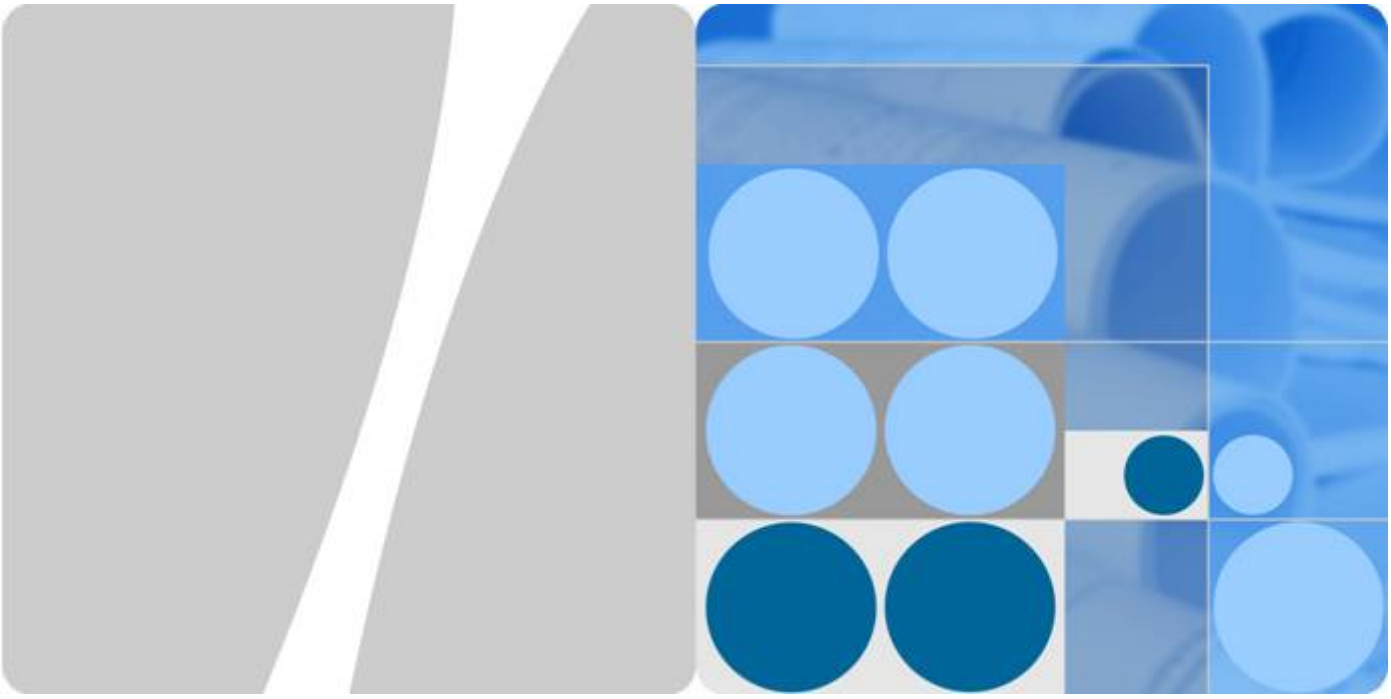


Anti-DDoS

User Guide

Date **2022-05-28**

Contents

1 Service Overview

1.1 What Is Anti-DDoS?

The Anti-DDoS service protects public IP addresses against Layer 4 to Layer 7 distributed denial of service (DDoS) attacks and sends alarms immediately when detecting an attack. Anti-DDoS improves the bandwidth utilization and ensures the stable running of user services.

Anti-DDoS monitors the service traffic from the Internet to public IP addresses and detects attack traffic in real time. It then scrubs attack traffic based on user-configured defense policies without interrupting service running. It also generates monitoring reports that provide visibility into the network traffic security.

1.2 Concepts

1.2.1 Scrubbing Principle and Black Hole Threshold

Anti-DDoS mitigates DDoS attacks and is enabled by default.

Scrubbing Principle

Anti-DDoS monitors service traffic in real time. Once an attack is detected, it diverts service traffic to the Anti-DDoS scrubbing system, which identifies the traffic from that IP address, discards the attack traffic, and forwards legitimate traffic to the target IP address.

Black Hole Threshold

The black hole threshold defines the basic attack mitigation capacity. When the scale of attack exceeds the threshold, the system will adopt a black hole policy to block the IP address.

Anti-DDoS provides a 300 Mbit/s mitigation capacity against DDoS attacks free of charge.

