Anti-DDoS Service

Service Overview

Issue	03
Date	2024-06-25

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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 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.

1.3 Black Hole Policy

To protect the usability of Huawei Cloud services in general, if the attack traffic on the cloud server exceeds the threshold, a black hole will be triggered to block all accesses from the Internet for a certain period of time.

What Is a Black Hole?

A black hole refers to a situation where access to a cloud server is blocked by Huawei Cloud because attack traffic targeting a cloud server exceeds a certain threshold.

Why Is the Blackhole Policy Required?

DDoS attacks will interrupt user services and cause adverse impacts on the AAD data center. Defense against DDoS attacks is costly on bandwidth consumption.

Bandwidth is purchased by HUAWEI CLOUD from carriers, and those carriers bill for bandwidth even if it was part of DDoS attack. Huawei Cloud provides Cloud Native Anti-DDoS Basic (Anti-DDoS) for free to protect your resources against DDoS attacks below a certain threshold, but if an attack exceeds a certain size, we will route the traffic to a black hole.

How Do I Deactivate a Black Hole?

When a server (ECS) enters is put in the black hole, you handle it by referring to **Table 1-2**.

Table 1-2 Black hole deactivation methods

Anti-DDoS Edition	Deactivation Policy	Deactivation Method
Cloud Native Anti-DDoS Basic (Anti-DDoS) **NOTE** Anti-DDoS is enabled by default.	• The system automatically deactivates the black hole 24 hours after the access to a cloud server is blocked. • If the system detects that the attack has not stopped, and attack traffic is still exceeding the configured threshold, the access will be blocked again.	You need to wait until the system deactivates it automatically.
Cloud Native Anti-DDoS Pro	The system automatically deactivates the black hole 24 hours after the access to a cloud server is blocked.	You need to wait until the system deactivates it automatically.
Advanced Anti-DDoS	Contact Huawei Cloud technical support to unblock in advance. You are advised to increase the elastic bandwidth to avoid being black-holed again.	You can upgrade the elastic protection bandwidth to deactivate the blackhole.

Black Hole Threshold

The black hole threshold refers to the basic attack mitigation capability provided by Huawei Cloud. When the scale of attack exceeds the threshold, Huawei Cloud executes a black hole policy to block the attacked IP address.

Scrubbing Principles

The system detects attack traffic in real time. Once detecting an attack on a cloud host, the system diverts the service traffic from the original network path to the Huawei Cloud DDoS scrubbing system. The Huawei Cloud DDoS scrubbing system identifies the traffic of the attacking IP address, discards attack traffic, and

forwards normal traffic to the target IP address to mitigate the damage to the server.

Self-Service Unblocking Rules

NOTE

If you have purchased Anti-DDoS Service (**CNAD Advanced**), you will be rewarded with three self-service blackhole-deactivation quotas for free every month. If the quotas are not used up in the current month, they will be cleared at the end of the month.

- There is a minimum block duration after which you can unblock a blocked IP address. The minimum block duration for the first time you unblock an IP address in a day is 30 minutes. Minimum block duration = $2^{(n-1)}$ x 30 minutes (*n* indicates the number of times you want to unblock the same IP address)

  For example, a 30-minute block duration is required for the first time you unblock an IP address, a 60-minute block duration for the second time, and a 120-minute block duration for the third time.
- For the same protected IP address, if it is blocked again less than 30 minutes after it is unblocked, you can unblock it 2^n x 30 minutes later (*n* indicates the number of times you are unblocking it).

  For example, if the IP address has been unblocked once at 10:20, and is blocked again at 10:40, the interval between the two time points is less than 30 minutes. This is the second time you unblock the IP address on the day. The IP address cannot be unblocked until the 120-minute block duration expires at 12: 40 (2x2x30 minutes after 10:40).

  NOTICE

  If you have unblocked any other IP address within 30 minutes, you cannot unblock the IP address even if the preceding conditions are met.

- Anti-DDoS Service automatically adjusts the allowed IP unblocking attempts and the interval based on the risk control.

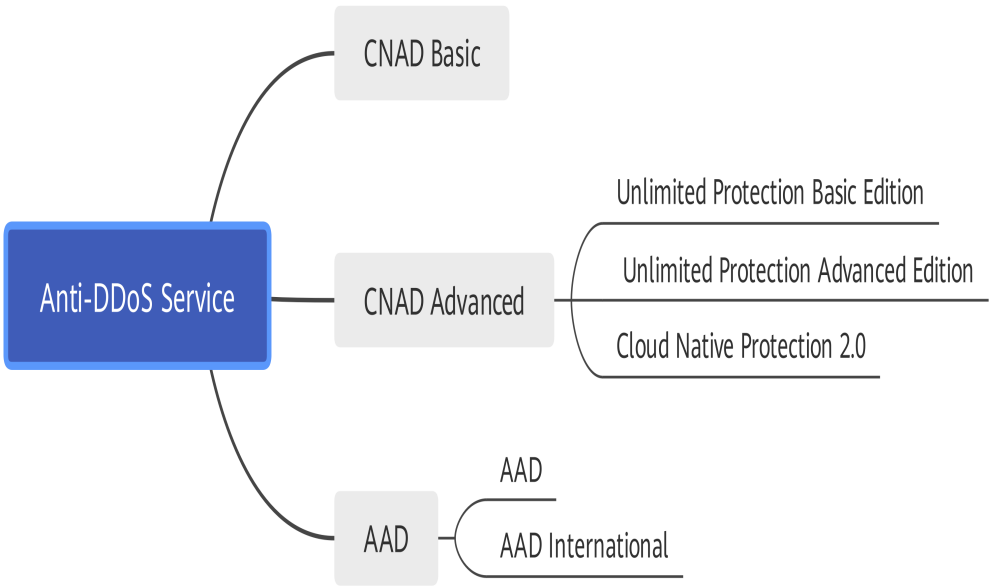
2 Understanding Anti-DDoS Service

2.1 Selecting Anti-DDoS Service Editions

Huawei Cloud provides multiple security solutions to defend against DDoS attacks. You can select an appropriate one based on your service requirements. Huawei Cloud Anti-DDoS Service provides three sub-services: Cloud Native Anti-DDoS Basic, Cloud Native Anti-DDoS Advanced, and Advanced Anti-DDoS.

