Anti-DDoS Service

Service Overview

Issue	01
Date	2025-11-24

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 Blackhole 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 Blackhole?

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 blackhole.

How Do I Deactivate a Blackhole?

After a blackhole is executed, Huawei Cloud continuously monitors the DDoS attack status. After the attack ends, Huawei Cloud automatically removes the blackhole from the ECS and restores Internet access.

When a server (ECS) enters a black hole, you can rectify the fault by referring to **Table 1-2**.

Table 1-2 Black hole deactivation methods

Type	Unblocking Policy	Unblocking Method
Anti-DDoS	• The blackhole is automatically removed after the traffic enters the blackhole for 24 hours. • 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. • **Buy CNAD Advanced** (standard edition, Unlimited Protection Basic Edition, or CNAD 2.0). The IP address is unblocked immediately when protection is added for the first time in the month.
CNAD Advanced	• The blackhole is automatically removed after the traffic enters the blackhole for 24 hours. • 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.
Advanced Anti-DDoS	The default blackhole duration is 30 minutes.	You need to wait until the system deactivates it automatically.

Blackhole Threshold

The blackhole 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 (120 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.

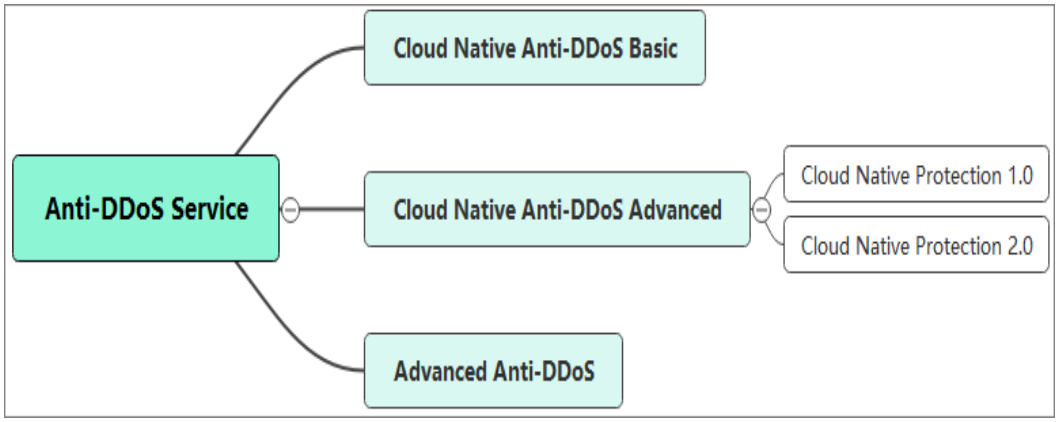
2 Understanding Anti-DDoS Service

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 security of network traffic.	You can use this service to protect your Huawei Cloud EIPs (IPv4 and IPv6) against the DDoS attacks if you have only basic 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. **NOTICE** CNAD Advanced can work with only cloud WAF. For details, see **Using WAF, ELB, and CNAD Advanced to Improve Website Service Security**.	
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.	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. • The quality of network access from users in the Chinese mainland to users outside the Chinese mainland cannot be guaranteed.	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.

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.	√	√
DNS DDoS attack	×	×	√
Connection DDoS attack	×	Supported only by the Unlimited Protection Advanced Edition.	√
DDoS attacks at the web application layer	×	× You are advised to **use WAF, ELB, and CNAD Advanced to improve website service security**.	√

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 CNAD Basic

2.2.1 What Is CNAD Basic

What Is CNAD Basic

Cloud Native Anti-DDoS Basic (CNAD Basic) defends Huawei Cloud elastic IP addresses (EIPs) 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.

NOTE

CNAD Basic does not support attack alarm notification and protection policy customization for public IP addresses of the GEIP and GA types.

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

  SYN flood attacks
- Game attacks

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

CNAD Basic also:

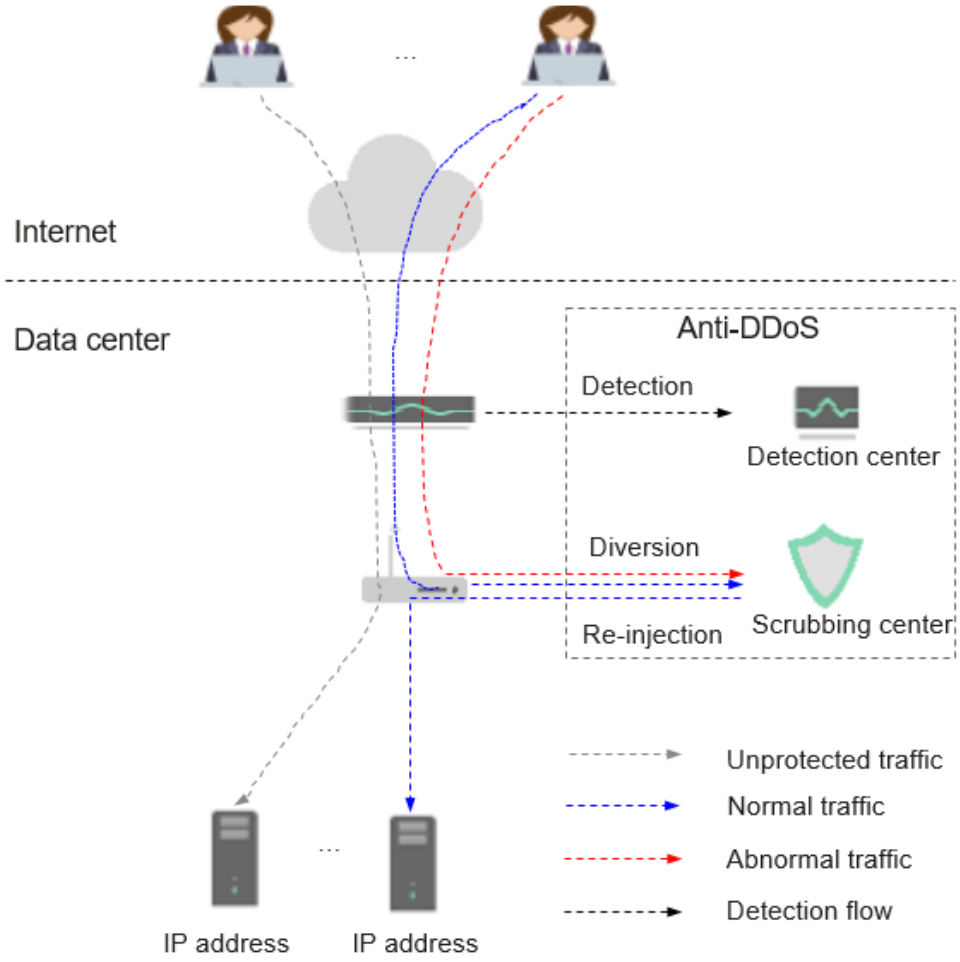
- Monitors the security status of a single public IP address and offers a monitoring report, covering the current protection status, protection settings, and the traffic and anomalies within the last 24 hours.
- Provides attack reports on all protected public IP addresses, covering the traffic cleaning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

2.2.2 Application Scenarios

CNAD Basic helps defend public IP addresses on Huawei Cloud against 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 Function

This section describes the main functions supported by Anti-DDoS. For detailed information on region availability of each feature, you can refer to the console.

Traffic Scrubbing

You can set a traffic scrubbing threshold for the protected EIP. When service traffic exceeds the traffic scrubbing threshold, Anti-DDoS scrubs the traffic to mitigate DDoS attacks. For more information, see **Setting a Traffic Scrubbing Threshold to Intercept Attack Traffic**.

Alarm Notification

If alarm notifications are enabled, alarm notifications will be sent to you (by SMS or email) if a DDoS attack is detected. For more information, see **Setting DDoS Alarm Notifications**.

Event Monitoring

Cloud Eye enables event monitoring for protected EIPs. When events like scrubbing, blocking, or unblocking occur, an alarm is triggered, ensuring you are promptly informed about the protection status. For more information, see **Enabling DDoS Alarm Notifications**.

Attack Logs

After you authorize Anti-DDoS to access Log Tank Service (LTS), you can use the Anti-DDoS logs recorded by LTS for quick and efficient real-time analysis, device O&M management, and analysis of service trends. For more information, see **Enabling Logging**.

Monitoring Reports

On the Anti-DDoS console, you can view the monitoring details of a specified EIP. This includes the current protection status, protection settings, and traffic and abnormal events within the last 24 hours. For more information, see **Viewing EIP Monitoring Reports**.

Interception Report

The Anti-DDoS console produces weekly interception reports. These reports provide EIP protection statistics, including the number of scrubbing times, scrubbed traffic volume, the top 10 attacked public IP addresses, and the total number of intercepted attacks. For more information, see **Viewing Interception Reports**.

Audit Logs

After CTS is enabled, you can view historical operation records. For more information, see **Viewing Logs on CTS**.

2.2.4 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 EIPs 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.