1.2.2 Common DDoS Attacks

DoS attacks are also called flood attacks. They are intended to exhaust the network or system resources on the target computer, causing service interruption or suspension. Consequently, legitimate users fail to access network services. A DDoS attack involves multiple compromised computers controlled by an attacker flooding the targeted server with superfluous requests. **Table 1-1** lists common DDoS attacks.

Table 1-1 Common DDoS attacks

Attack Type	Description	Example
Network layer attack	Occupies the network bandwidth with volumetric traffic, causing your service unable to respond to legitimate access requests.	NTP flood attack
Transport layer DDoS attack	Occupies the connection resources of the server, causing denial of services.	SYN flood attack and ACK flood attack
Session layer attack	Occupies SSL session resources of the server, causing denial of services.	SSL slow connection attack
Application layer attack	Occupies the application processing resources of the server and consumes its processing performance, causing denial of services.	HTTP GET flood attack and HTTP POST flood attack

1.3 Functions

The Anti-DDoS service protects public IP addresses against layer-4 to layer-7 distributed denial of service (DDoS) attacks and sends alarms immediately when detecting an attack. In addition, Anti-DDoS improves the bandwidth utilization to further safeguard user services.

Anti-DDoS monitors the service traffic from the Internet to public IP addresses to detect attack traffic in real time. It then scrubs attack traffic based on user-configured defense policies without interrupting service running. It also generates monitoring reports that provide visibility into the security of network traffic.

Anti-DDoS helps users mitigate the following attacks:

- Web server attacks

  Include SYN flood, HTTP flood, and low-rate attacks
- Game attacks

  Include UDP flood, SYN flood, TCP-based, and fragmentation attacks
- HTTPS server attacks

  Include SSL DoS and DDoS attacks

Anti-DDoS also provides the following functions:

- Monitors the security status of a single public IP address and offers a monitoring report, covering the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.
- Provides attack statistics reports on all protected public IP addresses, covering the traffic cleaning frequency, cleaned traffic amount, top 10 attacked public IP addresses, and number of blocked attacks.

1.4 Advantages

Anti-DDoS mitigates DDoS attacks for users. It delivers the following advantages.

- Premium protection

  Monitors DDoS attacks in real time, discards attack traffic, and forwards legitimate traffic to the destination IP address.

  Provides high-quality bandwidth to ensure service continuity and stability as well as user access speed.
- Complete and accurate

  A constantly updated database (carrying millions of blacklisted IP addresses) coupled with a 7-layer, smart cleaning mechanism ensures accurate traffic cleaning.
- Instantaneous response

  With industry-leading technology and powerful equipment, Anti-DDoS checks each packet and responds to any attack immediately without causing service delays.
- Enabled automatically

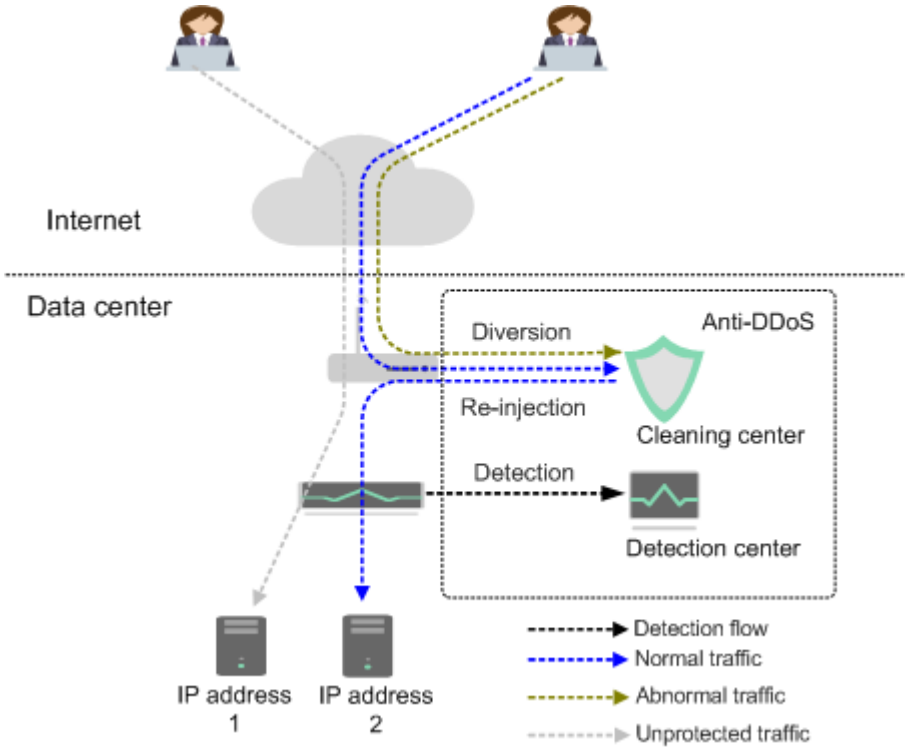
  This service is automatically enabled. No installation is required.
- Free of charge

  This service is free of charge.