Cloud Native Anti-DDoS Basic is free while Cloud Native Anti-DDoS Advanced and Advanced Anti-DDoS are paid services.

Figure 2-1 Introduction to Anti-DDoS Service



Service Description

Table 2-1 describes Anti-DDoS Service editions.

Table 2-1 Anti-DDoS service editions

Edition	Description	Application Scenario	DDoS Protection Capability
Cloud Native Anti-DDoS Basic	Cloud Native Anti-DDoS 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.	You can use this service to protect your Huawei Cloud EIPs (IPv4 and IPv6) against the DDoS attacks if you have only general security requirements.	Cloud Native Anti-DDoS Basic provides 500 Mbit/s DDoS attack defense for users free of charge.

Edition	Description	Application Scenario	DDoS Protection Capability
Cloud Native Anti-DDoS Advanced	Cloud Native Anti-DDoS Advanced is developed to improve the anti-DDoS capabilities of cloud services such as ECS, ELB, WAF, and EIP. Cloud Native Anti-DDoS Advanced takes effect for IP addresses on Huawei Cloud. You do not need to change the IP addresses. With few clicks on the console, you can enjoy always-on DDoS mitigation.	Cloud Native Anti-DDoS 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. Cloud Native Anti-DDoS Advanced can be used for the following scenarios: • Occasional DDoS attacks **NOTE** If you require Tbps-level cloud native protection, you are advised to select Cloud Native Anti-DDoS Advanced - Unlimited Protection Advanced Edition. • Huawei Cloud services with public IP addresses assigned for external communication **NOTICE** The CNAD Unlimited Protection Advanced edition must use EIPs in the dedicated resource pool of the Cloud Native Anti-DDoS Advanced unlimited protection editions. • 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,	• Cloud Native Anti-DDoS Advanced - Unlimited Protection Basic Edition Shared protection for not less than 20 Gbit/s of traffic • Cloud Native Anti-DDoS Advanced - Unlimited Protection Advanced Edition Unlimited protection, with up to 1 Tbit/s protection capability. Dedicated EIPs and service bandwidth are billed separately.

Edition	Description	Application Scenario	DDoS Protection Capability
		and IP addresses need to be protected from DDoS attacks.	
Advanced Anti-DDoS	Advanced Anti-DDoS works as a proxy and uses Advanced Anti-DDoS IP addresses to forward requests to origin servers. All public network traffic is diverted to the high-defense IP address so that the origin server is hidden from the public. This protects origin servers from DDoS attacks.	If your service servers and main customers are in the Chinese Mainland, the access of your customers outside the Chinese Mainland may be affected by network quality. Huawei Cloud, non-Huawei Cloud, and IDC hosts can be protected. Advanced Anti-DDoS applies to the following scenarios: ● Services are frequently attacked by DDoS attacks. Continuous protection is required to ensure service continuity. **NOTICE** ● Advanced Anti-DDoS does not support domain names that have no ICP licenses. To use Advanced Anti-DDoS to protect website services, ensure that the website domain name has an ICP license.	One high-defense IP address is able to defend against 1 Tbit/s network-, and application-layer DDoS attacks. The Advanced Anti-DDoS service offers more than 15 Tbit/s of defense capability. ● 15 Tbit/s of defense capability is the overall defense capability of the Advanced Anti-DDoS equipment room. ● 1 Tbit/s of defense capability refers to the maximum protection capability of a single high-defense IP address.

Edition	Description	Application Scenario	DDoS Protection Capability
Advanced Anti-DDoS International	If your service servers are deployed outside the Chinese Mainland and your main users are outside the Chinese Mainland, Advanced Anti-DDoS international is suitable for you.	If your service server is deployed outside the Chinese Mainland but your main service users are in the Chinese Mainland, there might be an average of about 300ms delay for users in the Chinese Mainland. **NOTE** If you want to use Advanced Anti-DDoS international edition, we recommended that you can use Advanced Anti-DDoS for your servers and customers outside the Chinese Mainland only.	Over 5 Tbit/s Advanced Anti-DDoS defense capability, supporting unlimited AnyCast defense.

DDoS Attack Types and Anti-DDoS Service Editions

Table 2-2 Workload types supported by Anti-DDoS Service editions

DDoS Attack	Cloud Native Anti-DDoS Basic	Cloud Native Anti-DDoS Advanced	Advanced Anti-DDoS
Malformed packets	√	√	√
Transport-layer DDoS attack	√ It can defend against SYN flood attacks (small packet attacks), but not so well as the Cloud Native Anti-DDoS Advanced or Advanced Anti-DDoS. You are advised to use Cloud Native Anti-DDoS Advanced or Advanced Anti-DDoS.	√	√

DDoS Attack	Cloud Native Anti-DDoS Basic	Cloud Native Anti-DDoS Advanced	Advanced Anti-DDoS
DNS DDoS attack	×	×	√
Connection DDoS attack	×	Supported only by the Unlimited Protection Advanced Edition.	√
DDoS attacks at the web application layer	×	×	√

NOTE

- The symbol "√" indicates that the service defends against the attack.
- The symbol "×" indicates that the service does not defend against the attack.

2.2 Cloud Native Anti-DDoS Basic

2.2.1 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:

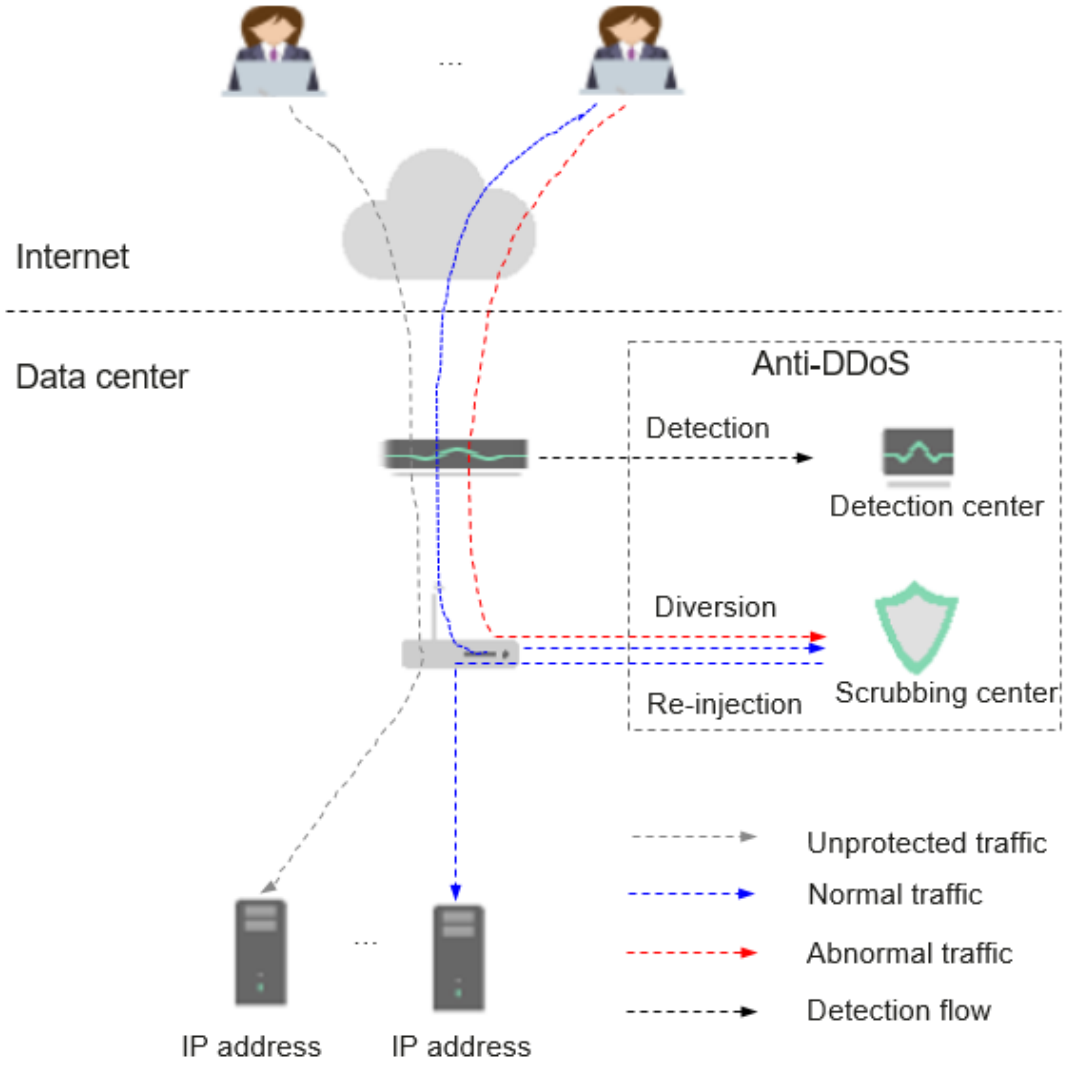
- Monitors the security status of a single public IP address and offers a monitoring report, covering the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.
- Provides attack reports on all protected public IP addresses, covering the traffic cleaning frequency, cleaned traffic amount, the top 10 attacked public IP addresses, and the number of blocked attacks.

2.2.2 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 2-2** shows the network topology.

Figure 2-2 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.

2.2.3 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.

2.3 Cloud Native Anti-DDoS Advanced

2.3.1 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

Table 2-3 describes the specifications supported by an instance of each edition.

NOTICE

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

Table 2-3 CNAD specifications

Specification	CNAD Unlimited Protection Basic Edition	CNAD Unlimited Protection Advanced Edition	Cloud Native Protection 2.0
Billing Mode	Yearly/Monthly	Yearly/Monthly	Yearly/Monthly and pay-per-use

Specification	CNAD Unlimited Protection Basic Edition	CNAD Unlimited Protection Advanced Edition	Cloud Native Protection 2.0
Bandwidth Type	Cloud native network and fully dynamic BGP (static BGP not supported).	Huawei cloud-native network, multi-line BGP	Cloud native network and fully dynamic BGP (static BGP not supported).
Protection Capability	Shared unlimited protection for not less than 20 Gbit/s of traffic	Shared unlimited protection for up to 1 Tbit/s of traffic	Chinese mainland: Shared unlimited protection, no less than 20 Gbit/s. Outside the Chinese mainland: cross-border protection for carriers.
Protected IP Addresses	The value ranges from 50 to 500 and must be a multiple of 5.	The value ranges from 50 to 500 and must be a multiple of 5.	50 to 1000 IP addresses. The number of protected IP addresses must be a multiple of 50.
Protection Times	Unlimited	Unlimited	Unlimited
IP Address Change Times	Not supported	Not supported	Not supported
Service Bandwidth	The supported value ranges from 100 Mbit/s to 20,000 Mbit/s.	Maximum value: 40,000 Mbit/s	A maximum of 20,000 Mbit/s is supported.

2.3.2 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.

2.3.3 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.

2.4 Advanced Anti-DDoS

2.4.1 Advanced Anti-DDoS

Advanced Anti-DDoS (AAD) ensures the continuity of important enterprise services. AAD can protect your servers against large volumetric DDoS attacks so your services can be reliable and stable. AAD offers high-defense IP addresses to provide services in place of the original server IP addresses for external systems. The malicious attacks targeting the origin servers can be diverted for scrubbing to ensure the stable running of mission-critical workloads. This service can be used to protect HUAWEI CLOUD, non-HUAWEI CLOUD, and IDC hosts.

NOTE

If an AAD instance has expired for more than 30 calendar days, AAD will stop forwarding service traffic and the instance will become invalid. If you do not need to use AAD anymore, switch your service traffic from AAD to the origin server 30 calendar days before the expiration date.

- AAD not deployed

  Without AAD, the origin servers are exposed to the Internet and are prone to paralysis once Distributed Denial-of-Service (DDoS) attacks occur.

