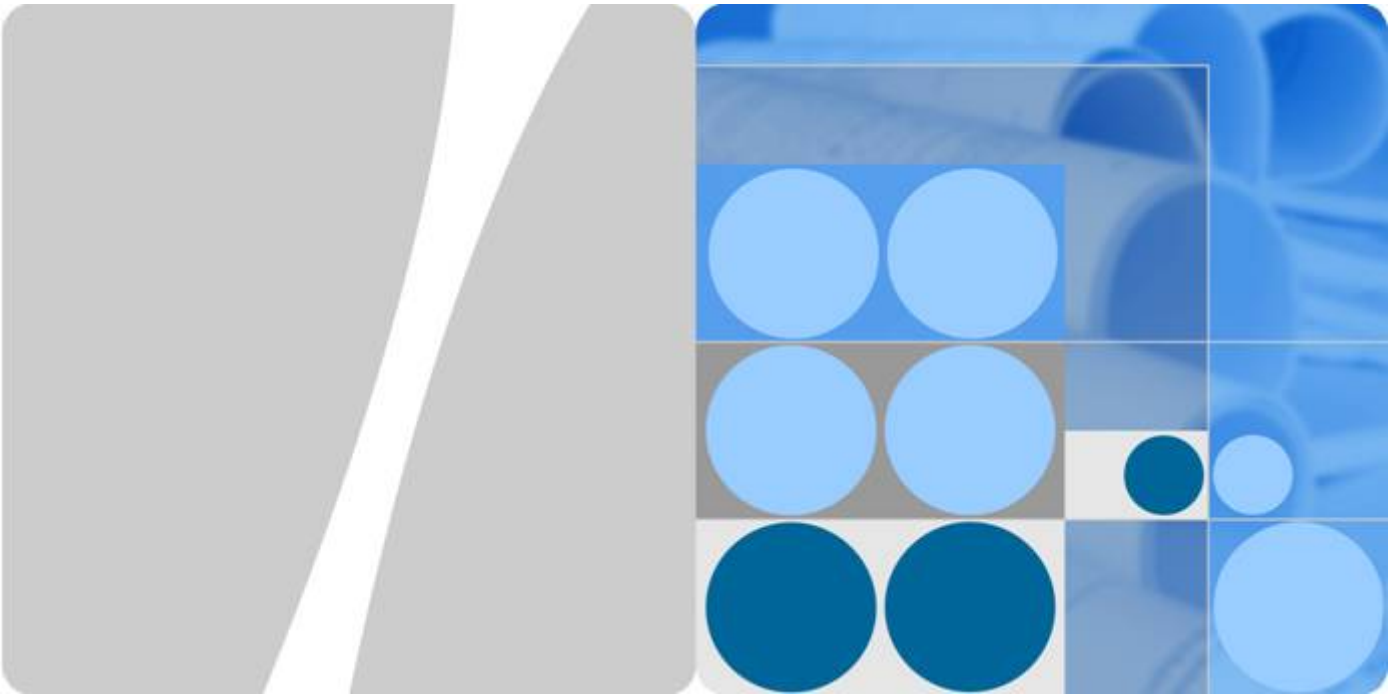


Anti-DDoS

Best Practices

Issue 02

Date 2020-04-01

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Copyright © Huawei Technologies Co., Ltd. 2020. 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.

Contents

1 Configuring Alarm Notifications.....1
2 Temporarily Disabling Anti-DDoS.....3
3 Connecting to a Server Routed to a Black Hole..... 5
4 Enhancing DDoS Mitigation Capabilities.....6
A Change History..... 7

 Copyright © Huawei Technologies Co., Ltd.

1 Configuring Alarm Notifications

Scenarios

The alarm notification function sends you alarm notifications (by SMS or email) if a DDoS attack is detected.

Prerequisites

- You have obtained a username and password for logging in to the management console.
- You have purchased at least one public IP address.

