ALIBABA CLOUD

Alibaba Cloud

Anti-DDoS

Anti-DDoS Origin User Guide

Document Version: 20201117

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.Purchase an Anti-DDoS Origin Enterprise instance

This topic describes how to purchase an Anti-DDoS Origin Enterprise instance.

Prerequisites

- The enterprise real-name verification is completed for your Alibaba Cloud account.

  You can purchase an Anti-DDoS Origin Enterprise instance only after you complete enterprise real-name verification.

- A purchase request is submitted on the Application for Anti-DDoS Origin page.

  You must submit your company information so that Alibaba Cloud can determine your business needs.

- The cloud assets that you want to protect include public IP addresses of ECS instances, public IP addresses of SLB instances, elastic IP addresses (EIPs), or IP addresses of WAF instances.

Context

Anti-DDoS Origin supports the Basic and Enterprise mitigation plans.

- Anti-DDoS Origin Basic is enabled by default. It provides a basic protection capacity of up to 5 Gbit/s against DDoS attacks for public IP addresses of Alibaba Cloud resources free of charge.
- Anti-DDoS Origin Enterprise must be purchased. It protects public IP addresses of Alibaba Cloud resources, including ECS instances, SLB instances, EIPs, and WAF instances. 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 more information about the billing methods of Anti-DDoS Origin, see Billing methods of Anti-DDoS Origin.

Procedure

1. Access the product homepage and click Buy Now.
2. Set **Product Type** to **Anti-DDoS Origin**.

   > **Note** Before you purchase an **Anti-DDoS Origin** instance, you must submit an application.

3. On the **Anti-DDoS Origin buy page**, set Mitigation Plan to **Enterprise** and configure the required parameters.

Parameter	Description
IP Version	The version of the IP protocol. Valid values: **IPV4** and **IPV6**.

Parameter	Description
Region	The region where the Anti-DDoS Origin instance resides. **Notice** ◦ The Anti-DDoS Origin instance must reside in the same region as the assets that you want to protect. The assets are cloud resources such as ECS instances, SLB instances, WAF instances, and EIPs. ◦ Anti-DDoS Origin Enterprise instances are available only in mainland China. If you want to purchase an Anti-DDoS Origin Enterprise instance outside mainland China, submit a ticket or contact sales.
Business Scale	The average network bandwidth of the business that you want to protect. The maximum bandwidth is 10 Gbit/s, and the minimum bandwidth is 100 Mbit/s. For more information about how to evaluate the business scale, see Instance specifications of Anti-DDoS Origin Enterprise.
IP Addresses	The total number of IP addresses that you want to protect. Valid values: **100** to **255**. Default value: **100**.
Mitigation Analysis (Beta)	The Mitigation Analysis feature is in public preview. It provides log analysis and reports of protected traffic free of charge. Valid values: **On** and **Off**. **Note** After you enable this feature, Mitigation Analysis (Beta) appears in the left-side navigation pane.
Resource Group	A resource group is a group of resources under an Alibaba cloud account. You can manage members, permissions, and resources in a resource group. Select an existing resource group or create one.
Quantity	The number of the Anti-DDoS Origin instances that you want to purchase. **Note** We recommend that you determine the number of the instances that you want to purchase based on the number of IP addresses that you want to protect in the current region. For example, if each instance can provide protection for 200 IP addresses, and you want to protect 400 IP addresses, you can purchase two instances.
Duration	The validity period of the Anti-DDoS Origin instance. You can select **Auto-renewal** as required.

4. Click **Buy Now**.
5. Complete the payment.

Result

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

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. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the **Assets** page, select a region.
3. On the **Assets** page, view protection information in the **DDoS Attack Protection Information** section.

   DDoS Attack Protection Information

   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 cleaning 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.Enable traffic rerouting to an on-demand instance

This topic describes how to enable traffic rerouting to an on-demand Anti-DDoS Origin instance in the Anti-DDoS console.

Prerequisites

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

> **Note** On-demand instances protect servers in on-premises data centers outside China and cloud assets based on CIDR blocks. You must contact sales personnel to purchase on-demand instances.

Procedure

1. Log on to the Anti-DDoS console.
2. In the top navigation bar, select the region where your on-demand Anti-DDoS Origin instance resides.
3. On the Assets page, click the **Others** tab.

