Anti-DDoS

User Guide (Paris)

Issue 01
Date 2018-08-15
Copyright © Huawei Technologies Co., Ltd. 2019. All rights reserved.
No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://e.huawei.com
## Contents

1 Introduction........................................................................................................................................... 1  
1.1 Functions............................................................................................................................................... 1  
1.2 Application Scenarios.......................................................................................................................... 2  
1.3 Accessing and Using Anti-DDoS......................................................................................................... 2  
1.3.1 How to Access Anti-DDoS.................................................................................................................. 2  
1.3.2 How to Use Anti-DDoS...................................................................................................................... 3  
1.3.3 Related Services.................................................................................................................................. 3  
1.3.4 User Permissions................................................................................................................................ 4  
2 Operation Guide.................................................................................................................................. 5  
2.1 Enabling Anti-DDoS.............................................................................................................................. 5  
2.2 Enabling Alarm Notification................................................................................................................... 6  
2.3 Adjusting Security Settings................................................................................................................... 7  
2.4 Viewing a Monitoring Report............................................................................................................... 9  
2.5 Viewing an Interception Report......................................................................................................... 10  
2.6 Disabling Anti-DDoS............................................................................................................................ 11  
3 FAQs................................................................................................................................................... 12  
3.1 What Is Anti-DDoS?............................................................................................................................... 12  
3.2 What Services Can I Use Anti-DDoS In?............................................................................................. 12  
3.3 How Do I Use Anti-DDoS?.................................................................................................................... 12  
3.4 What Kinds of Attacks Does Anti-DDoS Defend Against?.................................................................. 14  
3.5 Will I Be Promptly Notified When an Attack Is Detected?................................................................. 15  
A Change History................................................................................................................................... 16
1 Introduction

1.1 Functions

The Anti-DDoS traffic cleaning service (Anti-DDoS for short) defends against network- and application-layer distributed denial of service (DDoS) attacks and sends alarms immediately when detecting an attack. In addition, Anti-DDoS improves the utilization of bandwidth and ensures the stable running of users’ services.

Anti-DDoS monitors the service traffic from the Internet to ECSs, ELB instances, and BMSs to detect attack traffic in real time. It then cleans attack traffic according to user-configured defense policies so that services run as normal. In addition, monitoring reports are generated, presenting users with clear network security evaluations.

Anti-DDoS helps users cope with traffic attacks with ease. It can precisely identify connection exhaustion and slow-connection attacks and can help users defend against the following attacks:

- **Web server attacks**
  Such as SYN flood, HTTP flood, Challenge Collapsar (CC), and slow-connection attacks
- **Game attacks**
  Such as User Datagram Protocol (UDP) flood, SYN flood, Transmission Control Protocol (TCP), and fragment attacks
- **HTTPS server attacks**
  Such as SSL Dos and DDoS attacks
- **DNS server attacks**
  Such as attacks targeted at vulnerabilities in the Domain Name Server (DNS) protocol stack, DNS reflection attacks, DNS flood attacks, and DNS cache-miss attacks

Anti-DDoS also provides the following functions:

- Providing monitoring records for each elastic IP address (EIP), including the current defense status, current defense configurations, and the last 24 hours’ traffic and abnormalities
- Generating interception reports for all defended EIPs of a user. Statistics can be queried, including the number of cleaning times, cleaned traffic, the weekly top 10 most
1.2 Application Scenarios

Anti-DDoS defends against DDoS attacks only for ECSs, ELB instances, and BMSs.

Anti-DDoS devices are deployed at egresses of equipment rooms. Figure 1-1 shows the network topology.

The detection center detects network access traffic according to user-configured security policies. If an attack is detected, data is diverted to cleaning devices for real-time defense. Abnormal traffic is cleaned, and normal traffic is forwarded.

Figure 1-1 Network topology

1.3 Accessing and Using Anti-DDoS

1.3.1 How to Access Anti-DDoS

Anti-DDoS provides a web-based service management platform. You can access Anti-DDoS using the management console or HTTPS-based application programming interfaces (APIs).

