云防火墙

产品简介

产品文档

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2023-12-11 16:33:33

什么是云防火墙

腾讯云防火墙（Tencent Cloud Firewall，CFW）是一款基于公有云环境下的 SaaS 化防火墙，目前主要为用户提供互联网边界防护，并用于解决云上访问控制的统一管理与日志审计问题，具备传统防火墙功能的同时也支持云上多租户及弹性扩容，是用户业务上云的网络安全基础设施。

产品功能

云防火墙概览

云防火墙为用户提供统一的网络访问控制中心点，通过 控制台概览页 用户可以直观清晰的查看到与防火墙相关内容，包含下列模块：
资产防护概况：展示用户公网资产、内网资产、暴露端口及安全事件的数量，并为用户提供漏洞情报的参考。
防火墙状态监控：显示近7天内，互联网边界带宽峰值和 NAT 边界带宽峰值。
流量统计：展示24h - 6个月范围内，出站入站的流量大小及总流量大小。
安全策略配置：显示互联网边界、NAT 边界、VPC 边界的访问控制规则数量、剩余配额及各边界在入侵防御中，采用的安全策略。
日志存储统计：显示日志总内存、现有内存以及剩余可用容量。

云防火墙开关

互联网边界防火墙开关：系统自动识别云租户的公网 IP 及关联实例与绑定资产，通过云防火墙开关管理公网 IP 粒度的访问控制防护。目前云防火墙支持 BGP 公网 IP（三网 IP 不支持，下同）通过云防火墙开关中的公网 IP 列表（资产列表），用户可以快速查看每一个公网 IP 所关联的已有出站或入站规则，并通过访问控制模块进行统一管控。
VPC 间防火墙开关：系统自动识别云租户内网的 VPC 数量以及连通状态与方式，并通过 VPC 网络拓扑的可视化视图展示。首次使用 VPC 边界防火墙，需要开启统一的 VPC 边界防火墙开关，开关开启后，系统自动为用户配置所有互通 VPC 的两两关系的子防火墙，用户可以开启或关闭子防火墙，同时也能基于 VPC 的两两关系进行访问控制规则配置。
NAT 边界防火墙开关：NAT 边界防火墙是一种虚拟化的防火墙，原理类似于 NAT 网关，NAT 边界防火墙可以提供网络地址转换能力，以及访问控制及日志留存等安全审计功能。
开通并创建 NAT 边界防火墙实例后，系统自动识别选定地域内 VPC 中子网情况，用户仅需找到需要接入的子网，开启防火墙开关，系统便会自动修改子网路由，将该子网的互联网流量牵引至 NAT 防火墙，用户可以在NAT防火墙

上配置访问控制列表，进行流量过滤与管控。

资产中心

资产中心可以查看和管理各资产的相关数据及信息，您可以通过查看 TOP5 的核心资产与 TOP5 的高危资产，以及您全部公网资产、内网资产和私有网络的详细信息，来更好地把控资产现状、管理资产并预知和防控安全事件。

告警中心

告警中心可以查看资产受到网络攻击时的告警事件，当在访问控制、入侵防御和安全基线模块，配置好云防火墙所需的全部安全策略后，可通过持续关注来自云防火墙的告警，进行网络边界防护的安全运维工作。

流量中心

流量中心是基于互联网的出向、入向流量和 VPC 间流量的访问情况，分成外部访问统计、主动外联分析、VPC 间活动的可视化信息界面。

访问控制

访问控制规则是一个安全策略的集合，通过五元组形式定义，采用列表形式排列，对于每一条经过互联网边界的数据流，云防火墙都会根据规则列表执行顺序匹配五元组信息。若出现匹配的数据流，则按照该命中规则的动作，对该数据流执行相应的操作，以此满足租户对于公网 IP 的访问控制防护需求，并通过日志记录的形式满足用户安全运维审计的需求。企业安全组满足 VPC 子网间、VPC 间、混合云专线间的防护场景，保持基于五元组的配置习惯，可以更容易的管控安全组配置。

入侵防御

云防火墙根据防护模式，自动识别访问控制规则以外的未知风险，并对公网 IP 的南北向流量进行入侵防御规则检测，同时避免云服务器中的漏洞暴露在互联网中。

安全基线

安全基线指云防火墙通过观察一定时间范围内的流量访问情况，形成一个初步的 IP 地址或域名访问列表，用户可以根据安全评分、关联安全事件以及网络访问情况，通过添加或删除 IP 地址或域名，维护基线列表，从而形成最终的安全基线。

日志审计

云防火墙提供7天的规则命中日志记录功能，可以记录所有被执行防火墙动作的网络流量与对应生效规则，协助安全运维人员进行审计工作，当出现网络连接等故障时，可通过检索日志快速排障与修复。同时，也可以查看过去30天的操作历史，提升企业与网络安全管理员的工作效率，降低管理成本。

