Tencent Cloud Firewall

Getting Started

Product Documentation

Getting Started

Last updated：2024-01-24 15:34:30

This topic helps you get started with Tencent Cloud Firewall (CFW).

1. Cloud Firewall basics

What features does Cloud Firewall offer?

What are the benefits of using Tencent Cloud Firewall?

What are some application scenarios of Cloud Firewall?

What are the common concepts of Cloud Firewall?

2. Billing modes of Cloud Firewall

Paid editions of Tencent Cloud Firewall include IPS Edition, Premium Edition, Enterprise Edition, and Ultimate Edition. To meet the needs of different customers with different asset scales, the editions differ in their feature modules and default specifications. Among them, the Premium Edition, Enterprise Edition, and Ultimate Edition support elastic scaling based on performance specifications and asset scale. For more information, please see Purchase Guide.

3. Getting started

3.1 Major features of Cloud Firewall

Tencent Cloud Firewall (CFW) is a SaaS firewall based on the public cloud environment that provides network perimeter protection and addresses security and management needs for unified access control and log audit. In addition to the features of traditional firewalls, CFW supports multi-tenancy and elastic scaling and is an essential network security infrastructure for cloud migration. For more information, please see Overview.

3.2 Purchasing Cloud Firewall

Paid editions of Tencent Cloud Firewall include IPS Edition, Premium Edition, Enterprise Edition, and Ultimate Edition. You can purchase one of them on the Purchase Cloud Firewall page. For more information, please see Purchase Method.

3.3 Using Cloud Firewall

After you purchase Cloud Firewall, you can use it in the following ways:

Method 1: Log in to the Cloud Firewall console to perform operations.

Method 2: Use CFW with APIs. For more information, please see API Documentation.

4. Overview of console features

If you want to	See
Configure firewall toggles for your public IPs and the associated cloud assets.	-
Manage traffic and protect assets in the private network, or forward network traffic based on SNAT and DNAT.	NAT Firewall Toggle
Automatically detect VPC information and connections, and set a Cloud Firewall toggle for each pair of connected VPCs.	Inter-VPC Firewall Toggle
View and manage the data and information of each asset in the Cloud Firewall console.	-
View and process security event alerts and blocked access.	Alert Management
View the traffic access and bandwidth visually within a specified time frame.	Traffic Monitoring
Filter domain names, or filter traffic by geographic location.	-
Use the security baseline feature for product security and stability.	-
Identify unknown risks beyond access control rules, monitor the north-south traffic of public IP addresses based on intrusion defense rules, and prevent CVM vulnerabilities from being exposed to the Internet.	Intrusion Defense
View the Cloud Firewall logs.	Log Audit
View the details of all the traffic logs stored in Cloud Firewall for the past 6 months based on account, retrieve and query logs with search statements, and use reporting and statistical analysis services.	Log Analysis
Batch manage IP addresses with address templates.	Address Template

5. FAQs

What protocols does Cloud Firewall support?

What is peak bandwidth? Does it refer to uplink or downlink bandwidth?

Does it affect my business when the peak bandwidth is exceeded?

How long are CFW logs stored by default? What is the maximum storage capacity?

What requests are blocked automatically in Block mode? Why do alerts still appear when Block mode is enabled?

Why are requests from malicious IP addresses not blocked?

Is my business affected when I enable or disable Cloud Firewall, scale up, add CAM authorization, and enable or disable intrusion defense?

Can I modify the configurations for Cloud Firewall?

Can I renew my Cloud Firewall subscription when it expires? Will I lose all my resources when my subscription expires?

6. Feedback and suggestions

If you have any questions or suggestions when using Tencent Cloud Firewall, you can submit your feedback through the following channels. A dedicated person will contact you to solve your problems.

If you have any feedback regarding CFW documentation, such as incorrect links, content, or APIs, please click **Send Feedback** on the right side of the documentation page, or select the target content.

If you have any questions, please contact us or submit a ticket.