   > **Note** The **Others** tab shows the IP addresses of all your on-demand Anti-DDoS Origin instances. If you have not purchased on-demand instances, the **Others** tab contains no IP addresses.

4. Find the IP address of your on-demand instance and click **Start Redirection** in the Operation column. In the message that appears, click OK.

   Start Redirection

Result

If traffic rerouting is enabled, the IP address of your on-demand instance is in the **Redirecting** state. This indicates that the system is rerouting the traffic of protected assets to mitigate DDoS attacks. If you want to stop rerouting the traffic, click **Pause Redirection** in the Operation column.

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

Pause Redirection

4.Cleaning settings

4.1. Configure a cleaning threshold

This topic describes how to configure a cleaning threshold in the Anti-DDoS Basic console.

Context

Anti-DDoS Basic is applied to protect Alibaba Cloud assets by default. The service is provided free of charge after each asset is activated. The assets include Elastic Compute Service, Server Load Balancer, and Elastic IP Address instances. The maximum throughput of DDoS attacks that an asset encounters may exceed the specified cleaning threshold. In such cases, Anit-DDoS cleans attack traffic and performs other counter measures to ensure business continuity.

Procedure

1. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the **Assets** page, select a region.
3. Select the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud service for which you want to configure a cleaning threshold.
4. In a list of instances, find the target instance and click the **IP** address of the instance. If excessive instances exist, we recommend that you search for the target instance by using the **instance ID**, **instance name**, or **instance IP** as the search condition.

   
5. In the **Instances Details** dialog box, click **Cleaning Settings**.

   
6. In the **Cleaning Settings** dialog box, select **Default** or **Manual Setting** in the Cleaning Threshold field.
   - **Default**: Anti-DDoS Basic dynamically adjusts the cleaning threshold based on the traffic load of an asset.
   - **Manual setting**: You can select a specific threshold that includes two values. One indicates the minimum throughput and the other indicates the mininum packets per second (PPS).

     Recommendations:

     - Configure a cleaning threshold of which the value is slightly greater than the maximum bandwidth for actual incoming requests. If the specified value of a threshold is greater than expected, the effect of protection is compromised. If the specified value of a threshold is less than expected, legitimate access may be affected when traffic cleaning is triggered.
     - If legitimate access is affected, we recommend that you increase the value of the cleaning threshold.
     - During large promotions or activities for a website, we recommend that you increase the specified value of a cleaning threshold.

Result

The cleaning threshold is configured. When the maximum throughput of incoming requests that a

website can serve reaches the specified cleaning threshold, Anti-DDoS Basic launches traffic cleaning.

4.2. 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. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the **Assets** page, select a region.
3. Select the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud service for which you want to configure a cleaning threshold.
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 cleaning 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.

4.3. 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.

4.4. 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 cleaning threshold.

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

5.Instances

5.1. 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** Anti-DDoS Origin Enterprise instances must reside in the same region as the assets that you want to protect. The assets are cloud resources such as Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, Web Application Firewall (WAF) instances, and elastic IP addresses (EIPs).

Procedure

1. Log on to the Anti-DDoS console.
2. In the upper-left corner of the top navigation bar, select a region.
3. In the left-side navigation pane, choose **Anti-DDoS Origin > Manage Instances**.
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**.

   Add a protection package
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 (,).

IP address of a protected cloud service

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

5.2. View security reports

This topic describes how to view the total traffic of an instance, traffic of each IP address, and a list of event logs for DDoS attacks after you add a protection target to the instance.

Procedure

1.
2.
3. In the **Anti-DDoS Origin** console, find the instance whose operations log that you want to view, click **View Report** in the Actions column of the instance.

   
4. On the **Monitoring** tab, select a protection target and a time range. The console shows the trend of network traffic and event logs of DDoS attacks. The network traffic metric includes the inbound traffic and number of received data packets.

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

5.3. View operations logs

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

Procedure

1.
2.
3. On the **Instances** page, find the instance whose operations logs that you want to view, and click **Manage** in the Actions column of the instance.

4. On the Instance Details page, click the **Operations Log** tab.
5. On the **Operations Log** tab, specify a time range and query operations logs that are generated within the time range. Each operations log includes the operation time and a description.