日志分析

可在日志分析中查看基于登录账号的云防火墙，在过去6个月所存储的全部流量日志详情，同时日志分析支持基于检索语句的日志检索与查询，并提供报表与统计分析服务。

地址模板

为用户提供更方便快捷的方式批量管理 IP 域名。用户可以在地址模板中创建 IP 或域名模板，加入多个 IP 或域名，并将建立好的模板匹配访问控制中的相关规则。

产品优势

最近更新时间：2023-12-11 16:33:40

开启方便，无需部署

云防火墙采用 SDN 技术，提供公有云上的 SaaS 化防火墙，实现云上资产自动识别和一键开关，进行简单策略配置即可使用，提供无需部署成本（与传统硬件部署相比）的云防火墙功能。

稳定可靠，平滑扩展

具备主备容灾机制，保障性能稳定可靠。同时充分发挥 SaaS 化服务优势，支持带宽、资产及存储等弹性扩展，实现按需分配，平滑扩展。

统一管控，高效易用

云防火墙提供完整的互联网之间、VPC 之间流量的统一访问控制和安全隔离能力，为用户提供统一的访问控制平面。
互联网边界访问控制：基于对公网 IP 配置的访问控制规则，从而封堵或观察有威胁的访问目的流量，也可以阻断外部威胁访问源对云上资产发起的攻击行为。
VPC 边界访问控制：基于对租户内 VPC 之间配置访问控制规则，从而控制 VPC 之间的访问行为，实现 VPC 之间的安全隔离。
企业安全组：保持基于五元组的配置习惯，方便管理安全组配置，满足 VPC 子网间、VPC 间、混合云专线间的防护场景，支持阻断日志，轻松构建云上的 DMZ 区。
云防火墙遵循传统防火墙的规则配置模式，结合安全运维人员的使用场景，降低用户学习成本，提高产品易用性。

全程留存，日志审计

规则命中日志：当访问控制规则生效并命中后，云防火墙会记录被命中流量的五元组信息，并反馈用户对应规则，便于用户安全运维，在出现故障时，用户可以根据日志留存快速排障并修复。
用户操作日志：记录用户在云防火墙的操作情况及内容，包括所有账户的登录操作、云防火墙开关操作、针对规则的新增、删除、编辑操作，提升用户管理效率，降低管理成本。

应用场景

最近更新时间：2023-12-11 16:33:49

出站访问控制

出站访问控制是由内到外的场景，当您需要封堵云上 CVM 对某个外部地址或域名的访问时，可对所有需要管控的公网 IP 配置出站访问控制规则，以满足您的安全性需求。

入站访问控制

入站访问控制是由外到内的场景，当您需要禁止外部某个地址对云上 CVM 发起访问时，对所有需要管控的公网IP配置入站访问控制规则，以满足您的安全性需求。

命中日志审计

当您需要对云防火墙的访问控制规则的命中情况进行审计或出现故障需要对生效规则进行溯源时，可以通过云防火墙的规则命中日志审计功能，帮助您快速进行日志审计与故障修复，提升您的安全运维效率并降低运维成本。