Instance Specifications

Table 2-3 Specifications of different types of CNAD Advanced instances

Type	CNAD 1.0		CNAD 2.0	
Edition	**Unlimited Protection Basic Edition**	**Unlimited Protection Advanced Edition**	**Enterprise Edition**	**SME Edition**
Billing Mode	Yearly/ Monthly	Yearly/ Monthly	• The instance is billed on a yearly/ monthly basis. • Service bandwidth can be billed on a yearly/monthly or pay-per-use basis.	• The instance is billed on a yearly/monthly basis. • The public network line billing mode is only available for yearly/ monthly billing.
Protected objects	Huawei Cloud dynamic BGP EIPs	Anti-DDoS Service dedicated EIPs	• Chinese mainland: Dynamic BGP EIPs and Anti-DDoS Service dedicated EIPs • Outside the Chinese mainland: Premium BGP EIPs and Anti-DDoS Service dedicated EIPs	Chinese mainland: Dynamic BGP EIPs and Anti-DDoS Service dedicated EIPs

Type	CNAD 1.0		CNAD 2.0	
Edition	**Unlimited Protection Basic Edition**	**Unlimited Protection Advanced Edition**	**Enterprise Edition**	**SME Edition**
Region	Single-region protection	Single-region protection	• Chinese mainland: Cross-region protection is supported. • Outside the Chinese mainland: Only Hong Kong and Singapore are supported.	Chinese mainland: Select resources of any region in China for protection.
Protocol	IPv4 and IPv6	IPv4	IPv4 and IPv6	IPv4 or IPv6
Protected Objects (per Instance)	50 to 500	50 to 500	50 to 1,000	1 to 1,000
Service Bandwidth	100 Mbit/s to 20 Gbit/s	100 Mbit/s to 10 Gbit/s	100 Mbit/s to 20 Gbit/s	50 Mbit/s to 20 Gbit/s

Type	CNAD 1.0		CNAD 2.0	
Edition	**Unlimited Protection Basic Edition**	**Unlimited Protection Advanced Edition**	**Enterprise Edition**	**SME Edition**
Protection Capability	• Shared unlimited protection, no less than 20 Gbit/s, up to hundreds of Gbit/s. • If the service bandwidth exceeds the limit, the protection capability drops and ranges from 10 Gbit/s to 20 Gbit/s.	• Shared unlimited protection for up to 1 Tbit/s • If the service bandwidth exceeds the limit, the protection capability drops and ranges from 10 Gbit/s to 20 Gbit/s.	• Chinese mainland: Shared unlimited protection for at least 20 Gbit/s and up to 1 Tbit/s If the service bandwidth exceeds the limit, the protection capability drops and ranges from 10 Gbit/s to 20 Gbit/s. • Outside the Chinese mainland: carrier-based cross-border protection for up to 1 Tbit/s If the service bandwidth exceeds the limit, the protection capability drops to 5 Gbit/s.	Chinese mainland: Shared unlimited protection for at least 20 Gbit/s and up to 1 Tbit/s If the service bandwidth exceeds the limit, the protection capability drops and ranges from 10 Gbit/s to 20 Gbit/s.

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 Function

This section describes the main functions supported by CNAD Advanced. For detailed information on region availability of each feature, you can refer to the console.

Traffic Scrubbing

After your service is connected to CNAD Advanced, you can set basic protection policies for the protected objects. If the DDoS bandwidth on an IP address exceeds the configured threshold, CNAD Advanced is triggered to scrub attack traffic to ensure service availability. For more information, see **Configuring a Basic Protection Policy to Intercept Attack Traffic**.

Blacklist and Whitelist

You can configure an access control list to control access to your IP addresses. For more information, see **Blocking or Permitting Traffic from Specified IP Addresses Using a Blacklist and Whitelist**.

Port Blocking

If a destination port is unnecessary for access, you can set up a port blocking policy to block traffic from reaching the port, thereby minimizing DDoS attack risks. For more information, see **Blocking Traffic to a Specified Port**.

Protocol-based Blocking

After protocol blocking is enabled, the system limits the rate of traffic destined for Anti-DDoS Service objects based on the protocol type. This feature supports protocols such as UDP, TCP, and ICMP. For more information, see **Limiting Traffic to a Specified Protocol**.

Fingerprint Filtering

You can configure a fingerprint filtering rule to match the content of a specified location in a data packet. You can set actions for matched traffic, such as discarding, allowing, and rate limiting. For more information, see **Setting a Traffic Handling Policy Based on Fingerprint Features**.

Advanced Protection

If an origin server IP address frequently sends a high volume of abnormal connection packets within a short period, you can set up an advanced protection policy to add the IP address to the blacklist. Access it once the block period ends.

For more information, see **Using Advanced Protection Policies to Restrict Abnormal Connections**.

Region Blacklist

CNAD Advanced allows you to configure a policy to block traffic outside China. After the policy takes effect, access traffic from outside China will be discarded. For more information, see **Blocking Traffic to a Specified Port**.

Configuring Attack Filtering

CNAD Advanced offers common UDP reflection and other common filtering rules. You can enable rate limiting rules with just a few clicks. For more information, see **Filtering Attacks Based on One-Click Rate Limiting Rules**.

Alarm Notification

After you enable alarm notifications, a notification message will be sent to you (through the method you have configured) when an IP address is under DDoS attacks. For more information, see **Enabling Alarm Notifications for DDoS Attacks**.

Attack Logs

After you authorize CNAD Advanced to access Log Tank Service (LTS), you can use the attack logs recorded by LTS for quick and efficient real-time analysis, device O&M management, and analysis of service trends. For more information, see **Enabling Logging**.

Data Report

CNAD Advanced provides comprehensive reporting capabilities, allowing you to view data from both instance and protected object dimensions. These reports include traffic statistics, attack trends, and security events, offering valuable insights into the current network security posture. For more information, see **Viewing Statistics Reports**.

Event Monitoring

Cloud Eye enables event monitoring for protected EIPs and generates alarms for scrubbing, blocking, and unblocking events. This helps you learn about the protection status of CNAD Advanced in a timely manner. For more information, see **Setting Event Alarm Notifications**.

Audit Logs

After CTS is enabled, you can view historical operations recorded by CTS. For more information, see **Viewing CTS Traces**.

2.3.4 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

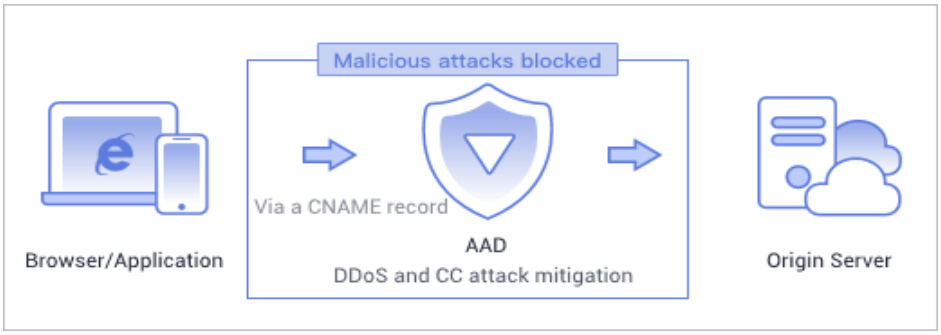
  Without AAD, the origin servers are exposed to the Internet and are prone to paralysis once Distributed Denial-of-Service (DDoS) attacks occur.

Figure 2-3 AAD not deployed

- AAD deployed

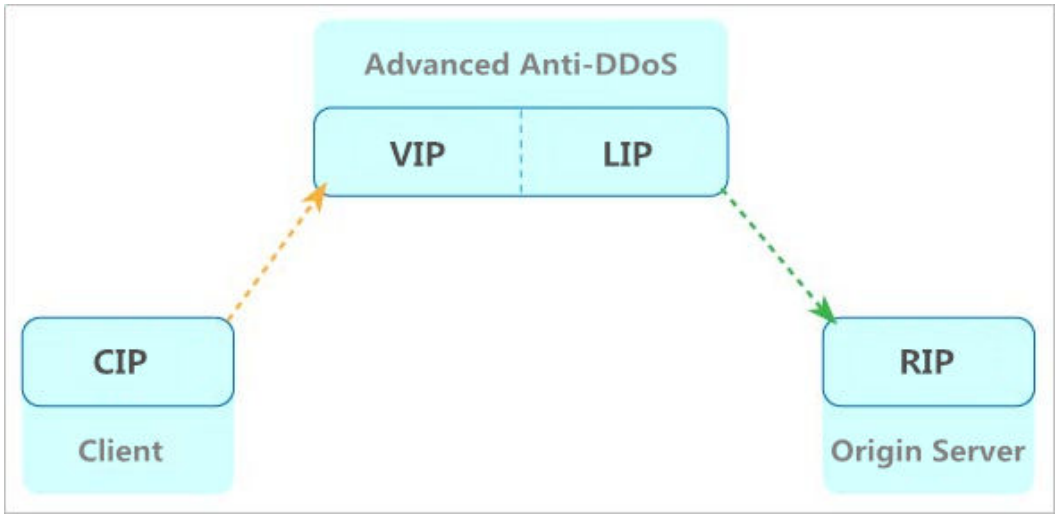
  You can connect AAD with your services. The domain name of website service is resolved into high-defense IP address, and the service IP address of the non-web service is changed to the high-defense IP address. All public network traffic is diverted to the high-defense IP address, and therefore user services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

