云防火墙

常见问题

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。
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默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

常见问题
- 基本介绍
- 带宽相关
- 防火墙相关
  - 云防火墙
  - 互联网边界防火墙
  - NAT 边界防火墙
  - VPC 间防火墙
- 功能相关
  - 流量中心
  - 访问控制
  - 零信任运维
  - 入侵防御
    - 基础防御
    - 防御策略
  - 告警中心
  - 安全基线
- 日志相关
- 账号相关
- 计费相关
- 其他

版权所有：腾讯云计算（北京）有限责任公司

常见问题
基本介绍

最近更新时间：2025-04-08 15:11:22

云防火墙是什么？

腾讯云防火墙（Cloud Firewall，CFW）是一款基于公有云环境下的 SaaS 化防火墙，主要为用户提供互联网边界的防护，解决云上访问控制的统一管理、日志审计的安全和管理需求。云防火墙不仅具备传统防火墙功能，同时也支持云上多租户和弹性扩容功能，是用户业务上云的第一个网络安全基础设施。

云防火墙是否可以防护非腾讯云上的资产？

防火墙仅能防护腾讯云账号下的 IP 资产，不支持非腾讯云的资产。

云防火墙是否能部署在专有云上？

TCE 专有云从380版本后，开始支持云防火墙服务。

云防火墙和安全组有什么区别？

云防火墙和安全组是两个独立的系统，在外网 EIP 开启互联网开关开启的状态下，策略同时放通，流量才放行。

- 二者控制的目标不一样。 互联网边界防火墙控制的是公网 IP 的公网访问流量，安全组控制的是 CVM 网卡的所有流量。
- 云防火墙和安全组作用的粒度不一样的，安全组作用于实例，云防火墙作用于公网 IPS 、NAT 边界防护和 VPC 间的对等连接或云联网。
- 安全组 ACL 只是云防火墙最基本功能，云防火墙更重要的是有全流量日志审计及入侵防御（IPS）的实时拦截能力。

云防火墙、WAF 产品的区别？

- Web 应用防火墙（WAF）只针对 Web 业务防护，对非 Web 类业务没有防护能力，且只防护由外对内的攻击。对业务的恶意主动外联没有监测和防护能力。
- 云防火墙包含全部业务防护，支持对 Web 漏洞的基础防护，同时支持内对外的主动外联流量检测。支持失陷主机和恶意外联的自动拦截。

云防火墙和安全运营中心都有流量威胁感知功能，这两者有什么差异？

云防火墙集成了企业级的 IPS 功能和 IDS 功能，对 0day 漏洞具备小时级的虚拟补丁能力，无需业务升级重启，这些能力是安全运营中心不具备的。

云防火墙可以防护 CDN 或 COS 吗？

云防火墙不支持 CDN、COS、高防 IP、SaaS-WAF、CDB 等 SaaS 化服务产品的防护。

流量是先经过防火墙再经过其他产品么？CDN流量会受防火墙保护么？

- CDN 节点 IP 属于 CDN 运营商所有，并不在您云墙保护范围内。
- 针对串行防火墙，仅在 CDN 回源 CLB/CVM 时才会经过云墙检测。高防 IP 回源到 CLB 也会过云墙，但是看到的都是高防 IP 的回源地址。
- 旁路防火墙由于架构原因无法获取 CDN 回源流量，建议切换为串行防火墙。
- 当前版本支持的公网 IP 类型为 BGP IP，暂不支持三网 IP。在识别用户资产时，云防火墙会自动过滤三网 IP。

云防火墙有 QPS 限制么？

云防火墙是 SaaS 化服务，对传统硬件防火墙的并发、新建、QPS 等均不限制，衡量云防火墙的唯一性能指标是实际的带宽吞吐量。

版权所有：腾讯云计算（北京）有限责任公司

外部入站流量是先经过云防火墙还是 WAF?

对于入方向流量

- Web 应用防火墙（WAF）和云防火墙共同组成了云上网络安全的整体边界防护，WAF 更偏向于对加密的 HTTPS 流量进行防护，非加密流量通过云防火墙集成的 IPS（入侵防御系统）基础规则和虚拟补丁等进行安全防护。
- 对于不同类型 WAF 和不同类型的互联网边界防火墙，其工作模式如下表所示：

防火墙类型	互联网边界旁路防火墙	互联网边界串行防火墙
SaaS-WAF	并行工作，流量不会经过防火墙	串行工作，流量先经过 WAF，再经过防火墙，防火墙源 IP 均为回源 IP
CLB-WAF	串行工作，流量先经过防火墙，再经过 CLB-WAF	串行工作，流量先经过防火墙，再经过 CLB-WAF

对于出方向流量

- 可以通过 NAT 边界防火墙，实现基于云服务器（CVM）颗粒度的主动外联控制，并且支持基于域名的访问控制，结合腾讯威胁情报，可对主动外联的恶意 IP 及域名进行自动拦截。
- 如未开启 NAT 边界防火墙，则只能在互联网边界防火墙，对 NAT网关后的流量进行访问控制，此时云防火墙看到的是公网 IP。

版权所有：腾讯云计算（北京）有限责任公司

带宽相关

最近更新时间：2025-04-14 16:41:32

带宽是什么，用户怎么挑选合适的带宽？

- 云防火墙的带宽与其他网络产品的带宽相互独立，因此云防火墙的带宽需要单独购买。
- 互联网边界防火墙带宽：试用云防火墙，开启互联网边界防火墙开关7天左右，根据控制台统计的出/入站流量峰值带宽购买。

> **说明：**
> 云防火墙为符合条件的腾讯云用户提供7天免费试用活动。您的腾讯云账号需满足以下条件：
> 1. 已进行 企业认证，且未参加过云防火墙免费试用活动。
> 2. 主账号及其子账号共计只能申请一次免费试用。

- NAT 和云防火墙相互独立，并相互串联。因此，需要挑选和NAT网关相同或更高容量的云防火墙带宽。
- 云联网和云防火墙相互独立，并相互串联。因此，需要挑选和云联网相同或更高容量的云防火墙带宽。

峰值带宽是指什么，是上行带宽还是下行带宽？

峰值带宽是指上行和下行带宽的最大值。例如，如果您购买了100Mbps带宽，那么云防火墙能够同时处理上行100Mbps和下行100Mbps。

业务带宽超过互联网边界防火墙带宽限制，会对我有业务影响么？

互联网边界防火墙的带宽超负荷不会导致客户业务流量丢包或影响流量速率，但将无法提供防护功能。

自2024年09月25日起，业务带宽超过互联网边界防火墙带宽100%时，将采取以下措施：
- 关闭部分互联网边界防火墙开关，将一部分流量 Bypass 转发，只防护带宽规格的流量。
- 串行和旁路模式处置方法一致，关闭部分开关限制流量。
- 支持配置防火墙开关权重，设置自动关闭防火墙开关的优先级。

> **说明：**
> 自动关闭开关后，可以手动开启互联网边界防火墙开关，如若业务打开超过互联网边界防火墙带宽，继续采取以上措施。

例如：
- 互联网边界带宽1000Mbps，其中分配旁路模式600Mbps，互联网边界开关打开5个；当旁路模式的总业务带宽达到610Mbps，关闭1个互联网边界开关，云防火墙防护业务带宽保持为600Mbps。
- 互联网边界带宽1000Mbps，其中分配串行模式400Mbps，其中广州地域200Mbps，广州地域互联网边界开关打开4个；当广州地域业务带宽达到310Mbps，关闭2个互联网边界开关，云防火墙防护广州地域的业务带宽保持为200Mbps。