1.5 Application Scenarios

Anti-DDoS devices are deployed at egresses of data centers. **Figure 1-1** shows the network topology.

Figure 1-1 Network topology



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

Anti-DDoS provides a 300 Mbit/s mitigation capacity against DDoS attacks for free. Traffic from the attacked public IP addresses will be routed to the black hole and the legitimate traffic will be discarded.

1.6 Accessing and Using Anti-DDoS

1.6.1 How to Access Anti-DDoS

- Management console

  Log in to the management console, click in the upper left corner, and select the desired region and project. Click on the left and choose **Security** > **Anti-DDoS**.
- HTTPS-compliant APIs

  You can access Anti-DDoS using APIs. For details, see the *Anti-DDoS API Reference*.

1.6.2 How to Use Anti-DDoS

Description:

- Enable Anti-DDoS to defend IP addresses against DDoS attacks.

- Enable alarm notification, which sends notifications by SMS or email when an IP address is under a DDoS attack.
- Adjust the defense policy based on service needs during defense.
- View monitoring and interception reports after the defense is enabled to check network security situations.
- You are not allowed to disable Anti-DDoS after it has been enabled.

1.6.3 Related Services

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 operations. For details, see the *Cloud Trace Service User Guide*.

Table 1-2 Anti-DDoS operations that CTS supports

Operation	Trace Name
Enabling Anti-DDoS	openAntiddos
Disabling Anti-DDoS	deleteAntiddos
Adjusting Anti-DDoS security settings	updateAntiddos

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 obtain this permission, contact the users who have the Security Administrator permissions. For details, see *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 through the endpoint you have configured, such as SMS or email, if your IP address is DDoS attacked.

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

1.6.4 Permission Management

The system provides two types of default permissions: user management and resource management. User management refers to management of users, user groups, and user group permissions. Resource management refers to control of operations over cloud service resources.

2 Viewing a Public IP Address

Scenarios

This topic describes how to view a public IP address.

NOTICE

- Anti-DDoS automatically enables the protection by default.
- You are not allowed to disable Anti-DDoS after it has been enabled.

Prerequisites

- You have obtained a username and password for logging in to the management console.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select the region and project.

Step 3 Click . Under **Security**, choose **Anti-DDoS**.

Step 4 On the **Public IP Addresses** tab, view all protected public IP addresses. **Table 2-1** describes the parameters.

NOTE

- Click **Enable Anti-DDoS for All IP Addresses** to enable the protection for all unprotected IP addresses in the current region.
- After the default Anti-DDoS protection settings are enabled, traffic is scrubbed when its volume reaches 120 Mbit/s. You can modify Anti-DDoS protection settings according to **Configuring an Anti-DDoS Protection Policy**.
- Anti-DDoS provides a 300 Mbit/s mitigation capacity against DDoS attacks. Traffic from the attacked public IP address will be routed to the black hole.
- The **All statuses** drop-down box enables you to specify a status so that only public IP addresses of the selected status are displayed.
- Enter a public IP address or a keyword of a public IP address in the search box and click or to search for the desired public IP address.

Table 2-1 Parameter description

Parameter	Description
Public IP Address	Public IP address protected by Anti-DDoS **NOTE** If Anti-DDoS is enabled for a public IP address, you can click the IP address to go to its **Monitoring Report** page.
Protection Status	Protection status of a public IP address. The values are: • **Normal** • **Configuring** • **Disabled** • **Cleaning** • **Black hole**

----End

3 Enabling Alarm Notification

Scenarios

When alarm notification is enabled in Anti-DDoS, you will receive alarm messages through the endpoint you have configured, such as SMS or email, if your IP address is DDoS attacked. If you do not enable this function, you have to log in to the management console to view alarms.

Prerequisites

- You have obtained a username and password for logging in to the management console.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the management console and select the region and project.

Step 3 Click  . Under **Security**, choose **Anti-DDoS**.

Step 4 On the **Anti-DDoS** page, click the **Alarm Notifications** tab and configure the alarm notification. For details about the parameter settings, see **Figure 3-1**.