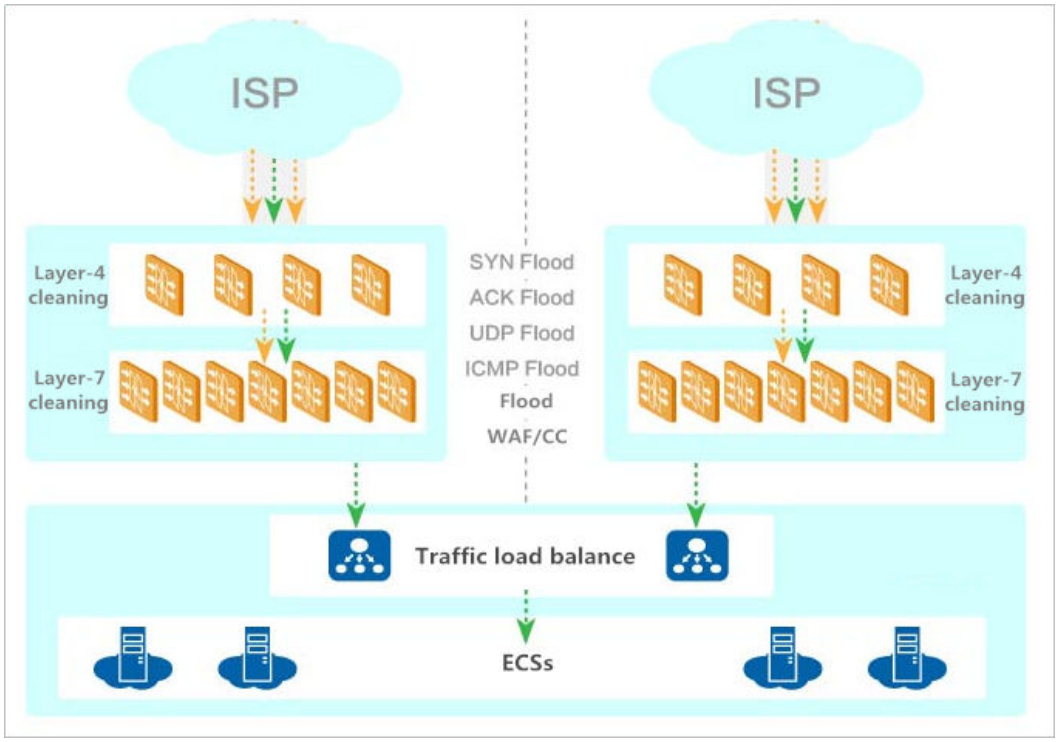
  An IP address used to communicate with the origin server IP address in place of the customer IP address in the AAD data center

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: • Random allocation: The system automatically evaluates and allocates the optimal access point to the user. Only IPv4 addresses are supported. • 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. • CN East 6: 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 pay for more. A maximum of 500 ports are supported in the Chinese mainland, and a maximum of 200 ports are supported outside the Chinese mainland. **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: 10 Gbit/s to 100 Gbit/s, 300 Gbit/s, 400 Gbit/s, 500 Gbit/s, 600 Gbit/s To achieve enhanced protection, specify **Elastic Protection Bandwidth**.

Parameter	Description
Elastic Protection Bandwidth	You can change the elastic protection bandwidth three times a day for each instance. Value range: 10 Gbit/s to 100 Gbit/s, 200 Gbit/s, 300 Gbit/s, 400 Gbit/s, 500 Gbit/s, 600 Gbit/s, 700 Gbit/s, 800 Gbit/s, 1000 Gbit/s 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.
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, this duration may vary based on the number of black holes triggered within the current day and the peak attack traffic. **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 (only attack events can be recorded)	√	√
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 Function

This section describes the main functions supported by Advanced Anti-DDoS. For detailed information on region availability of each feature, you can refer to the console.

Blacklist and Whitelist

You can configure an IP address blacklist or whitelist to block or allow access requests from specified IP addresses. For more information, see **Blocking or Permitting Traffic from Specified IP Addresses Using a Blacklist and Whitelist**.

Region Blacklist

Advanced Anti-DDoS can block traffic in a specified region. Once the policy is in effect, access traffic from the designated region will be discarded. For more information, see **Blocking Traffic From Specified Locations**.

Protocol-based Blocking

Advanced Anti-DDoS offers a one-click mode to block traffic based on protocol type. If there is no UDP service, you are advised to disable the UDP protocol. Once the UDP protocol blocking is enabled, the rate of UDP access traffic will be restricted if it exceeds 2 Mbit/s. For more information, see **Blocking Traffic of a Specified Protocol**.

Frequency Control Rules

You can set frequency control rules to limit the access frequency of a single IP address, cookie, or referer to the origin server of a protected website. You can also enable policy-based, domain name, and URL rate limiting to identify and mitigate CC attacks. For more information, see **Mitigating CC Attacks Using Frequency Control Policies**.

Intelligent CC

If you enable intelligent CC attack protection, Advanced Anti-DDoS uses built-in AI-powered models to analyze traffic to your website, identify CC attacks and abnormal features in HTTP requests on the origin server, and generate specific precise protection and access control rules for your website. In this way, Advanced Anti-DDoS can then automatically protect your website from CC attacks. For more information, see **Using Intelligent CC Policies to Defend Against CC Attacks**.

Alarm Notification

After you enable alarm notifications, a notification message will be sent to you (through the method you have configured) when an IP address is under DDoS attacks or elastic billing is triggered. For more information, see **Enabling Alarm Notifications for DDoS Attacks**.

Attack Logs

After you authorize Advanced Anti-DDoS to access Log Tank Service (LTS), you can use the logs recorded by LTS for quick and efficient real-time analysis, device O&M management, and analysis of service trends. For more information, see **Enabling Logging**.

Data Report

After your services are connected to Advanced Anti-DDoS, you can view the DDoS and CC attack protection reports to learn about the network security status of your services. For more information, see **Viewing Statistics**.

Event Monitoring

Cloud Eye can monitor Advanced Anti-DDoS events and generate alarms when events such as black hole, scheduling, and attacks occur. It helps you learn about the protection status of Advanced Anti-DDoS in a timely manner. For more information, see **Setting Event Alarm Notifications**.

Audit Logs

After you enable CTS, the system starts recording operations on Anti-DDoS Service. You can view the operation records of the last 7 days on the CTS console. For more information, see **Viewing CTS Traces**.

2.4.5 Advantages

Compared with traditional Hardware-based DDoS protection, Advanced Anti-DDoS provides instantaneous protection once you connect your services to the service. You can view DDoS attack protection logs to learn the network security status of your services in real time.

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

Edition Differences

Table 3-1 Edition Differences

Product	CNAD Basic (Anti-DDoS)	CNAD Advanced	AAD
Billing Mode	Free	Yearly/Monthly, pay-per-use for clean traffic	Yearly/Monthly, "basic bandwidth + elastic bandwidth"
Protected Objects	Huawei Cloud EIPs	Huawei Cloud EIPs	Chinese mainland: Internet-accessible domain names, IP addresses, and ports Outside the Chinese mainland: Internet-accessible domain names, IP addresses, and ports
Access Mode	Transparent network access through the Huawei Cloud native network, ensuring low latency.	Transparent network access through the Huawei Cloud native network, ensuring low latency.	Access via DNS redirection or direct IP address leveraging multi-line BGP, yielding strong protection capabilities.
Protection Capability	• Chinese mainland: no higher than 5 Gbit/s • Outside the Chinese mainland: no more than 500 Mbit/s	20 Gbit/s to 1 Tbit/s. The protection capability varies depending on the instance specifications. For details, see **Table 3-2**.	Up to 1 Tbit/s. Instances of different access types cannot be used together. For details, see **Table 3-3**.

Product	CNAD Basic (Anti-DDoS)	CNAD Advanced	AAD
Attack Type	Transport-layer DDoS attacks, such as malformed packet attacks and SYN flood attacks	Transport-layer DDoS attacks, such as malformed packet attacks and SYN flood attacks Connection-based DDoS attacks (supported only by Unlimited Protection Advanced Edition)	Transport-layer DDoS attacks, such as malformed packet attacks and SYN flood attacks Connection-based DDoS attacks, DNS DDoS attacks, and web application-layer DDoS attacks

Instance Specifications

Table 3-2 Specifications of different types of CNAD Advanced instances

Type	CNAD 1.0		CNAD 2.0	
Edition	Unlimited Protection Basic Edition	Unlimited Protection Advanced Edition	Enterprise Edition	SME Edition
Billing Mode	Yearly/ Monthly	Yearly/ Monthly	• The instance is billed on a yearly/ monthly basis. • Service bandwidth can be billed on a yearly/monthly or pay-per-use basis.	• The instance is billed on a yearly/monthly basis. • The public network line billing mode is only available for yearly/ monthly billing.
Protected objects	Huawei Cloud dynamic BGP EIPs	Anti-DDoS Service dedicated EIPs	• Chinese mainland: Dynamic BGP EIPs and Anti-DDoS Service dedicated EIPs • Outside the Chinese mainland: Premium BGP EIPs and Anti-DDoS Service dedicated EIPs	Chinese mainland: Dynamic BGP EIPs and Anti-DDoS Service dedicated EIPs

Type	CNAD 1.0		CNAD 2.0	
Edition	**Unlimited Protection Basic Edition**	**Unlimited Protection Advanced Edition**	**Enterprise Edition**	**SME Edition**
Region	Single-region protection	Single-region protection	• Chinese mainland: Cross-region protection is supported. • Outside the Chinese mainland: Only Hong Kong and Singapore are supported.	Chinese mainland: Select resources of any region in China for protection.
Protocol	IPv4 and IPv6	IPv4	IPv4 and IPv6	IPv4 or IPv6
Protected Objects (per Instance)	50 to 500	50 to 500	50 to 1,000	1 to 1,000
Service Bandwidth	100 Mbit/s to 20 Gbit/s	100 Mbit/s to 10 Gbit/s	100 Mbit/s to 20 Gbit/s	50 Mbit/s to 20 Gbit/s

Type	CNAD 1.0		CNAD 2.0	
Edition	**Unlimited Protection Basic Edition**	**Unlimited Protection Advanced Edition**	**Enterprise Edition**	**SME Edition**
Protection Capability	• Shared unlimited protection, no less than 20 Gbit/s, up to hundreds of Gbit/s. • If the service bandwidth exceeds the limit, the protection capability drops and ranges from 10 Gbit/s to 20 Gbit/s.	• Shared unlimited protection for up to 1 Tbit/s • If the service bandwidth exceeds the limit, the protection capability drops and ranges from 10 Gbit/s to 20 Gbit/s.	• Chinese mainland: Shared unlimited protection for at least 20 Gbit/s and up to 1 Tbit/s If the service bandwidth exceeds the limit, the protection capability drops and ranges from 10 Gbit/s to 20 Gbit/s. • Outside the Chinese mainland: carrier-based cross-border protection for up to 1 Tbit/s If the service bandwidth exceeds the limit, the protection capability drops to 5 Gbit/s.	Chinese mainland: Shared unlimited protection for at least 20 Gbit/s and up to 1 Tbit/s If the service bandwidth exceeds the limit, the protection capability drops and ranges from 10 Gbit/s to 20 Gbit/s.

