

**SecurityInfo**

# **Best Practices**

**Issue** 01  
**Date** 2025-06-11



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. 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 Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property 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 Cloud 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 Cloud Computing Technologies Co., Ltd.**

Address: Huawei Cloud Data Center Jiaoxinggong Road  
Qianzhong Avenue  
Gui'an New District  
Gui Zhou 550029  
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

---

# Contents

**1 Best Practices for Using Huawei Accounts..... 1**

**2 Best Practices in Enabling High-Risk Ports.....7**

**3 Disposal of Spam Mails Sent to External Systems..... 13**

3.1 What Is Spam Email and How It Is Harmful..... 13

3.2 How Huawei Cloud Handles Resources That Send Spam Email..... 14

**4 UDP-based Amplification Attack Check.....15**

4.1 Overview..... 15

4.2 Detecting UDP-based Amplification Attacks..... 16

4.3 Solution and Prevention Measures..... 17

# 1 Best Practices for Using Huawei Accounts

To safeguard your Huawei Cloud accounts and help you set up a secure channel to access Huawei Cloud resources, we recommend the following settings on IAM.

## Enabling Login Protection

After login protection is enabled, you and users created using your account will be authenticated by a virtual MFA device, SMS, or email during console login. This improves account security and prevents phishing attacks or accidental password leakage.

**Step 1** Enable login protection for the account. [Table 1-1](#) shows an example.

**Table 1-1** User roles

User Roles	Procedure
Huawei Cloud Account	<a href="#">Access the Security Settings page</a> . Select <b>Critical Operations &gt; Login Protection</b> , click <b>Enable</b> . In the displayed pane, select <b>Enable</b> .

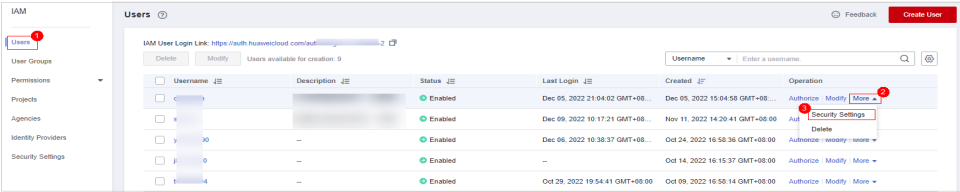
### NOTE

- Your Huawei Cloud account is created after you successfully register with Huawei Cloud. Your account has full access permissions for your cloud resources and makes payments for the use of these resources.
- Your HUAWEI ID is a unified identity that you can use to access all Huawei services.

**Step 2** Enable login protection for each IAM user under your Huawei Cloud account.

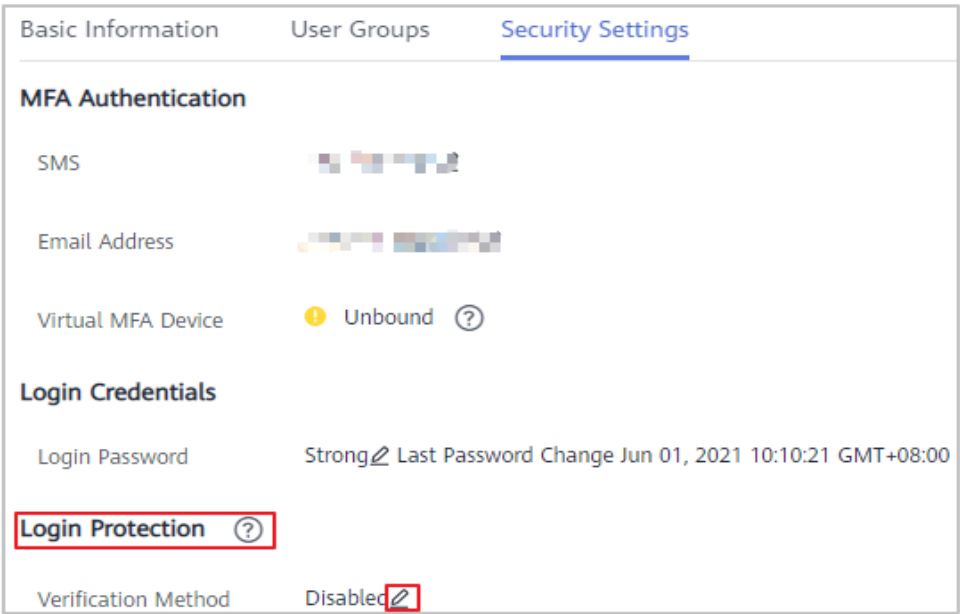
1. Choose **Identity and Access Management > Users** and click **Security Settings** in the row where an IAM user resides.