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

5.4. Upgrade instance types

If the clean bandwidth and the protected IP addresses of your Anti-DDoS Origin Enterprise instance do not meet your business needs, 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 **Clean Bandwidth** 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 needs, you can purchase an Anti-DDoS Origin Enterprise instance. For more information, see Purchase an Anti-DDoS Origin Enterprise instance.

Procedure

1. Log on to the Anti-DDoS console.
2. In the upper-left corner of the top navigation bar, select a region.
3. In the left-side navigation pane, choose **Anti-DDoS Origin > Manage Instances**.
4. Find the purchased instance and choose **More > Upgrade** in the Actions column.
5. On the **Upgrade/Downgrade** page, upgrade the instance type.
6. Read and select **Anti-DDoS Origin Terms of Service** and click **Buy Now**.
7. Complete the payment.

5.5. Specify an alias

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

Procedure

1.
2.
3. In the **Anti-DDoS Origin** console, find the target instance, and click the Edit icon next to the alias of the instance.

   
4. In the **Edit Alias** dialog box, enter an alias, and click **OK**.

   > **Note** The alias must be 2 to 50 characters in length and can contain letters, digits, and underscores (_).

Result

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

6.Mitigation settings (public preview)

6.1. 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 ticket 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 ticket to request technical support.

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

Enable cross-border traffic blocking

1. Log on to the Anti-DDoS console.
2. In the left-side navigation pane, choose **Anti-DDoS Origin > Mitigation Settings**.
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. Log on to the Anti-DDoS console.
2. In the left-side navigation pane, choose **Anti-DDoS Origin > Mitigation Settings**.
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.

6.2. 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 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 the policy configuration function is in public preview and is free of charge. It is available only if you have purchased an Anti-DDoS Origin Enterprise instance. If you want to enable this feature, submit a ticket.

- 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 for you to use the policy configuration function, 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, they 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 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 these IP addresses are also denied. For more information, see Configure the ICMP Blocking policy.
Source Port Blocking	Denies requests from the UDP or TCP protocol over the source or destination ports to mitigate UDP reflection attacks.	Configure the protocols and ports to deny requests. After you enable this policy, requests from the specified protocol and ports are denied. 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 included in the blacklist are denied, and requests from the IP addresses included in the whitelist are allowed. For more information, see Configure the Blacklist and Whitelist policy.
Byte-Match Filter	Matches bytes for the content of specific packets to limit the rates of, deny, or allow 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. Log on to the Anti-DDoS console.
2. In the left-side navigation pane, choose **Anti-DDoS Origin > Mitigation Settings**.
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**.

     Create a policy template

     After you create the policy template, it 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.

   Add IP Addresses

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 required cloud service. **Note** An IP address can be added to only one policy template. If an IP address is already added to a different policy template, you cannot select it.

   iii. Click **OK**.

   After you add the IP addresses, requests from these IP addresses are processed based on the policies in this template. By default, no policies are enabled in the 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.

   ICMP Blocking

   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 for blocking. Valid values: **TCP** and **UDP**.
Type	The type of port for blocking. Valid values: **Source Port** and **Destination Port**.
Port Range	The range of ports for blocking. 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 from the specified protocol and ports. The value is fixed as **Block**.

iv. Click **OK**.
After you add a port blocking rule, it automatically takes effect. Requests from 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. Separate multiple IP addresses with spaces or line breaks.

iv. Click **OK**.
After you configure the Blacklist and Whitelist policy, it immediately takes effect. Requests from the IP addresses included in the blacklist are denied, and requests from the IP addresses 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.

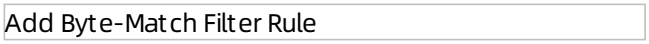
9. (Optional)Configure the Byte-Match Filter policy.To configure the Byte-Match Filter policy, perform the following steps:
   i. On the Policy Configuration tab, click **Configure** for the **Byte-Match Filter** option.

   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.
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 set **Bandwidth**. Valid values of **Bandwidth**: 1 to 100000.

   iv. Click **OK**.
   After you configure the Byte-Match Filter policy, it automatically takes effect. Requests that meet the rules are denied, allowed, or limited based on the policy. You can manage the 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.