Table 3-3 AAD instance specifications

Item	AAD - Website	AAD - IP Access
Billing Mode	Yearly/Monthly	Yearly/Monthly
Protected Object	Internet-accessible domain names	Internet-accessible IP addresses and ports

Item	AAD - Website	AAD - IP Access
Region	Chinese mainland and outside the Chinese mainland	Chinese mainland and outside the Chinese mainland
Protocol	• Chinese mainland: IPv4 and IPv6 • Outside the Chinese mainland: IPv4	• Chinese mainland: IPv4 and IPv6 • Outside the Chinese mainland: IPv4
Protected Objects (per Instance)	• Chinese mainland: up to 500 • Outside the Chinese mainland: up to 200	• Chinese mainland: up to 500 • Outside the Chinese mainland: up to 200
Service bandwidth	Up to 2000 Mbit/s	Up to 2000 Mbit/s
Elastic Bandwidth	Supported	Supported
Protection Capability	Up to 1 Tbit/s	Up to 1 Tbit/s
QPS	Up to 100,000 QPS	-

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.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in **Figure 4-1**.

- **Huawei Cloud**: Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer**: As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

Figure 4-1 Huawei Cloud shared security responsibility model

Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in **Figure 4-1**, customers can select different cloud service types (such as IaaS, PaaS, and SaaS) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the PaaS middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

On-premises (On-Prem): Software and IT infrastructure that are deployed and managed by customers within their own data centers, rather than be deployed by remote cloud service providers.

Infrastructure as a Service (IaaS): Cloud service providers offer compute, network, storage, and more infrastructure services, including **Elastic Cloud Server (ECS)**, **Virtual Private Network (VPN)**, and **Object Storage Service (OBS)**.

Platform as a Service (PaaS): Cloud service providers deliver platforms required for application development and deployment, such as **ModelArts** and **GaussDB**. Customers do not need to maintain the underlying infrastructure.

Software as a Service (SaaS): Cloud service providers offer complete application software, such as **Huawei Cloud Meeting**. Customers use the software directly without the need to install the application, maintain it, or manage its underlying platform or infrastructure.

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.
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.

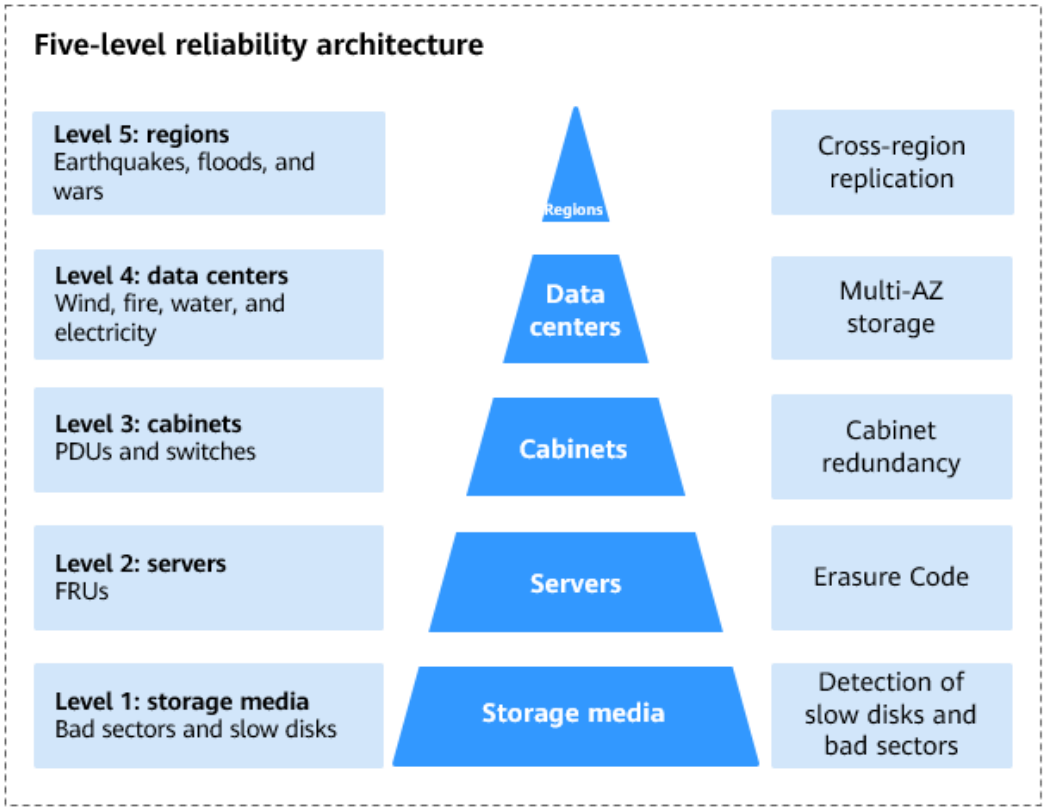
CTS allows you to configure key event notification. You can add DDoS-related high-risk and sensitive operations as key operations to be monitored and tracked by CTS. If a key operation in the monitoring list is triggered when a user uses Anti-DDoS, CTS records the operation log and sends a notification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

4.5 Service Resilience

Huawei Cloud Anti-DDoS Service has a global presence, with data centers strategically located worldwide. All data centers are operational. For added resilience, two data centers in separate cities are configured as disaster recovery sites for each other. In the event that a data center in City A experiences an outage, the corresponding data center in City B will seamlessly take over, ensuring uninterrupted service delivery and regulatory compliance. To mitigate the impact of hardware failures, natural disasters, or other catastrophic events, Huawei Cloud Anti-DDoS Service implements a comprehensive Disaster Recovery (DR) plan.

The Anti-DDoS Service's five-level reliability architecture ensures high availability, fault tolerance, and scalability.

With a multi-zone deployment model, Huawei Cloud Anti-DDoS Service caters to global customers and offers enhanced redundancy. Key components, including the management plane and engines, are deployed in active/standby or clustered configurations to guarantee high uptime and minimal service disruptions.



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.

Sub-service	Monitored Object	Monitored Item
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

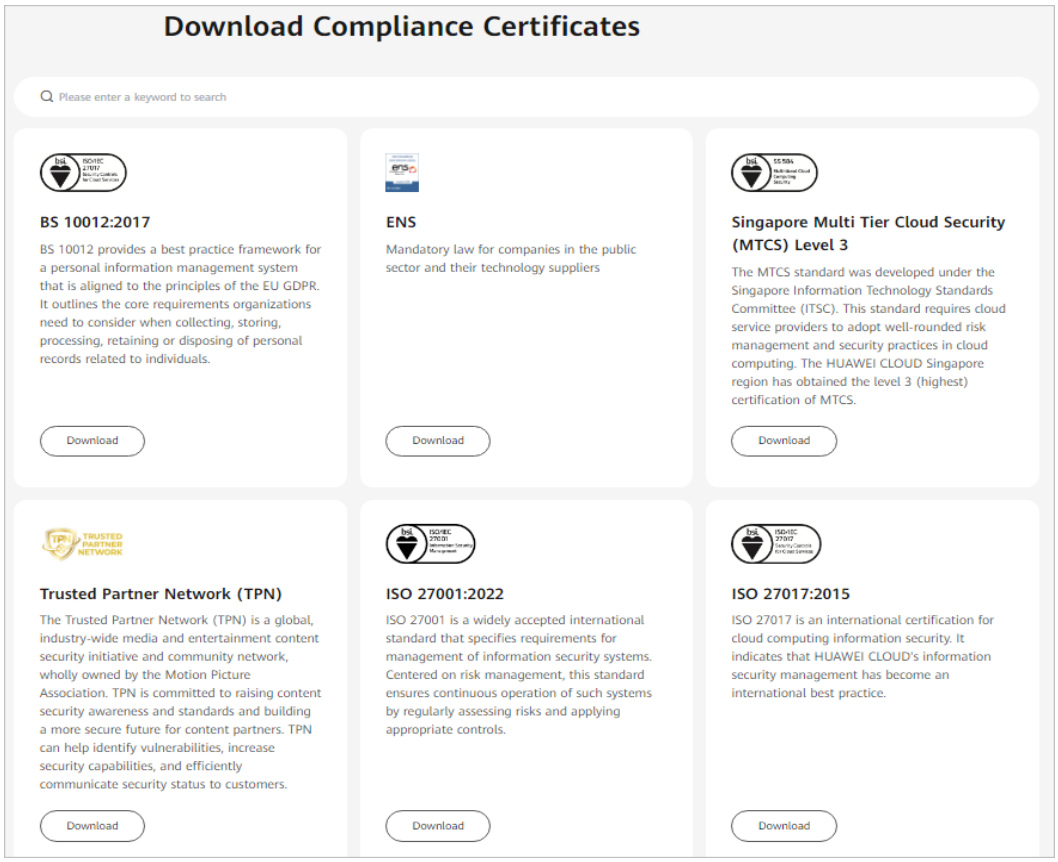
Anti-DDoS works with Cloud Eye to monitor the protected resources in your account in real time, reporting alarms and sending notifications based on your settings. You can obtain the information about the protected resources in real time.

