云防火墙

常见问题

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 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默示的承诺或保证。

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
  - NAT 边界防火墙
  - VPC 间防火墙
- 功能相关
  - 流量中心
  - 访问控制
  - 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：2023-12-11 16:52:14

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？

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。
云防火墙包涵全部业务防护，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。

云防火墙可以防护 CDN 或 COS 吗？

云防火墙不支持 CDN、COS、高防 IP、Saas-WAF、cdb 等除数据库外的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，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。
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。

外部入站流量是先经过云防火墙还是 WAF？

对于入方向流量

SaaS-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。
SaaS-WAF 和云防火墙是并行工作，流量经过 SaaS-WAF 后，不再经过云防火墙。 如果需要串行部署，需要使用 CLB-WAF，流量先经过云防火墙，再经过 CLB-WAF。
说明：
saas-waf 回源到 clb/cvm 的流量也不会经过云防火墙，源站 cvm 主动外联可通过 nat 防火墙去识别检测。

对于出方向流量

可以通过 NAT 边界 FW（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 FW，则只能在互联网边界 FW，对 NAT gateway 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：2023-12-11 16:43:40

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。
NAT 和云防火墙相互独立，并相互串联。因此，需要挑选相同或更高容量的云防火墙带宽，来以确保边界防火墙带宽和 NAT 边界吞吐量满足用户的需求。

峰值带宽是指什么，是上行带宽还是下行带宽？

峰值带宽指的是上行和下行的带宽最大值。例如果购买100Mbps带宽，那么云防火墙能够同时处理上行100Mbps和下行100Mbps。

业务带宽超峰值带宽限制，会对我有业务影响么？

互联网边界防火墙属于旁路部署，超过防护带**不会造成客户业务流量丢包，不会影响客户流量速率**；NAT 防火墙是属于串联，超过防护带宽会造成客户业务流量丢包。如果公网流量大于购买的云防火墙边界带宽，则云防火墙**不承诺对超出带宽的流量进行防护。**对超出部分的流量，我们会做放行处理。
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。

出入站的带宽是分别计算的吗？若出站带宽超出购买规格，会影响入站流量的规则匹配吗？

是的，出入站的带宽是分别计算的。
云防火墙对超出购买带宽部分不承诺防护，若仅是出站的流量超出购买带宽无法匹配规则，不会影响入站流量的规则匹配。

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：
NAT 边界防火墙的带宽，和互联网边界防火墙保持一致。通过扩展互联网边界防火墙带宽，即可以扩展 NAT 边界防火墙带宽。

云防火墙的带宽支持任意升降吗？

带宽仅支持扩容，不支持降配。

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：2023-12-11 16:43:53

云防火墙支持防护哪些协议？

互联网边界防火墙目前支持 TCP、HTTP 以及 HTTPS 协议。
NAT 边界防火墙支持 TCP、UDP、ICMP、HTTP、HTTPS、SMTP、SMTPS 以及 FTP 协议。
VPC 间防火墙支持 TCP、UDP 以及 ICMP 协议。

云防火墙如何防护 UDP 协议？

由于互联网边界防火墙不支持防护 UDP 协议，我们建议您同时开启互联网边界防火墙和NAT防火墙。

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：2023-12-11 16:44:01

NAT 防火墙出去的数据会不会过两遍防火墙?

过两遍，一道管理内网 IP，一道管理公网 IP。

NAT 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边界开关上绑定 EIP，网络是否会闪断？

绑定不会造成闪断。

NAT边界开关开启或关闭某个 VPC 时该网络是否会闪断？

开启：若用户仅选择开启某个子网，系统会自动在当前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：若用户仅选择关闭某个子网，系统会自动关闭下一跳指向 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 边界开关页面左侧操作栏中，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 边界开关自动同步资产的周期是多长？

10分钟。

NAT 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 防火墙如何更换 VPC ？

在 NAT 防火墙右上角有设置按钮，点击之后选择重新选择接入 VPC。

NAT 防火墙可以绑定多少 VPC ？

暂无限制。

NAT 边界防火墙创建失败？

若您 VPC 下有使用专线和对等连接，您的 VPC 需要预留至少一个24/子网供给防火墙接入使用，防火墙才能创建成功。

开启NAT 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。

版权所有：腾讯云计算（北京）有限责任公司

VPC 间防火墙

最近更新时间：2023-12-11 16:44:11

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，为了不影响业务的正常运行，我们会在预留50%缓冲带宽的前提下，在临界情况下启用防火墙逃生通道，将 VPC 间防火墙切换到 BYPASS 模式。
说明：
BYPASS 机制下，云防火墙不处理任何流量，直接放行全部流量。
建议您持续关注云防火墙带宽告警，在带宽较高时，适当关闭一部分开关。

功能相关
流量中心

最近更新时间：2023-12-11 16:44:18

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，10s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。