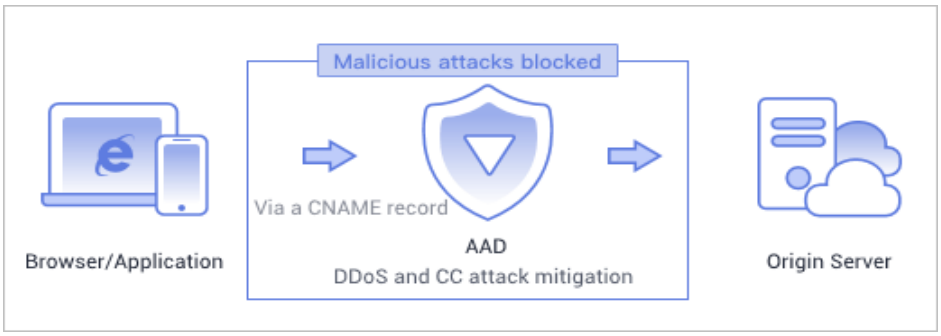
  Figure 2-3 AAD not deployed

- AAD deployed

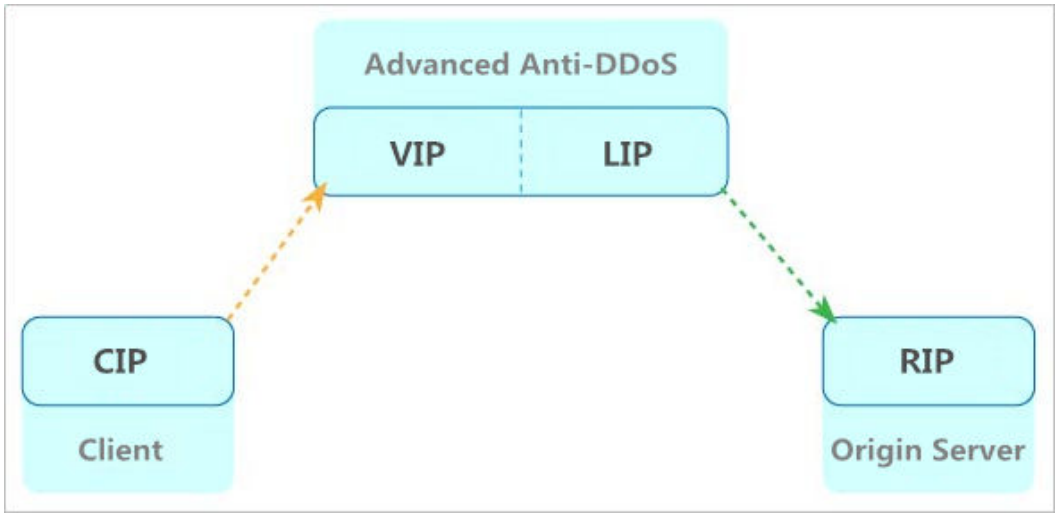
  You can connect AAD with your services. The domain name of website service is resolved into high-defense IP address, and the service IP address of the non-web service is changed to the high-defense IP address. All public network traffic is diverted to the high-defense IP address, and therefore user services on the origin servers are protected against DDoS attacks.

  Figure 2-4 AAD deployed

AAD Mechanism

The AAD service uses the high-defense IP address to proxy services for origin servers. All public network traffic is diverted to the high-defense IP address, and therefore user services on the origin servers are protected against DDoS attacks. The following figure illustrates the mechanism of AAD traffic diversion and forwarding.



- Customer

  Customer who accesses the origin server
- Origin server IP address

  A public IP address used by the origin server (also known as the IP address that is protected against exposures)
- High-defense IP address

  An IP address used to provide services for customers in place of the origin server IP address
- Back-to-origin IP address

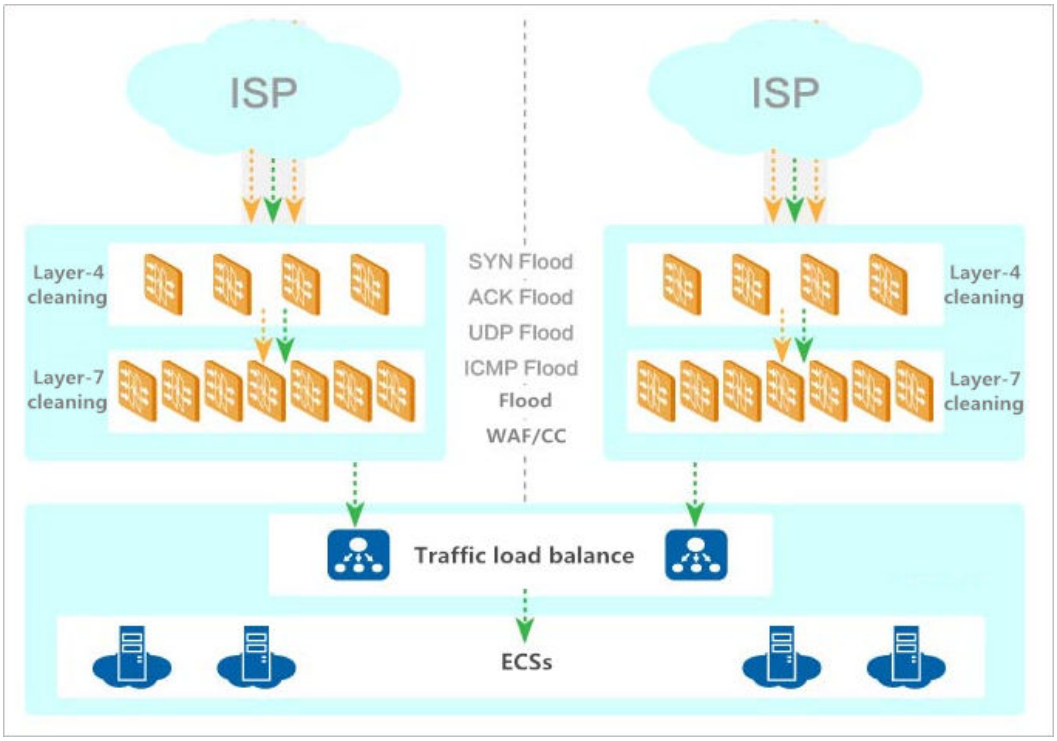
  An IP address used to communicate with the origin server IP address in place of the customer IP address in the AAD data center

AAD provides defense against a wide range of network-, and application-layer DDoS attacks, including SYN flood, UDP flood, ACK flood, ICMP flood, DNS query flood, NTP reply flood, and CC attacks.