7.Mitigation analysis (public preview)

7.1. 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. Log on to the Anti-DDoS console.
2. In the upper-left corner of the top navigation bar, select a region.
3. In the left-side navigation pane, choose **Anti-DDoS Origin > Mitigation Analysis (Beta)**.
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

7.2. 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. Log on to the Anti-DDoS console.
2. In the upper-left corner of the top navigation bar, select a region.
3. In the left-side navigation pane, choose **Anti-DDoS Origin > Mitigation Analysis (Beta)**.
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.

   Mitigation Logs
5.
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 results.

Manage the query results

You can view the query results in a log distribution histogram, on the Raw Logs tab, or by using a chart. You can also configure alerts and saved searches.

> **Note** By default, 100 results are returned. For information about how to obtain more than 100 results, see LIMIT syntax.

- Log distribution histogram

  The log distribution histogram shows the distribution of query results in different time ranges.

  - Move the pointer over a green rectangle to view the time range that is represented by the rectangle. You can also view the number of log entries that are obtained within the time range.
  - Click a rectangle to view a more fine-grained log distribution. You can also view the query results on the **Raw Logs** tab.

- Raw Logs tab

  On the **Raw Logs** tab, you can view the query results. You can perform the following operations:

- Quick analysis: analyzes the distribution of a field within a period of time. For more information, see Quick analysis.
- Contextual query: queries the contextual data of the specified log entries in the raw log file. Choose > **Context View**. A contextual query is performed. For more information, see Context query.
- LiveTail: monitors log data in real time and extracts key information. Choose > **LiveTail**. Log monitoring and extraction are performed. For more information, see LiveTail.

  > **Note** LiveTail can monitor and extract the log data that is collected by Logtail.

- Key-value pair arrangement: displays log entries in key-value pairs. Choose > **Warp/Unwarp Key-value Pairs**. Log entries are displayed in key-value pairs.
- Log download: downloads logs. In the upper-right corner of the Raw Logs tab, click the icon. In the Log Download dialog box, select a download range and tool, and then click OK. Logs are downloaded. For more information, see Download logs.
- Column settings: sets fields. In the upper-right corner of the Raw Logs tab, click **Column Settings**. Select fields from the section on the left. Click **Add** to add the fields to the section on the right. The columns that correspond to the added fields appear on the **Raw Logs** tab. The field names are column names. The columns list the field values.

  > **Note** To view the log content on the **Raw Logs** tab, you must select **Content**.

  Column settings

- Content column settings: If the content of a field exceeds 3,000 characters, the excess characters are hidden. In this case, the message **The character string is too long and has been truncated** is displayed in front of the key value. You can click **Display Content Column** to modify the configurations.

  > **Note** If the content display limit is set to 10,000 characters, excess characters are not delimited.

  The following table describes the parameters in the Display Content Column dialog box.

Parameter		Description
Key-Value Pair Arrangement		Valid values: **New Line** and **Full Line**.
Hide Default Key-value Pairs		If you turn on this switch, the reserved fields of Log Service are hidden.
Default JSON Data Level		The level of JSON expansion.
Truncate Character String	**Key**	The key of the truncated value. By default, a field value is truncated if it contains more than 3,000 characters. The value of this parameter is null if no field values exceed 3,000 characters.
	Status	Specifies whether to enable the value truncation feature. By default, the feature is enabled. ■ **Enable**: If the value length exceeds the specified **truncate step**, the excess characters are truncated. ■ **Disable**: If the value length exceeds the specified **truncate step**, the excess characters are not truncated.
	Truncate Step	Specifies the maximum number of characters that can be displayed for a value. This parameter also specifies the number of incremental characters that are displayed each time you click Show. Valid values: 500 to 10000. Default value: 3000.

- Charts

  If you enable analytics when you configure indexes for fields and use query statements to query logs, you can view the analysis results on the **Graph** tab.

  - Multiple chart types are provided in Log Service, including tables, line charts, and bar charts. You can select a chart type to display the analysis results. For more information, see Chart overview.
  - Log Service allows you to create dashboards for real-time data analysis. You can click **Add to New Dashboard** to save your query statements as a chart to a specified dashboard. For more information, see Create and delete a dashboard.