Figure 1-1 Users



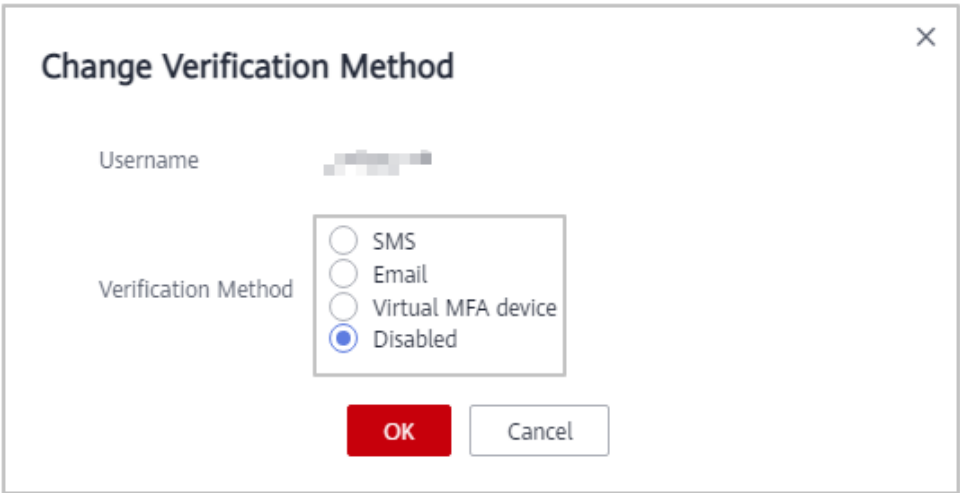
2. Click  in the **Login Protection** area.

Figure 1-2 Security Settings



3. In the displayed **Change Verification Method** dialog box, select **SMS**, **Email**, or **Virtual MFA device** for **Verification Method**, and click **OK**.

Figure 1-3 Change Verification Method



----End

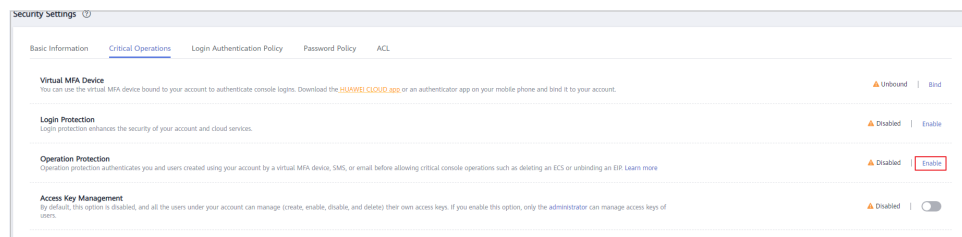
## Enabling Critical Operation Protection

After critical operation protection is enabled, if you or users created using your account perform a **critical operation**, such as deleting a resource and generating an access key, a password and a verification code are required for additional authentication. This prevents risks and loss caused by misoperations.

**Step 1** Access the **Security Settings** page as an administrator.

**Step 2** Select **Critical Operations**, locate the **Operation Protection** row, and click **Enable**.

Figure 1-4 Critical Operations



**Step 3** On the displayed pane, select **Enable** for **Operation Protection**. Then, select **Self-verification** or **Verification by another person**.

