Anti-DDoS Service

Service Overview

Issue 01

Date 2024-03-21

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Understanding DDoS Attacks

1.1 What Is a DDoS Attack?

DoS attacks are also called flood attacks. They intend 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** describes the 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 to be unable to respond to legitimate access requests.	NTP flood attack
Transport layer DDoS attack	Occupies the connection resources of the server, resulting in denial of services.	SYN flood, ACK flood, and ICMP flood attacks.
Session layer attack	Occupies SSL session resources of the server, resulting in denial of services.	SSL slow connection attack

Attack Type	Description	Example
Application layer attack	Occupies the application processing resources of the server and consumes its processing performance, resulting in denial of services.	HTTP GET flood attack and HTTP POST flood attack

1.2 How Can I Report to the Network Monitoring Department When a DDoS Attack Occurs?

When your services are under large volumetric DDoS attacks, you can use Advanced Anti-DDoS (AAD) to keep services stable. In addition, it is recommended that you report to the network monitoring department immediately.

Reporting Process

1. You need to report to the local network monitoring department as soon as DDoS attacks occur and provide related information as required.
2. The network monitoring department determines whether your case can be filed and performs relevant network monitoring process.

   NOTE

   For details about the standards of filing a case, contact the local network monitoring department.

3. After your case is officially filed, Huawei Cloud will cooperate with the network monitoring department to provide attack evidence.

What Evidence Can Huawei Cloud Provide?

After your case is filed in the network monitoring department, Huawei Cloud will provide the following assistance:

- Huawei Cloud will provide responsible personnel in the network monitoring department with traffic logs and attack information about your services on Huawei Cloud.

  NOTE

  Because the data will be used as legal evidence, it cannot be provided to you directly. You can view information about the attack traffic on the HUAWEI CLOUD management console.

- HUAWEI CLOUD cannot analyze traffic logs and attack information, or identify the attacker.

  NOTE

  Because HUAWEI CLOUD is not a judge, it is impossible to judge who is guilty. Nor does it have law enforcement rights, who cannot conduct a case investigation. HUAWEI CLOUD can only serve as an evidence provider and witness.

- HUAWEI CLOUD will respond to the network monitoring department in a timely manner and assist their work.

  In case of security attacks, you are advised to actively request the network police to file your case and conduct investigation by referring to the standards for case filing of the local network monitoring department.

View information about attack traffic:

You can view traffic statistics and attack events on the HUAWEI CLOUD management console.

2 Understanding Anti-DDoS Service

2.1 Cloud Native Anti-DDoS Basic

2.1.1 What Is Cloud Native Anti-DDoS Basic

What Is Cloud Native Anti-DDoS Basic

Cloud Native Anti-DDoS Basic (CNAD Basic) defends public IP addresses (ECSs and ELBs) on Huawei Cloud against Distributed Denial of Service (DDoS) attacks, such as flood attacks and resource consumption attacks, at the network- and application-layer. It also provides real-time alarms for attack interception, effectively improving your bandwidth utilization and ensuring service stability and reliability.

Features

CNAD Basic 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 services. It also generates monitoring reports that provide visibility into the network traffic security.

CNAD Basic helps users mitigate the following attacks:

- Web server attacks

  Including SYN flood.

- Game attacks

  Including User Datagram Protocol (UDP) flood, SYN flood, Transmission Control Protocol (TCP), and fragment attacks

CNAD Basic also:

- 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.