- Management console

If you have an account, you can log in to the management console directly. On the home page, choose Security > Anti-DDoS to access the Anti-DDoS service.
1.3.2 How to Use Anti-DDoS

Anti-DDoS allows you to:

- Enable Anti-DDoS defense for IP addresses, which defends them against DDoS attacks.
- Enable alarm notification, which sends notifications by email when an IP address is under a DDoS attack.
- Adjust security settings based on service needs during defense.
- View monitoring and interception reports after the defense is enabled to check network security situations.
- Disable Anti-DDoS defense if you do not want to use it.

1.3.3 Related Services

ECS, ELB, and BMS

Anti-DDoS protects ECSs, ELB instances, and BMSs against DDoS attacks.

**NOTE**

- ECS is a computing server that consists of CPUs, memory, images, and Elastic Volume Service (EVS) disks and that allows on-demand allocation and elastic scaling. For details, see the *Elastic Cloud Server User Guide*.
- ELB is a service that automatically distributes access traffic to multiple ECSs to balance their service loads. ELB enables you to achieve higher levels of fault tolerance in your applications and expand application service capabilities. For more information, see the *Elastic Load Balance User Guide*.
- BMS provides dedicated bare metal servers for you. With excellent computing performance, the servers address your requirements for high performance and stability in core application scenarios. For details, see the *Bare Metal Server User Guide*.

CTS

Cloud Trace Service (CTS) provides you with a history of Anti-DDoS operations. After enabling CTS, you can view all generated traces to review and audit performed Anti-DDoS operations. For details, see the *Cloud Trace Service User Guide*.

- Anti-DDoS operations that can be recorded by CTS

<table>
<thead>
<tr>
<th>Operation</th>
<th>Trace Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling Anti-DDoS</td>
<td>openAntiddos</td>
</tr>
<tr>
<td>Disabling Anti-DDoS</td>
<td>deleteAntiddos</td>
</tr>
<tr>
<td>Adjusting Anti-DDoS security settings</td>
<td>updateAntiddos</td>
</tr>
</tbody>
</table>

- Using CTS to view Anti-DDoS audit logs
a. Log in to the management console.

b. Click in the upper left to select a region and project.

c. Select Cloud Trace Service under Management & Deployment.

d. In the left navigation pane, choose Trace List.

e. You can use filters to query traces. The following four filters are available:

   - **Trace Source, Resource Type, and Search By**
     - Select query conditions from the drop-down list, for example, choose Anti-DDoS > anti-ddos > Trace name > openAntiddos to query all Anti-DDoS enabling operations.
     - **Trace name**: This option allows you to select a trace name, such as openAntiddos.
     - **Resource ID**: This option allows you to select or manually enter the ID of the instance for which you want to view audit logs.
     - **Resource name**: This option allows you to select or manually enter the name of the instance for which you want to view audit logs.

   - **Operator**: Select a specific operator (at user level rather than tenant level).

   - **Trace Status**: Available options include All trace statuses, normal, warning, and incident. You can only select one of them.

   - **Start time and end time**: You can specify the time period to query traces.

f. Click on the left of the record to be queried to extend its details.

g. In the row containing the desired record, click View Trace.

### IAM

Identity and Access Management (IAM) provides the permission management function for Anti-DDoS. Only users who have Anti-DDoS Administrator permissions can use Anti-DDoS. To apply for Anti-DDoS Administrator permissions, contact a user with Security Administrator permissions. For details, see the Identity and Access Management User Guide.

### SMN

The Simple Message Notification (SMN) service provides the notification function. When alarm notification is enabled in Anti-DDoS, you will receive alarm messages by email if your IP address is under a DDoS attack.

For details about SMN, see the Simple Message Notification User Guide.

### 1.3.4 User Permissions

The public cloud system provides two types of permissions by default: user management and resource management.

- **User management** refers to the management of users, user groups, and user group rights.
- **Resource management** refers to the control operations that can be performed by users on cloud service resources.
2 Operation Guide

2.1 Enabling Anti-DDoS

Enabling Anti-DDoS for an IP address automatically defends it against DDoS attacks.