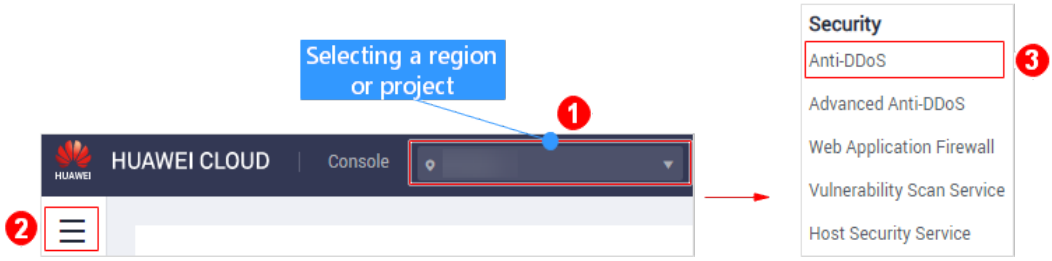
Procedure

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**. The **Security Console** is displayed.

Figure 1-1 Anti-DDoS



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

 Copyright © Huawei Technologies Co., Ltd.

Figure 1-2 Configuring alarm notifications

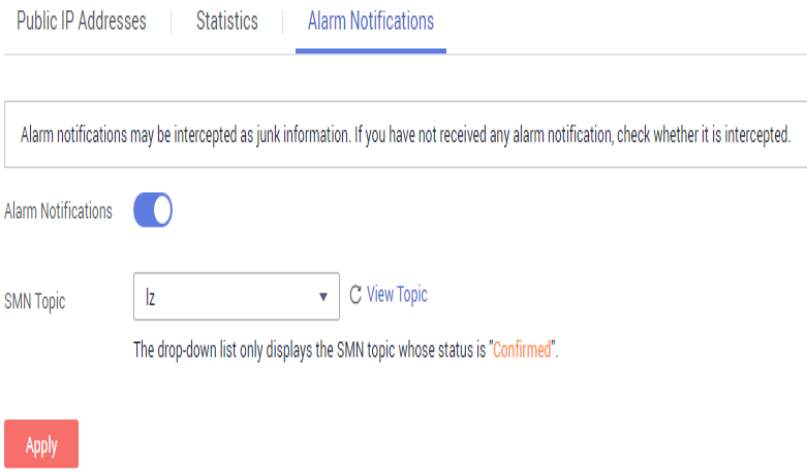


Table 1-1 Configuring alarm notifications

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 .	
SMN Topic	You can select an existing topic or click **View Topic** to create a topic. For details about topics, see the *Simple Message Notification User Guide*.	N/A

Step 5 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

2 Temporarily Disabling Anti-DDoS

You can set the traffic cleaning threshold to 1000 Mbit/s, a value so large that your public IP address gets almost no protection from DDoS attacks.

NOTE

This value is suitable for temporary disabling of protection for commissioning or other special purposes. You are advised not to use it for a long time.

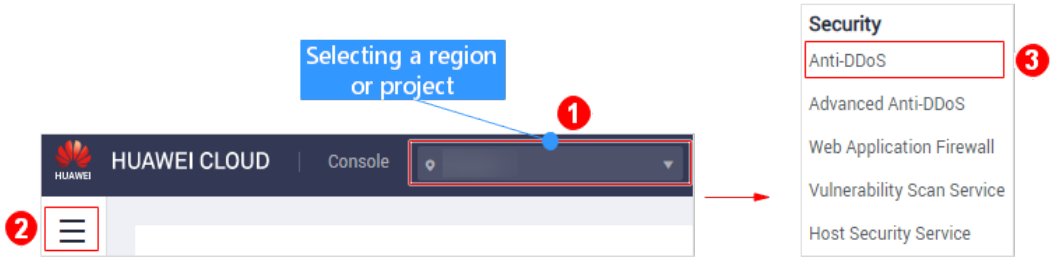
Procedure

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**. The **Security Console** is displayed.