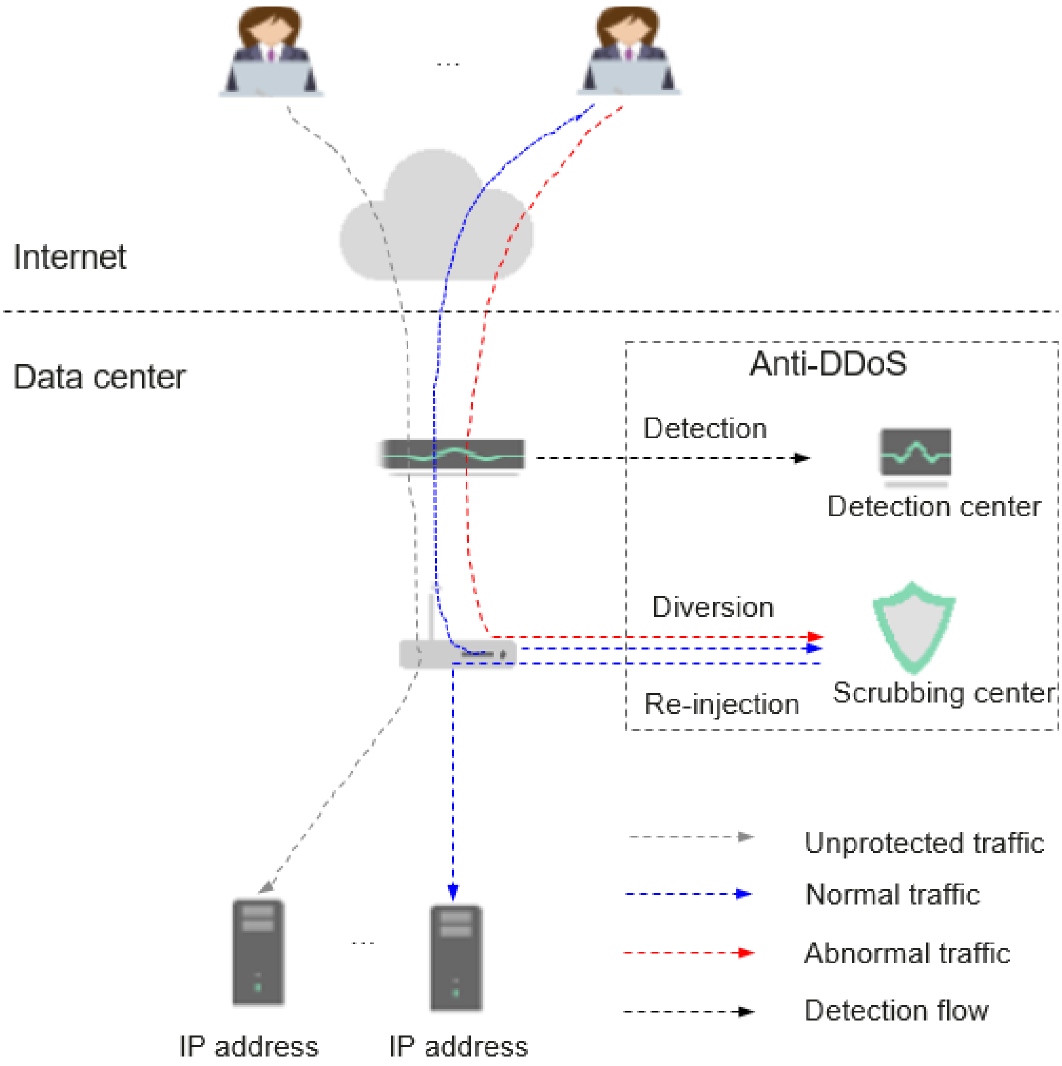
- Provides attack reports on all protected public IP addresses, covering the traffic cleaning frequency, cleaned traffic amount, the top 10 attacked public IP addresses, and the number of blocked attacks.

2.1.2 Application Scenarios

CNAD Basic protects public IP addresses on Huawei Cloud only from DDoS attacks.

CNAD Basic devices are deployed at egresses of data centers. **Figure 2-1** shows the network topology.

Figure 2-1 Network topology



The detection center monitors network access traffic based on security policies you configure. If an attack is detected, data is diverted to scrubbing devices for real-time defense. Abnormal traffic is cleaned, and normal traffic is forwarded.

Anti-DDoS provides 500 Mbit/s of mitigation capability against DDoS attacks for free. If access traffic to a public IP address exceeds the specified black hole threshold (500 Mbit/s for free Anti-DDoS), CNAD Basic redirects all traffic destined for the IP address to a black hole. This means legitimate traffic will be discarded. To get more DDoS mitigation capabilities, Huawei Cloud Advanced Anti-DDoS (AAD) is recommended.

2.1.3 Advantages

CNAD Basic mitigates DDoS attacks against workloads on Huawei Cloud. With CNAD Basic, you can enjoy:

- Premium protection

  Detects DDoS attacks in real time, discards attack traffic, and forwards legitimate traffic to destination IP addresses.

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

- Complete and accurate protection

  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 scrubbing devices, CNAD Basic checks each packet and responds to any attack immediately without causing service delays.