Step 1  Log in to the management console.

Step 2  Click in the upper left to select a region and project.

Step 3  Choose Security > Anti-DDoS. The Anti-DDoS service page is displayed.

Step 4  Choose Anti-DDoS > Instance List, locate the row containing the instance IP address for which you want to enable Anti-DDoS, and click Enable Anti-DDoS.

Step 5  In the Enable Anti-DDoS dialog box, configure parameters as prompted.
### Table 2-1 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Cleaning</td>
<td><strong>Threshold</strong>&lt;br&gt;Total traffic detected by Anti-DDoS, including TCP traffic and UDP traffic.&lt;br&gt;Set this parameter based on the actual service access traffic. You are advised to set a value close to, but not exceeding, the purchased bandwidth.&lt;br&gt;The value of this parameter is not the threshold that triggers Anti-DDoS. Different attack types have different built-in thresholds.&lt;br&gt;If service traffic triggers Anti-DDoS, only attack traffic is intercepted. If service traffic does not trigger Anti-DDoS, no traffic is intercepted.</td>
</tr>
</tbody>
</table>
| CC Defense                 | **Disable**: Disable the defense. <br>**Enable**: Enable the defense. **NOTE**: CC defense is available only for clients supporting the full HTTP protocol stack because CC defense works in redirection or redirection+verification code mode. If your client does not support the full HTTP protocol stack, you are advised to disable CC defense.  |}

**Step 6** Click **OK** to save the configurations and enable defense.

### End

## 2.2 Enabling Alarm Notification

The alarm notification function sends you alarm notifications (by email) if a DDoS attack is detected. If you do not enable this function, you have to log in to the management console to view alarms.

**Step 1** Log in to the management console.

**Step 2** Click 📍 in the upper left to select a region and project.

**Step 3** Choose **Security > Anti-DDoS**. The Anti-DDoS service management page is displayed.
**Step 4** In the upper right corner, click **Configure Alarm Notification**.

![Configure Alarm Notification](image)

**Table 2-2** Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-DDoS Alarm Notification</td>
<td>Indicates whether the alarm notification function is enabled. There are two values:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Status: enabled" /> <img src="image" alt="Status: disabled" /></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the function is in disabled state, click <img src="image" alt="Status: disabled" /> to set it to <img src="image" alt="Status: enabled" />.</td>
<td></td>
</tr>
<tr>
<td>Topic</td>
<td>You can select an existing topic or click <strong>Create Topic</strong> to create a topic.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For details about groups, see the <strong>Simple Message Notification User Guide</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 5** Click **OK** to enable alarm notification.

----End

## 2.3 Adjusting Security Settings

You can adjust security settings after Anti-DDoS defense is enabled.

**Step 1** Log in to the management console.

**Step 2** Click ![Location](image) in the upper left to select a region and project.

**Step 3** Choose **Security > Anti-DDoS**. The Anti-DDoS service page is displayed.

**Step 4** Choose **Anti-DDoS > Instance List**, locate the row containing the instance IP address for which you want to modify security settings, and click .
The Advanced Settings page is displayed.

**Table 2-3 Parameter description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Cleaning Threshold</td>
<td>Total traffic detected by Anti-DDoS, including TCP traffic and UDP traffic</td>
</tr>
<tr>
<td></td>
<td>Set this parameter based on the actual service access traffic. You are</td>
</tr>
<tr>
<td></td>
<td>advised to set a value close to, but not exceeding, the purchased bandwidth.</td>
</tr>
<tr>
<td></td>
<td>The value of this parameter is not the threshold that triggers Anti-DDoS.</td>
</tr>
<tr>
<td></td>
<td>Different attack types have different built-in thresholds.</td>
</tr>
<tr>
<td></td>
<td>If service traffic triggers Anti-DDoS, only attack traffic is intercepted.</td>
</tr>
<tr>
<td></td>
<td>If service traffic does not trigger Anti-DDoS, no traffic is intercepted.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| CC Defense       | - Disable: Disable the defense.  
- Enable: Enable the defense.  
**NOTE**  
CC defense is available only for clients supporting the full HTTP protocol stack because CC defense works in redirection or redirection+verification code mode. If your client does not support the full HTTP protocol stack, you are advised to disable CC defense.  
- **HTTP Request Rate:**  
This option is available only when CC defense is enabled.  
You are advised to set this parameter to the maximum number of HTTP requests that can be processed by a deployed service. Anti-DDoS automatically cleans traffic if the total number of detected requests exceeds this threshold. If the value is too large, CC defense will not be triggered promptly.  
  - If the actual HTTP request rate is lower than the configured value, the deployed service is able to process all HTTP requests, and Anti-DDoS does not need to be involved.  
  - If the actual HTTP request rate is equal to or higher than the configured value, Anti-DDoS triggers CC defense to analyze and check each request, which affects responses to normal requests. |