- **Self-verification:** You or IAM users themselves perform verification when performing a critical operation.
- **Verification by another person:** The specified person completes verification when you or IAM users perform a critical operation. Only SMS and email verification is supported.

**Figure 1-5** Operation Protection

**Operation Protection**

Operation protection provides an additional layer of security for cloud resources.  
You and users created using your account will be authenticated by a virtual MFA device, SMS, or email before being allowed to perform a critical operation.

Operation Protection ☒ **Enable**

You and users created using your account will need to perform identity verification by using the method you specify here.

☐ Self-verification  
☒ **Verification by another person**  
Specify a mobile number for identity verification.

+86 (Chinese... Enter a mobile number.

6-digit code Send Code

[Email Address Verification](#)

☐ **Disable**  
Identity verification will not be required for performing a critical operation.

Cancel OK

**Step 4** Click **OK**.

-----End

## Configuring a Login Authentication Policy

A login authentication policy includes many aspects of account security, including session timeout, account lockout, recent login information, and custom login

prompt. You can configure a login authentication policy to better safeguard your account, preventing password leakage caused by forgetting to log out or phishing attacks.

**Step 1** [Access the Security Settings page](#) as an administrator.

**Step 2** Select **Login Authentication Policy** and configure required parameters as shown in the following figure.

**Figure 1-6** Login Authentication Policy

The screenshot shows the 'Security Settings' page with the 'Login Authentication Policy' tab selected. The page includes sections for Session Timeout, Account Lockout, Account Disabling, Recent Login Information, and Custom Information. A 'Save' button is at the bottom.

**Security Settings** ⓘ

Basic Information   Critical Operations   **Login Authentication Policy**   Password Policy   ACL

**Session Timeout**

Log out if no operations are performed within  hours .

**Account Lockout** Takes effect for both you and IAM users created using your account

Lock the account for  minutes if  login attempts fail within  minutes.

**Account Disabling** Takes effect only for IAM users created using your account

☐ Disable account upon login if it is not used within the validity period

**Recent Login Information**

☒ Display last login information upon successful login

**Custom Information**

Display custom information upon login.

7/60

**Save**

**NOTE**

You can provide your custom information which will be displayed when you log in.

----End

## Configuring Password Policies

You can specify minimum password length, restrict consecutive identical character, and disallow previously used passwords to ensure that strong passwords of high complexity are used.



- Step 1** Access the **Security Settings** page as an administrator.
- Step 2** Select **Password Policy** and configure required parameters as shown in the following figure.

**Figure 1-7** Password Policy

The screenshot shows the 'Security Settings' page with the 'Password Policy' tab selected. The page is divided into three main sections: 'Password Composition & Reuse', 'Password Expiration', and 'Minimum Password Age'. Each section contains specific configuration options and input fields.

**Security Settings** ?

Basic Information   Critical Operations   Login Authentication Policy   **Password Policy**   ACL

**Password Composition & Reuse**

Must contain at least  of the following character types: uppercase letters, lowercase letters, digits and special characters.

Minimum Number of Characters

☐ Restrict consecutive identical characters

☒ Disallow previously used passwords

Number of Recent Passwords Disallowed

**Password Expiration**

☒ Prompt password change 15 days before expiration and force password change upon expiration

Password Validity Period (days)

**Minimum Password Age**

☐ Allow a password to be changed only after it is used for a specified time

**Save**

----End


# 2 Best Practices in Enabling High-Risk Ports


To safeguard your Huawei Cloud resources and help you set up a secure access channel to your Huawei Cloud resources, we recommend the following security policies for enabling high-risk ports.

## Configuring Security Groups and Network ACL to Control Inbound Access

You can configure inbound rules in security groups and network ACLs to protect the ECSs in the security group and the subnets associated with the network ACL.

- Step 1 Go to the **Security Groups** page.
1. Log in to the management console.