冷却期后，如果业务带宽低于互联网边界防火墙带宽，防火墙开关自动恢复打开：

超量次数（月）	冷却期时长
3次及以下	2小时
4次~7次	1天
8次及以上	3天

例如：

- 南北向带宽1000Mbps，其中分配旁路模式600Mbps，互联网边界开关打开5个；当业务带宽达到610Mbps，关闭1个互联网边界开关，只开启4个互联网边界开关。云防火墙防护业务带宽保持为600Mbps。最近一个月内超量2次，2小时后互联网边界开关恢复，互联网边界开关打开5个。
- 南北向带宽1000Mbps，其中分配旁路模式600Mbps，互联网边界开关打开5个；当业务带宽达到610Mbps，关闭1个互联网边界开关，只开启4个互联网边界开关。云防火墙防护业务带宽保持为600Mbps。最近一个月内超量10次，3天后互联网边界开关恢复，互联网边界开关打开5个。

请持续关注云防火墙带宽告警，在带宽较高时，关闭一部分云防火墙开关，或扩展带宽以保证流量全部防护，确保业务安全。

业务带宽超过 NAT 边界防火墙带宽限制，会对我有业务影响么？

- NAT 边界防火墙是属于串联模式，防护带宽取决于实例规格，业务带宽超过 NAT 边界防火墙带宽100%时，会造成网络延迟增大或拥堵丢包，请根据业务情况及时关注防火墙带宽。
- 请持续关注云防火墙带宽告警，在带宽较高时，关闭一部分云防火墙开关，或扩展带宽以保证监控正常运行，确保业务安全。

业务带宽超过 VPC 边界防火墙带宽限制，会对我有业务影响么？

- VPC 边界防火墙是属于串联模式，防护带宽取决于实例规格，业务带宽超过 VPC 边界防火墙带宽100%时，会造成网络延迟增大或拥堵丢包，请根据业务情况及时关注防火墙带宽。
- 请持续关注云防火墙带宽告警，在带宽较高时，关闭一部分云防火墙开关，或扩展带宽以保证监控正常运行，确保业务安全。

云防火墙互联网边界带宽会限制流量吗？

云防火墙不会限制流量。

出入向的带宽是分别计算的吗？若出向带宽超出购买规格，会影响入向流量的规则匹配吗？

- 是的，出入向的带宽是分别计算的。
- 互联网边界防火墙、NAT 边界防火墙计算流量峰值的方式为取出向/入向流量的最大值。

互联网边界防火墙和 NAT 边界防火墙的带宽是分别计算的吗？

是的，互联网边界防火墙和 NAT 边界防火墙的带宽是分别计算的。

> **说明**
> 使用 NAT 边界防火墙带宽，需要消耗通用南北向带宽，如需扩展请扩展通用南北向带宽即可。

云防火墙的带宽支持任意升降吗？

带宽支持扩容，降配需要 提交工单 审核。

云防火墙的带宽限制取决于接入的 CVM 的带宽么？

不是，云防火墙带宽规格是按照用户实际使用的带宽来设置配额的，即要保证在同一时间下消耗的流量带宽值不能超过云防火墙的带宽参数。

防火墙相关
云防火墙

最近更新时间：2025-07-03 17:39:32

云防火墙支持防护哪些协议?

- 互联网边界防火墙（旁路模式）目前支持 TCP 协议。
- 互联网边界防火墙（串行模式）目前支持 TCP、UDP、ICMP、HTTP、HTTPS、SMTP、SMTPS、TLS/SSL、DNS 以及 FTP 协议。
- NAT 边界防火墙支持 TCP、UDP、ICMP、HTTP、HTTPS、SMTP、SMTPS、DNS 以及 FTP 协议。
- VPC 间防火墙支持 TCP、UDP、ICMP、HTTP、HTTPS、SMTP、SMTPS、DNS 以及 FTP 协议。

云防火墙如何防护 UDP 协议?

- 互联网边界防火墙（串行模式）支持防护 UDP 协议。
- 互联网边界防火墙（旁路模式）不支持防护 UDP 协议。

云防火墙和安全运营中心（SOC）之间的流量威胁感知功能有何不同?

云防火墙规则 = 基础规则（SOC） + 云防火墙自定义规则，这意味着云防火墙的规则比 SOC 的规则更为丰富。
基础规则检测出来的告警，既可以在云防火墙中看到，也可以在 SOC 中看到，而自定义规则产生的警报则只能在云防火墙中看到。

云防火墙是否具有冗余性?

互联网边界防火墙采用集群部署方式，而 NAT 边界防火墙和 VPC 间防火墙默认采用主备部署方式。

云防火墙是否支持单区高可用?

分为两种情况：互联网边界采用集群物理机部署，实现多活机制，不受可用区影响；NAT 边界防火墙、VPC 边界防火墙采用虚拟化技术，目前支持跨地域可用区部署。在进行容灾切换时，我们会同步会话表，确保连接不会中断。连接的时间延迟大约10秒，这主要是因为需要几秒钟的时间通过心跳机制来判断是否存在可用区异常。

购买云防火墙后，无法进入云防火墙控制台，页面不断刷新，该如何解决?

针对首次进行授权操作的用户，可尝试访问 资产中心页面，届时页面将弹出提示框，引导用户完成角色授权，授权完成之后即可正常访问云防控制台。

云防火墙是否支持腾讯云专线到 IDC 机房的防护以及是否支持部署在物理机房?

腾讯云防火墙是 SaaS 化的，不支持部署在物理机房。

如何查看当前云防火墙版本号?

1. 登录 云防火墙控制台，在左侧导航栏中，选择**防火墙开关** > **NAT 边界开关/VPC 边界开关** > **防火墙实例**。
2. 在防火墙实例页签，单击**实例 ID**，进入防火墙实例详情页面，查看云防火墙的**引擎版本**号。

网络拓扑
防火墙实例
1
防火墙开关
创建实例
引擎更新
同步资产
同步路由
实例ID
2
实例名称
部署模式
地域
出口公网IP
内网IP
防火墙实例
网络拓扑
规格调整
实例ID
新增模式
实例名称
出口公网IP
内网IP
多个(4)
所属地域
华东地区(上海)、上海二区(主)、上海二区(备)
引擎版本
3
实例规格
Mbps
条
已下发规则：
条

互联网边界防火墙

最近更新时间：2025-04-14 16:41:32

什么是互联网边界防火墙?

- 互联网边界是指互联网与腾讯云内网的边界，互联网边界流量就是您的云上资产与互联网之间通信的流量，也称南北向流量。
- 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。

互联网边界防火墙支持防护哪些资产?

当前版本支持的资产类型为：云服务器 CVM、负载均衡 CLB、NAT 网关、VPN 网关，目前支持中国大陆及中国香港地域资产。

什么类型的公网 IP 不会出现在互联网边界防火墙的开关列表中?

