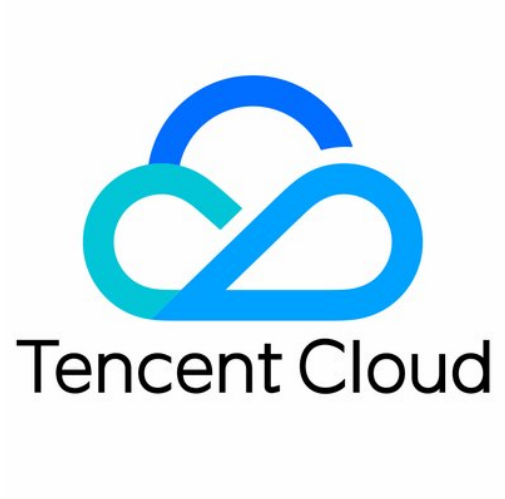
Tencent Cloud Firewall

CFW Policy

Product Documentation



Contents

CFW Policy
Privacy Policy
Data Processing And Security Agreement

CFW Policy
Privacy Policy

Last updated：2024-01-17 10:37:48

1. INTRODUCTION

This Module applies if you use Cloud Firewall ("**Feature**"). This Module is incorporated into the privacy policy located at （"Privacy Policy"). Terms used but not defined in this Module shall have the meaning given to them in the Privacy Policy. In the event of any conflict between the Privacy Policy and this Module, this Module shall apply to the extent of the inconsistency.

2. CONTROLLERSHIP

The controller of the personal information described in this Module is as specified in the Privacy Policy.

3. AVAILABILITY

This Feature is available to users globally.

4. HOW WE USE PERSONAL INFORMATION

We will use the information in the following ways and in accordance with the following legal bases:

Personal Information	Use	Legal Basis
Firewall Engine Operation Monitoring Data: APPID, firewall engine information (including the engine region, usage rate, bandwidth, operation parameters)	We use this information to ensure the Feature functions as required, including to maintain the normal operation and maintenance of the Feature. Please note that this data is stored in our TencentDB for MySQL feature.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.
User Operation Configuration Data: APPID,	We use this information to	We process this

firewall switch status (such as of your asset data, and whether assets are switched on or off)	ensure the Service functions as required, including to maintain the normal operation and maintenance of the Feature. Please note that this data is stored in our TencentDB for MySQL feature.	information as it is necessary for us to perform our contract with you to provide the Feature.
Billing Data: APPID, UIN, purchase duration, bandwidth, version configuration (including console purchase items and agreed package quota (such as quota on the number of protected assets, protected area, number of ACLs, number of banned lists, number of honeypots, number of enterprise security groups, log storage capacity))	We use this information for billing purposes. Please note that this data is stored and backed up in our TencentDB for Redis feature.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.

5. HOW WE STORE AND SHARE PERSONAL INFORMATION

As specified in the Privacy Policy.

6. HOW WE SHARE PERSONAL INFORMATION

As specified in the Privacy Policy.

7. DATA RETENTION

We will retain personal information in accordance with the following:

Personal Information	**Retention Policy**
Firewall Engine Operation Monitoring Data	Stored for 60 days.
User Operation Configuration Data	Stored for 60 days.
Billing Data	Stored for 60 days, otherwise if you terminate your subscription for the Feature we will delete your data within 14 days (whichever is earlier).

Data Processing And Security Agreement

Last updated：2024-01-17 10:37:48

1. BACKGROUND

This Module applies if you use Cloud Firewall ("**Feature**"). This Module is incorporated into the Data Processing and Security Agreement located at ("DPSA"). Terms used but not defined in this Module shall have the meaning given to them in the DPSA. In the event of any conflict between the DPSA and this Module, this Module shall apply to the extent of the inconsistency.

2. PROCESSING

We will process the following data in connection with the feature:

Personal Information	**Use**
Asset Data: information about your Tencent Cloud assets (hosts, public IP addresses, web services, gateway, VPC, subnets, and databases) that are protected by this Feature: asset instance ID/ name, IP address, asset type, region, private network, resource label, resource tags, inbound and outbound peak bandwidth, inbound and outbound cumulative traffic, cyberattack, exposed ports, exposed vulnerabilities, and host security	We only process this data for the purposes of providing the Feature to you. Please note that this data is shared from our other Tencent Cloud features (in accordance with your configurations and access permissions), stored in our TencentDB for MySQL ("**MySQL**") and Cloud Data Warehouse ("**Warehouse**") features, and backed up in our Cloud Object Storage ("**COS**") feature.
CFW Business Data: inbound and outbound bandwidth, inbound and outbound cumulative flow rate, name of loophole, exposed port, firewall configuration data (access control rules, intrusion defence protection rules, intrusion defence protection model, ban list, release list, isolation list, honeypot probe configuration, honeypot network configuration, address template), other firewall configuration data (on and off data of the firewall, NATFW instance configuration data)	We only process this data for the purposes of providing the Feature to you. Please note that this data is stored in our MySQL and Warehouse features, and backed up in our COS feature.
Attacker Data: log data of attacker information to be identified or intercepted: IP address, geographic location, attack packet (including	We only process this data for the purposes of providing the

payload), attack type, attack event type, attack tracing and attacker information	Feature to you. Please note that this data is stored in our MySQL and Warehouse features, and backed up in our COS feature.
Log Data: Access control logs (which contains data including rules direction, hit time, access source, source port, your access destination, destination port, agreement (network communication service agreement, TCP, UDP and HTTP), policies in effect); Intrusion prevention logs (which contains data including attack event type, risk level, external access source, source port, your access destination, destination port, agreement (network communication service agreement, TCP, UDP and HTTP), time of occurrence, policies, decision source); Traffic logs (which contains data including traffic direction, time, external access source, source port, your access destination, destination port, agreement (network communication service agreement, TCP, UDP and HTTP), stream bytes, region, operator); and Operation logs (which contains data including time, operation account, operation type, operation behavior, operation details, risk level)	We only process this data for the purposes of providing the Feature to you, including to enable you to review logs relating to your assets and/or attacks on your assets. Please note that this data is stored in our Elasticsearch Service feature, and backed up in our COS feature.

3. SERVICE REGION

As specified in the DPSA.

4. SUB-PROCESSORS

As specified in the DPSA.

5. DATA RETENTION

We will store personal data processed in connection with the Feature as follows (unless otherwise required by applicable Data Protection Laws):

Personal Information	**Retention Policy**
Asset Data	We retain such data until you terminate your subscription for the Feature, upon which such data will be deleted within 14 days.

CFW Business Data	By default, we retain such data for 7 days (unless the storage capacity exceeds 50GB, in which such data will be deleted earlier). If you purchase the log analysis service of this Feature (which is interdependent with our Message Queue CKafka feature), we retain such data for 6 months (for the storage capacity limit determined by you). If you reach your storage capacity limit, the data will be replaced on a rolling.
Attacker Data	By default, we retain such data for 7 days (unless the storage capacity exceeds 50GB, in which such data will be deleted earlier). If you purchase the log analysis service of this Feature (which is interdependent with our Message Queue CKafka feature), we retain such data for 6 months (for the storage capacity limit determined by you). If you reach your storage capacity limit, the data will be replaced on a rolling.
Log Data	By default, we retain such data for 7 days (unless the storage capacity exceeds 50GB, in which such data will be deleted earlier). If you purchase the log analysis service of this Feature (which is interdependent with our Message Queue CKafka feature), we retain such data for 6 months (for the storage capacity limit determined by you). If you reach your storage capacity limit, the data will be replaced on a rolling.

You can request deletion of such personal data in accordance with the DPSA.