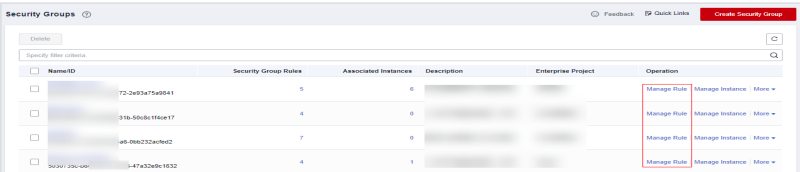
2. Click  in the upper left corner of the management console and select a region and a project.

3. In the navigation pane on the left, click  and choose **Network > Virtual Private Cloud**.

4. In the navigation pane on the left, choose **Access Control > Security Groups**.

- Step 2 Check each security group and delete high-risk port inbound rules.
1. On the **Security Groups** page, locate a security group and click **Manage Rule** in the **Operation** column.

Figure 2-1 Security Groups page



2. Click the **Inbound Rules** tab, check for the protocols and ports listed in **Protocol & Port** in [Table 2-1](#), and find the policy whose **Action** is **Allow** and **Source** is **0.0.0.0/0**.

Figure 2-2 Checking security group policies

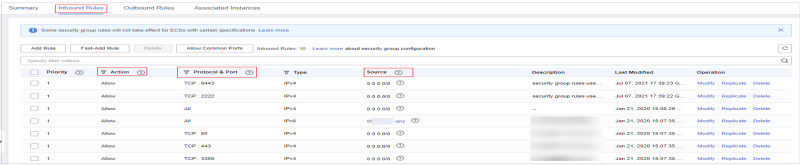


Table 2-1 High-risk ports

Protocol Port (1)	Service	Protocol Port (2)	Service
TCP: 20, 21	File Transfer Protocol (FTP)	TCP: 3306	MySQL (database)
TCP: 22	Secure Shell (SSH)	TCP: 3389	Windows Remote desktop protocol (RDP)
TCP: 23	Telnet (remote terminal protocol)	TCP: 3690	Subversion (SVN, an open-source version control system)
TCP: 25	Simple Mail Transfer Protocol (SMTP)	TCP: 4848	GlassFish (application server)
TCP/UDP: 53	Domain Name System (DNS)	TCP: 5000	Sybase/DB2 (database)
TCP: 69	Trivial File Transfer Protocol (TFTP)	TCP: 5432	PostgreSQL (database)
TCP: 110	Post Office Protocol 3 (POP3)	TCP: 5900-5902	Virtual Network Console (VNC)
TCP: 111, 2049	Network File System (NFS)	TCP: 5984	CouchDB (database)
TCP: 137, 139, 445	Server Message Block (SMB) protocol (NetBIOS)	TCP: 6379	Redis (database)
TCP: 143	Internet Message Access Protocol (IMAP)	TCP: 7001-7002	WebLogic (web app system)
TCP: 389, 636	Lightweight Directory Access Protocol (LDAP)	TCP: 7199, 7000, 7001, 9160, 9042	Apache Cassandra
TCP: 512-514	Linux rexec (remote login)	TCP: 7778	Kloxo (virtual host management system)

Protocol Port (1)	Service	Protocol Port (2)	Service
TCP: 873	Rsync (data image backup tool)	TCP: 8000	Ajenti (Linux server management panel)
TCP: 1194	OpenVPN (virtual private channel)	TCP: 8069, 10050-10051	Zabbix (system network monitoring)
TCP: 1352	Lotus	TCP: 8443	Plesk (virtual server management panel)
TCP: 1433	SQL Server (database management system)	TCP: 8080, 28015, 29015	RethinkDB
TCP: 1521	Oracle (database)	TCP: 8080-8089	Jenkins and JBoss (application server)
TCP: 1500	ISPmanager (server control panel)	TCP: 8088, 50010, 50020, 50030, 50070	Hadoop (distributed file system)
TCP: 1723	Point-to-Point Tunneling Protocol (PPTP)	TCP: 8848, 9848, 9849, 7848	Nacos service
TCP: 2082-2083	cPanel (VM control system)	TCP: 9080-9081, 9090	WebSphere (application server)
TCP: 2181	ZooKeeper (reliable coordination service for distributed systems)	TCP: 9200, 9300	Elasticsearch (Lucene search server)
TCP: 2601-2604	Zebra (route)	TCP: 11211	Memcached (cache system)
TCP: 3128	Squid (caching proxy)	TCP: 27017-27018	MongoDB (database)
TCP: 3311-3312	kangle (web server)	TCP: 50000	SAP Management Console