当前版本支持的公网 IP 类型为 BGP IP，暂不支持三网 IP。在识别用户资产时，云防火墙会自动过滤三网 IP。

当公网 IP 配额不足时，如何扩容提升防护能力?

高级版，企业版，旗舰版可通过弹性扩容提升规格，每扩展1Mbps带宽，同时增加1个公网 IP 数配额。

被标注“其它”类型的资产是什么?

互联网边界防火墙针对用户的公网 IP 进行资产识别，若有未与资产绑定的公网 IP，将会被识别为“其它”，此 IP 关联的规则，在绑定资产后即可正常生效。

为什么我开了互联网防火墙开关，IP 还是可以访问?

IP 开启互联网防火墙开关后，请前往访问控制、互联网边界规则，检查该 IP 的规则策略类型是阻断还是观察，只有策略为阻断的情况下才会拦截，IP 规则策略类型详情如下所示：

- 放行：放通命中规则的流量，记录命中次数但不记录访问控制日志，且记录流量日志。
- 观察：放通命中规则的流量，记录命中次数并记录访问控制日志与流量日志。
- 阻断：拦截命中规则的流量，记录命中次数并记录访问控制日志，流量日志记录一个请求数据包信息。

版权所有：腾讯云计算（北京）有限责任公司

NAT 边界防火墙

最近更新时间：2025-04-14 17:27:22

NAT 边界防火墙出去的数据会不会过两遍防火墙?

如果在互联网边界开关开启了 NAT 防火墙的公网 IP，在出向流量会先经过 NAT 防火墙，后经过互联网边界防火墙。

NAT 边界防火墙新增模式和接入模式有什么区别?

- 新增模式：若当前地域没有 NAT 网关，新增模式可以通过 NAT 边界防火墙内置的 NAT 功能，实现指定实例通过防火墙访问互联网。
- 接入模式：若当前地域已有NAT 网关，或者希望公网对外的出口 IP 保持不变，接入模式可以将 NAT 边界防火墙平滑接入到 NAT 网关与 CVM 实例之间。

使用 NAT 边界防火墙可以替代原来的 NAT 网关么?

NAT 防火墙可以替代原来的 NAT 网关。

NAT 边界防火墙可以只对某个子网启用么?

一个防火墙开关对应一个子网，可以选择同时开启当前子网关联的路由表的全部子网的防火墙，也可以只针对当前子网开启防火墙。

NAT 边界防火墙开关上绑定 EIP，网络是否会闪断?

绑定不会造成闪断。

NAT 边界防火墙开关开启或关闭某个 VPC 时该网络是否会闪断?

- 开启：由于路由更改，会出现1~2秒的网络闪断。若用户仅选择开启某个子网，系统会自动为当前子网创建新的路由表，复制现有的全部路由策略，在新路由表中增加一条下一跳指向 NAT 边界防火墙的路由策略，并关闭原访问公网的路由策略，因此该子网的互联网流量，将会经过 NAT 边界防火墙。
- 关闭：由于路由更改，会出现1~2秒的网络闪断。若用户仅选择关闭某个子网，系统会自动为当前子网创建新的路由表，复制现有的全部路由策略，并关闭下一跳指向 NAT 边界防火墙的路由策略，该子网将会断开与互联网的连接。

NAT 边界防火墙开关配置端口转发(DNAT)是否支持配置连续端口?

端口转发不支持在同一规则下同时配置多个端口，每个 DNAT 端口需要使用一条规则。

NAT 边界防火墙可以配置 SNAT么? 要如何配置?

1. 登录 云防火墙控制台，单击选择**防火墙开关** > **NAT 边界开关**，进入NAT 边界开关页面。
2. 在NAT 边界开关页面右侧操作栏中，单击**实例配置** > **出口绑定** > **新建规则**。
3. 选择相应的子网或私有网络使用的外部 IP后单击**确定** 即可。

如何确认子网都开了防火墙?

1. 登录 云防火墙控制台，单击选择**防火墙开关** > **NAT 边界开关**，进入NAT 边界开关页面。
2. 在 NAT 边界开关菜单，单击**防火墙开关**页查看所有已开启和未开启的子网信息。

NAT 边界防火墙开关里实例配置-域名解析开关开了后，需要重启服务器么? 不操作会生效么?

不需要重启服务器，重启服务器仅是让配置生效快些，这个跟在私有网络控制台上配置 DNS 生效时间是一样的。刷新网络配置可用以下命令：

- Linux：可执行 dhclient
- windows: ipconfig /flushdns

NAT 边界防火墙开关自动同步资产的周期是多长?

10分钟。

NAT 边界防火墙限速可以配置多少条规则?

100条。

NAT 边界防火墙接入模式下可以同时接多少个 NAT 网关?

默认可以同时接5个，超过建议使用新的 NAT 边界防火墙实例来接入。

NAT 边界防火墙子网开关被关闭是什么原因?

1. 默认设置因素：NAT 防火墙开关在初始配置时，默认处于关闭状态，需要手动开启。
2. 私有网络及路由表关联因素：在私有网络环境下，路由表中的云防火墙的高可用 VIP 开关处于特定状态时，例如流量过载、维护或升级状态等，可能会触发系统逻辑，致使 NAT 防火墙开关被关闭。

NAT 边界防火墙的子网开关无法开启是什么原因?

可能资产规模在后台轮询间隔内发生变化，但尚未被同步导致，您可登录 云防火墙控制台 ，单击**防火墙开关>互联网边界开关>同步资产**，主动调用后台接口重新读取并同步子网的资产信息后，再尝试开启。

NAT 边界防火墙如何更换 VPC ?

在 NAT 防火墙实例页面，选择更改的防火墙，单击**更多**，选择接入配置，可以重新选择接入VPC。

NAT 边界防火墙可以绑定多少 VPC ?

暂无限制。

开启 NAT 边界防火墙后，分配的弹性 IP 为什么不支持访问?

新分配的 EIP 需要绑定才可以被访问。

NAT 边界防火墙实例个数是否有个数限制?

NAT 防火墙的实例个数是有限制的；受版本通用配额限制，高级版，企业版，旗舰版 分别是1个、2个、3个。

将某个子网从 NAT 边界防火墙（新增模式）切换到 NAT 网关，是否能在不影响网络的前提下实现?

1. 为各 VPC 购买 NAT 网关。
2. 修改路由表，将下一条指向 NAT 网关。
3. 关闭防火墙功能并销毁防火墙实例。

以上操作确保内网资源能够访问外网，由于用户的部分应用需要对出口 IP 进行白名单操作，最好联系相关人员将 NAT 网关的 EIP 添加到白名单中；否则，可能导致部分应用无法访问。

如何在 NAT 边界防火墙阻断后核实数据?

在 NAT 边界防火墙的状态监控—连接数—会话视角处，进行“阻断操作”后刷新界面，如果原本的数据仍然存在，可进行如下操作：

1. 进行“阻断操作”后，该界面的状态不会立即更新，这是正常的；因此，不建议连续执行此操作。
2. 可以通过查看企业安全组来确认规则是否已下发。当企业安全组的自动下发按钮开关处于打开状态时，规则会自动下发；如果未打开，则需要手动下发。

NAT 边界防火墙的入向黑名单/白名单能力，是和串行模式一致，还是和旁路模式一致?