**Step 6**  
Click **OK** to save the settings.

----End

### 2.4 Viewing a Monitoring Report

This section describes how to view the monitoring report of an instance IP address. This report includes the current defense status, current defense configurations, and the last 24 hours' traffic and abnormalities.

**Step 1**  
Log in to the management console.

**Step 2**  
Click **in the upper left to select a region and project.**

**Step 3**  
Choose **Security > Anti-DDoS.** The Anti-DDoS service management page is displayed.

**Step 4**  
Choose **Anti-DDoS > Instance List,** locate the row containing the instance IP address whose monitoring details you want to view, and click the instance IP address or **View Monitoring Report.**

**Step 5**  
On the **Monitoring Report** page, view monitoring details about the IP address.
You can view information such as the current defense status, current defense configurations, traffic within 24 hours, and abnormalities within 24 hours.

A 24-hour defense traffic chart is generated from data points taken in five-minute intervals. It includes the following information:
- **Traffic (Kbps)** displays the traffic status of the selected ECS, including the incoming attack traffic and normal traffic.
- **Packets per Second** displays the packet rate data of the selected ECS, including the attack packet rate and normal incoming packet rate.

Attack event list within one day: records DDoS attacks on the ECS within one day, including cleaning events and black hole events.

**NOTE**

On the **Monitoring Report** page, click to download monitoring reports to view monitoring details about instance IP addresses.

---End

### 2.5 Viewing an Interception Report

This section describes how to view defense statistics, including the number of cleaning times, cleaned traffic, weekly top 10 most frequently attacked ECSs, ELB instances, or BMSs, and total number of intercepted attacks of all instance IP addresses of a user.

**Step 1** Log in to the management console.

**Step 2** Click in the upper left to select a region and project.

**Step 3** Choose **Security > Anti-DDoS**. The Anti-DDoS service management page is displayed.

**Step 4** Choose **Anti-DDoS > Security Report** to view defense statistics about all IP addresses of a user.

You can view the weekly security report generated on a specific date. Currently, statistics, including the number of cleaning times, cleaned traffic, weekly top 10 most frequently attacked ECSs, ELB instances, or BMSs, and total number of intercepted attacks over the past four weeks can be queried.
2.6 Disabling Anti-DDoS

You can disable Anti-DDoS as required.

**Step 1** Log in to the management console.

**Step 2** Click in the upper left to select a region and project.

**Step 3** Choose Security > Anti-DDoS. The Anti-DDoS service page is displayed.

**Step 4** Choose Anti-DDoS > Instance List, locate the row containing the instance IP address for which you want to disable defense, and click Disable Anti-DDoS.

**Step 5** In the warning dialog box that is displayed, click OK to disable defense for the IP address.

---End
3.1 What Is Anti-DDoS?

The Anti-DDoS traffic cleaning service (Anti-DDoS for short) defends against network- and application-layer distributed denial of service (DDoS) attacks and sends alarms immediately when detecting an attack. In addition, Anti-DDoS improves the utilization of bandwidth and ensures the stable running of users’ services.

Anti-DDoS monitors the service traffic from the Internet to ECSs, ELB instances, and BMSs to detect attack traffic in real time. It then cleans attack traffic according to user-configured defense policies so that services run as normal. In addition, monitoring reports are generated, presenting users with clear network security evaluations.