- Enabled automatically

  This service is automatically enabled when you purchase an EIP. No expensive scrubbing device or time-consuming installation is required.

- Free of charge

  This service is free. You can use the service without purchasing any additional resources.

2.2 Cloud Native Anti-DDoS Advanced

2.2.1 What Is CNAD?

What Is CNAD?

Cloud Native Anti-DDoS Advanced (CNAD) provides higher DDoS protection capability for cloud services on Huawei Cloud such as Elastic Cloud Server (ECS), Elastic Load Balance (ELB), Web Application Firewall (WAF), and Elastic IP (EIP). CNAD defends against the DDoS attacks targeting the IP addresses on Huawei Cloud and it provides higher protection capabilities for cloud services. With few clicks on the console, you can enjoy always-on DDoS mitigation on Huawei Cloud.

Features

CNAD has the following features:

- Transparent access

  You can directly protect public IP addresses on Huawei Cloud without modifying domain name resolution or configuring origin server protection.

- Unlimited protection

  Huawei Cloud provides high DDoS mitigation capability based on the network and resource capabilities in the current region. The protection capability provided grows with the improvement of Huawei Cloud's network capabilities.

- Joint protection

  Enabling the joint protection will automatically engage AAD for DDoS mitigation.

- IPv4/IPv6 protection

  CNAD can protect IP addresses using IPv4 and IPv6 protocols.

- Traffic scrubbing

  CNAD scrubs traffic when detecting that the incoming traffic of an IP address exceeds a certain threshold.

- IP address blacklist or whitelist

  You can configure an IP address blacklist or whitelist to block or allow access from specified IP addresses.

- Protocol-based access block

  Traffic accessing CNAD is blocked in one click based on the protocol type. For example, if there is no User Datagram Protocol (UDP) traffic, you are advised to disable UDP for CNAD.

Specifications

CNAD supports the CNAD Unlimited Protection Basic, and CNAD Unlimited Protection Advanced. **Table 2-1** lists the service specifications supported by each instance of each edition.

NOTICE

CNAD protection is only available for cloud resources in the same region.

Table 2-1 Parameter description

Parameter	Description
Billing Mode	Yearly/Monthly
Protection Level	Unlimited protection advanced edition and basic edition.
Resource Location	Region where the protection resource is located
IP Version	● The advanced edition supports only IPv4. ● The basic edition supports IPv4+IPv6.
Protected IP Addresses	The value ranges from 50 to 500.

Parameter	Description
Service Bandwidth	Clean service bandwidth forwarded to the origin server from the AAD scrubbing center. It is recommended that the service bandwidth be greater than or equal to the egress bandwidth of the origin server. Otherwise, packet loss may occur or services may be affected. The configuration range is as follows: ● Unlimited Protection Basic Edition: 100 Mbit/s to 20,000 Mbit/s ● Unlimited Protection Advanced Edition: The configuration scope varies depending on the region.
Instance Name	The name must be 32 or fewer characters in length. The name can contain only letters, digits, underscores (_), and hyphens (-).
Required Duration	The unit of the validity period is month or year. **NOTICE** ● Your subscription will be renewed each month for monthly billing. ● Your subscription will be renewed each year for yearly billing.
Enterprise Project	This option is only available when you are logged in using an enterprise account, or when you have enabled enterprise projects.
Quantity	Number of CNAD instances to be purchased.

2.2.2 Application Scenarios

CNAD Advanced is used to protect your Huawei Cloud services (with public IP addresses assigned to) from DDoS attacks, meeting your requirements for immense protection capability and high network quality.

CNAD Advanced can be used for the following scenarios:

- Services that are deployed on Huawei Cloud and have public IP addresses assigned for external communication
- Services with high bandwidth requirements and high Queries per Second (QPS), such as online video and live streaming
- IPv6 protection
- A large number of public IP addresses on Huawei Cloud.

  A large number of ports, domain names, and IP addresses need to be protected from DDoS attacks.

2.2.3 Advantages

CNAD is a software-based advanced DDoS mitigation service. With few clicks on the console, you can enjoy always-on and stronger DDoS mitigation for your Huawei Cloud services, such as ECSs, ELBs, WAF, and EIPs.

- Quick access

  You do not need to configure forwarding rules. By connecting your services to CNAD, you can quickly improve the protection capability for you EIPs on Huawei Cloud.

  NOTE

  The Unlimited Protection Advanced Edition can protect only exclusive EIPs.