Service Architecture

Employing multi-layer filtering and protection technologies, such as layered defense and distributed scrubbing, the AAD service can effectively detect and filter out attack traffic. **Figure 2-5** illustrates the network topology of the AAD service.

Figure 2-5 Network topology



2.4.2 Specifications

Table 2-4 describes the AAD specifications. The specifications of an AAD instance cannot be downgraded.

Table 2-4 AAD instance specifications

Parameter	Description
Access Type	Two types are supported: **Website** and **IP access**. **NOTE** Websites: Huawei Cloud uses intelligent algorithms to select the optimal access point for you and does not provide fixed high-defense IP addresses. This type is recommended for users using "Domain Name Access". IP access: provides only IP port protection and fixed high-defense IP addresses. This type is recommended for users using "Layer 4 Forwarding Rules".
Instance	Each user can purchase a maximum of five instances by default.
Line	Line: **BGP**.

Parameter	Description
Service access point	You can select one of the following options based on your geographical location: • North China 1: China Mobile, China Telecom, China Unicom, Beijing Education Network, Dr. Peng, Hebei Broadcast & Television, and Chongqing Broadcast & Television are supported. • CN East 2: China Mobile, China Telecom, and China Unicom are supported.
IP type	• IPv4: To protect an IPv4 origin server, you need to select IPv4. • IPv6: To protect an IPv6 origin server, you need to select IPv6.
Number of protected domain names (available only when **website access** is selected)	Each instance protects 50 domain names for free. You can protect up to 200 domain names at an additional cost. **NOTICE** The number of domain names includes the total number of top-level domain names (for example, example.com), single domain names/subdomain names (for example, www.example.com), and wildcard domain names (for example, *.example.com). Each AAD instance can protect 50 single domain names or wildcard domain names, or protect one top-level domain name and 49 subdomain names or wildcard domain names related to the top-level domain name.
Basic Protection Bandwidth	Value range: 10Gbps, 20Gbps, 30Gbps, 60Gbps, 100Gbps, 300Gbps, 400Gbps, 500Gbps, 600Gbps, 800Gbps, 1000Gbps. To achieve enhanced protection, specify **Elastic Protection Bandwidth**.
Elastic Protection Bandwidth	You can change the elastic protection bandwidth three times a day for each instance. Value range: 10Gbps, 20Gbps, 30Gbps, 40Gbps, 50Gbps, 60Gbps, 70Gbps, 80Gbps, 100Gbps, 200Gbps, 300Gbps, 400Gbps, 500Gbps, 600Gbps, 700Gbps, 800Gbps, 1000Gbps. If there is no attack detected or the attack traffic does not exceed the basic protection bandwidth, you are not billed for the elastic protection function. If the attack peak is greater than the selected elastic protection bandwidth, the high-defense IP address will be blocked by a black hole. You can change the elastic protection bandwidth for your AAD instance based on service requirements. **NOTE** The elastic protection bandwidth must be greater than or equal to the basic protection bandwidth. If the two are set to the same value, the elastic protection bandwidth function does not take effect.

Parameter	Description
Service Bandwidth	The service bandwidth indicates the bandwidth used by AAD to forward traffic from the AAD scrubbing center to the origin server. A 100 Mbit/s of service bandwidth is provided for each instance for free. You can buy up to 2 Gbit/s of service bandwidth at an additional cost. If the service traffic from your AAD instance to origin server is fewer than 100 Mbit/s, you can use the free service bandwidth.
Forwarding Protocol	• Layer-4 protocol: TCP and UDP • Layer-7 protocol: HTTP/WebSocket and HTTPS/ WebSockets
Access Mode	• Connecting website services to an AAD instance To connect a website service to AAD, you can set a Canonical Name (CNAME) record in the DNS configuration. • Connecting non-website services to an AAD instance Non-website services include applications and PC client services. For such services, you can configure CNAME records in DNS or directly configure high-defense IP addresses on clients to use AAD.
Black Hole Deactivation Time	The black hole lasts 30 minutes by default. However, depending on the number of black holes triggered and peak attack traffic of the day, it may last up to 24 hours. **NOTE** If you need to unblock access before a black hole becomes ineffective, contact Huawei technical support.
Protected objects	You can use AAD to protect hosts on Huawei Cloud, other clouds, and IDCs.

Differences Between IPv4 and IPv6 IP Addresses in AAD

AAD supports IPv4 and IPv6 high-defense IP addresses. The following table describes the differences between the two types of IP addresses.

CAUTION

To protect an IPv4 origin server, select an IPv4 instance. To protect an IPv6 origin server, select an IPv6 instance. When purchasing an instance, pay attention to the type of the IP addresses to be protected.

Function	IPv4 high-defense addresses	IPv4 high-defense addresses
Blacklist or whitelist	√	√
Regional traffic blocking	√	×
Protocol traffic blocking	√	√
CC defense	√	√
Basic web protection	√	√
Updating a domain name certificate	√	√
Modifying resolution lines for high-defense IP addresses of a domain name	√	√
Changing an origin server IP address	√	√
CNAME-based automatic scheduling	√	√
Viewing attack events	√	√
Viewing attack types	√	√
Viewing CC attack protection	√	√
Obtaining the real source IP address	√	×

2.4.3 Application Scenarios

The AAD service can be used in a wide range of industries, such as entertainment (gaming), finance, government, e-commerce, media assets, and online education.

- Entertainment (gaming)

  The entertainment (gaming) industry is fragile to DDoS attacks. The AAD service can provide protection for users during service peaks, such as business activities and holidays, ensure high availability and continuity of games, and improve user experience.

- Finance

  The AAD service keeps up with the compliance requirements of the finance industry and ensures timeliness, security, and stability of online transactions.

- Government

  The AAD service meets the security requirements of e-Government cloud construction standards, provides security assurance for major conferences, activities, and sensitive periods, ensures that people's livelihood services are available, and maintains government credibility.

- E-Commerce

  The AAD service protects user access to the Internet and ensures service continuity during activities such as e-Commerce promotion.

- Enterprises

  The AAD service ensures continuous service availability for enterprises, mitigates economic and image loss caused by DDoS attacks, and reduces maintenance and security costs.