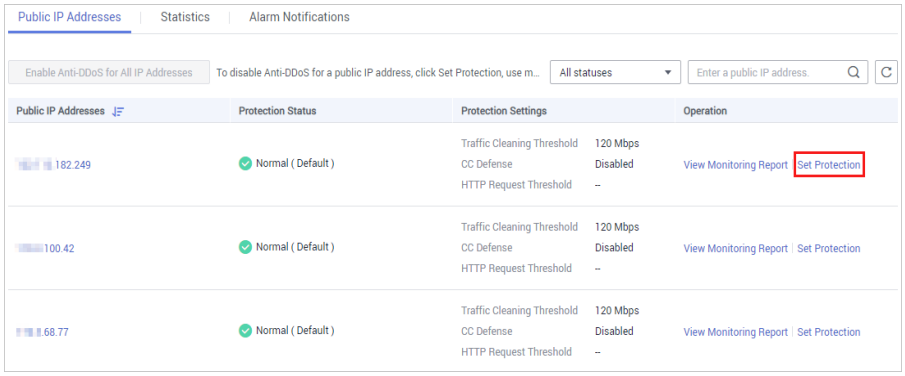
Figure 2-1 Anti-DDoS



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

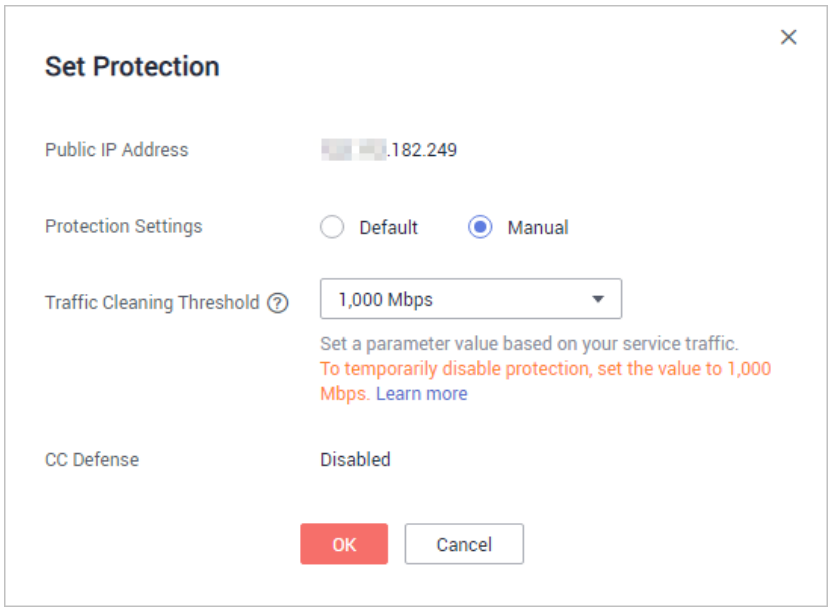
 Copyright © Huawei Technologies Co., Ltd.

Figure 2-2 Public IP address



Step 5 In the displayed dialog box, set **Protection Settings** to **Manual** and **Traffic Cleaning Threshold** to **1,000 Mbps**.

Figure 2-3 Set Protection



Step 6 Click **OK**.

----End

 Copyright © Huawei Technologies Co., Ltd.

3 Connecting to a Server Routed to a Black Hole

Scenarios

When your server is attacked by volumetric traffic, the carrier black hole will be triggered to block accesses from the Internet. However, services on HUAWEI CLOUD or cloud services in the same region as the server can still connect to the server.

Prerequisites

- You have obtained a username and password for logging in to the management console.
- You have purchased at least one public IP address.

Procedure

Step 1 Log in to the management console.

Step 2 Choose **Computing** > **Elastic Cloud Server**. The **Elastic Cloud Server** page is displayed.

NOTE

Ensure the ECS can be accessed and in the same region as the server.

Step 3 Use a remote desktop tool or run a command to connect to the server.

----End

After an ECS is successfully connected to the server in the black hole state, transfer files from the server to the ECS. You can also change the configuration file on the server using this method.

 Copyright © Huawei Technologies Co., Ltd.

4 Enhancing DDoS Mitigation Capabilities

Anti-DDoS provides a 5 Gbit/s mitigation capacity against DDoS attacks for free. Attack traffic that exceeds 5 Gbit/s will be routed to a black hole and legitimate traffic will be discarded.

To resume services quickly, you are advised to purchase HUAWEI CLOUD Advanced Anti-DDoS to expand protection capabilities.

 Copyright © Huawei Technologies Co., Ltd.

A Change History

Released On	Description
2020-04-01	This is the second official release. Updated some screenshots.
2019-06-21	This is the first official release.

 Copyright © Huawei Technologies Co., Ltd.