能力一致，封禁最大上限一致。

如何统计 NAT 边界防火墙和 VPC 防火墙实例中的规则数量?

下发规则数 = 源地址个数 × 目的地址个数 × 端口个数 × 协议个数。

- 访问源目地址个数：IP/IP 段、资产类型都计为1个。资产分组、资产标签和模板则按拆分后的地址数量计算。
- 目的端口个数：按英文逗号分隔算，若无英文逗号则计为1个。
- 协议个数：四层 ANY 计为3个，七层 ANY 计为6个。HTTP/HTTPS 或 SMTP/SMTPS计为2个，单个协议计为1个。

NAT 网关上添加的 DNAT 规则会自动同步到 NAT 边界防火墙吗?

NAT 边界防火墙实例创建前，在 NAT 网关上添加的规则会在开启防火墙开关后自动同步 DNAT 规则至防火墙。但是，创建防火墙之后在 NAT 上添加的规则，在防火墙同步过来后不会生效，因此需要用户在云防火墙控制台上手动添加。

在关闭或销毁 NAT 边界防火墙后，DNAT 规则会自动同步到 NAT 网关吗?

当 NAT 防火墙被销毁后，用户在云防火墙控制台上添加的 DNAT 规则会被防火墙同步到 NAT 网关；如果该 NAT 网关再次连接到 NAT 防火墙，之前在防火墙上创建的 DNAT 规则则不会自动同步回 NAT 防火墙。

NAT 边界防火墙/VPC 防火墙引擎更新是否会通知用户?

如果引擎有更新，控制台会弹出提示窗口；每个引擎版本只会提示一次。
用户可以前往 防火墙开关 > **NAT 边界开关**页面，在防火墙实例页签，单击**引擎更新**，查看引擎是否为最新版本。

NAT 边界防火墙带宽超量后会有什么影响?

带宽超量后会限流，限流的结果可能是网络延迟增大，连接访问超时后可能导致丢包的现象，建议及时扩容带宽。

假如 VPC1、VPC2、VPC3都独占 IP，所有 IP 都用完了，剩下没绑定的 VPC 会走哪个 IP?

若当前只剩下一个未被独占的 IP 时，无法使用独占 IP 功能，剩下的一个 IP 不允许勾选独占。

NAT 边界防火墙最后配置了一条全阻断规则前面没有放通规则，curl 以及 ping 测试正常拦截，为什么 telnet 测试可以通?

访问控制规则里有配置七层规则会放通，因为要检测七层规则，所有的流量都要先放行 TCP 三次握手，所以这里 telnet 能通。

VPC 间防火墙

最近更新时间：2025-02-11 17:13:22

为什么有部分 VPC 间防火墙开关无法开启?

由于路由和网段冲突等原因，云防火墙对产生冲突的开关进行了限制，您可以根据开关错误提示消除冲突后，再尝试开启 VPC 间防火墙。

VPC 里自动创建的防火墙子网以及路由表里的防火墙路由是什么?

开启了 VPC 间防火墙开关后，引流控制所需的防火墙子网和防火墙路由将自动创建，请勿尝试手动删除，以免影响云防火墙的使用。若您希望更改防火墙子网网段，可以 提交工单 联系我们。

VPC 间防火墙负责引流 VPC 间的哪些子网?

VPC 间防火墙引流的范围取决于您在 VPC 间的路由配置，云防火墙只对正确配置了 VPC 间路由的子网进行引流操作。

VPC 间防火墙的带宽达到规格限制，会有什么影响，应该如何处理?

在当前版本中，由于 VPC 间防火墙采用用户独占资源的部署形式，目前尚不支持弹性扩容。
因此，当 VPC 间防火墙的带宽超出能力规格后，防火墙会丢弃超带宽部分数据包，可能会造成网络延迟、拥堵或阻塞。为了您的业务正常运行，建议您合理预估带宽规格，提前扩容防火墙带宽。

VPC 间防火墙是否能防护第三方 VPC 访问的流量?

可通过 VPC 间防火墙云联网模式进行防护。

VPC 间防火墙最大支持多大带宽?

20G。

VPC 间防火墙支持对 UDP 的阻断吗?

VPC 防火墙是串行在用户网络中，真实更改了客户路由，所有 UDP 协议的流量都能进行阻断。

VPC 间防火墙能覆盖 VPN 和专线间的防护吗?

支持，需要通过 购买云联网 打通。

为什么要拆分 VPC 间防火墙实例?

一个防火墙本质上是由多个防火墙实例组成的。在之前的版本中会将实例概念弱化，不便于监控和分析每个防火墙实例的状态。因此，在新版本中，我们强化了防火墙实例的概念，使其信息层级与 NAT 防火墙对齐，界面结构更加清晰。

同地域多实例解决了什么问题?

在之前的版本中，我们会在每个地域部署一个防火墙实例，用以实现网络接入。然而，由于路由策略的限制，当 VPC 数量过多时，无法实现有效防护。
目前，VPC 间防火墙支持在同一地域下部署多个防火墙实例（私有网络模式），从而实现对更多 VPC 的防护。

路由模式的配置解决了哪些痛点?

由于不同用户的网络结构不同，因此当 VPC 数量过多时，开关数量会变得复杂且难以维护。通过对单点模式、多点模式、全互通模式、自定义路由模式的灵活选择，用户可以根据网络拓扑结构选择合适的路由引流方案，从而简化开关控制逻辑。

云联网模式 VPC 墙是否支持接入后新增防火墙部署地域?

不支持，若想新增部署地域需销毁实例重建。

版权所有：腾讯云计算（北京）有限责任公司

云防火墙配置针对53端口的 UDP 解析请求的阻断逻辑是什么？

当触发 ACL 拦截规则时，云防火墙会伪造 DNS 应答包，即云防火墙代替 DNS 服务器发送 NXDOMAIN 响应包，以阻断 DNS 请求。这样做是为了防止被阻断的 DNS 请求重试并通过。如果需要允许 DNS 请求，建议在配置中将 DNS 放行规则置于最前。此配置会导致 `/etc/resolv.conf` 文件中指定的 DNS 服务器不会尝试向下一个地址请求解析。

功能相关
流量中心

最近更新时间：2025-02-25 10:46:52

云防火墙流量带宽图的具体延迟时间多长？

一般情况下延迟1分钟。

流量中心多长时间更新一次？流量日志多久更新一次？

流量中心列表10分钟更新一次，流量日志实时更新。

云防火墙流量峰值匹配不上？

- 流量图显示均值带宽，其中：均值带宽是指统计时间刻度内的均值。
- 峰值是根据10秒内的流量进行统计来计算的，10秒报一个单 IP 的均值，然后一段时间范围内取最大为峰值。
- 告警和计费都是基于页面上看到的流量统计。