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.

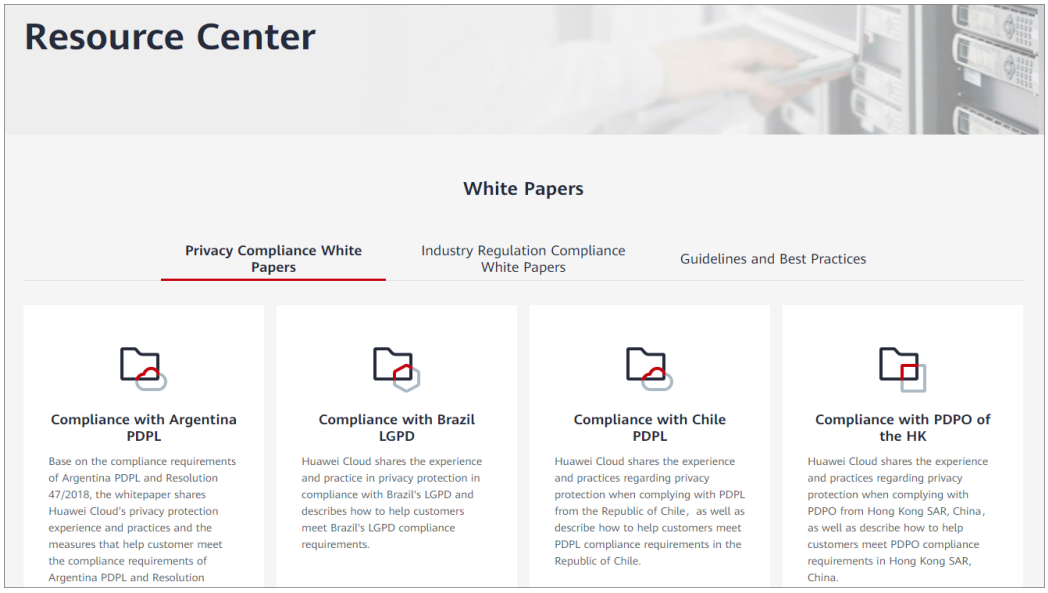
Figure 4-2 Downloading compliance certificates



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 Limitations and Constraints

This section describes some limitations and constraints on using Anti-DDoS Service.

Protected Objects

Sub-service	Service Edition	Projected Object	Region
CNAD Basic	Free of charge	Huawei Cloud EIPs	Region where the EIP is located.
CNAD Advanced	Standard	Huawei Cloud dynamic BGP EIPs	Region where cloud resources are located. Multi-region protection is not supported.
	Unlimited Protection Basic Edition	Huawei Cloud dynamic BGP EIPs	Region where cloud resources are located. Multi-region protection is not supported.
	Unlimited Protection Advanced Edition	Dedicated EIPs of Huawei Cloud Anti-DDoS Service	Region where cloud resources are located. Multi-region protection is not supported.
	Cloud Native Anti-DDoS 2.0	• Chinese Mainland: Huawei Cloud dynamic BGP EIPs and Anti-DDoS dedicated EIPs • Other regions: Premium BGP EIPs and Anti-DDoS dedicated EIPs of Huawei Cloud	• Multi-region protection is supported in the Chinese mainland. • Only Hong Kong and Singapore are supported outside the Chinese mainland.
AAD	AAD	Protected domain names and dedicated high-defense IP addresses	There is no region restriction.

Protection Quotas

- CNAD Advanced
  - Standard Edition: Each instance can protect one EIP up to 10 times, supports IP address changes up to 5 times, and provides a service bandwidth of 100 Mbit/s.
  - Unlimited Protection Basic Edition: Each instance can protect up to 500 dynamic BGP EIPs, with a maximum service bandwidth of 20,000 Mbit/s.
  - Unlimited Protection Advanced Edition: Each instance can protect up to 500 Anti-DDoS Service dedicated EIPs, with a maximum service bandwidth of 10,000 Mbit/s.
  - CNAD 2.0 in the Chinese mainland: Each instance can protect up to 1000 EIPs with a maximum service bandwidth of 20,000 Mbit/s (pay-per-use billing supported). CNAD 2.0 in other regions: Each instance can protect up to 500 EIPs.
- AAD
  - Chinese mainland: Each instance can protect up to 500 domain names, with 2,000 Mbit/s service bandwidth and 1,000 Gbit/s protection bandwidth. For IP access, each instance supports up to 500 forwarding rules, 1,000 Gbit/s protection bandwidth, and 2,000 Mbit/s service bandwidth.
  - Other regions: Each instance can protect up to 200 domain names, with a maximum of 2,000 Mbit/s service bandwidth. For IP access, each instance supports up to 200 forwarding rules with a maximum of 2,000 Mbit/s service bandwidth.
- Anti-DDoS scheduling center: Each scheduling rule supports scheduling for up to 10 IP addresses, with each user supporting a maximum of 500 scheduling rules.

Domain Name Access

- **ICP filing** must be conducted on the domain names to be connected to AAD.
- A maximum of 20 origin server IP addresses or one origin server domain name (for example, www.domain.com) is supported. A wildcard domain name can be *.domain.com.

6 Permissions Management

6.1 CNAD Basic

If you need to assign different permissions to employees in your enterprise to access your CNAD Basic resources, IAM is an ideal choice for fine-grained permissions management. IAM provides functions such as identity authentication, permissions management, and access control. If your Huawei Cloud account does not require IAM for permissions management, you can skip this section.

IAM can be used free of charge. You pay only for the resources in your account.

With IAM, you can control the access to Huawei Cloud resources through authorization. For example, if you want certain software developers in your enterprise to use CNAD Basic without the ability to delete resources or perform high-risk operations, you can grant them only the necessary permissions for using CNAD Basic resources.

IAM supports role/policy-based authorization and identity policy-based authorization.

The differences and relationships between the two authorization models are as follows:

Table 6-1 Differences between role/policy-based authorization and identity policy-based authorization

Authorization Model	Core Relationship	Permission	Authorization Method	Scenario
Role/Policy-based Authorization	User-permission-authorization scope	• System-defined roles • System-defined policies • Custom policies	Granting a role or policy to a subject	To authorize a user, you need to add it to a user group first and then specify the scope of authorization. It is hard to provide fine-grained permissions control using authorization by user groups and a limited number of condition keys. This method is suitable for small- and medium-sized enterprises.
Identity Policy-based Authorization	User-policy	• System-defined identity policies • Custom identity policies	• Granting an identity policy to a subject • Attaching identity policies to principals	You can authorize a user by attaching an identity policy to it. User-specific authorization and a variety of key conditions allow for more fine-grained permissions control. However, this model can be hard to set up. It requires a certain amount of expertise and is suitable for medium- and large-sized enterprises.

Assume that you want to grant IAM users the permissions needed to create ECSs in CN North-Beijing4 and OBS buckets in CN South-Guangzhou. With role/policy-based authorization, the administrator needs to create two custom policies and assign both to the IAM users. With identity policy-based authorization, the administrator only needs to create one custom identity policy and configure the condition key **g:RequestedRegion** for the policy, and then attach the policy to the principals or grant the principals the access permissions to the specified regions. Identity policy-based authorization is more flexible than role/policy-based authorization.

Policies/identity policies and actions in the two authorization scenarios are not interoperable. You are advised to use the identity policy-based authorization model. **Role/Policy-based Permissions Management** and **Identity Policy-based Permissions Management** describe the system permissions of the two models.

For details about IAM, see **IAM Service Overview**.

Role/Policy-based Permissions Management

CNAD Basic supports role/policy-based authorization. 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 Basic is a project-level service deployed and accessed in specific physical regions. When you set **Scope** to **Region-specific projects** and select the specified projects (for example, **ap-southeast-2**) in the specified regions (for example, **AP-Bangkok**), the users only have permissions for resources in the selected projects. If you set **Scope** to **All resources**, the users have permissions for resources in all region-specific projects. When accessing Anti-DDoS, the users need to switch to a region where they have been authorized.

Table 1 lists all CNAD Basic system permissions. System-defined policies in role/policy-based authorization and identity policy-based authorization are not interoperable.

Table 6-2 CNAD Basic system permissions

Role/Policy Name	Description	Type
Anti-DDoS Administrator	Administrator permissions for CNAD Basic.	System-defined role
Anti-DDoS FullAccess	All permissions for CNAD Basic	System-defined policy
Anti-DDoS ReadOnlyAccess	Read-only permissions for CNAD Basic	System-defined policy

Table 6-3 lists the common operations supported by each system-defined policy or role of CNAD Basic. Select the policies or roles as required.

