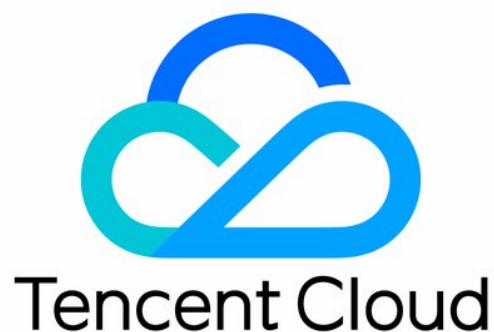


Anti-DDoS Advanced

Comparison of Anti-DDoS Protection

Schemes

Product Documentation



Copyright Notice

©2013-2024 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Comparison of Anti-DDoS Protection Schemes

Last updated : 2023-04-28 16:48:50

Based on Tencent's many years of practical experience in security and attack protection in various fields such as social networking, gaming, news, and finance, Anti-DDoS provides a rich set of comprehensive security solutions, satisfying your needs in security protection against different DDoS attacks in different business scenarios.

This document describes the basic information and use cases of different Anti-DDoS solutions.

Note :

To customize a dedicated security solution, please [submit a ticket](#) for assistance.

Product	Applicable User	Protected Target	Connection Method	Billing Mode	Protection Capability	Configuration
Anti-DDoS Basic	Tencent Cloud users	Applicable to Tencent Cloud services such as CVM and CLB	No configuration required	Free of charge	<ul style="list-style-type: none">It mainly protects the businesses that are less likely to suffer attacks and volumes of traffic. If you need a higher protection capability, Anti-DDoS Pro is recommended.By default, general users can enjoy protection capability of up to 2 Gbps, while VIP users up to 10 Gbps. If your business is	Tencent Cloud service IPs are automatically protected with no configuration required.

Product	Applicable User	Protected Target	Connection Method	Billing Mode	Protection Capability	Configuration
					frequently attacked, Tencent Cloud will adjust the basic protection capability based on historical attacks to ensure the overall stability of the Tencent Cloud platform. <ul style="list-style-type: none">Up to 2 Gbps protection capability for regions outside the Chinese mainland is provided for all users.	
Anti-DDoS Pro Light	Tencent Cloud users in Beijing, Shanghai, Guangzhou, Chengdu and Nanjing regions	Applicable to Tencent Cloud Lighthouse	It takes effect after a protected IP is bound in the Anti-DDoS console. For more information, see Getting Started .	Billed by protected IPs + validity period	Up to 10 Gbps protection capability	Simply bind your Lighthouse instance IP to the purchased instance.

Product	Applicable User	Protected Target	Connection Method	Billing Mode	Protection Capability	Configuration
Anti-DDoS Pro	Tencent Cloud users in Beijing, Shanghai, and Guangzhou regions	Applicable to Tencent Cloud services such as CVM, CLB, WAF, CPM, BM CLB, NAT IP, EIP, GAAP IP, and applications configured with a lot of Tencent Cloud service IPs	It takes effect after a protected IP is bound in the Anti-DDoS console. For more information, see Getting Started .	Billed by protected IPs + business bandwidth	<ul style="list-style-type: none"> Tencent Cloud provides an all-out protection. The maximum protection capability can be adjusted dynamically based on the actual network conditions of the region. HTTP CC protection is supported. 	Simply bind your Tencent Cloud service IP to the purchased instance.
Anti-DDoS Advanced (Chinese Mainland)	Users whose businesses are deployed in the Chinese mainland	Applicable to TCP, UDP, HTTP, and HTTPS businesses (WebSocket supported by default)	The traffic is sent to the proxy through the Anti-DDoS Advanced instance and then forwarded to the backend real server IP. For more information, see Website Business Connection and Non-website Business Connection .	Billed by base bandwidth + elastic bandwidth + business bandwidth + forwarding rules	HTTP/HTTPS CC protection is supported. Protection lines include BGP lines and non-BGP lines: <ul style="list-style-type: none"> BGP lines provide TB-level protection capability. Non-BGP lines provide up to 1 Tbps protection capability. 	By configuring connection based on a forwarding rule, you can use an Anti-DDoS Advanced instance as the address to provide your business and hide your real server.

Product	Applicable User	Protected Target	Connection Method	Billing Mode	Protection Capability	Configuration
Anti-DDoS Advanced (Outside Chinese Mainland)	Users whose businesses are deployed outside the Chinese mainland	Applicable to TCP, UDP, HTTP, and HTTPS businesses (WebSocket supported by default)	The traffic is sent to the proxy through the Anti-DDoS Advanced instance and then forwarded to the backend real server IP. For more information, see Website Business Connection and Non-website Business Connection .	Billed by base bandwidth + elastic bandwidth + business bandwidth + forwarding rules	<ul style="list-style-type: none"> Up to 400 Gbps protection capability is provided. HTTP/HTTPS CC protection is supported. The cleansing centers are deployed in regions such as Hong Kong (China), Taiwan (China), Singapore, Seoul, Tokyo, Virginia, Silicon Valley, and Frankfurt. 	By configuring connection based on a forwarding rule, you can use an Anti-DDoS Advanced instance as the address to provide your business and hide your real server.

Product	Applicable User	Protected Target	Connection Method	Billing Mode	Protection Capability	Configuration
Anti-DDoS Advanced (Global Enterprise Edition)	Users whose businesses are deployed outside the Chinese mainland	I Applicable to Tencent Cloud services such as CVM and CLB	It takes effect after a protected IP is bound in the Anti-DDoS console. For more information, see Getting Started .	Billed by all-out bandwidth + pay-as-you-go business bandwidth + quarterly business bandwidth	<ul style="list-style-type: none">Tbps-level protection capability is provided.The cleansing nodes are deployed in regions such as Hong Kong (China), Singapore, Seoul, Tokyo, Mumbai, Silicon Valley, Virginia, Moscow, Frankfurt, and Bangkok.	Simply bind your Tencent Cloud resource to the purchased instance.