为什么部分流量日志中前往目标443端口的请求没有包含域名信息？

1. TCP 握手未完成或建立连接失败。
2. 访问时未通过域名。
3. 客户端请求未携带 SNI。

云防火墙的流量分析 VPC 在哪些地区部署，是否采用就近分析？

目前仅在广州地区部署。实际上，根据客户的业务需求，在每个地区都设有一个集群进行就近处理。

云防火墙 NDR 的最大分析流量是多少，引流的 Private Link 性能上限是多少？

Private Link 的性能上限未能达到理论值，实际上限取决于服务器的内网带宽。

如何判断流量是内网流量还是公网流量，通过专线导入的其他云流量应如何判定？

根据源地址的 IP 类型判断。由于专线连接的对端 VPC 属于内网，因此该流量被认定为内网流量。

如果大部分流量是 HTTPS，流量分析传入的入侵防御引擎的规则是否仍然有效？

入侵防御规则中也包括对 HTTPS 有效的规则，特别是那些漏洞利用流量，可以通过正则表达式匹配到特征，因此即使是加密流量也能检测到一些警报。

流量分析记录的日志大小是多少？

单个会话的最大记录为1000字节。实际上，数据经过压缩处理，并非传输的所有数据包都被记录。

版权所有：腾讯云计算（北京）有限责任公司

访问控制

最近更新时间：2025-02-25 10:46:52

未配置任何规则时，云防火墙默认规则是放行还是拦截？

云防火墙默认放行所有流量，打开云防火墙开关后，云防火墙会开始记录流量日志并产生入侵防御告警，但由于没有配置规则，所以此时不会阻断任何流量。

云防火墙 CFW 如何配置实现只允许访问放行的端口？

1. 开启互联网防火墙后，单击选择 访问控制 > **互联网边界规则** > **入站规则**，进入入站规则页面。
2. 在入站规则页面中，单击**添加规则**放行您需要的端口，同时添加一条阻断所有端口的规则即可。

> **说明：**
> 互联网防火墙在无规则的情况下默认放行所有流量。

配置访问控制规则后，需要多长时间生效？

云防火墙配置规则后，需要10秒到1分钟左右使规则生效。

云墙支持通过域名进行访问控制么？

互联网防火墙和 NAT 防火墙均支持在出站规则中使用域名，VPC 间防火墙也支持域名访问控制规则。

云防火墙支持通过域名来配置限制策略吗？

目前中国大陆和中国香港地区资产支持通过域名来配置限制策略。

云防火墙是否有地域封禁功能？

企业版及以上版本有地域封禁功能。

在云防火墙添加入站规则时，无法选择部分地址模板的原因是什么？

无论是入站的访问源还是访问目的，都无法选择域名模板。出站的访问源无法选择域名模板，但访问目的可以选择，这是因为入站的来源不可能会是域名。

云防火墙（CFW）的访问控制与私有网络（VPC）中安全组的功能有何不同？

VPC 安全组功能较为有限，通常用于为服务器特定服务设置白名单。推荐使用 CFW 的企业安全组，它支持智能算法来统一部署策略。

云防是否支持防护 UDP 协议？

NAT 边界防火墙、企业安全组、VPC 间防火墙支持 UDP 防护，互联网边界旁路墙不支持。

NAT 防火墙规则条目可以扩展多少条？

可以扩展到2万条。

为什么在互联网边界防火墙配置禁止境外地域访问后，告警中心仍然产生观察规则条目？

1. 如果 ACL 日志中未发现相应的阻断请求，需要检查是否存在其他优先级更高的放行规则。
2. 如果 ACL 日志中记录了相应的阻断请求，这可能是由于旁路抢答机制引起的。如果担心此问题，可以在告警中心手动封禁所有来自境外的攻击告警。

为什么配置了访问控制规则后，有些请求仍然出现在告警中心展示且未被拦截？

- 可能是访问控制规则尚未生效。
- 在访问控制规则已生效的情况下，可能是由于互联网边界防火墙的旁路漏包现象导致。旁路防火墙通过镜像网络流量进行分析，其中一部分流量可能被入侵防御系统匹配并产生告警，但实际上这些访问请求已经被拦截。

云防火墙的访问控制支持配置特定生效时间段吗？

建议在 常用工具页面 选择**自动化工具**来配置规则的生效时间，并根据具体场景配置规则的启用与停用时间。详情请参见 添加自动化任务 。

开启 NAT 防火墙访问控制的长连接有哪些使用限制？

1. 引擎需要保持最新，建议进行更新，详情请参见 防火墙引擎升级 。
2. 最大连接数受到带宽规格的限制，详情请参见 防火墙常见问题 。

当获得域名后，如果该域名解析的 IP 与现有 IP 规则发生冲突，应如何处理？

处理优先级较高的规则。

云防火墙域名限制规则下发为 IP 后，攻击者能否通过修改 host 绕过？

云防火墙基于权威 DNS 解析生成的 IP 规则进行拦截，攻击者修改本地 host 不影响规则生效，因此无法绕过。

零信任运维

最近更新时间：2024-04-22 17:25:32

iOA 和云防火墙的关系?

- 计费关系：云防火墙零信任运维套餐为联合售卖模式，自带 iOA SaaS 版，包含 iOA基础套餐 全部功能，可前往 iOA 控制台 查看和使用。
- 功能关系：通过在用户的办公网中部署 iOA，可以构建基于身份的零信任安全体系。防火墙通过获取 iOA 的身份，可实现基于办公网身份认证体系的鉴权和访问控制，带来更连贯更便捷的运维体验。在云防火墙控制台进行资产的接入，无需再前往 iOA 控制台部署连接器、接入资产、分配权限等操作，节省您手动部署的时间，提升部署效率。

地域主备 EIP 的作用?

- EIP 作用：基于 iOA 的零信任安全体系，运维内网资产需要有一个公网 EIP 用于与 iOA 安全网关进行通信。云防火墙通过集成 iOA 连接器，无需手动部署，仅需选择 EIP 绑定即可。
- 主备 EIP：一个地域最多支持绑定两个 EIP，可构建两个连接器实现主备容灾配置。

接入对网络有影响么?

不会。云防火墙资产接入仅会打通资产与办公网之间的数据链路，对于办公网访问授权资源相当于加了一层身份认证网关，对网络无影响。接入操作会在您对应的 VPC 中创建一个29网段的子网用于引流。

什么是身份视角和规则视角?

零信任运维底层采用白名单形式，即配置基于身份和资产的访问控制白名单。通过规则形式展示出来即为规则视角。
身份视角是基于白名单规则，通过对应身份具有的资源权限进行聚合，以身份的视角查询或配置拥有的资源权限，方便您进行配置。

微信远程运维中开启“禁用端口”功能后，会禁止哪些 IP 的端口?

开启后，将自动下发互联网边界访问控制规则和企业安全组规则，阻断公网 IP 对资产登录协议端口的全部互联网访问，该指令仅生效于开启了互联网边界开关的公网 IP。

> **说明：**
> 如果开启“封禁端口”后资产登录协议端口发生修改，需要重新开启一次“封禁端口”功能。

资产未启用互联网边界开关，该资产的登录协议端口会被封禁么?

不会被封禁。

为什么配置了安全访问控制，扫码授权后，没有跳出让输入资源密码?

请检查您的资源机默认端口是否已更改，如果非22端口或3389端口，请到 访问控制 > **身份访问规则** > **实例管理**中修改。

支持 Windows 的远程桌面微信授权么?

支持。

Windows 中使用 cmd 进行远程运维时出现乱码?