操作日志审计

当您需要对云防火墙的操作进行管理时，可以通过使用云防火墙的用户操作日志功能，快速定位操作时间、操作内容与操作账号，以满足您的管理需求。

相关概念

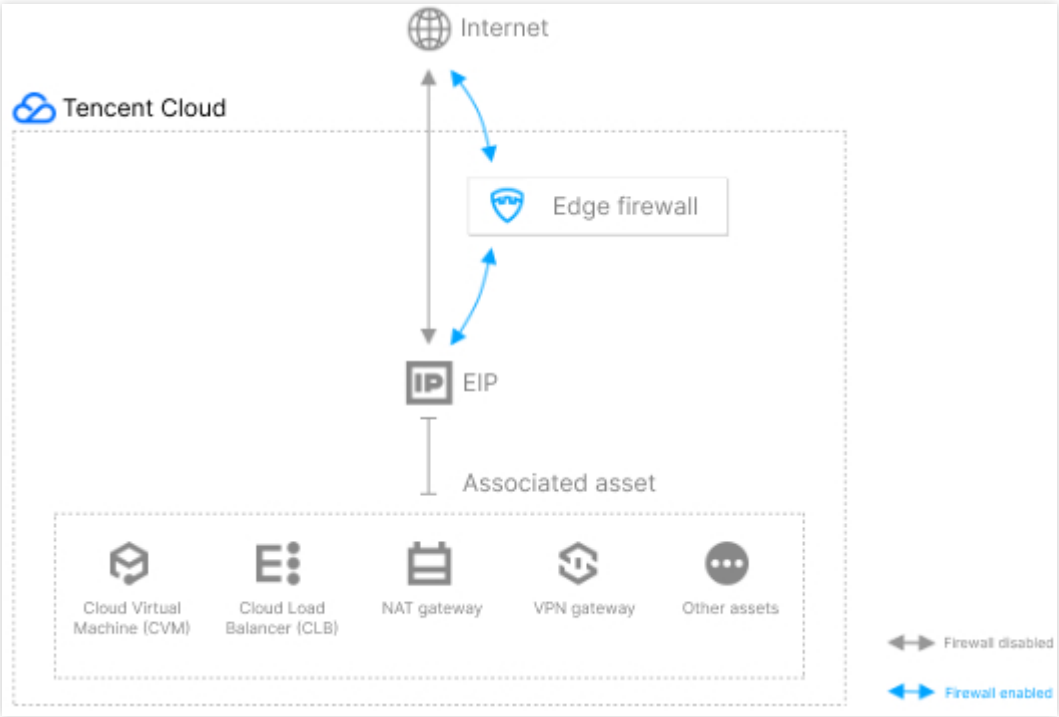
最近更新时间：2023-12-11 16:35:47

互联网边界

互联网边界是指互联网与腾讯云内网的边界，互联网边界流量指云上资产与互联网之间通信的流量，也称为南北向流量。
南北向流量必须是公网 IP 之间的流量。根据方向，又可以分为“出站流量”与“入站流量”：
出站流量：云上资产通过绑定的公网 IP 向互联网发起通信的流量。
入站流量：互联网向云内资产的公网 IP 发起通信的流量。

互联网边界防火墙

互联网边界防火墙是检测南北向流量的防火墙，是一种集群式防火墙。互联网边界防火墙生效于您的弹性公网 IP 的关联资产与外部互联网之间，原理如下图所示：



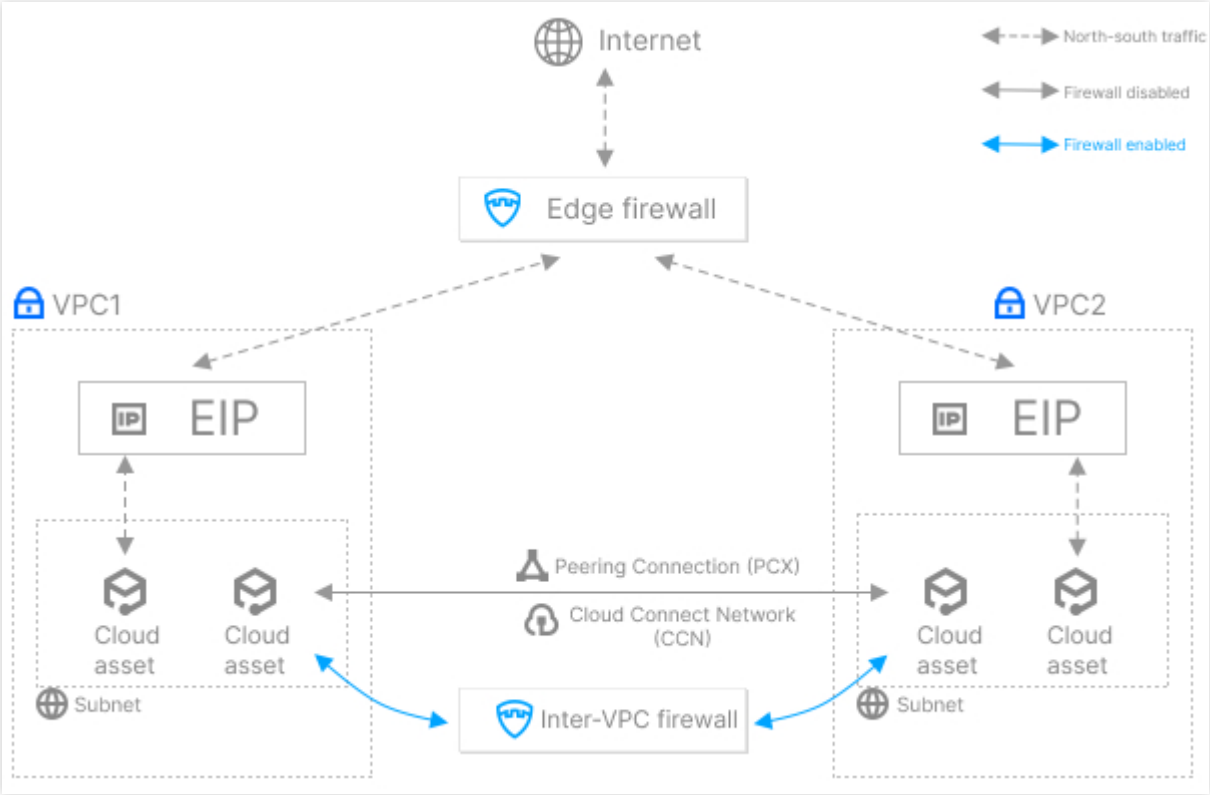
互联网边界防火墙支持访问控制与日志审计，并内置入侵防御模块，无需复杂的网络接入配置与镜像文件安装，支持即开即用，缺省集群化部署，支持性能平滑扩展。