Table 6-3 Common operations supported by system-defined policies of CNAD Basic

Operation	Anti-DDoS Administrator	Anti-DDoS FullAccess	Anti-DDoS ReadOnlyAccess
Querying the default protection policy of CNAD Basic	√	√	√

Operation	Anti-DDoS Administrator	Anti-DDoS FullAccess	Anti-DDoS ReadOnlyAccess
Configuring the default protection policy of CNAD Basic	√	√	×
Deleting the default protection policy of CNAD Basic	√	√	×
Querying CNAD Basic specifications	√	√	√
Querying configured CNAD Basic policies	√	√	√
Updating CNAD Basic policies	√	√	×
Enabling CNAD Basic	√	√	×
Querying weekly defense statistics	√	√	√
Querying the traffic of a specified EIP	√	√	√
Querying events of a specified EIP	√	√	√
Querying the defense status of a specified EIP	√	√	√
Querying the list of defense statuses of EIPs	√	√	√

Operation	Anti-DDoS Administrator	Anti-DDoS FullAccess	Anti-DDoS ReadOnlyAccess
Querying Anti-DDoS tasks	√	√	√
Querying alarm configuration	√	√	√
Updating alarm configuration	√	√	×
Querying LTS configurations	√	√	√
Updating LTS configurations	√	√	×
Querying quotas	√	√	√
Querying resource tags	√	√	√

Roles or policies on which the Cloud Native Anti-DDoS Basic console depends

Table 6-4 Roles or policies of services on which the Cloud Native Anti-DDoS Basic console depends

Console Function	Dependent Services	Policy/Role Required
Configuring CNAD Basic logs on LTS	Log Tank Service (LTS)	The **LTS ReadOnlyAccess** system policy is required to select log group and log stream names created in LTS.
Enabling alarm notifications	Simple Message Notification (SMN)	The **SMN ReadOnlyAccess** system policy is required to obtain SMN topic groups.
Querying tags	Tag Management Service (TMS)	The TMS ReadOnlyAccess system policy is required to query tags.

Identity Policy-based Permissions Management

CNAD Basic supports identity policy-based authorization. **Table** shows all system-defined identity policies of CNAD Basic. System-defined identity policies and system-defined policies in the two authorization models are not interoperable.

Table 6-5 System-defined identity policies of CNAD Basic

Policy Name	Description	Policy Type
Anti-DDoSFullAccessPolicy	All permissions for CNAD Basic.	System-defined
Anti-DDoSReadOnlyPolicy	Read-only permissions for CNAD Basic. Users granted these permissions can only view CNAD Basic information.	System-defined

Table 6-6 lists the common operations supported by CNAD Basic system-defined identity policies.

Table 6-6 Common operations supported by system-defined identity policies of CNAD Basic

Operation	Anti-DDoSFullAccessPolicy	Anti-DDoSReadOnlyPolicy
Querying the default protection policy of CNAD Basic	√	√
Configuring the default protection policy of CNAD Basic	√	×
Deleting the default protection policy of CNAD Basic	√	×
Querying CNAD Basic specifications	√	√
Querying configured CNAD Basic policies	√	√
Updating CNAD Basic policies	√	×
Enabling CNAD Basic	√	×
Querying weekly defense statistics	√	√

Operation	Anti-DDoSFullAccessPolicy	Anti-DDoSReadOnlyPolicy
Querying the traffic of a specified EIP	√	√
Querying events of a specified EIP	√	√
Querying the defense status of a specified EIP	√	√
Querying the list of defense statuses of EIPs	√	√
Querying Anti-DDoS tasks	√	√
Querying alarm configuration	√	√
Updating alarm configuration	√	×
Querying LTS configurations	√	√
Updating LTS configurations	√	×
Querying quotas	√	√
Querying resource tags	√	√

Identity Policies on Which Console Functions Depend

Table 6-7 Identity policies for services on which the CNAD Basic console functions depend

Console Function	Dependent Services	Identity Policy Required
Configuring Anti-DDoS logs on LTS	Log Tank Service (LTS)	The log groups and log streams created in LTS can be selected only after the **LTSReadOnlyAccessPolicy** system identity policy is added.
Enabling alarm notifications	Simple Message Notification (SMN)	SMN topic groups can be obtained only after the **SMNReadOnlyPolicy** system identity policy is added.

Console Function	Dependent Services	Identity Policy Required
Querying tags	Tag Management Service (TMS)	Tags can be queried only after the system identity policy **TMSReadOnlyPolicy** is added.

Helpful Links

- **IAM Service Overview**
- **Using IAM to Grant Anti-DDoS Permissions**

6.2 CNAD Advanced

If you need to assign different permissions to personnel in your enterprise to access your CNAD Advanced resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides functions such as identity authentication, permissions management, and access control. If your Huawei account works good for you and you do not need an IAM account to manage user permissions, then you may skip over this chapter.

IAM can be used free of charge. You pay only for the resources in your account.

With IAM, you can control the access to Huawei Cloud resources through authorization. For example, you can allow some software developers in your enterprise to access CNAD Advanced resources without giving them the ability to delete CNAD Advanced instances or perform other risky actions. To do this, you can create IAM users and assign them the appropriate permissions.

IAM supports role/policy-based authorization and identity policy-based authorization.

The differences and relationships between the two authorization models are as follows:

Table 6-8 Differences between role/policy-based authorization and identity policy-based authorization

Authorization Model	Core Relationship	Permission	Authorization Method	Scenario
Role/Policy-based Authorization	User-permission-authorization scope	• System-defined roles • System-defined policies • Custom policies	Granting a role or policy to a subject	To authorize a user, you need to add it to a user group first and then specify the scope of authorization. It is hard to provide fine-grained permissions control using authorization by user groups and a limited number of condition keys. This method is suitable for small- and medium-sized enterprises.
Identity Policy-based Authorization	User-policy	• System-defined identity policies • Custom identity policies	• Granting an identity policy to a subject • Attaching identity policies to principals	You can authorize a user by attaching an identity policy to it. User-specific authorization and a variety of key conditions allow for more fine-grained permissions control. However, this model can be hard to set up. It requires a certain amount of expertise and is suitable for medium- and large-sized enterprises.

Assume that you want to grant IAM users the permissions needed to create ECSs in CN North-Beijing4 and OBS buckets in CN South-Guangzhou. With role/policy-based authorization, the administrator needs to create two custom policies and assign both to the IAM users. With identity policy-based authorization, the administrator only needs to create one custom identity policy and configure the condition key **g:RequestedRegion** for the policy, and then attach the policy to the principals or grant the principals the access permissions to the specified regions. Identity policy-based authorization is more flexible than role/policy-based authorization.

Policies/identity policies and actions in the two authorization scenarios are not interoperable. You are advised to use the identity policy-based authorization model. **Role/Policy-based Permissions Management** and **Identity Policy-based Permissions Management** describe the system permissions of the two models.

For details about IAM, see **IAM Service Overview**.

Role/Policy-based Permissions Management

CNAD Advanced supports role/policy-based authorization. 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 Advanced is a project-level service and is deployed in different physical regions. When you set **Scope** to **Region-specific projects** and select the specified projects (for example, **ap-southeast-2**) in the specified regions (for example, **AP-Bangkok**), the users only have permissions for ECSs in the selected projects. If you set **Scope** to **All resources**, the users have permissions for ECSs in all region-specific projects. When accessing CNAD Advanced, users need to switch to a region where they have been authorized.

Table 2 lists all system permissions of CNAD Advanced. System-defined policies in role/policy-based authorization and identity policy-based authorization are not interoperable.

Table 6-9 System-defined permissions for CNAD

Role/Policy Name	Description	Type
CNAD FullAccess	All permissions for CNAD Advanced.	System-defined policy
CNAD ReadOnlyAccess	Read-only permissions for CNAD Advanced.	System-defined policy

Table 6-10 describes the common operations supported by each system-defined permission of CNAD. Select the permissions as needed.

Table 6-10 Common operations supported by system policy of CNAD Advanced

Operation	CNAD ReadOnlyAccess	CNAD FullAccess
Querying quotas	√	√
Querying details about a protection policy	√	√
Querying statistics	√	√
Querying asset security status	√	√
Querying weekly security statistics	√	√

Operation	CNAD ReadOnlyAccess	CNAD FullAccess
Creating an alarm notification	×	√
Deleting an alarm notification	×	√
Querying an alarm notification	√	√
Upgrading an instance	×	√
Binding a protected IP address to an instance	×	√
Creating a protection policy	×	√
Updating a protection policy	×	√
Deleting a protection policy.	×	√
Binding a protection policy to a protected IP address	×	√
Removing a protection policy from a protected IP address	×	√
Adding a blacklist or whitelist rule	×	√
Deleting a blacklist or whitelist rule	×	√
Updating the tag of a protected IP address	×	√
Querying the scrubbing scope	√	√
Querying the instance list	√	√
Querying the protection policy list	√	√
Querying the list of protected IP addresses	√	√
Querying details of an instance	√	√

Operation	CNAD ReadOnlyAccess	CNAD FullAccess
Querying details of a protection policy	√	√
Querying the list of protected IP addresses	√	√
Querying total traffic	√	√
Querying attack traffic	√	√
Querying the total number of data packets	√	√
Querying the number of attack packets	√	√
Querying DDoS mitigation trend	√	√
Querying the peak traffic scrubbed	√	√
Querying attack types	√	√
Querying attack events	√	√
Querying top 10 attacked IP addresses	√	√
Creating an instance	×	√

Roles or Policies Required for Operations on the CNAD Advanced Console

Table 6-11 Roles or policies that are required for performing operations on the CNAD Advanced console

Console Function	Dependent Services	Policy/Role Required
Enabling LTS	Log Tank Service (LTS)	The **LTS ReadOnlyAccess** system policy is required to select log group and log stream names created in LTS.
Enabling alarm notifications	Simple Message Notification (SMN)	The **SMN ReadOnlyAccess** system policy is required to obtain SMN topic groups.
Configuring instance tags	Tag Management Service (TMS)	Tag keys can be created only after the **TMS FullAccess** system policy is added.