请执行 chcp 65001 指令或使用 cmd 最下方给出的链接扫码登录。

入侵防御
基础防御

最近更新时间：2024-11-04 22:00:22

哪些流量经过入侵防御模块的检查？

当前版本的互联网边界防火墙、NAT 边界防火墙以及 VPC 间防火墙都支持入侵防御功能。详情以高级设置中的入侵防御开关是否开启为准。

入侵防御防护模式为拦截模式时会拦截哪些事件？

在拦截模式下，防火墙会根据以下特征进行拦截。

- 威胁情报：自动拦截高置信度的网络攻击/恶意访问，支持自动拦截出站恶意访问。
- 基础防御：针对部分高置信度的规则支持自动拦截，其他规则仍然产生安全事件告警。
- 虚拟补丁：支持自动拦截所有被检测为漏洞利用的流量。

告警列表中的风险如何手动拦截？可以自己增加拦截 IP 吗？

对于告警列表中告警次数多或危险等级高的风险，用户可以手动进行拦截。同时，用户可以自行在入侵防御的拦截列表中导入需要拦截的 IP 信息，当该 IP 进行访问时，将直接被云防火墙拦截。

拦截模式中，什么情况下会自动拦截？为什么开启了拦截模式还会有告警？

- 拦截模式中，云防火墙会自动拦截高置信度风险以及拦截列表中的 IP。
- 对于低置信度的风险将进行告警，不会自动拦截，用户可在告警中心中手动对告警 IP 进行拦截。

严格模式中，对恶意 IP 的拦截是怎样实行的？

严格模式中威胁情报、基础防御、虚拟补丁均为全局拦截模式，会对所有产生告警的 IP 进行拦截。高置信度风险及拦截列表中的 IP 将在首次访问时被拦截，其他恶意 IP 将在首次访问告警后，第二次访问时被直接拦截。

为什么恶意 IP 没有被拦截？

云防火墙的入侵防御功能是基于会话的，仅会拦截有攻击特征的会话访问。如果用户未将该 IP 加入拦截列表，则不会拦截该 IP 的正常访问会话。

拦截模式什么时候开？

一般从观察告警模式切换到阻断拦截模式，业务没有变化，观察1-2天即可持续开启。

策略是否精准，直接开拦截阻断后对业务造成影响怎么办？

入侵防御模块中，系统仅将高精准度的规则可设置为拦截模式，特别是虚拟补丁的还没出现过误报。如果开阻断后出现任何问题，可以随时联系我们获取相关帮助。

云防火墙拦截模式开启后，是否会影响到云内网地址间的通信？

- 如果您启用了互联网边界防火墙与 NAT 边界防火墙的拦截模式，云防火墙仅会防护南北向流量，这部分开关关联的东西向流量不会经过防火墙。
- 如果您启用了 VPC 间防火墙的拦截模式，云防火墙会对东西向流量进行检查和拦截，可能会影响到云内网间地址的通信。

IP 被入侵防御误拦截了要怎么办？

1. 登录 云防火墙控制台 ，单击**日志审计** > **入侵防御日志**可查询源或目的 IP 是否有明确的拦截记录。

2. 当遇到紧急情况时，您可以进入 入侵防御，**关闭“启用拦截列表”，将拦截列表停用，并进入** 告警中心 > **阻断拦截统计**查看所有拦截统计，排查定位拦截来源。
3. 在定位并修复故障原因后，可打开“启用拦截列表”开关，将该功能重新开启。

有误拦或无法访问的情况，如何快速定位恢复访问?

- 对于公网 IP 的防火墙开关修改为关闭状态，则流量不经过云防火墙。
- IPS 修改为观察模式，确认非 IPS 拦截导致。
- 策略配置 any 即该公网 IP 全通，确认非云防火墙策略导致。

> **说明：**
> 若完成以上操作仍有误拦和无法访问的情况，请 提交工单 。

为什么之前在入侵防御的拦截列表里的 IP不见了?

1. 在拦截列表内，当某一个 IP 的生效时间到期后，列表会自动删除该 IP，此时该 IP 后续的流量访问将不会被防火墙拦截。
2. 为了避免黑名单自动移除存在安全隐患的 IP，可以在列表右侧操作栏，单击**编辑**，对需要操作的 IP 的终止时间和日期进行修改。

在入侵防御的忽略列表的 IP 还会被拦截么?

忽略列表中的 IP 地址，会直接绕过 IDPS 功能。

我要针对某个 IP 忽略某个指定的检测规则要如何配置?

暂时不支持某项特定规则检测的忽略操作。

什么情况解析域名的流量不会经过云防火墙?

- 腾讯云 CVM 可能会使用腾讯自建的 DNS 解析服务，产生的 DNS 报文不会经过互联网边界，因此导致缺失该部分域名访问的告警与日志。
- 若您希望某台 CVM 能够正常使用云防火墙的域名检测与告警功能，可手动将/etc/resolv.conf 文件下的解析地址改为8.8.8.8。

入侵防御与访问控制的关系?

- 云防火墙判定顺序：**封禁列表** > **访问控制规则** > **放通列表** >**入侵防御规则**。
- 入侵防御功能只生效于开启了防火墙开关的资产，未开启防护的资产的流量不会经过防火墙处理。

版权所有：腾讯云计算（北京）有限责任公司

防御策略

最近更新时间：2024-06-18 16:46:51

威胁情报的拦截模式支持哪些流量的自动拦截？

开启威胁情报拦截模式，NAT 边界防火墙会对出站方向的威胁情报告警进行自动拦截，互联网边界防火墙和入站方向仍然是观察告警模式。

虚拟补丁的拦截模式支持哪些流量的自动拦截？

开启虚拟补丁拦截模式，互联网边界防火墙会对所有互联网边界流量的漏洞利用和漏洞攻击进行自动识别，针对告警的连接进行自动拦截。

云防火墙的IPS虚拟补丁和主机安全产品的补丁有什么区别？

- 主机上的补丁，一般是由官方发布，官方的补丁发布时间比较长，一般要几周甚至几月才能修复，且有些需要重启 CVM 云服务器。
- 云墙上的 IPS 虚拟补丁，是根据漏洞的利用特征，在云防火墙 IPS 系统中实时更新的防御规则，可以做到小时级别的更新，且不需要对业务有任何改造，也不需要重启业务系统。
- 云墙的 IPS 虚拟补丁与主机安全产品（例如主机安全）结合，实现了网络和主机端的立体防御，这是一种有效的防护主机安全的组合。

有了虚拟补丁，我还需要在主机修复补丁吗？

还是需要的，虚拟补丁可以为您做最前线的防护，但是根本漏洞还是需要做彻底的解决，才能做到最安全。

入侵防护相应规则的危险等级是如何定义的？

- 基础防御和虚拟补丁的危险等级是基于这次攻击可能带来的危害定义的。
- 威胁情报的危险等级是基于这个 IP 或者域名在我们的历史大数据中曾经产生过的攻击危害程度来定义的。

云防火墙的威胁情况情报包更新审核机制是怎样的？

情报分为高精准情报包和重保情报包，有以下特点：

- 高精准情报包有完整的去误报流程。
- 重保情报包针对重保场景，主要针对非真人 IP，仅用于严格模式使用，拦截/观察模式默认不开启。

入侵防御里面虚拟补丁，是否能识别 shiro 漏洞的流量？

可以检测，但是不一定可以覆盖全部场景，因为有些是加密流量。

云防火墙支持防护哪些漏洞？

详情请到 入侵防御 > **情报中心**搜索查看。

防火墙是怎么判断有 web 攻击的？

外部黑客在扫描嗅探的时候会带特征过来，例如 weblogic 这个漏洞，扫描到攻击特征时防火墙就会判定为尝试攻击。

认证暴力猜解的防护，支持哪些协议类型？

支持以下协议：MySQL、Oracle、SSH、Redis、MongoDB、IMAP、POP3、FTP、SMTP、SQLServer 和 RDP。

针对存在的挖矿攻击，应该怎么处理？

- 没有购买主机安全 ，不一定需要重装机器，手工杀毒即可，挖矿即为处于中毒的状态。
- 如果购买过主机安全，可以直接使用主机安全来清除威胁。

版权所有：腾讯云计算（北京）有限责任公司

告警中心

最近更新时间：2025-02-25 10:46:53

安全基线的告警信息消失了?