Protocol Port (1)	Service	Protocol Port (2)	Service
TCP: 8080	DisConf (distributed configuration management platform)	TCP: 60010, 60030	HBase
TCP: 8888	Spring Cloud Config (distributed configuration center)	TCP: 3000	Grafana (data visualization)
TCP: 8761	Eureka (service registration and discovery component)	TCP: 8983	Solr (open-source enterprise-search platform)
TCP: 8500, 8502	Consul (service registration and discovery component)	TCP: 3123-3124, 8081, 6123	Flink (big data processing platform)
TCP: 8070, 8080	Apollo (distributed configuration management platform)	TCP: 4040, 7077, 8080-8081	Spark (big data processing platform)
TCP: 8090	Diamond (distributed configuration management system)	TCP: 8080, 11800, 12800	SkyWalking (distributed system monitoring)
TCP: 2379-2380	Etcd (distributed key-value storage system)	TCP: 8080	WebTTY (Web TTY management page)
TCP: 15672	RabbitMQ (message queue)	TCP: 80, 443	NextCloud (private network hard disk)
TCP: 8161, 61616	ActiveMQ (message queue)	TCP: 9001, 9090	Minio (cloud storage management tool)
TCP: 8083, 8086, 8635	InfluxDB (time series database)	TCP: 18083	EMQX (IoT access platform)
TCP: 6030-6032, 6041	TDengine (time series database)	TCP: 1090, 1099	Java-RMI protocol (Java remote method invocation protocol)
TCP: 9092-9095, 9999	Kafka (distributed stream processing platform)	TCP: 8000	JDWP (Java remote debugging interface)
TCP: 2375	Docker (application container engine)	TCP: 8009	Tomcat AJP protocol (binary communication protocol)

Protocol Port (1)	Service	Protocol Port (2)	Service
TCP: 5601	Kibana (data visualization)	TCP: 8888	Jupyter Notebook (web applications for interactive computing)
TCP: 177	xmanager/xwin (Linux remote GUI)	TCP: 6443, 8443, 10250-10256	Kubernetes (container orchestration engine)
TCP: 8081	Nexus (repository manager)	TCP: 80/443, 8080	GitLab (code hosting platform)
UDP: 161, 162	Simple Network Management Protocol (SNMP)	TCP: 5555	ADB (Android debugging tool)
TCP: 1883, 8883	MQTT (IoT message protocol)	TCP: 6000-6063	X11 (Linux remote GUI)
TCP: 8888	Napster (P2P file sharing protocol)	-	-

3. Check for and eliminate high-risk port policies. You can click **Modify** or **Delete** in the **Operation** column.

**Figure 2-3** High-risk port policies for security groups

Priority	Action	Protocol & Port	Type	Source	Description	Last Modified	Operation
1	Allow	TCP: 8443	IPv4	0.0.0.0	security group rules use...	Jul 07, 2021 17:39:23 G...	<a href="#">Modify</a> <a href="#">Replicate</a> <a href="#">Delete</a>
1	Allow	TCP: 2222	IPv4	0.0.0.0	security group rules use...	Jul 07, 2021 17:39:22 G...	<a href="#">Modify</a> <a href="#">Replicate</a> <a href="#">Delete</a>
1	Allow	All	IPv4	0.0.0.0	-	Jan 21, 2020 15:08:29 ...	<a href="#">Modify</a> <a href="#">Replicate</a> <a href="#">Delete</a>

#### NOTE

- You are advised to delete the **Allow** policies for ports that do not need to be open to the external network.
- To allow external access from certain IP addresses, you are advised to set **Source** to the IP addresses in the whitelist. For details, see [Enabling Specified IP Addresses to Remotely Access ECSs in a Security Group](#).
- You are not advised to enable high-risk port policies for all IP addresses.