- Drill-down analysis allows you to view deeper analysis results, which reveal more details. You can set the drill-down parameters and add the chart to a dashboard. Click a chart value to trigger a drill-down event. You can view deeper analysis results. For more information, see Configure a drill-down event for a chart.

- Alert

  You can click **Save as Alert** on the Search & Analysis page to create an alert for the query results. For more information, see Create an alert rule.

- Saved search

  You can also click **Save Search** on the Search & Analysis page to create a saved search. For more information, see Saved search.

7.3. 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. Log on to the Anti-DDoS console.
2. In the upper-left corner of the top navigation bar, select a region.
3. In the left-side navigation pane, choose **Anti-DDoS Origin > Mitigation Analysis (Beta)**.
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.

8.Black hole policies

8.1. View the duration of a black hole

A server may encounter a distributed denial of service (DDoS) attack. After a black hole is triggered due to the attack, access from clients to the public IP address of the server is blocked for a period of time. The access is unblocked after the duration of the black hole expires. The default black hole duration for an asset changes based on the region where the asset resides. You can view the duration of a black hole for an asset in the Anti-DDoS Basic console.

Context

The default duration of a black hole is 2.5 hours and you cannot disable the black hole during the period. In practical scenarios, the black hole duration depends on the attack situation and may range from 30 minutes to 24 hours. The duration of a black hole changes based on the following factors:

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

You can refer to the Anti-DDoS Pro console for more details about the black hole triggering threshold and black hole duration.

> Note
>
> - If excessive breaches of the black hole threshold occur on an asset, Alibaba Cloud reserves the right to extend the black hole duration and decrease the black hole threshold for the asset.
> - Blackhole filtering is a service that Internet service providers (ISPs) provide for Alibaba Cloud. Specific black hole triggering thresholds are predefined by ISPs. In most cases, the duration of a black hole is greater than or equal to 30 minutes. The duration of each black hole for an account changes based on the security credits of the account.

For more information about black hole policies that Alibaba Cloud provides, see Blackhole filtering policy of Alibaba Cloud.

Procedure

1. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the **Assets** page, select a region.
3. On the top of the Assets page, view **DDoS Attack Protection Information**. The duration after **Blackholing Disabled At** in the DDoS Attack Protection Information section refers to the black hole duration for an asset in the specified region.

8.2. Configure DDoS Protection notification settings

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

Manage message recipients

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

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

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

8.3. 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. Log on to the Alibaba Cloud Anti-DDoS Basic console.
2. On the top of the **Assets** page, select a region.
3. Select the **ECS**, **SLB**, **EIP (including NAT)**, or **Others** tab based on the type of cloud service for which you want to configure a cleaning threshold.
4. In a list of instances, find the target instance and click the **IP** address of the instance. If excessive instances exist, we recommend that you search for the target instance by using the **instance ID**, **instance name**, or **instance IP** as the search condition.
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.

8.4. 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.

8.5. Anti-DDoS Basic black hole threshold for web hosting

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

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

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

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

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

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

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

8.6. 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 a black hole.

Procedure

1. Log on to the Anti-DDoS console.
2. In the upper-left corner of the top navigation bar, select a region.
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

9.Best Practices

9.1. 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.

9.2. Upgrade Anti-DDoS Origin to Anti-DDoS Pro

This topic describes how to improve protection capacity by upgrading Anti-DDoS Origin to Anti-DDoS Pro. Given the design of Anti-DDoS Origin, the effect of protection may be compromised or the protection capacity cannot meet your business requirements. In such cases, we recommend that you upgrade Anti-DDoS Origin to Anti-DDoS Pro.

Context

For more information about scenarios to which Anti-DDoS Origin is applicable, see Scenarios.

If you encounter one of the following issues when using Anti-DDoS Origin, we recommend that you upgrade Anti-DDoS Origin to Anti-DDoS Pro.

- A protection target encounters continuous DDoS attacks that last for a long period of time.
- A protection target encounters HTTP flood attacks. However, Anti-DDoS Origin cannot defend against these types of attacks.
- Other specific issues.

> **Note** Alibaba Cloud will refund you the remaining balance of a paid Anti-DDoS Origin instance.

Procedure

1. Contact Alibaba Cloud Technical Support by using DingTalk.

   To join the DingTalk group, scan the following QR code.