Console Function	Dependent Services	Policy/Role Required
Purchasing a CNAD Instance	Enterprise Project Management Service (EPS)	You can select an enterprise project when purchasing an instance only after adding the **EPS ReadOnlyAccess** system policy.

Identity Policy-based Permissions Management

CNAD Advanced supports identity policy-based authorization. **Table 1** lists all the system-defined identity policies for CNAD Advanced. System-defined identity policies and system-defined policies in the two authorization models are not interoperable.

Table 6-12 System-defined identity policies for CNAD Advanced

Policy Name	Description	Policy Type
CNADReadOnlyPolicy	Read-only permissions for CNAD Advanced. Users granted these permissions can only view CNAD Advanced information.	System-defined identity policies
CNADFullAccessPolicy	All permissions for CNAD Advanced.	System-defined identity policies

Table 6-13 lists the common operations supported by system-defined identity policies of CNAD Advanced.

Table 6-13 Common operations supported by system-defined identity policies of CNAD Advanced

Operation	CNADReadOnlyPolicy	CNADFullAccessPolicy
Querying quotas	√	√
Querying details about a protection policy	√	√
Querying statistics	√	√
Querying asset security status	√	√
Querying weekly security statistics	√	√

Operation	CNADReadOnlyPolicy	CNADFullAccessPolicy
Creating an alarm notification	×	√
Deleting an alarm notification	×	√
Querying an alarm notification	√	√
Upgrading an instance	×	√
Binding a protected IP address to an instance	×	√
Creating a protection policy	×	√
Updating a protection policy	×	√
Deleting a protection policy.	×	√
Binding a protection policy to a protected IP address	×	√
Removing a protection policy from a protected IP address	×	√
Adding a blacklist or whitelist rule	×	√
Deleting a blacklist or whitelist rule	×	√
Updating the tag of a protected IP address	×	√
Querying the scrubbing scope	√	√
Querying the instance list	√	√
Querying the protection policy list	√	√
Querying the list of protected IP addresses	√	√
Querying details of an instance	√	√

Operation	CNADReadOnlyPolicy	CNADFullAccessPolicy
Querying details of a protection policy	√	√
Querying the list of protected IP addresses	√	√
Querying total traffic	√	√
Querying attack traffic	√	√
Querying the total number of data packets	√	√
Querying the number of attack packets	√	√
Querying DDoS mitigation trend	√	√
Querying the peak traffic scrubbed	√	√
Querying attack types	√	√
Querying attack events	√	√
Querying top 10 attacked IP addresses	√	√
Creating an instance	×	√

Identity Policies on Which Console Functions Depend

Table 6-14 Identity policies of services on which Cloud Native Anti-DDoS Basic console functions depend

Console Function	Dependent Services	Policy/Role Required
Enabling LTS	Log Tank Service (LTS)	The log groups and log streams created in LTS can be selected only after the **LTSReadOnlyAccessPolicy** system identity policy is added.
Enabling alarm notifications	Simple Message Notification (SMN)	SMN topic groups can be obtained only after the **SMNReadOnlyPolicy** system identity policy is added.

Console Function	Dependent Services	Policy/Role Required
Configuring instance tags	Tag Management Service (TMS)	Tag keys can be created only after the **TMSReadOnlyPolicy** system identity policy is added.
Purchasing a CNAD Advanced instance	Enterprise Project Management Service (EPS)	Enterprise projects can be selected only after the **EPSReadOnlyPolicy** system identity policy is added.

Helpful Links

- **IAM Service Overview**
- **Using IAM to Grant Anti-DDoS Permissions**
- **Anti-DDoS Permissions and Actions**

6.3 AAD

If you need to assign different permissions to personnel in your enterprise to access your AAD resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides functions such as identity authentication, permissions management, and access control. If your Huawei account works good for you and you do not need an IAM account to manage user permissions, then you may skip over this chapter.

IAM can be used free of charge. You pay only for the resources in your account.

With IAM, you can control the access to Huawei Cloud resources through authorization. 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.

There are two types of IAM authorization: policy/role authorization and identity policy authorization.

The differences and relationships between the two authorization models are as follows:

Table 6-15 Differences between role/policy-based authorization and identity policy-based authorization

Authorization Model	Authorization Using	Permission	Authorization Method	Scenario
Role/Policy-based Authorization	User-permission-authorization scope	• System-defined roles • System-defined policies • Custom policies	Granting a role or policy to a subject	To authorize a user, you need to add it to a user group first and then specify the scope of authorization. It is hard to provide fine-grained permissions control using authorization by user groups and a limited number of condition keys. This method is suitable for small- and medium-sized enterprises.
Identity Policy-based Authorization	User-policy	• System-defined identity policies • Custom identity policies	• Granting an identity policy to a subject • Attaching identity policies to principals	You can authorize a user by attaching an identity policy to it. User-specific authorization and a variety of key conditions allow for more fine-grained permissions control. However, this model can be hard to set up. It requires a certain amount of expertise and is suitable for medium- and large-sized enterprises.

Assume that you want to grant IAM users the permissions needed to create ECSs in CN North-Beijing4 and OBS buckets in CN South-Guangzhou. With role/policy-based authorization, the administrator needs to create two custom policies and assign both to the IAM users. With identity policy-based authorization, the administrator only needs to create one custom identity policy and configure the condition key **g:RequestedRegion** for the policy, and then attach the policy to the principals or grant the principals the access permissions to the specified regions. Identity policy-based authorization is more flexible than role/policy-based authorization.

Policies/identity policies and actions in the two authorization scenarios are not interoperable. You are advised to use the identity policy-based authorization model. **Role/Policy-based Permissions Management** and **Identity Policy-based Permissions Management** describe the system permissions of the two models.

For details about IAM, see **IAM Service Overview**.

Role/Policy-based Permissions Management

AAD supports role/policy-based authorization. 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 deployed and accessed without specifying any physical region. AAD permissions are assigned to users in the global project, and users do not need to switch regions when accessing AAD.

Table 1 lists all AAD system permissions. System-defined policies in role/policy-based authorization and identity policy-based authorization are not interoperable.

Table 6-16 System-defined permissions for AAD

Role/Policy Name	Description	Type
CAD Administrator	Administrator permissions for AAD. This role has all permissions for AAD.	System-defined role
AAD FullAccess	All permissions for AAD	System-defined policy
AAD ReadOnlyAccess	Read-only permissions for AAD.	System-defined policy

Table 6-17 describes the common operations supported by each system-defined permission of AAD. Select the permissions as needed.

Table 6-17 Common operations supported by system permissions of AAD

Operation	CAD Administrator	AAD ReadOnlyAccess	AAD FullAccess
Querying details of an instance	√	√	√
Querying the instance list	√	√	√
Creating an instance	√	×	√
Modifying an instance	√	×	√
Querying the certificate list	√	√	√
Uploading a certificate	√	×	√

Operation	CAD Administrator	AAD ReadOnlyAccess	AAD FullAccess
Deleting a certificate	√	×	√
Obtaining domain name details	√	√	√
Obtaining the domain name list	√	√	√
Adding a domain name.	√	×	√
Editing a domain name	√	×	√
Deleting a domain name	√	×	√
Querying a protection policy	√	√	√
Querying the list of domain names with an enabled protection policy	√	√	√
Creating a protection policy	√	×	√
Updating a protection policy	√	×	√
Deleting a protection policy.	√	×	√
Creating a blacklist or whitelist rule	√	×	√
Deleting a blacklist or whitelist rule	√	×	√
Querying the blacklist and whitelist rule list	√	√	√
Querying quotas	√	√	√
Querying a forwarding rule	√	√	√
Exporting forwarding rules	√	×	√
Adding a forwarding rule	√	×	√

Operation	CAD Administrator	AAD ReadOnlyAccess	AAD FullAccess
Modifying a forwarding rule	√	×	√
Deleting a forwarding rule	√	×	√
Viewing statistics reports	√	√	√
Querying an alarm notification	√	√	√
Creating an alarm notification	√	×	√

Roles or Policies on Which AAD Console Functions Depend

Table 6-18 Roles or policies required for AAD console operations

Console Function	Dependent Services	Policy/Role Required
Adding a domain name	Cloud Certificate Manager (CCM)	If the origin server uses the HTTPS forwarding protocol, pulling certificates requires the **SCM ReadOnlyAccess** permission.
Configuring AAD logs	Log Tank Service (LTS)	The **LTS ReadOnlyAccess** system policy is required to select log group and log stream names created in LTS.
Enabling alarm notifications	Simple Message Notification (SMN)	The **SMN ReadOnlyAccess** system policy is required to obtain SMN topic groups.
Configuring instance tags	Tag Management Service (TMS)	Tag keys can be created only after the **TMS FullAccess** system policy is added.
Purchasing an AAD instance	Enterprise Project Management Service (EPS)	You can select an enterprise project when purchasing an instance only after adding the **EPS ReadOnlyAccess** system policy.

Identity Policy-based Permissions Management

AAD supports identity policy-based authorization. **Table 1** lists all the system-defined identity policies for AAD. System-defined identity policies and system-defined policies in the two authorization models are not interoperable.