**Step 3** In the navigation pane on the left, choose **Access Control > Network ACLs**.

**Step 4** Check all the network ACLs that are enabled and associated with subnets. Delete high-risk port policies from the inbound rules.

1. In the network ACL list, locate a rule and click **Manage Rule** in the **Operation** column.

Figure 2-4 Network ACL page

NameID	Status	Network A...	Associated...	Description	Operation
9b0c0000-0000-0000-0000-000000000000	Enabled	5	1	test	Associate Subnet Manage Rule More

- Click the **Inbound Rules** tab, check for the protocols and ports listed in **Protocol & Port** in [Table 2-1](#), and find the policy whose **Action** is **Allow** and **Source** is **0.0.0.0/0**.

Figure 2-5 Checking network ACL policies

Priority	Action	Protocol & Port	Type	Source	Description	Last Modified	Operation
1	Allow	TCP: 8443	IPv4	0.0.0.0/0	security group rules use...	Jul 07, 2021 17:39:23 (3)	Modify Enable Delete
1	Allow	TCP: 2222	IPv4	0.0.0.0/0	security group rules use...	Jul 07, 2021 17:39:23 (3)	Modify Enable Delete
1	Allow	All	IPv4	0.0.0.0/0	security group rules use...	Jan 21, 2020 16:55:26	Modify Enable Delete
1	Allow	All	IPv4	0.0.0.0/0	security group rules use...	Jan 21, 2020 16:57:35	Modify Enable Delete
1	Allow	TCP: 80	IPv4	0.0.0.0/0	security group rules use...	Jan 21, 2020 16:57:35	Modify Enable Delete
1	Allow	TCP: 443	IPv4	0.0.0.0/0	security group rules use...	Jan 21, 2020 16:57:35	Modify Enable Delete
1	Allow	TCP: 5555	IPv4	0.0.0.0/0	security group rules use...	Jan 21, 2020 16:57:35	Modify Enable Delete

- Check for and eliminate high-risk port policies. You can click **Modify** or **Delete** in the **Operation** column.

#### NOTE

- You are advised to delete the **Allow** policies for ports that do not need to be open to the external network.
- To allow external access from certain IP addresses, you are advised to set **Source** to the IP addresses in the whitelist.
- You are not advised to open high-risk ports to all IP addresses.

----End

## Using VPN/IPsec to Control Internal Access to Ports

By default, ECSs in a VPC cannot communicate with your physical data center or private network. To connect ECSs in a VPC to your data center or private network, you are advised to use Huawei Cloud **Virtual Private Network (VPN)**.

## Using Huawei Cloud Native Services to Enhance Security

Our cloud native services provide a range of features to enhance security.

### Databases

**Relational Database Service (RDS)** provides a comprehensive performance monitoring system, implements **a range of security measures**, and offers a professional database management platform, allowing you to easily configure and scale databases on the cloud. On the RDS console, you can perform almost all necessary tasks and no programming is required. The console simplifies operations and reduces routine O&M workloads, so you can stay focused on application and service development.

Application middleware

**Distributed Cache Service (DCS)** provides **multiple features** to improve the reliability and security of tenant data, such as VPC, security group, whitelist, SSL encrypted connection for public network access, automatic backup, data snapshot, and cross-AZ deployment.

# 3 Disposal of Spam Mails Sent to External Systems

---

## 3.1 What Is Spam Email and How It Is Harmful

### What Is Spam Email?

Spam email is unsolicited and unwanted junk email that is sent out in bulk to an indiscriminate recipient without the permission of the recipient. Usually, spam email always:

- Has no title, no sender, or source address.
- Has false information in the subject or content.
- Includes fraud information.
- Contains immoderate or illegal content.
- Hides harmful information such as viruses in the content.

