Anti-DDoS

User Guide

Issue	01
Date	2022-09-30

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2022. 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

HUAWEI 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: https://www.huawei.com

Email: support@huawei.com

Contents

1 Enabling Alarm Notification

Scenarios

The alarm notification function sends you alarm notifications (by SMS or 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.

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

Table 1-1 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 ●.	●

Parameter	Description	Example Value
SMN Topic	You can select an existing topic or click **View Topic** to create a topic. For more information about SMN topics, see .	N/A

Step 4 Click **Apply** to enable alarm notification.

----End

2 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 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 4 In the **Set Protection** dialog box, modify desired parameters. **Table 2-1** describes the parameters.

Table 2-1 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 and enable **CC Defense**. **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.
CC Defense	● **Disable**: disables the defense. ● **Enable**: enables the defense. **NOTE** Challenge Collapsar (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.

Parameter	Description
HTTP Request Threshold	This parameter is required only when **CC Defense** is set to **Enable**. The unit is qps (short for queries per second). QPS is a common measure of the amount of search traffic an information retrieval system, such as a search engine or a database, receives during one second. This parameter is used to defend against a large number of malicious requests targeting websites. Defense against CC attacks, which aim to exhaust server resources by sending specially crafted GET or POST requests, is triggered when the HTTP request rate on a site reaches the selected value. In the EIP address protection, the maximum recommended value is **5000**. In ELB protection, the value can be larger. You are advised to set this parameter to the maximum number of HTTP requests that can be processed by the deployed service. Anti-DDoS will automatically scrub traffic if detecting that the total number of requests exceeds the configured HTTP request threshold. If the value is too large, CC defense will not be triggered promptly. ● If the actual HTTP request rate is smaller 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 greater than or equal to the configured value, Anti-DDoS triggers CC defense to analyze and check each request, which affects responses to normal requests.

Step 5 Click **OK** to save the settings.

----End

3 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 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 4 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

4 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 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

A Change History

Released On	Description
2022-09-30	This is the first official release.