Figure 3-1 Configuring alarm notifications

Table 3-1 Configuring alarm notifications

Parameter	Description	Example Value
Alarm Notifications	Indicates whether the alarm notification function is enabled. There are two values: •  : enabled •  : disabled If the function is in the disabled state, click  to set it to  .	
SMN Topic	You can select an existing topic or click **View Topic** to create a topic. For more information about SMN topics, see Simple Message Notification User Guide.	N/A

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

----End

4 Configuring an Anti-DDoS Protection Policy

Scenarios

You can adjust your Anti-DDoS protection policy after Anti-DDoS is enabled.

Prerequisites

You have obtained a username and password for logging in to the management console.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner of the management console and select the region and project.

Step 3 Click  . Under **Security**, choose **Anti-DDoS**.

Step 4 Click the **Public IP Addresses** tab, locate the row that contains the IP address for which you want to set protection, and click **Set Protection** in the **Operation** column.

Step 5 In the **Set Protection** dialog box, modify the parameters. **Figure 4-1** describes the parameters.**Table 4-1** describes the parameters.

Figure 4-1 Protection settings

Table 4-1 Parameter description

Parameter	Description
Protection Settings	• **Default**: In this mode, **Traffic Cleaning Threshold** is fixed at **120 Mbps**. When the service UDP traffic is greater than 120 Mbps or the TCP traffic is greater than 35,000 pps, traffic scrubbing is triggered and Anti-DDoS will automatically intercept the attack traffic. • **Manual**: In this mode, you can set the value of **Traffic Cleaning Threshold** based on your service needs. **NOTE** • Mbps = Mbit/s (short for 1,000,000 bit/s). It is a unit of transmission rate and refers to the number of bits transmitted per second. • PPS, short for Packets Per Second, is a measure of throughput for network devices. It means the number of packets sent per second.
Traffic Cleaning Threshold	Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the threshold. • When **Protection Settings** is set to **Default**, the value of **Traffic Cleaning Threshold** is **120 Mbps** by default. • When **Protection Settings** is set to **Manual**, the value of **Traffic Cleaning Threshold** can be set based on your service needs. You are advised to set the threshold to a value closest to the purchased bandwidth but not greater than the purchased bandwidth. **NOTE** If service traffic triggers scrubbing, only attack traffic is intercepted. If service traffic does not trigger scrubbing, no traffic is intercepted. Set this parameter based on the actual service access traffic. You are advised to set a value closest to, but not exceeding, the purchased bandwidth.

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

----End

5 Viewing a Monitoring Report

Scenarios

This section describes how to view the monitoring report of a public IP address. This report includes the protection status, protection settings, and the last 24 hours' traffic and anomalies.

Prerequisites

You have obtained a username and password for logging in to the management console.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select the region and project.

Step 3 Click . Under **Security**, choose **Anti-DDoS**.

Step 4 Click the **Public IP Addresses** tab, locate the row that contains the IP address of which you want to view its monitoring report, and click **View Monitoring Report**.

Step 5 On the **Monitoring Report** page, view monitoring details about the public 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** displays the traffic status of the selected ECS, including the incoming attack traffic and normal traffic.
  - **Packet Rate** displays the packet rate of the selected ECS, including the attack packet rate and normal incoming packet rate.
- The attack event list within one day records DDoS attacks on the ECS within one day, including cleaning events and black hole events.

NOTE

- Click  to download monitoring reports to view monitoring details about the public IP address.
- On the traffic monitoring report page, click Inbound attack traffic or Inbound normal traffic to view details about the **Inbound attack traffic** or **Inbound normal traffic.**
- On the packet rate monitoring report page, click Inbound attack packet rate or Inbound normal packet rate to view details about the **Inbound attack packet rate** and **Inbound normal packet rate**.

----End

6 Viewing an Interception Report

Scenarios

This section describes how to view the protection statistics, including the traffic cleaning frequency, cleaned traffic amount, weekly top 10 attacked public IP addresses, and total number of intercepted attacks of all public IP addresses of a user.

Prerequisites

You have obtained a username and password for logging in to the management console.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the management console and select the region and project.

Step 3 Click . Under **Security**, choose **Anti-DDoS**.

Step 4 Click the **Statistics** tab to view the protection statistics about all public IP addresses.

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 public IP addresses, and total number of intercepted attacks over the past four weeks can be queried.

NOTE

Click to download interception reports to view defense statistics of a time range.

----End

7 FAQs

7.1 About Anti-DDoS

7.1.1 What Is Anti-DDoS?

The Anti-DDoS service protects public IP addresses against layer-4 to layer-7 distributed denial of service (DDoS) attacks and sends alarms immediately when detecting an attack. In addition, Anti-DDoS improves the bandwidth utilization and ensures the stable running of user services.