   > **Note** If you have any questions when you upgrade Anti-DDoS Origin to Anti-DDoS Pro, contact Alibaba Cloud Technical Support by using DingTalk.

2. Alibaba Cloud support engineers will evaluate your environment to determine whether you can upgrade to Anti-DDoS Pro.
3. If all conditions are met, Alibaba Cloud will refund you the remaining balance of a paid Anti-DDoS Origin instance. The amount of the refund changes based on the specifications and remaining subscription duration of the Anti-DDoS Origin instance.
4. Purchase an Anti-DDoS Pro instance and add your assets to the instance for protection.

9.3. Best practices for automatic deactivation of black holes

To ensure business continuity, you must learn how to recover your business by deactivating a black hole that is applied to the IP address of a protection target. A black hole may still be activated if the protection target encounters an instantaneous amount of high-traffic DDoS attacks. Anti-DDoS Origin Enterprise supports automatic deactivation of black holes in response to such requirements.

Prerequisites

The solution applies to only Anti-DDoS Origin Enterprise instances. This is because you must call an Anti-DDoS Origin API operation to complete auto-deactivation. Before implementing the solution, make sure that the IP address of the required protection target 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

Anti-DDoS Origin allows you to deactivate black holes manually or automatically. However, manual deactivation may result in delays and unexpected errors. For more information, see Deactivate blackhole filtering. If your business requires a high level of stability and continuity, you can use the following method to set up automated responses and deactivation for black holes.

1. Create an alarm rule in the CloudMonitor console to monitor the blackhole events of an Anti-DDoS Origin Enterprise instance.

   > **Note** Only if blackhole events occur on the protected IP addresses, CloudMonitor sends messages. You must add IP addresses that you want to protect to the instance as protection targets.

2. Create an alarm rule and specify an action of calling the DeleteBlackhole API operation of Anti-DDoS Origin to deactivate the black holes.

Likewise, the preceding method also allows you to automatically call an API operation of Alibaba Cloud DNS. The operation helps change DNS records for a domain that is under DDoS attacks and associate the name of the domain with the IP address of an Anti-DDoS Pro instance.

Procedure

1. Log on to the CloudMonitor console.
2. In the left-side navigation pane, choose **Alarms > Alarm Rules**.
3. On the **Alarm Rules** page, select the **Event Alarm** tab.
4. Click **Create Event Alert** to create a rule for blackholing events.
   - In the **Product Type** field, select **Anti-DDoS Advanced**.
   - In the **Event Name** field, select **ddosbgp_event_blackhole**.

   
5. In the event alarm, select alarm types based on your business requirements and click **OK**. CloudMonitor supports the following alarm types:
   - **MNS queue**
   - **Function Compute**
   - **URL callback**
   - **Log Service**

   After you create the event alarm, the alarm automatically triggers a response to any blackhole events. Then, CloudMonitor sends an alarm message to the target that you specified in the Alarm Type section. The following shows a sample alarm message.

   Sample alarm message

```
{
  "action": "add", //The action. The value of add indicates that an event begins, and the value of del indicates that an event ends.
  "bps": 0, //The throughput of a DDoS attack. Unit: Mbit/s.
  "pps": 0, //The packet forwarding rate of a DDoS attack. Unit: packets per second (PPS).
  "instanceId": "ddosbgp-cn-78v17******", //The ID of an Anti-DDoS Origin instance.
  "ip": "47. *. *. *", //The IP address to which a black hole is applied.
  "regionId": "cn-hangzhou", //The ID of a region where the Anti-DDoS Origin instance resides.
  "time": 1564104493000, //The time when the event begins. Unit: milliseconds.
  "type": "blackhole"  //The event type. The value of defense indicates a cleaning event, and the value of blackhole indicates a blackholing event.
}
```

6. Specify an alarm action that calls the DeleteBlackhole API operation to deactivate black holes.

9.4. 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 submit a ticket 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 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.

9.5. 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.**xxxx**

   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 网站接入.
- **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 Supported custom ports.
- **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 WAF back-to-origin CIDR blocks.
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.

9.6. 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 an SLB 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 Before you begin.

   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 an SLB 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 Resolve a domain name.
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.

9.7. 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 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.

Protection mechanism

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.

Create / Modify Event Alert

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**.
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 event-triggered alert rule.

Event alert rules

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>
```