私有网络

私有网络（Virtual Private Cloud，VPC）是一块您在腾讯云上自定义的逻辑隔离网络空间，与您在数据中心运行的传统网络相似，托管在腾讯云私有网络内的是您在腾讯云上的服务资源，包括云服务器、负载均衡、云数据库等。
私有网络 VPC 为您提供：
弹性公网 IP：用于互联网访问。
对等连接：支持私有网络间互通，详情请参见 对等连接文档 。
云联网：支持私有网络间互通，详情请参见 云联网文档。
通过对等连接、云联网可以实现云上 VPC 互通，VPC 之间的流量也被称为东西向流量，详情可参见 私有网络文档。

VPC 间防火墙

VPC 间防火墙是检测 VPC 间东西向流量的防火墙，是一种分布式防火墙。VPC 间防火墙生效于您的两个 VPC 之间，原理如下图所示：



VPC 间防火墙部署在对等连接及云联网联通的两个 VPC 间，支持访问控制、拓扑可视与日志审计等功能，无需复杂的路由配置与镜像文件安装，支持即开即用，用户独享式资源配置。

访问控制

访问控制是流量过滤规则的集合，生效于同一类流量的所有规则组成一张访问控制列表，每一条访问控制规则分为规则主体和描述两部分：

规则主体：允许或不允许某个地址的端口访问另一个地址的端口的某种协议的通信。

访问源：发起通信的地址，一般是 IP。

访问目的：接收通信的地址，可以是 IP，也可以是域名。

目的端口：访问目的地址的端口号。

协议：通信双方所使用的网络协议。

策略：若某个流量符合以上四个条件，则视为命中流量，防火墙会按照这条规则的策略执行以下动作。

放行：允许访问，记录流量日志，但不记录规则命中。

观察：允许命中的流量通过，记录流量日志与规则命中。

阻断：不允许命中的流量通过，不记录流量日志，但记录规则命中。

规则描述：记录本条访问控制规则的用途。

注意：

合理、规范的填写规则描述有助于提高规则的可读性，降低后期维护成本，提升效率。

规则优先级

执行顺序是规则在列表中的位置，执行顺序为1的规则优先级最高。对于每一个经过防火墙的数据流，防火墙会按照列表的从上到下顺序依次匹配规则：

若数据流命中某一条规则，防火墙会执行该规则对应的策略，不再继续匹配。

若数据流没有命中当前规则，则继续匹配下一条规则。

若数据流没有命中任何一条规则，防火墙会放行该数据流。

在一张访问控制列表中，执行顺序的取值区间为1 - n 的整数，1为最高优先级，n 为规则总数，也就是当前规则列表中的最低优先级，一般用于通配规则。

执行顺序满足两个原则：**连续原则、不可重复原则**。

连续原则：执行顺序必须是连续正整数，若当前规则数为 n，则执行顺序最大值为 n。

不可重复原则：同一个列表中的执行顺序不可重复。

执行顺序的连续性与不可重复性由以下三点保证：

添加规则时：执行顺序为 n+1。

插入规则时：执行顺序为插入位置的执行顺序值，被插入的所有规则会自动向后移动一位，执行顺序值+1。

编辑规则时：通过修改执行顺序可以移动规则，执行顺序可以被修改为目标位置的执行顺序值，最小为1，最大为 n。输入目标位置的执行顺序值，该规则会插入到目标位置，被插入的所有规则会自动向后移动一位，执行顺序值 +1。

入侵防御

入侵防御是一种监控网络传输，检查是否有可疑活动的系统，在检测到可疑事件时发出告警或者采取主动反应措施。云防火墙集成腾讯云威胁情报、基础防御以及虚拟补丁等功能，对您的互联网边界流量进行实时监控、统计与分析，主动发现外部入侵与恶意外联等未知风险，并提供实时的防护与告警。

日志

规则命中日志：规则命中日志中记录规则命中情况，帮助运维人员进行安全审计工作，规则命中日志显示被放行、观察、阻断的数据流的五元组信息，支持通过按钮查看对应生效的规则。
操作日志：云防火墙操作日志分为用户登录日志、开关操作日志和规则操作日志。
用户登录日志：记录该用户全部账号的登录情况。
开关操作日志：记录云防火墙开关情况。
规则操作日志：记录用户对于访问控制规则的新增、删除、编辑操作。