2.4.4 Advantages

AAD provides instantaneous protection once you connect your services to AAD. You can view DDoS attack protection details on its dashboard to learn about the network security state.

AAD helps you defend against large volume DDoS attacks, with high precision, flexibility, reliability, and availability.

- **Immense defense capability**

  One high-defense IP address is able to defend against 1000 Gbit/s network-, and application-layer DDoS attacks. The AAD service offers more than 15 Tbit/s defense capability.

- **High availability**

  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.

- **Flexible protection**

  You can buy both the basic bandwidth protection and elastic bandwidth protection of AAD for a higher protection capability. The protection bandwidth can be adjusted depending on your needs.

- **Professional operations team**

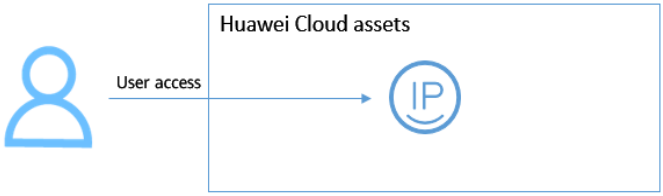
  You will get a 24/7 service support from a professional operations team.

3 Edition Differences

Deployment Modes

Anti-DDoS Service can be deployed in two modes.

- Transparent mode: This mode directly improves the anti-DDoS capability of your assets on Huawei Cloud.



- Proxy mode: Your server IP address is hidden behind AAD high-defense IP addresses, which defend your server against DDoS attacks, ensuring your service continuity.

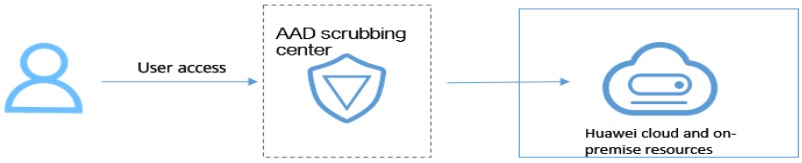


Table 3-1 Differences between the transparent mode and the proxy mode

Item	Transparent	Proxy
Billing	Yearly/Monthly	Yearly/Monthly

Item	Transparent	Proxy
Edition	Anti-DDoS (free) CNAD Unlimited Protection - Basic Edition CNAD Unlimited Protection - Advanced Edition	AAD AAD International
Application scenarios	Services whose servers are deployed on Huawei Cloud and can be accessed through public IP addresses	Services whose servers are deployed on Huawei Cloud or non-Huawei Cloud and can be accessed through the public network
Protected objects	IP	IP addresses or domain names
Advantages	Transparent access, directly protecting server addresses Huawei cloud native network, low latency	Hide the server address from external networks. AAD scrubbing center provides strong protection. Applicable to Huawei Cloud and non-Huawei Cloud scenarios

Edition Specifications

Table 3-2 Edition specifications

Item	CNAD Basic	CNAD Unlimited Protection - Basic Edition	CNAD Unlimited Protection - Advanced Edition	CNAD Advanced - Cloud Native Protection 2.0	AAD - Website Protection
Billing Mode	Free	Yearly/ Monthly	Yearly/ Monthly	Instances are billed in yearly/ monthly mode. Service bandwidth is billed in yearly/ monthly or pay-per-use mode.	Yearly/ Monthly
Access mode	Transparent access	Transparent access	Transparent access	Transparent access	DNS resolution
Network	Native network	Cloud native network and fully dynamic BGP (static BGP not supported).	Cloud native network, multi-line BGP	Cloud native network and fully dynamic BGP (static BGP not supported).	Multi-line BGP
Protected objects	Huawei Cloud EIPs	Huawei Cloud EIPs	Huawei Cloud exclusive EIPs	Huawei Cloud EIPs	Domain names accessible to the Internet (Huawei Cloud + on-premises)
Protocol	IPv4 and IPv6	IPv4 and IPv6	IPv4	IPv4 and IPv6	IPv4 and IPv6
Objects	Unlimited	50-500	50-500	50-1000	50-200

Item	CNAD Basic	CNAD Unlimited Protection - Basic Edition	CNAD Unlimited Protection - Advanced Edition	CNAD Advanced - Cloud Native Protection 2.0	AAD - Website Protection
Service bandwidth	N/A	100Mbps-20Gbps	100Mbps-40Gbps	100Mbps-20Gbps	100Mbps-2Gbps

NOTICE

An AAD instance supports only one IP protocol (IPv4 or IPv6). If you need multiple protocols, purchase multiple AAD instances.

Protection Capabilities Supported by Each Edition

Table 3-3 Protection capabilities supported by each edition

Item	CNAD Basic (free)	CNAD Unlimited Protection - Basic Edition	CNAD Unlimited Protection - Advanced Edition	AAD - Website Protection	AAD - IP Protection
Protection capability	• Chinese mainland region: no higher than 5 GB • Regions outside the Chinese mainland: no more than 500 MB	Shared protection for not less than 20 Gbit/s of traffic	Shared protection for up to 1 Tbit/s of traffic	1 Tbit/s (multiple instances can be accumulated)	1T

Item	CNAD Basic (free)	CNAD Unlimited Protection - Basic Edition	CNAD Unlimited Protection - Advanced Edition	AAD - Website Protection	AAD - IP Protection
DDoS protection	Scrubbing threshold	• Blacklist or whitelist • Scrubbing threshold • Protocol blocking • Waterm arking	• Blacklist or whitelist • Scrubbing threshold • Protocol blocking • Waterm arking • Connection protection	• Blacklist or whitelist • Cross-border blocking • UDP blocking **NOTICE** Currently, the international edition can only be configured offline.	• Blacklist or whitelist • Cross-border blocking • UDP blocking **NOTICE** Currently, the international edition can only be configured offline.
Application protection	N/A	Exclusive WAF support	Exclusive WAF support	• 3000 QPS by default • If the QPS is greater than 3000, Huawei Cloud WAF or exclusive WAF are required.	Exclusive WAF support

