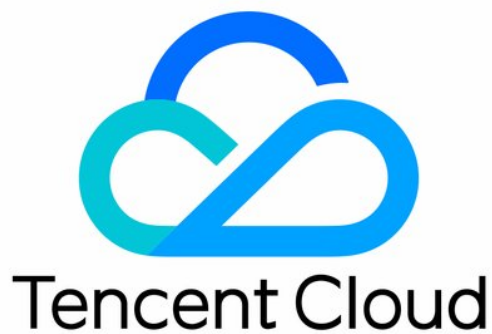


Anti-DDoS

Comparison of Anti-DDoS Solutions 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

 Tencent Cloud

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 Solutions

Last updated : 2024-07-01 11:20:28

Based on Tencent's rich experience in security and attack protection in various fields such as social networking, gaming, news, and finance, Anti-DDoS provides a wide variety of 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 editions.

Note:

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

Edition	Region scope	Protection scope	How to activate	Billable items	Capability	Configuratio
Anti-DDoS Basic	Tencent Cloud users	Tencent Cloud services such as CVM and CLB	No configuration required	Free of charge	A protection capability of 2 Gbps is offer to all users by default. However, if your service is frequently attacked, Tencent Cloud may adjust the basic protection capability based on historical attacks to ensure the overall stability of the Tencent Cloud platform.	Tencent Cloud service IPs are automaticall protected with no configuration required.
Anti-DDoS Pro (Standard)	Beijing, Shanghai, and	CVM, CLB, WAF, CBM, BM CLB, NAT IP,	Add the IPs to protect in the Anti-DDoS	Billed by the number of protected IPs and	Tencent Cloud provides all-out protection.	Purchase ar Anti-DDoS Pro instance and bind it

	Guangzhou regions	EIP, GAAP IP, and customers using a large number of cloud IPs.	console. See Getting Started .	service bandwidth	The maximum protection capability is adjusted dynamically based on the actual network conditions of the region.	with the IPs of Tencent Cloud resources to protect.
Anti-DDoS Pro (Enterprise)	Global Tencent Cloud regions	CVM, private CLB, CBM, NAT Gateway	Create an Anti-DDoS EIP and bind it with the resources you want to protect. See Getting Started .	Chinese mainland: The protection capability adopts the "base protection + elastic protection" mode. Outside the Chinese mainland: Tencent Cloud Anti-DDoS cleansing center provides all-out protection.	Chinese mainland: Offers BGP lines and non-BGP lines. Both support a Tbps-level protection capability. Outside Chinese mainland: Up to Tbps-level protection capability. Tencent Cloud Anti-DDoS cleansing center provides all-out protection. The maximum protection capability is adjusted dynamically based on the actual network conditions of the region. A maximum of Tbps-level	You can enjoy DDoS protection capability simply by creating an Anti DDoS EIP and binding it to the Anti-DDoS Pro instance, with no need to adjust your business.

					protection capability is supported.	
Anti-DDoS Pro (Custom)	Global Tencent Cloud regions. This edition is in beta test. To purchase it, contact us .	Applicable to Tencent Cloud services such as CVM, CLB, WAF, CBM, BM CLB, NAT IP, EIP, GAAP IP, and businesses configured with a lot of Tencent Cloud service IPs that need to be protected.	It takes effect after you bind a protected IP in the Anti-DDoS console.	Billed by "the number of protected IPs + business bandwidth"	Up to 50 Gbps	You can enjoy a higher DDoS protection capability simply by purchasing an Anti-DDoS Pro instance and binding it to the Tencent Cloud service IP to be protected with no need to adjust your business.
Anti-DDoS Advanced (Chinese Mainland)	All internet users whose business is deployed in the Chinese mainland	Applicable to TCP, UDP, HTTP, and HTTPS businesses (WebSocket is supported by default.)	Traffic is processed by the Anti-DDoS Advanced instance and then forwarded to the real server IP. For more information, see Website Business Connection and Non-Website Business Connection .	Billed by "base protection + elastic protection + business bandwidth + the number of forwarding rules"	HTTP/HTTPS CC protection is supported. Protection lines include BGP lines and non-BGP lines: BGP lines provide a Tbps-level protection capability. Non-BGP lines also provide a Tbps-level protection capability.	Create a forwarding rule to bind the Anti-DDoS Advanced IP forwarding rules, you can use an Anti-DDoS Advanced instance as the internet-facing address of the real server to hide your real server.

<p>Anti-DDoS Advanced (Global Standard)</p>	<p>Regions outside the Chinese mainland</p>	<p>TCP, UDP, HTTP, and HTTPS businesses (WebSocket is supported by default.)</p>	<p>Traffic is processed by the Anti-DDoS Advanced instance and then forwarded to the backend real server IP. See Website Business Connection and Non-Website Business Connection.</p>	<p>Billed by "base protection + elastic protection + business bandwidth + the number of forwarding rules"</p>	<p>Up to 400 Gbps Support HTTP/HTTPS CC protection Cleansing centers are deployed in Hong Kong (China), Singapore, Seoul, Tokyo, Virginia, Silicon Valley, and Frankfurt.</p>	<p>By configuring forwarding rules, you can use an Anti-DDoS Advanced instance as the internet-facing address of the real server to hide your real server.</p>
<p>Anti-DDoS Advanced (Global Enterprise)</p>	<p>Regions outside the Chinese mainland</p>	<p>CVM and CLB</p>	<p>Add the IP to protect in the Anti-DDoS console. See Getting Started.</p>	<p>Billed by "all-out protection + pay-as-you-go bandwidth + quarterly subscription"</p>	<p>A Tbps-level protection capability is provided. Cleansing nodes are deployed in Hong Kong (China), Singapore, Seoul, Tokyo, Mumbai, Silicon Valley, Virginia, Frankfurt, and Bangkok.</p>	<p>Purchase an Anti-DDoS Advanced instance and bind it with the IPs of the Tencent Cloud resources to be protected.</p>