Anti-DDoS monitors the service traffic from the Internet to public IP addresses to detect attack traffic in real time. It then scrubs attack traffic based on user-configured defense policies without interrupting service running. It also generates monitoring reports that provide visibility into the security of network traffic.

7.1.2 What Are a SYN Flood Attack and an ACK Flood Attack?

A SYN flood attack is a typical denial of service (DoS) attack. Utilizing the loop hole in the Transmission Control Protocol (TCP), the attacker sends a huge number of forged TCP connection requests to the target to exhaust its resources (fully loaded CPU or insufficient memory). Consequently, the target fails to respond to normal connection requests.

An ACK flood attack works in a similar mechanism as a SYN flood attack.

An ACK flood attack is when an attacker attempts to overload a server with TCP ACK packets. Like other DDoS attacks, the goal of an ACK flood is to deny service to other users by slowing down or crashing the target using junk data. The targeted server has to process each ACK packet received, which uses so much computing power that it is unable to serve legitimate users.

7.1.3 What Are a UDP Attack and a TCP Attack?

Exploiting the interaction characteristics of UDP and TCP, attackers use botnets to send large numbers of various TCP connection packets or UDP packets to exhaust the bandwidth resources of target servers. As a result, the servers become slow in processing capability and fail to work properly.

7.1.4 What Is the Million-level IP Address Blacklist Database?

The million-level IP address blacklist database refers to the database of millions of malicious IP addresses collected by experts in the past years. When users' services are attacked by these IP addresses, Anti-DDoS responds to those attacks first to defend your servers in a timely manner.

7.1.5 How Will Anti-DDoS Be Triggered to Scrub Traffic?

Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold.

- When the service traffic reaches this threshold, Anti-DDoS intercepts only attack traffic.
- If the service traffic does not reach the threshold, Anti-DDoS will not intercept the traffic, regardless of whether it is attack traffic.

7.1.6 Does Anti-DDoS Traffic Cleaning Affect Normal Services?

Anti-DDoS traffic cleaning exerts no adverse impacts on normal traffic.

7.1.7 How Does Anti-DDoS Scrub Traffic?

Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold.

7.1.8 What Are the Restrictions of Anti-DDoS?

The protection capability of Anti-DDoS depends on user network egress bandwidth.

7.2 About Basic Functions

7.2.1 Which Types of Attacks Does Anti-DDoS Mitigate?

Anti-DDoS helps users mitigate the following attacks:

- Web server attacks

  Include SYN flood, HTTP flood, and low-rate attacks
- Game attacks

  Include UDP flood, SYN flood, TCP-based, and fragmentation attacks
- HTTPS server attacks

  Include SSL DoS and DDoS attacks
- DNS server attacks

  Include attacks exploiting DNS protocol stack vulnerabilities, DNS reflection attacks, DNS flood attacks, and DNS cache miss attacks

7.2.2 What Is the Difference Between ELB Protection and ECS Protection?

An EIP can be bound to a load balancer or ECS. Anti-DDoS protects EIP against DDoS attacks. There is no difference between ELB and ECS protection.

7.2.3 Why Is the Number of Times of Cleaning Different from the Number of Attacks for the Same Public IP Address?

Cleaning is triggered automatically when an attack is detected on a public IP address. The cleaning lasts for a while. (Only attack traffic is cleaned, and users' services will not be affected.) If, during the cleaning, another attack is detected on the same public IP address, the attack will be cleaned together with the previous attack. Consequently, the number of attacks increases by one while the number of times of cleaning does not.

7.3 About Alarm notification

7.3.1 Will I Be Promptly Notified When an Attack Is Detected?

Yes, if you enable alarm notification.

On the console, click the **Alarm Notifications** tab to enable the alarm notification function, which enables you to receive alarms through the endpoint you have configured if a DDoS attack is detected. For details, see .

7.3.2 What Should I Do If I Receive an Alarm Notification?

It is normal if you receive an alarm notification. After the alarm notification function is enabled for your Anti-DDoS service, you will receive notifications through the endpoint you have configured when the public IP address is under DDoS attacks.

You can log in to the management console to .

A Change History

Released On	Description
2022-05-28	Removed the CC defense function.
2021-09-30	This issue is the second official release. • Modified parameters of the black hole threshold in **Scrubbing Principle and Black Hole Threshold**. • Updated some screenshots in **Configuring an Anti-DDoS Protection Policy**.
2020-09-30	This issue is the first official release.