### How Is Spam Email Harmful?

Email is one of the important communication tools in today's society. Spam email will:

- Reduce communication quality: Spam email occupies a large amount of network bandwidth, affects the network transmission speed, and may cause mail server congestion.
- Damage the interests of the recipient: Spam usually contains hidden phishing links that may cause data leakage of recipients. Recipients may be then tricked into leaking credentials or business secrets. Spam email is repeated and spread quickly, it takes a lot of time and money for the recipient to stop it.
- Spread harmful information: Spam email is always used to spread harmful information such as rumors.



## 3.2 How Huawei Cloud Handles Resources That Send Spam Email

### Overview

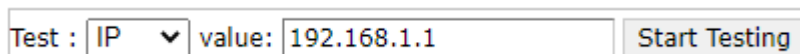
Using resources on Huawei Cloud to send spam email violates [Huawei Cloud User Agreement](#) and other related laws and regulations. IP addresses that are used to send out spam email in bulk will be recorded in the blocklist by the international anti-spam organization. IP addresses in the blocklist cannot be used for accessing websites, receiving emails, or sending emails. Once the IP address you obtained from Huawei Cloud is in the blocklist, the image of Huawei Cloud is severely damaged. If Huawei Cloud receives an external complaint that spam email is sent by resources of a Huawei Cloud user, Huawei Cloud will send a warning email to the user and take risk control measures (including but not limited to blocking ports and freezing IP addresses involved).

### Rectification Suggestion

Huawei Cloud will implement risk control measures based on the complaint types.

You can open the [anti-spam organization](#) address, enter your IP address, and click **Start Testing** to check whether the IP address is listed by the organization as a spammer. Then handle the complaint accordingly.

**Figure 3-1** Anti-spam organization



Test :  value:

- If no IP address records are displayed on the page and the initial page is displayed, the IP address has not been blocked by the anti-spam organization.  
Stop using the server with this IP address to send spam email as soon as possible and protect the mail address from malicious use. If the rectification is not completed within the time specified in the warning email, your resources may be blocked (including but not limited to blocking ports and freezing IP addresses).
- If your IP address is displayed on the page, the IP address has been blocked by the anti-spam organization.  
The anti-spam organization has added your IP address to their blocklist. This means this IP address cannot be used to access websites or send emails anymore. Stop using this IP address to send spam email as soon as possible and protect your mail address.  
Since the IP address blocklisted by the anti-spam organization is managed by Huawei Cloud, the image of Huawei Cloud is severely damaged. Huawei Cloud will permanently freeze the IP address. The IP address cannot be unfroze in any cases. Bind a new IP address to the server.

# 4 UDP-based Amplification Attack Check

## 4.1 Overview

### What Are DDoS Attacks

DoS (Denial of Service) 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.

### What Are UDP-based Amplification Attacks

UDP-based amplification attacks are a form of DDoS attacks that are highly destructive, easy to trigger, and difficult to trace.

**Figure 4-1** shows how such an attack works. An UDP-based amplification attack does not directly work on the target server. Instead, the attacker sends special UDP-based request packets to some open internet servers via IP addresses forged as that of the target server. These request packets will bring out high volumes of data to overwhelm the target server.

**Figure 4-1** How a UDP-based amplification attack works



## 4.2 Detecting UDP-based Amplification Attacks

This section describes how to detect UDP amplification attacks on your server.

1. Log in to the server as user **root**.

### NOTE

In this example, the server sends ten 800-byte UDP packets per second when it is running properly.

2. Run the following command to check the current network connections and processes:

### **netstat -anpt**

You are advised to run the **netstat -anpt** command to check whether the current network connections and processes are normal. If the current connections and processes have been stopped or hidden, you can use the **tcpdump** packet capture tool to capture packets for analysis.