告警类型后面的数字表示当前列表中未处置的告警数量（ BOT 攻击展示全部告警数量）。如果对应的安全基线告警开关没有开启，控制台将不会显示安全基线的选项。

为什么拦截后还要封禁?

入侵防御功能对网络攻击的检测是基于会话的，只有当封禁该 IP（加入到拦截列表）时，才会对 IP 的所有访问操作进行拦截。

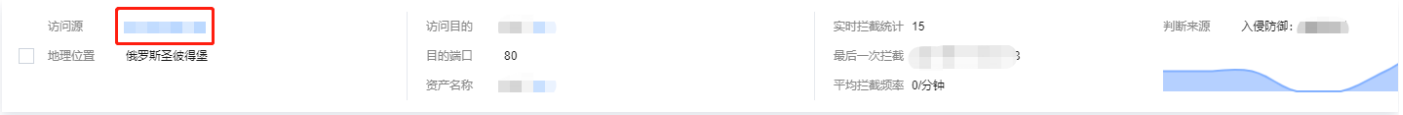
对事件进行操作后，想修改怎么办?

登录 云防火墙控制台，进入 入侵防御 模块，可以在“拦截列表”或“忽略列表”中删除。

如何查看某IP的威胁画像?

- 在安全事件告警中，您可以参考 安全事件告警-事件详情 中的查看威胁画像。

- 在阻断拦截统计中，您可以直接单击 **IP 地址**进行跳转。



IP 地址右侧出现红色感叹号?

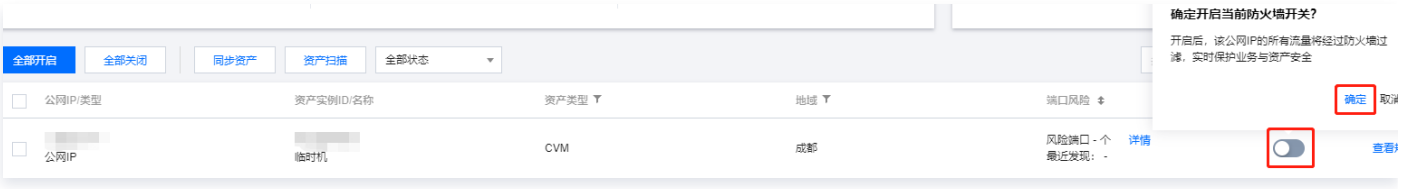
该 IP 可能是腾讯云 CDN 地址 ，我们不建议您手动拦截或封禁。如果您已开启入侵防御拦截模式，云防火墙会自动拦截来源于这个地址的攻击流量；对于正常流量我们将放行，请您放心。

告警中心数据多久更新一次?

告警中心数据10分钟更新一次。

购买 CFW 后，需要做什么操作，告警中心才会有流量趋势图?

1. 在 防火墙开关 页面中，选择相应实例单击**防火墙开关 > 确定**，开启防火墙开关。



2. 在开启防火墙开关后，云防火墙的访问控制缺省为全通模式，入侵防御缺省是观察模式，因此对业务系统无任何影响。

为什么在告警中心阻断统计看不到数据?

1. 请确认您是否已开启相应的防火墙开关并已设置阻断或拦截模式。
2. 在阻断统计下方选择全部策略，查看是否可以看到相应的事件。
3. 若仍无法看到相应的事件，请 联系我们 以便进一步核实，感谢您的理解和支持。

告警中心设置告警对象不勾选主账号和子账号的情况下，还能收到带宽告警吗?

若未勾选接收告警的主账号和子账号，将不会收到告警中心的短信、站内信和微信通知，但控制台依然会显示告警。

防火墙拦截模式下，告警中心产生的威胁情报告警为何无法执行封禁操作（显示为灰色）?

当前互联网旁路防火墙尚不支持 UDP 协议的封禁功能，请核实是否为 UDP 协议。

防火墙设置了告警，但是基于威胁情报的入站攻击行为没有触发短信告警，这正常吗?

通常，只有出站方向的攻击行为会触发威胁情报告警。威胁情报针对入站方向的告警一般程度较轻，因此不会触发告警、地域等功能点。

为什么自动封禁的事件也会展现在防火墙告警中心?

处理流程是是告警，再处置。当首次检测到攻击时，系统会发出告警并自动处置，即将其拉入黑名单。当第二次检测到攻击时，该事件会被拦截，并记录在拦截统计中。

防火墙告警中心的告警事件未能实时展示的原因是什么?

告警中心主要用于报表统计和日志聚合，通常存在15-20分钟的延时。

攻击告警汇总中，跟踪告警事件是根据什么来汇总显示的?

同一天的告警，在源目 IP、命中规则一致的情况下，告警中心会将端口不一致的至多50个端口的事件汇聚成一条告警事件；需要注意的是：威胁情报的入站告警会将目的 IP 的资产汇聚在一起（如下图）

处置告警中心失陷主机相关告警事件后，如何将失陷主机数量从1调整为0?

需要忽略告警事件，这样计数才能调整为0。如果需要封禁攻击 IP，可以在 入侵防御-封禁列表 中添加 ACL 规则。
如果在忽略之后再次将 IP 加入封禁列表，失陷主机的计数将会重新变为1。

为什么在告警中心中的攻击告警统计中，查看非近7天的曲线图没有数据?