4 Security

4.1 Shared Responsibilities

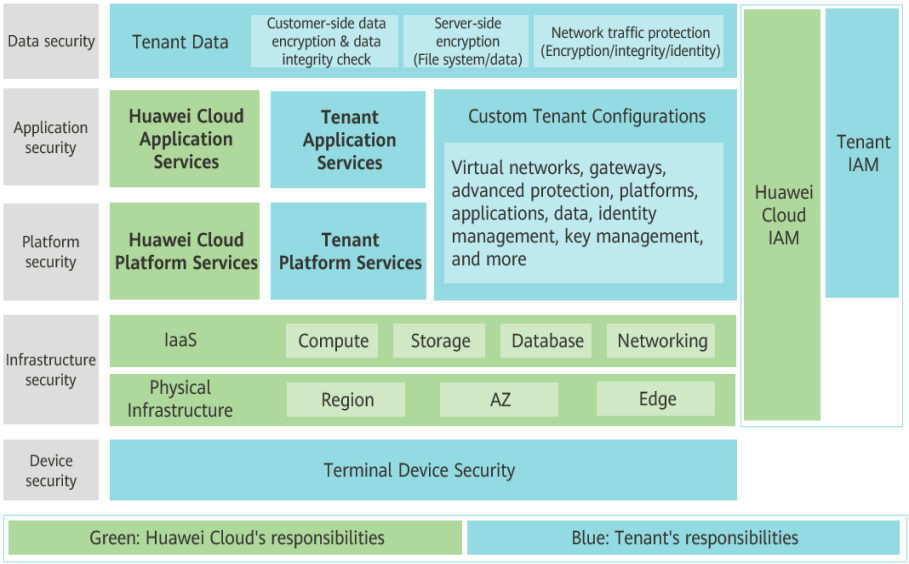
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Figure 4-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 4-1 Huawei Cloud shared security responsibility model



4.2 Identity Authentication and Control

Credential Authentication

No matter whether you access the Anti-DDoS service through the console or calling APIs, you are required to provide the identity credential and verify the identity validity. In addition, login and login authentication policies are provided to harden identity authentication security. Based on Identity and Access Management (IAM), Anti-DDoS supports three identity authentication modes: **username and password**, **access key**, and **temporary access key**. In addition, **login protection** and **login authentication policies** are provided.

Access Control

Anti-DDoS uses IAM to control access, assigning system roles and implementing fine-grained permission management. For details about permission management, see:

- **Permission Management for Anti-DDoS**

4.3 Data Protection

To prevent data leakage, Anti-DDoS does not store your sensitive user data. It encrypts your data during transmission.

Measure	Description
Transmission encryption (HTTPS)	Your personal data (such as certificate) is encrypted using TLS 1.2 during transmission. All the calls made to Anti-DDoS APIs use HTTPS to encrypt data during transmission.

Measure	Description
Personal data protection	To protect your personal data against data leakage and unauthorized modification, Anti-DDoS controls the access to your data and records logs for the operations performed on your data.
Privacy protection	Anti-DDoS can mask the sensitive data in the audited data.
Data destruction	If you delete your Anti-DDoS instance or deregister your account, Anti-DDoS will delete the audit instance.

4.4 Audit and Logging

Cloud Trace Service (CTS) keeps track of user activities and resource changes on your cloud resources. It helps you collect, store, and query operational records for security analysis, audit and compliance, and fault location.

CTS allows you to configure key event notification. You can add DDoS-related high-risk and sensitive operations as key operations to be monitored and tracked by CTS. If a key operation in the monitoring list is triggered when a user uses Anti-DDoS, CTS records the operation log and sends a notification to the related subscribers in real time.

4.5 Service Resilience

Huawei Cloud data centers are deployed around the world. All data centers are running properly. Data centers in two cities are deployed as disaster recovery center for each other. If a data center in city A is down, the data center in city B automatically takes over the job and serves your applications and data in compliance with the regulations to ensure service continuity. Huawei Cloud provides a DR plan for all data centers, in order to minimize the service interruptions caused by hardware failures, natural disasters, or other disasters.

4.6 Risk Monitoring

You can view Anti-DDoS monitoring data.

Viewing Anti-DDoS Reports

You can log in to the Anti-DDoS console to view the monitoring information about the protected resources. The details about the monitoring information are as follows:

Sub-service	Monitored Object	Monitored Item
Anti-DDoS	Public IP address	You can view the monitoring report of a public IP address, covering the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.
CNAD	Protected objects	You can view the received traffic, attack traffic, traffic cleaning frequency, peak cleaned traffic amount, attack type distribution, and top 10 attacked public IP addresses.
Advanced Anti-DDoS (AAD)	High-defense IP address Protected domain dame	DDoS attack defense. The **Dashboard** page gives an overview of the peak ingress traffic, peak attack traffic, and number of DDoS attacks, and shows the attack type distribution, DDoS attack events, and top 5 attack types scrubbed on two tab pages **Traffic** and **Packet Rate**. CC attack defense. The **Dashboard** page gives an overview of number of requests and attacks, attack type distribution, and top 5 attacked source IP addresses.