3. Run the following command to capture packets and analyze UDP traffic attacks:

### **tcpdump -nn udp**

**Figure 4-2** shows an example of the captured packets.

**Figure 4-2** UDP attack packets

```
[root@ecs-9be0 tmp] $ tcpdump -nn udp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:36:51.396455 IP .32872 > .19867: UDP, length 1460
16:36:51.396473 IP .32872 > .19867: UDP, length 1460
16:36:51.396475 IP .32872 > .19867: UDP, length 1460
16:36:51.396478 IP .32872 > .19867: UDP, length 1460
16:36:51.396480 IP .32872 > .19867: UDP, length 1460
16:36:51.396483 IP .32872 > .19867: UDP, length 1460
16:36:51.396485 IP .32872 > .19867: UDP, length 1460
16:36:51.396487 IP .32872 > .19867: UDP, length 1460
16:36:51.396490 IP .32872 > .19867: UDP, length 1460
16:36:51.396492 IP .32872 > .19867: UDP, length 1460
16:36:51.396495 IP .32872 > .19867: UDP, length 1460
16:36:51.396497 IP .32872 > .19867: UDP, length 1460
16:36:51.396500 IP .32872 > .19867: UDP, length 1460
16:36:51.396502 IP .32872 > .19867: UDP, length 1460
16:36:51.396505 IP .32872 > .19867: UDP, length 1460
16:36:51.396507 IP .32872 > .19867: UDP, length 1460
16:36:51.396509 IP .32872 > .19867: UDP, length 1460
16:36:51.396512 IP .32872 > .19867: UDP, length 1460
16:36:51.396514 IP .32872 > .19867: UDP, length 1460
16:36:51.396517 IP .32872 > .19867: UDP, length 1460
16:36:51.396519 IP .32872 > .19867: UDP, length 1460
16:36:51.396521 IP .32872 > .19867: UDP, length 1460
16:36:51.396524 IP .32872 > .19867: UDP, length 1460
16:36:51.396526 IP .32872 > .19867: UDP, length 1460
```

- a. Run the following command to temporarily save the captured packet information to the **udp.pcap** file in the **/home** folder:
- b. Run the following command to analyze the captured packet information.

**tcpdump -nn -r /home/udp.pcap|awk -F'.' '{print \$1}'|sort|uniq -c**

**Figure 4-3** Captured packet analysis result

```
[root@ecs-9be0 home] $ tcpdump -nn -r /home/udp.pcap|awk -F"." '{print $1}'|sort|uniq -c
reading from file /home/udp.pcap, link-type EN10MB (Ethernet)
 1701 16:40:45
 55566 16:40:46
 56007 16:40:47
 55692 16:40:48
 56272 16:40:49
 55062 16:40:50
 56007 16:40:51
 55188 16:40:52
 55944 16:40:53
 56952 16:40:54
 55818 16:40:55
 56196 16:40:56
 55188 16:40:57
 55314 16:40:58
 55629 16:40:59
```

According to step 3, the checked device is sending dozens of 1460-byte UDP data packets to another IP address, which is far greater than the normal traffic. This indicates that the device is likely being used as an amplifier for UDP reflection attacks.

According to step b, the number of UDP connections per second is more than 50,000, indicating that the services provided by the device are used by attackers to launch UDP amplification attacks. So, necessary protection measures must be taken to prevent server resources from being exhausted by attack traffic.

## 4.3 Solution and Prevention Measures

You can take measures to defend against UDP amplification attacks based on service requirements. The following provides some recommended protection measures for your reference.

- Pay attention to the latest security advisories and bulletins released by security vendors, and implement targeted protection policies against such attacks in a timely manner.
- Use firewalls to control access to the UDP ports of ECSs.
- Configure security groups to control access to UDP ports. For details, see [Configuring Security Group Rules](#).
- Configure local IP addresses, disable external access, disable the UDP protocol, and enable login authentication.
- Adjust some parameters and restart the server to disable UDP.
- Create a profile of normal packet sizes based historical data, so you can easily detect overly small or overly large packets that may be part of the attack traffic.