Table 6-19 System-defined identity policies of AAD

Policy Name	Description	Policy Type
AADReadOnlyAccess-Policy	All permissions for AAD	System-defined identity policies
AADFullAccessPolicy	Read-only permissions for AAD. Users granted these permissions can only view AAD information.	System-defined identity policies

Table 6-20 lists the common operations supported by system-defined identity policies of AAD.

Table 6-20 Common operations supported by system-defined identity policies of AAD

Operation	AADReadOnlyAccessPolicy	AADFullAccessPolicy
Querying details of an instance	√	√
Querying the instance list	√	√
Creating an instance	×	√
Modifying an instance	×	√
Querying the certificate list	√	√
Uploading a certificate	×	√
Deleting a certificate	×	√
Obtaining domain name details	√	√
Obtaining the domain name list	√	√
Adding a domain name.	×	√
Editing a domain name	×	√
Deleting a domain name	×	√
Querying a protection policy	√	√

Operation	AADReadOnlyAccessPolicy	AADFullAccessPolicy
Querying the list of domain names with an enabled protection policy	√	√
Creating a protection policy	×	√
Updating a protection policy	×	√
Deleting a protection policy.	×	√
Creating a blacklist or whitelist rule	×	√
Deleting a blacklist or whitelist rule	×	√
Querying the blacklist and whitelist rule list	√	√
Querying quotas	√	√
Querying a forwarding rule	√	√
Exporting forwarding rules	×	√
Adding a forwarding rule	×	√
Modifying a forwarding rule	×	√
Deleting a forwarding rule	×	√
Viewing statistics reports	√	√
Querying an alarm notification	√	√
Creating an alarm notification	×	√

Identity Policies on Which Console Functions Depend

Table 6-21 Identity policies of services on which AAD console functions depend

Console Function	Dependent Services	Policy/Role Required
Adding a domain name	Cloud Certificate Manager (CCM)	If the origin server uses the HTTPS forwarding protocol, pulling certificates requires the **SCMReadOnlyPolicy** permission.
Configuring AAD logs	Log Tank Service (LTS)	The log groups and log streams created in LTS can be selected only after the **LTSReadOnlyAccessPolicy** system identity policy is added.
Enabling alarm notifications	Simple Message Notification (SMN)	SMN topic groups can be obtained only after the **SMNReadOnlyPolicy** system identity policy is added.
Configuring instance tags	Tag Management Service (TMS)	Tag keys can be created only after the **TMSReadOnlyPolicy** system identity policy is added.
Purchasing an AAD instance	Enterprise Project Management Service (EPS)	Enterprise projects can be selected only after the **EPSReadOnlyPolicy** system identity policy is added.

Helpful Links

- **IAM Service Overview**
- **Creating a User and Granting the AAD Access Permission**
- **AAD Permissions and Actions**

7 Related Services

AAD can protect public IP addresses of services such as ECS, ELB, WAF, and EIP. In addition, AAD has the following relationships with other cloud services:

Table 7-1 Related Services

Service	Relationship with Other Cloud Services	Related Feature
Cloud Trace Service (CTS)	After you enable CTS, CTS records DDoS mitigation operations for later query, audit, and backtrack.	• **Key Operations Recorded by CTS (Anti-DDoS)** • **Key Operations Recorded by CTS (CNAD)** • **Key Operations Recorded by CTS (AAD)**
Simple Message Notification (SMN)	Simple Message Notification (SMN) provides the notification function. When alarm notification is enabled, you will receive alarm messages by SMS or email if your IP address is DDoS attacked.	• **Enabling Alarm Notifications (Anti-DDoS)** • **Enabling Alarm Notifications (CNAD)** • **Enabling Alarm Notifications (AAD)**
Log Tank Service (LTS)	Attack logs are recorded in Log Tank Service (LTS), which enable real-time decision making and analysis, device O&M management, and service trend analysis.	• **Configuring Anti-DDoS Logs**

Service	Relationship with Other Cloud Services	Related Feature
Cloud Eye Service (CES)	Cloud Eye monitors metrics related to Anti-DDoS Service. You can learn about the protection status in a timely manner and set corresponding protection policies based on the metrics in Cloud Eye.	• **Setting Alarm Rules (CNAD)** • **Setting Alarm Rules (AAD)** • **Setting Event Alarm Notifications (Anti-DDoS)** • **Setting Event Alarm Notifications (CNAD)** • **Configuring Event Alarm Notifications (AAD)**
Identity and Access Management (IAM)	Identity and Access Management (IAM) provides the permission management function for Anti-DDoS Service. Only users with required permissions can use Anti-DDoS Service.	• **Permission Management (Anti-DDoS)** • **Permission Management (CNAD)** • **Permission Management (AAD)**
Enterprise Management	You can create enterprise projects based on the enterprise organization structure. Then you can manage resources across different regions by enterprise project, grant different permissions to user groups, and add them to enterprise projects. Anti-DDoS Service can be interconnected with Enterprise Management. You can manage Anti-DDoS Service resources by enterprise project and grant different permissions to users.	• **Purchasing a CNAD Instance** • **Purchasing an AAD Instance**
Tag Management Service (TMS)	You can use tags to classify cloud resources by dimension, such as usage, owner, or environment. Tags allow you to better manage AAD instances.	• **Configuring Instance Tags (CNAD Advanced)** • **Configuring Instance Tags (Advanced Anti-DDoS)**

8 Basic Concepts

DDoS Attack

Denial of Service (DoS) attacks 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 Distributed Denial of Service (DDoS) attack involves multiple compromised computers controlled by an attacker flooding the targeted server with superfluous requests.

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.

Traffic Scrubbing

Anti-DDoS Service monitors workload traffic in real time and scrubs attack traffic through the DDoS traffic scrubbing center without affecting normal services.

Traffic Cleaning Threshold

Anti-DDoS scrubs traffic when detecting that the incoming traffic of an IP address exceeds the traffic cleaning threshold. It will discard attack traffic and permit normal service traffic.

SYN flood attack

A SYN flood attack is a typical denial of service (DoS) attack. Utilizing the loop hole in the Transmission Control Protocol (TCP), the attacker sends a huge number of forged TCP connection requests to the target to exhaust its resources (fully loaded CPU or insufficient memory). Consequently, the target fails to respond to normal connection requests.

ACK Flood

In an ACK flood attack, an attacker sends a large volume of TCP ACK packets to overwhelm a server. Similar to other types of Distributed Denial-of-Service (DDoS)

attacks, ACK flood attacks utilize malicious traffic to saturate the target system, thereby slowing it down or causing it to become unresponsive. As a consequence, the targeted server becomes unavailable to serve legitimate users. Specifically, the server is forced to dedicate excessive computational resources to processing each incoming ACK packet, leading to a significant degradation in performance and ultimately rendering it incapable of providing services to legitimate users.

UDP Attack

In UDP attacks, attackers exploit the characteristics of UDP protocol interactions to launch a massive influx of malformed or spoofed UDP packets against servers via botnets. This results in the depletion of network bandwidth resources on the affected servers, significantly reducing their processing capacity and causing them to malfunction.

TCP Attack

In TCP attacks, attackers exploit the characteristics of TCP protocol interactions to launch a massive influx of malformed or spoofed TCP connections against servers via botnets. This results in the depletion of network bandwidth resources on the affected servers, significantly reducing their processing capacity and causing them to malfunction.

CC Attack

A Challenge Collapsar (CC) attack is a type of DDoS attack targeting web applications. In this attack, an attacker sends a massive volume of forged HTTP requests to the target network server, designed to exhaust its resources and render it unavailable. As a result, legitimate users are unable to access the services.

Slow Connection Attack

Slow HTTP attacks are a variation of CC attacks. Here is how slow HTTP attacks work:

An attacker establishes a connection with a large content length from the client to the server, then sends packets to the server at a slow rate (e.g., one byte every one to ten seconds), maintaining the connection.

If the attacker continues to create such connections, the server's available connections are gradually consumed, causing the server to reject normal user requests.

Transparent Access

Transparent access refers to a deployment model for the Anti-DDoS Service, where the service directly assigns an elastic IP address (EIP) to the protected resources on the cloud. This allows users to access the protected resources directly through the assigned EIP.

SDK Access

To connect to Anti-DDoS Service, you can also use the Software Development Kit (SDK). For details about the SDKs supported by the Anti-DDoS Service, see the **SDK List**.

Anti-DDoS Service Dedicated EIPs

An Anti-DDoS Service dedicated EIP is a dedicated EIP for CNAD. Compared with common EIPs that defend against attacks in the local equipment room of Huawei Cloud, the dedicated EIP of Anti-DDoS Service defends against attacks in the DDoS scrubbing center and provides Terabit-level bandwidth and strong protection capabilities.

Basic Protection Bandwidth

The basic protection bandwidth is purchased by customers. If the peak attack traffic is less than or equal to the basic protection bandwidth, customers do not need to pay extra fees.

Elastic Protection Bandwidth

Elastic protection bandwidth is the maximum available defense bandwidth. The elastic protection bandwidth is not a part that is added on top of the basic protection bandwidth. If the elastic protection bandwidth is the same as the basic protection bandwidth, the elastic bandwidth will not work.

BGP

Border Gateway Protocol (BGP) is a routing protocol used between autonomous systems (ASs). BGP is the only protocol that can process many connections between unrelated routing domains.

Anycast

Anycast is a networking technique that enables a single IP address to be shared among multiple devices, typically servers, located in different geographic locations. When a packet is sent to the shared IP address, a router uses its standard routing algorithms, such as Border Gateway Protocol (BGP), to determine the best path to forward the packet to the nearest device. It is usually used to provide high reliability and load balancing.