Viewing DDoS Monitoring on CES

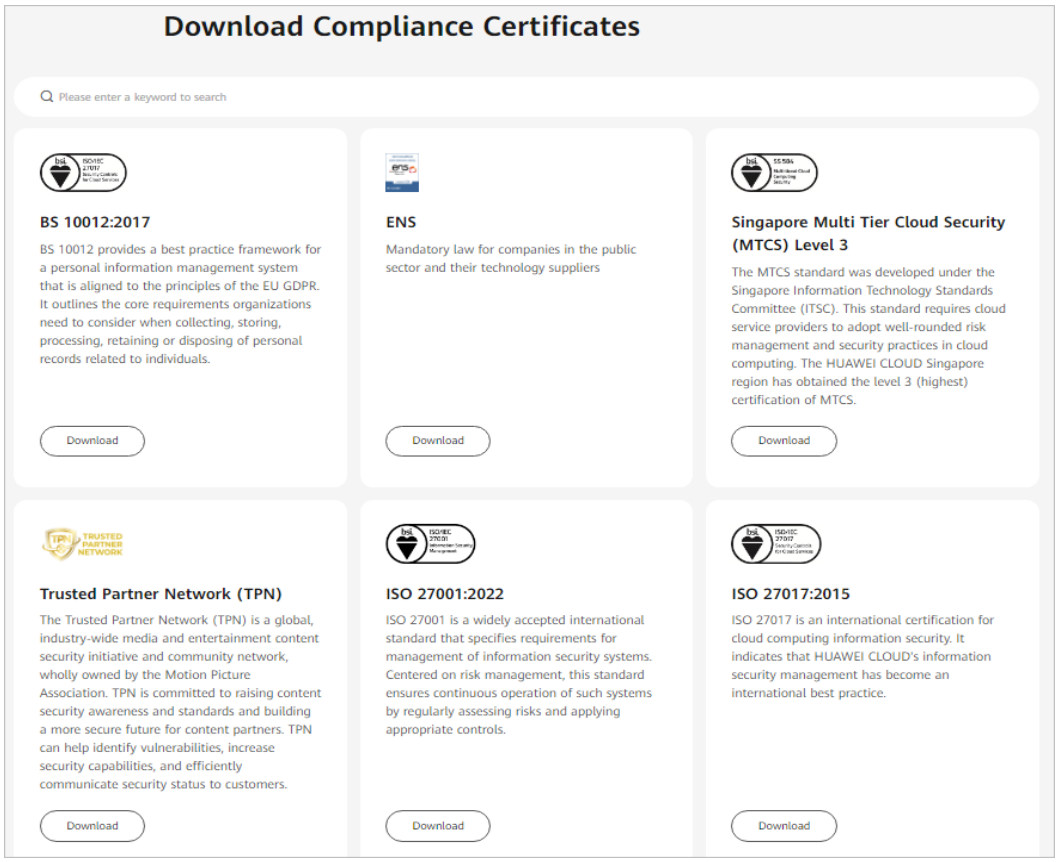
Anti-DDoS works with Cloud Eye to monitor the protected resources in your account in real time, reporting alarms and sending notifications based on your settings. You can obtain the information about the protected resources in real time.

4.7 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can **download** them from the console.

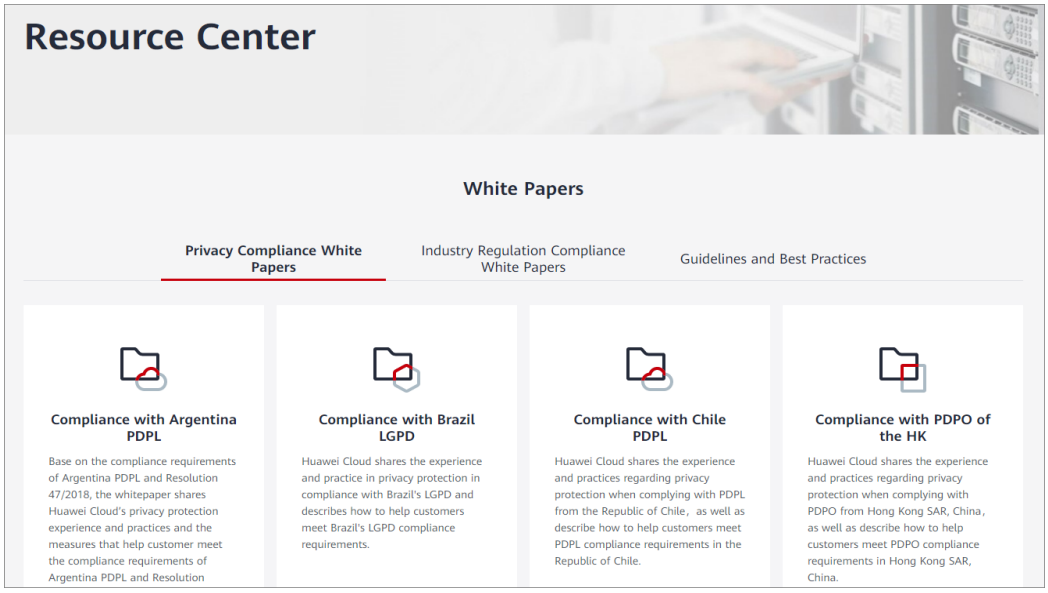
Figure 4-2 Downloading compliance certificates



Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 4-3 Resource center



5 Permissions Management

5.1 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 5-1 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 5-1 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
Anti-DDoS FullAccess	All permissions for Anti-DDoS	-
Anti-DDoS ReadOnlyAccess	Read-only permissions for Anti-DDoS	-

5.2 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 5-2 lists all the system roles supported by CNAD Pro.

Table 5-2 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*"
            ]
        }
    ]
}
```

5.3 AAD Permissions

If you need to assign different permissions to employees in your enterprise to access your AAD 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 AAD 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 AAD resources but must not delete them or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using AAD resources.

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

AAD 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.

AAD is a global service and can be deployed in any region. AAD permissions are assigned to IAM users in the global project, so IAM users can access AAD 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 AAD, 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 AAD users the permissions to manage only a certain type of resources.

Table 5-3 lists all the system roles supported by AAD.

Table 5-3 AAD system role

Role/Policy Name	Description	Type	Dependency
CAD Administrator	Administrator permissions for AAD	System role	Either the CAD Administrator and BSS Administrator roles or the Tenant Administrator role is required for purchasing an AAD instance or upgrading the specifications of an AAD instance. • **BSS Administrator**: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project. • **Tenant Administrator**: has all permissions on all services except on IAM. **NOTICE** The CAD Administrator system role is about to go offline. To ensure the normal use of AAD, grant the AAD FullAccess or AAD ReadOnlyAccess system policy to users as soon as possible.
AAD FullAccess	All permissions for AAD	Policy	Either the AAD FullAccess and BSS Administrator roles or the Tenant Administrator role is required for purchasing an AAD instance or upgrading the specifications of an AAD instance. • **BSS Administrator**: has all permissions on account center, billing center, and resource center. It is a project-level role, which must be assigned in the same project. • **Tenant Administrator**: has all permissions on all services except on IAM.
AAD ReadOnlyAccess	Read-only permissions for AAD. Users granted these permissions can only view AAD information.	Policy	None.

AAD FullAccess Policy Content

```
{
        "Version": "1.1",
```

```
        "Statement": [{
            "Action": [
                "aad:*"
            ],
            "Effect": "Allow"
        }]
}
```

AAD ReadOnlyAccess Policy Content

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

