Anti-DDoS

Best Practices

Issue 01

Date 2024-05-11

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

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Configuring Alarm Notifications

Scenario

An alarm notification will be sent to the endpoint you have configured if a DDoS attack is detected after you enable the alarm notification.

Prerequisites

- You have enabled Simple Message Notification (SMN).
- You have purchased at least one public IP address.

Constraints

- Simple Message Notification (SMN) is a paid service. For details, see **Product Pricing Details**.
- Before enabling alarm notification, **create a topic** and **add a subscription to the topic** in SMN.

Procedure

Step 1 Log in to the management console.

Step 2 Select a region in the upper part of the page, click ≡ in the upper left corner of the page, and choose **Security & Compliance** > **Anti-DDoS Service**. The **Anti-DDoS** page is displayed.

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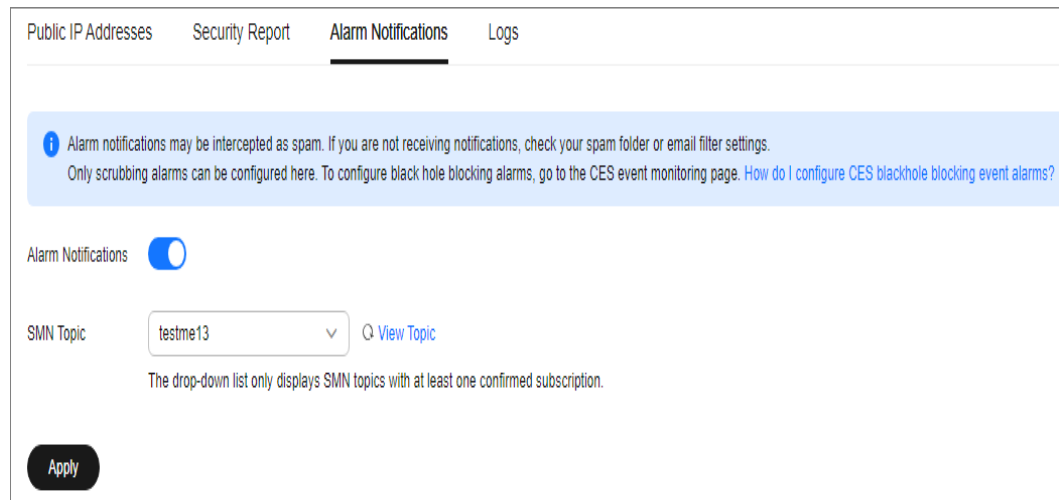
Figure 1-1 Configure alarm notifications

Table 1-1 Parameters required for configuring alarm notifications

Parameter	Description
Alarm Notifications	Indicates whether to enable the alarm notification. The options are as follows: ● : enabled ● : disabled
SMN Topic	You can select an existing topic or click **View Topic** to create a topic.

Click **View Topic** to switch to the SMN console where you can create a topic and configure the endpoint to receive the alarm notifications. To create a topic, perform the following steps:

1. Follow the instructions described in **Creating a Topic** to create a topic.

2. Follow the instructions described in **Adding a Subscription** to configure an endpoint, such as mobile number or email address, to receive the alarm notifications.

For more information about topics and subscriptions, see **Simple Message Notification**.

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

----End

2 Connecting to a Server Routed to a Black Hole

Scenario

When your server is under a traffic flooding attack, a black hole will be triggered to block all accesses from the Internet. You can connect to a server which a black hole has been triggered for through an ECS.

Prerequisites

- You have purchased at least one public IP address.
- The username and password for logging in to an ECS have been obtained.
- The username and password for logging in to a server which a black hole has been triggered for have been obtained.

Constraints

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

Procedure

Step 1 Log in to the management console.

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

Step 3 Click and choose **Computing** > **Elastic Cloud Server**.

Step 4 Log in to the ECS that can be accessed and in the same region as the server which a black hole has been triggered for.

Select a login method and log in to the ECS.

- For details about how to log in to a Windows ECS, see Windows ECS Login Overview.
- For details about how to log in to a Linux ECS, see **Linux ECS Login Overview**.

Step 5 **Table 2-1** describes how to connect to a server which a black hole has been triggered for.

Table 2-1 Server connection

ECS OS	Blackholed Server OS	Connection Method
Windows	Windows	Use MSTSC to log in to the server which a black hole has been triggered for. 1. Search for **mstsc** in the ECS and click it to open the **Remote Desktop Connection** dialog box. 2. Click **Show Options** in the displayed dialog box. 3. Enter the EIP and username (**Administrator** by default) of the server which a black hole has been triggered for. 4. Click **OK** and enter the login password as prompted to log in to the server.
	Linux	Use a remote login tool, such as PuTTY or Xshell, to log in to the server.
Linux	Windows	1. Install a remote connection tool, such as **rdesktop**. 2. Run the following command to log in to the server which a black hole has been triggered for. **rdesktop -u** *Username* **-p** *Password* **-g** *Resolution EIP bound to the server which a black hole has been triggered for*
	Linux	Run the following command to log in to the server which a black hole has been triggered for. **ssh** *EIP bound to the server which a black hole has been triggered for*

----End

Follow-up Operation

Once you have connected your ECS to a server in the black hole state, you can transfer files to the server and can make whatever configuration changes are necessary.