告警中心的攻击告警统计曲线图仅统计近7天的数据。

安全基线

最近更新时间：2023-09-22 14:13:04

云防火墙的安全基线是什么？

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。
当安全基线设置完成后，每新增一个在基线之外的 IP 地址或域名访问都会触发安全告警。用户可以在告警列表中对 IP 地址或域名进行处理，安全基线适用于重保期间的流量基线防护。

为什么基线检测时间是灰色的无法选择？

您可以查看上面基线评分的任务状态，基线学习状态下是不可选基线检测时间的。

- 基线学习时间：加入基线时间到基线结束时间范围内的统计数据。
- 基线检测时间：加入基线时间到当前时间范围内的统计数据。

版权所有：腾讯云计算（北京）有限责任公司

日志相关

最近更新时间：2024-07-04 15:27:21

云防火墙日志默认存储多长时间？最大存储容量是多少？

- 云防火墙免费默认存储7天内的日志，最大50GB存储容量。
- 开通日志分析服务后，云防火墙会默认存储6个月内的日志，存储容量1000GB起售，最大可扩展至300TB。

日志审计与分析与 CLS 是什么关系？

目前日志审计是云防火墙内置，与 CLS 无关。防火墙日志可以通过 Ckafka 投递至 CLS，方便用户自行分析。

访问控制日志、入侵防御日志、流量日志分别记录什么流量？

- 访问控制日志记录命中访问控制规则的流量。
- 入侵防御日志记录命中入侵防御规则的流量。
- 流量日志记录放行的流量，以及拦截流量的一个请求数据。

可以把防火墙日志拿出来做归档吗？

可以，日志支持导出和日志投递功能，投递到客户的 kafka。

日志如何下载？

- 您可通过日志投递功能将日志转投出来分析使用（前提是 购买腾讯云消息队列 Ckafka 实例）配置参考 日志分析 。
- 或登录 云防火墙控制台 ，单击左侧操作栏中**日志审计** > **流量日志**进入流量日志页面，单击右上角 ，即可下载日志。

> **说明**
> 基于当前检索条件导出，最多可支持导出100万条日志，每月享有一定导出额度。

日志投递需要多长时间才能投递成功？

投递日志需1分钟左右的时间，所以相关日志更新会有稍许延迟。

投递出来的日志是否有 tags 标记日志类型？

日志中没有标识日志类型的 tags，建议您在投递日志的时候，选择不同的 topic，以区分不同的日志。

拦截模式已开启，为什么日志中还会出现观察类型的？

虚拟补丁是自动拦截，如果入侵里有漏洞攻击且命中虚拟补丁就会自动拦截。基础规则支持高置信度的基础规则自动拦截，若基础规则不为高置信度则不拦截。

流量日志是否会记录被访问控制规则或入侵防御拦截的 IP 流量日志？

流量日志记录放行的流量，以及被访问控制规则或入侵防御拦截的 IP 流量的一个请求数据包信息。

被拦截的攻击，是否会产生日志？

- 访问控制规则：阻断模式拦截访问数据，记录规则命中次数，同时记录访问控制日志。
- 入侵检测：命中入侵检测策略的生成入侵检测事件，您可通过日志分析查看具体的拦截日志。

如何查看投递出来的日志中的访问/攻击是被阻断还是放行？

日志中的 strategy 字段标识了该访问是阻断或观察的。

> **说明**
> 流量日志无 strategy 字段值。

账号相关

最近更新时间：2024-11-14 17:38:22

云防火墙可以给其他腾讯云账号使用么？

云防火墙不可以跨账号使用，云防火墙仅能防护当前腾讯云主账号下的云资产。

进行角色创建授权会影响业务正常进行吗？

不会，创建角色授权是用户通过授权允许云防火墙后台系统读取您的云上资源、私有网络、子网等数据，用来构建页面操作所需数据呈现，不会进行任何影响业务的自动化操作。

告警中心设置告警对象不勾选主账号和子账号的情况下，还能收到带宽告警么？

若未勾选接收告警的主账号和子账号，将不会收到告警中心的短信、站内信和微信通知，但控制台依然会显示告警。

如何给子账号授权云墙的权限？

您需要先在CAM角色处创建云防火墙角色，之后在子账号处添加以下6个权限即可：

- QcloudCFWFullAccess
- QcloudSSAFullAccess
- QcloudVSSFullAccess
- QcloudCWPFullAccess
- QcloudAccessForCFWRole
- QcloudCamSubaccountsAuthorizeRoleFullAccess

云服务器概览页无法打开提示您没有权限执行此操作，失败信息描述：you are not authorized to perform operation(cfw:DescribeCfwUserStatus)？

该细项权限暂未加入 CAM，请暂时给该子账号配置以下权限：

- QcloudCFWFullAccess
- QcloudCFWReadOnlyAccess

计费相关

最近更新时间：2024-11-04 22:00:22

云防火墙是否支持修改配置？

云防火墙可以通过升级扩容来提升已购买的配置，暂时不支持自主降低已购买的版本配置。

云防火墙到期后可以续费吗？到期后资源会被系统回收吗？

云防火墙使用期限只支持在购买时选择，在到期之后会自动停止服务，需要继续使用可以重新购买，对业务不会造成影响。

- 若在产品到期14天内续费，可以恢复配置信息。
- 产品到期14天后，系统回收所有云防火墙的资源且无法恢复，只能重新购买后再次配置。

一个账号可以购买几个云防火墙？

一个账号能购买一个云防火墙，目前云防火墙提供三个收费版本，分别是高级版、企业版和旗舰版。

云防火墙是否可以退费？

云防火墙产品遵守腾讯云 云服务退货说明 ，若您在购买云防火墙后有任何不满意，我们支持五天无理由退款。如需退款，请 提交工单 联系我们，产品使用超过5天后，不支持退款。

其他

最近更新时间：2023-10-26 19:23:51

概览页面中，公网资产是否会被自动识别？如何实现的？

会自动识别，是通过腾讯云接口，CAM 授权拿到这些；这个账号下的所有资产是通过云 api 枚举出来的。

开启防火墙后，想先开启观察模式，暂时不进行拦截阻断。应该怎么设置？

打开公网 IP 防火墙开关即可，开启防火墙开关后，默认是观察告警模式，不需要配访问控制列表 ACL， 访问控制缺省为全通。

IP被拦截了，我需要在哪里确定是不是被云防火墙拦截的？

- 登录 云防火墙控制台 ，通过单击**日志审计** > **入侵防御日志**和**访问控制日志**模块查询IP是不是被云墙拦截了。
- 另在 告警中心 > **攻击拦截统计**页面，可以查询云防火墙在入侵防御模块中所进行的拦截工作。

如何查看云防火墙版本？

可在 概览页面 左上角查看当前账号的套餐版本和到期日期。

云防火墙是否可以根据 MAC 地址做限制？

云防火墙不会根据 MAC 地址做限制。云网络屏蔽掉了二层，只能通过 IP 寻址。CVM 之间就不是通过 ARP 而是 IP 寻址。

云墙带宽告警阈值是否可以调整或关闭？

带宽告警是云墙重要指标，超过带宽将会无法对超过部分的流量进行防护，您可以在控制台调整第一二级告警阈值，不支持关闭。

云防火墙的开关、扩容、添加 CAM 授权、入侵防御开关是否会对业务造成影响？

- 互联网边界防火墙开启不会对业务有影响；NAT 防火墙和 VPC 防火墙开启会对云联网有一个1-2s的闪断，建议您在业务非高峰期操作。
- 互联网边界防火墙的扩容不会对业务有影响；NAT 防火墙的扩容可能会产生1-2s的闪断，请 提交工单 咨询。
- 云防火墙的扩容、入侵防御的开关和添加 CAM 授权不会对业务造成影响。

在消息中心配置了接收人但配置未生效？

- 如果您在消息中心配置了接收人仍未收到消息推送或与配置内容不一致，可能是因为 通知设置 > 消息中心订阅设置 暂未开启。
- 云防火墙默认会推送非订阅消息，会根据 通知设置 中的接收人和接受内容进行推送。如果需要启用消息中心配置，请开启 通知设置 > 消息中心订阅设置 。

版权所有：腾讯云计算（北京）有限责任公司