3.2 What Services Can I Use Anti-DDoS In?

Anti-DDoS supports traffic cleaning only for ECSs, ELB instances, and BMSs.

3.3 How Do I Use Anti-DDoS?

Enabling Anti-DDoS for an IP address automatically defends it against DDoS attacks.

**Step 1**  Log in to the management console.

**Step 2**  Click 🗺️ in the upper left to select a region and project.

**Step 3**  Choose Security > Anti-DDoS. The Anti-DDoS service page is displayed.

**Step 4**  Choose Anti-DDoS > Instance List, locate the row containing the instance IP address for which you want to enable Anti-DDoS, and click Enable Anti-DDoS.
Step 5 In the Enable Anti-DDoS dialog box, configure parameters as prompted.

![Enable Anti-DDoS dialog box]

Table 3-1 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Cleaning Threshold</td>
<td>Total traffic detected by Anti-DDoS, including TCP traffic and UDP traffic&lt;br&gt;Set this parameter based on the actual service access traffic. You are advised to set a value close to, but not exceeding, the purchased bandwidth.&lt;br&gt;The value of this parameter is not the threshold that triggers Anti-DDoS. Different attack types have different built-in thresholds.&lt;br&gt;If service traffic triggers Anti-DDoS, only attack traffic is intercepted. If service traffic does not trigger Anti-DDoS, no traffic is intercepted.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC Defense</td>
<td>• <strong>Disable</strong>: Disable the defense.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable</strong>: Enable the defense.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
</tr>
<tr>
<td></td>
<td>CC defense is available only for clients supporting the full HTTP protocol stack because CC defense works in redirection or redirection+verification code mode. If your client does not support the full HTTP protocol stack, you are advised to disable CC defense.</td>
</tr>
<tr>
<td></td>
<td>• <strong>HTTP Request Rate</strong>:</td>
</tr>
<tr>
<td></td>
<td>This option is available only when CC defense is enabled.</td>
</tr>
<tr>
<td></td>
<td>You are advised to set this parameter to the maximum number of HTTP requests that can be processed by a deployed service. Anti-DDoS automatically cleans traffic if the total number of detected requests exceeds this threshold. If the value is too large, CC defense will not be triggered promptly.</td>
</tr>
<tr>
<td></td>
<td>- If the actual HTTP request rate is lower than the configured value, the deployed service is able to process all HTTP requests, and Anti-DDoS does not need to be involved.</td>
</tr>
<tr>
<td></td>
<td>- If the actual HTTP request rate is equal to or higher than the configured value, Anti-DDoS triggers CC defense to analyze and check each request, which affects responses to normal requests.</td>
</tr>
</tbody>
</table>

**Step 6**  Click **OK** to save the configurations and enable defense.

---End

### 3.4 What Kinds of Attacks Does Anti-DDoS Defend Against?

Anti-DDoS helps users cope with traffic attacks with ease. It can precisely identify connection exhaustion and slow-connection attacks and can help users defend against the following attacks:

- Web server attacks
  Such as SYN flood, HTTP flood, Challenge Collapsar (CC), and slow-connection attacks
- Game attacks
  Such as User Datagram Protocol (UDP) flood, SYN flood, Transmission Control Protocol (TCP), and fragment attacks
- HTTPS server attacks
  Such as SSL Dos and DDoS attacks
- DNS server attacks
  Such as attacks targeted at vulnerabilities in the Domain Name Server (DNS) protocol stack, DNS reflection attacks, DNS flood attacks, and DNS cache-miss attacks
3.5 Will I Be Promptly Notified When an Attack Is Detected?

Yes, if you have enabled alarm notification.

In the upper right corner of the console, click **Configure Alarm Notification** to enable the alarm notification function, which enables you to receive alarms (by email) if a DDoS attack is detected.
## Change History

<table>
<thead>
<tr>
<th>Released On</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-08-15</td>
<td>This is the first official release.</td>
</tr>
</tbody>
</table>