- Elastic protection

  To defend against surging attacks, Huawei Cloud provides as high DDoS mitigation capability as possible to keep your services stable and secure.

- Immense bandwidth capacity

  Multi-line BGP protection bandwidth helps defend against DDoS attacks with ease, meeting the security requirements of online promotions and rollouts.

- Excellent scrubbing capability

  Automated attack detection and adaptive defense policies support real-time protection. Service traffic is distributed in clusters, which features high performance, low latency, and high stability.

- Various protection reports

  Multi-dimensional reports and detailed traffic statistics help you quickly learn of the current network security status.

3 Permissions Management

3.1 Anti-DDoS Permissions

If you need to assign different permissions to employees in your enterprise to access your Anti-DDoS resources, IAM is an ideal choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you efficiently manage access to your Anti-DDoS resources.

With IAM, you can use your Huawei Cloud account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, some software developers in your enterprise need to use Anti-DDoS resources but must not delete them or perform any high-risk operations. To achieve this purpose, you can create IAM users for the software developers and grant them only the permissions required for using Anti-DDoS resources.

If your Huawei Cloud account does not need individual IAM users for permissions management, skip this topic.

Anti-DDoS Permissions

By default, new IAM users do not have any permissions. You need to add a user to one or more groups, and attach permission policies or roles to these groups. Users inherit permissions from their groups and can perform specified operations on cloud services based on the permissions.

To assign Anti-DDoS permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing Anti-DDoS, the users need to switch to a region where they have been authorized.

Table 3-1 lists all the system policies supported by Anti-DDoS. Huawei Cloud services interwork with each other, and roles of Anti-DDoS are dependent on roles of other services to take effect. When assigning Anti-DDoS permissions to users, you also need to assign dependent roles for the Anti-DDoS permissions to take effect.

Table 3-1 Anti-DDoS system policies

Policy Name	Description	Dependency
Anti-DDoS Administrator	Administrator permissions for Anti-DDoS.	It depends on the **Tenant Guest** role. **Tenant Guest**: a global role, which must be assigned in the Global project

3.2 CNAD Permissions

If you need to assign different permissions to employees in your enterprise to access your CNAD Pro resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you efficiently manage access to your CNAD Pro resources.

With IAM, you can use your Huawei Cloud account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, some software developers in your enterprise need to use CNAD Pro but must not delete CNAD Pro resources or perform any high-risk operations. To achieve this purpose, you can create IAM users for the software developers and grant them only the permissions required for using CNAD Pro resources.

If your Huawei Cloud account does not need individual IAM users for permissions management, skip this section.

CNAD Pro Permissions

By default, new IAM users do not have any permissions. You need to add a user to one or more groups, and attach permission policies or roles to these groups. Users inherit permissions from their groups and can perform specified operations on cloud services based on the permissions.

CNAD is a global service and can be deployed in any region. CNAD permissions are assigned to IAM users in the global project, so IAM users can access CNAD in any region without having to switch over among regions.

You can grant users permissions by using roles and policies.

- Roles: Role-based permission management is a coarse-grained authorization mechanism that defines permissions based on users' job responsibilities. This mechanism provides a limited number of service-level roles for authorization. If one role has a dependency role required for accessing CNAD Pro, assign both roles to the users. Roles are not an ideal choice for fine-grained authorization and secure access control.
- Policies: Policy-based permission management is a type of fine-grained authorization mechanism that grants permissions to perform operations on specific cloud resources. This mechanism allows for more flexible policy-based authorization and meets secure access control requirements. For example, you

can grant CNAD Pro users the permissions to manage only a certain type of resources.

Table 3-2 lists all the system roles supported by CNAD Pro.

Table 3-2 System-defined roles of CNAD Pro

Role/Policy Name	Description	Type	Dependency
CNAD FullAccess	Full permissions for CNAD	Policy	Either the CNAD FullAccess and BSS Administrator roles or the Tenant Administrator role is required for purchasing a CNAD instance.
CNAD ReadOnlyAccess	Read-only permissions for CNAD	Policy	None.

CNAD FullAccess Policy Content

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "cnad:*:*"
                        ]
                }
        ]
}
```

CNAD ReadOnlyAccess Policy Content

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "cnad:*:get*",
                                "cnad:*:list*"
                        ]
                }
        ]
}
```