

云防火墙

CFW 政策

产品文档



腾讯云

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

CFW 政策

 隐私协议

 数据处理和安全协议

CFW 政策

隐私协议

最近更新时间：2024-01-17 10:37:48

1. 简介

本模块仅在您使用 Cloud Firewall（简称“功能”）时适用。本模块已纳入位于[隐私政策](#)部分的隐私政策中。本模块中使用但未作定义的术语应具有在隐私政策中规定的含义。如果隐私政策与本模块之间发生任何冲突，对于此等不一致，本模块适用。

2. 控制方

本模块中所述个人信息控制方见隐私政策中的规定。

3. 可用性

本功能可供全球用户使用。

4. 我们如何使用个人信息

我们将按照以下法律依据和方式使用信息：

个人信息	用途	法律依据
防火墙引擎运行监控数据 ：APPID、防火墙引擎信息（包括引擎区域、使用率、带宽、运行参数）	我们使用此类信息来确保功能按要求运行，包括维持本功能的正常运维。 请注意，此数据将存储在云数据库 MySQL 功能中。	我们会处理此类信息，因为这对于我们履行与您签订的合约向您提供本服务而言是必要的。
用户操作配置数据 ：APPID、防火墙开关状态（如资产数据，以及资产是处于打开还是关闭状态）	我们使用此类信息来确保服务按要求运行，包括维持本功能的正常运维。 请注意，此数据将存储在云数据库 MySQL 功能中。	我们会处理此类信息，因为这对于我们履行与您签订的合约向您提供本服务而言是必要的。
计费数据 ：APPID、UIN、购买持续时	我们将此类信息用于计费目	我们会处理此类信息，因为这

间、带宽、版本配置（包括控制台购买项目和约定的包配额（如受保护资产数量、保护区域、ACL 数量、禁止列表数量、蜜罐数量、企业安全群组数量、日志存储容量））	的。 请注意，此类数据将存储和备份在我们的云数据库 Redis 功能中。	对于我们履行与您签订的合同向您提供本服务而言是必要的。
---	---	-----------------------------

5. 我们如何存储和共享个人信息

见隐私政策中的规定。

6. 我们如何共享个人信息

见隐私政策中的规定。

7. 数据保留

我们将根据下列规定保留个人信息：

个人信息	保留政策
防火墙引擎运行监控数据	存储 60 天。
用户操作配置数据	存储 60 天。
计费数据	此类数据存储 60 天，或者在您终止对本功能的订阅之后 14 天（以较早者为准）内由我们为您删除。

数据处理和安全协议

最近更新时间：2024-01-17 10:37:48

1. 背景

本模块仅在您使用 Cloud Firewall（简称“**功能**”）时适用。本模块已纳入位于（“**DPSA**”）的数据处理和**安全协议**中。本模块中使用但未作定义的术语应具有在 **DPSA** 中规定的含义。如果 **DPSA** 与本模块之间发生任何冲突，对于此等不一致，本模块适用。

2. 处理

我们将因本功能处理以下数据：

个人信息	用途
<p>资产数据：受本功能保护的腾讯云资产（主机、公共 IP 地址、网络服务、网关、VPC、子网和数据库）信息：资产实例 ID/名称、IP 地址、资产类型、区域、专用网络、资源标签、资源标签、入站和出站峰值带宽、入站和出站累积流量、网络攻击、暴露端口、暴露漏洞及主机安全性</p>	<p>我们仅为了向您提供本功能而处理此数据。</p> <p>请注意，此类数据分享自我们的其他腾讯云功能（根据配置和访问权限），存储在我们的云数据库 MySQL (“MySQL”) 和云数据仓库 (“Warehouse”) 功能中，并备份在我们的对象存储 (“COS”) 功能中。</p>
<p>CFW 业务数据：入站和出站带宽、入站和出站累积流量、漏洞名称、暴露端口、防火墙配置数据（访问控制规则、入侵防御防护规则、入侵防御防护模型、禁止列表、发布列表、隔离列表、蜜罐探测配置、蜜罐网络配置、地址模板）、其他防火墙配置数据（防火墙开启和关闭数据、NATFW 实例配置数据）</p>	<p>我们仅为了向您提供本功能而处理此数据。</p> <p>请注意，此类数据将存储在我们的 MySQL 和 Warehouse 功能中，并备份在我们的 COS 功能中。</p>
<p>攻击者数据：要识别或拦截的攻击者信息的日志数据：IP 地址、地理位置、攻击数据包（包括有效负载）、攻击类型、攻击事件类型、攻击跟踪和攻击者信息</p>	<p>我们仅为了向您提供本功能而处理此数据。</p> <p>请注意，此类数据将存储在我们的 MySQL 和 Warehouse 功能中，并备份在我们的 COS 功能中。</p>
<p>日志数据：</p> <p>访问控制日志（其中包含的数据包括规则方向、命中时间、访问源、源端口、访问目的地、目的地端口、协议（网络通信服务协议、TCP、UDP 和 HTTP）、生效的政策）；</p> <p>入侵防御日志（其中包含的数据包括攻击事件类型、风险等级、外部访问源、源端口、访问目的地、目的地端口、协议（网络通</p>	<p>我们仅为了向您提供本功能等目的而处理此类数据，包括帮助您查看与资产和/或针对资产的攻击相关日志的目的。</p> <p>请注意，此类数据将存储在 Elasticsearch Service 功能中，并备份在我们的 COS 功能中。</p>

信服务协议、TCP、UDP 和 HTTP）、发生时间、策略、决策来源）；
 流量日志（其中包含的数据包括流量方向、时间、外部访问源、源端口、访问目的地、目的地端口、协议（网络通信服务协议、TCP、UDP 和 HTTP）、流字节、区域、运营商）；
 操作日志（其中包含的数据包括时间、操作帐户、操作类型、操作行为、操作细节、风险等级）

3. 服务区域

见 DPSA 中的规定。

4. 分包处理方

见 DPSA 中的规定。

5. 数据保留

我们将存储因本功能而处理的个人数据，具体如下所述（除非适用的数据保护法另有规定）：

个人信息	保留政策
资产数据	我们将一直为您保留此类数据，除非您终止对本功能的订阅，此类数据将在终止订阅之日起 14 天内删除。
CFW 业务数据	默认情况下，我们将为您保留此类数据 7 天（除非存储容量超过 50GB，在这种情况下，此类数据将提前删除）。如果您购买本功能的日志分析服务（与我们的消息队列 CKafka 功能相互依存），我们将为您保留此类数据 6 个月（以您确定的存储容量限制为准）。如果达到存储容量限制，数据将被滚动替换。
攻击者数据	默认情况下，我们将为您保留此类数据 7 天（除非存储容量超过 50GB，在这种情况下，此类数据将提前删除）。如果您购买本功能的日志分析服务（与我们的消息队列 CKafka 功能相互依存），我们将为您保留此类数据 6 个月（以您确定的存储容量限制为准）。如果达到存储容量限制，数据将被滚动替换。
日志数据	默认情况下，我们将为您保留此类数据 7 天（除非存储容量超过 50GB，在这种情况下，此类数据将提前删除）。如果您购买本功能的日志分析服务（与我们的消息队列 CKafka 功能相互依存），我们将为您保留此类数据 6 个月（以您确定的存储容量限制为准）。如果达到存储容量限制，数据将被滚动替换。

您可以根据 DPSA 请求删除此类个人数据。