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：2023-12-11 16:53:26

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。

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。

企业安全组无法自动双向下发，复选框是灰色的？

仅当访问源地址填写为实例、子网、私有网络地址时，方可通过自动双向下发，分配一条相同的出站规则（执行顺序为最高），适用于内对内的双向放行的场景。

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。

版权所有：腾讯云计算（北京）有限责任公司

入侵防御
基础防御

最近更新时间：2023-12-11 16:44:31

哪些流量经过入侵防御模块的检查？

互联网防火墙和 NAT 防火墙的流量都会经过入侵检测模块的检查。

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？

不会。拦截模式开启后，只会影响云上业务的互联网流量，不会影响到云内网地址间的通信。

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**菜单，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：**拦截列表** > **访问控制** > **忽略列表** > **入侵防御**。
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：2023-12-11 16:44:40

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 虚拟补丁结合主机安全产品如云镜，实现网络+主机端的立体防御，是防护主机安全的最佳组合。

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 mysql、oracle、ssh、redis、mongodb、imap、pop3、ftp、smtp、sqlserver 和 rdp 协议。

针对存在的挖矿攻击，应该怎么处理？

没有购买云镜（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。
如果购买过云镜（主机安全），可以直接使用云镜来清除威胁。

告警中心

最近更新时间：2024-07-05 15:52:07

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？

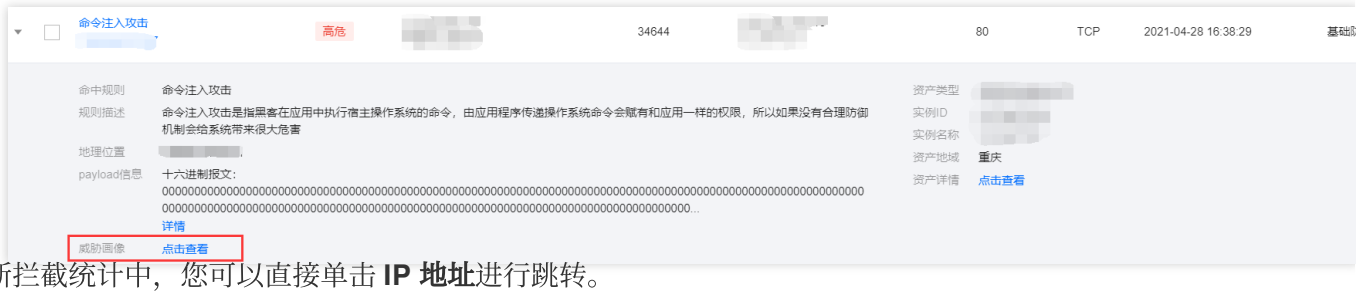
入侵防御功能对网络攻击的检测是基于会话的，只有当封禁该 IP（加入到拦截列表）时，才会对 IP 的所有访问操作进行拦截。

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和站内信通知，但控制台依然会显示告警。

版权所有：腾讯云计算（北京）有限责任公司

安全基线

最近更新时间：2023-12-11 16:44:57

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：2023-12-11 16:53:48

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。

日志存储超过套餐规定时间或容量会怎么处理？

使用50G默认日志存储容量时，留存超过7天和50GB外的日志将会被自动覆盖。
开通日志分析服务后，留存超出6个月的日志将被淘汰。
开通日志分析服务后，如果日志存储已达购买容量上限，系统将按照时间顺序，滚动覆盖最早的日志以存储新的日志。如果持续超出购买的日志存储容量，滚动日志总量达到购买容量的9倍后系统将不再存储新的日志。
说明：
例如您购买了1000GB日志存储，若持续超出日志存储容量，系统将在总量达到10000GB后停止记录新的日志。
为了更好地帮助您分析和查询日志，我们建议您 扩容日志存储量 或使用 日志投递 功能。

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。防火墙日志可以进行投递，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。

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6万条日志。

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，基础规则目前还没有支持自动拦截，如果入侵里有漏洞攻击且命中虚拟补丁就会自动拦截。因此，基础规则现在还是观察模式。预计后续版本会支持高置信度的基础规则自动拦截，以及支持永久拦截。

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？

流量日志不会记录被访问控制规则或入侵防御拦截的 IP 流量，仅记录放行的流量。

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，但不记录流量日志。
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。

日志投递中的支撑环境接入不能选择已购 CKafka？

您需要在 CKafka 实例里添加了接入方式，配置使用公网域名接入，支撑环境接入方式暂未开放，具体请查询 消息队列 CKafka 控制台。

账号相关

最近更新时间：2023-12-11 16:54:11

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：

QcloudCFWReadOnlyAccess

QcloudAccessForCFWRole

QcloudAccessForCFWRoleInUploadLog

QcloudAccessForCFWRoleInVPCFireWall

QcloudCFWFullAccess

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：2023-12-11 16:47:11

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。

版权所有：腾讯云计算（北京）有限责任公司

其他

最近更新时间：2023-12-11 16:47:27

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？

暂不支持查看版本，可在 概览页 右侧查看当前账号的套餐和到期日期。

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。

版权所有：腾讯云计算（北京）有限责任公司