```
     ? Action=DeleteBlackhole
     &InstanceId=<yourOnDemandInstanceId>
     &Ip=<yourOnDemandInstanceIp>
     ```

4. Call the DescribeTopTraffic API operation to check whether the DDoS attack stops.

   You must specify the following request parameters:

   ```
   ? Action=DescribeTopTraffic
   &Ipnet=<onDemandInstanceIpnetToQuery>
   &InstanceId=<yourOnDemandInstanceId>
   &StartTime=<startTimeToQuery>
   &EndTime=<endTimeToQuery>
   ```

   If the value of the AttackBps parameter returned by the API operation is smaller than 300000 for more than 30 minutes, the DDoS attack stops. This parameter indicates the volume of attack traffic, in Kbit/s.

5. After the DDoS attack stops, call the ModifyOnDemaondDefenseStatus API operation during off-peak

hours to stop traffic redirection in the on-demand Anti-DDoS Origin instance.

> **Note** We recommend that you call this API operation during off-peak hours to minimize service impact caused by traffic switching.

You must specify the following request parameters:

```
? Action=ModifyOnDemaondDefenseStatus
&DdosRegionId=<yourDdosRegionId>
&DefenseStatus=UnDefense
&InstanceId=<yourOnDemandInstanceId>
```