云防火墙

常见问题

文档版本 22

发布日期 2024-04-29

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 产品咨询类

1.1 云防火墙支持线下服务器吗?

不支持，云防火墙支持云上region级服务。

1.2 云防火墙支持跨账号使用吗?

云防火墙支持跨账号防护，防护前需进行以下设置：

- 互联网边界跨账号防护请参见**多账号管理概述**。
- VPC边界跨账号防护需在“步骤三：配置企业路由器”添加VPC连接时，将当前账号A的企业路由器共享至其他账号B，共享成功后在账号B中添加连接，后续配置仍在账号A中进行，VPC边界防火墙介绍请参见**VPC边界防火墙概述**。

1.3 云防火墙与 Web 应用防火墙有什么区别?

云防火墙和Web应用防火墙是华为云推出的两款不同的产品，为您的互联网边界和VPC边界、Web服务提供防护。

WAF和CFW的主要区别说明如**表1-1**所示。

表 1-1 CFW 和 WAF 的主要区别说明

类别	云防火墙	Web应用防火墙
定义	云防火墙（Cloud Firewall，CFW）是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持按需弹性扩容、AI提升智能防御能力、灵活扩展满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙服务是为用户业务上云提供网络安全防护的基础服务。	Web应用防火墙（Web Application Firewall，WAF），通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。 有关Web应用防火墙的详细介绍，请参见**什么是Web应用防火墙**。
防护对象	• 弹性公网IP和VPC边界。 • 支持对Web攻击的基础防护。 • 支持外部入侵和主动外联的流量防护。	• 针对域名或IP，华为云、非华为云或云下的Web业务。 • 支持对Web攻击的全面防护。
功能特性	• 资产管理与入侵防御：对已开放公网访问的服务资产进行安全盘点，进行实时入侵检测与防御。 • 访问控制：支持互联网边界访问流量的访问控制。 • 流量分析与日志审计：VPC间流量全局统一访问控制，全流量分析可视化，日志审计与溯源分析。	SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击防护。

1.4 云防火墙和安全组、网络 ACL 的访问控制有什么区别?

云防火墙、安全组、网络ACL都可以实现通过IP地址/IP地址组设置访问控制策略，为您的互联网边界和VPC边界、弹性云服务器、子网提供防护。

云防火墙和安全组、网络ACL的主要区别如**表1-2**所示。

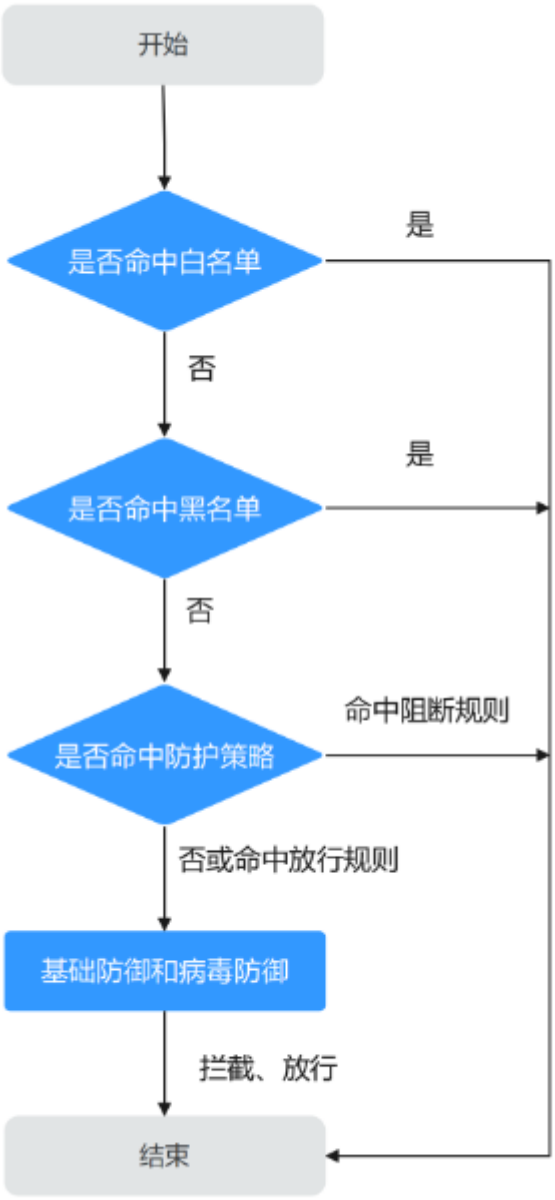
表 1-2 云防火墙和安全组、网络 ACL 访问控制的主要区别

类别	云防火墙	安全组	网络ACL
定义	云防火墙（Cloud Firewall，CFW）是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持按需弹性扩容、AI提升智能防御能力、灵活扩展满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙服务是为用户业务上云提供网络安全防护的基础服务。	安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器、云容器、云数据库等实例提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当实例加入该安全组后，即受到这些访问规则的保护。 有关安全组的详细介绍，请参见**安全组和安全组规则**。	网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的网络流量。 有关网络ACL的详细介绍，请参见**网络ACL**。
防护场景	• 互联网边界 • VPC边界 • SNAT场景	弹性云服务器	子网
功能特性	• 支持五元组（即源IP地址、目的IP地址、协议、源端口、目的端口）过滤。 • 支持通过地理位置、域名、域名组、黑/白名单过滤。 • 支持入侵防御系统（IPS）、病毒防御（AV）功能。	支持三元组（即协议、端口和对端地址）过滤。	支持五元组（即源IP地址、目的IP地址、协议、源端口、目的端口）过滤。

1.5 云防火墙的防护顺序是什么？

云防火墙匹配防护规则的优先级由高到低为：白名单 -> 黑名单 -> 防护策略（ACL）-> 基础防御（IPS）= 病毒防御（AV）。

图 1-1 防护顺序



- 设置黑/白名单请参见**管理黑/白名单**。
- 添加防护规则请参见**添加防护规则**。
- 设置IPS防护模式请参见**配置入侵防御策略**，自定义IPS规则请参见**自定义IPS特征**。
- 开启病毒防御请参见**开启病毒防御**。

1.6 VPC 个数和 VPC 边界防护流量峰值如何计算?

专业版云防火墙默认防护2个VPC，提供200Mbps的VPC边界流量防护，如果您需要防护更大的VPC间流量，可以通过购买VPC数量扩展，每个VPC支持200M的VPC边界流量防护。

例如：业务部署需要防护1Gbps的VPC边界流量，则云防火墙默认防护2个VPC（200M），您还需购买4个VPC（4*200M），VPC边界防护流量=默认值（200M）+4*VPC（200M）= 1Gbps。

1.7 是否支持同时部署 WAF、DDoS 高防和 CFW?

支持，因WAF分为三种模式：独享模式、ELB模式和云模式，不同的模式，流量走势不同，具体如下：

- 独享模式/ELB模式：互联网 -> DDoS高防 -> CFW -> WAF（独享模式/ELB模式）-> 源站
- 云模式：互联网 -> DDoS高防 -> WAF（云模式）-> CFW -> 源站

说明

- 若购买了DDoS高防或云模式WAF，请谨慎配置阻断的防护规则，建议配置放行的防护规则或白名单。
- 购买独享模式WAF或ELB模式WAF时，按业务需要配置即可。
- 具体介绍请参见**CFW与WAF、DDoS高防、CDN同时使用时的注意事项**。

1.8 资源部署在 DEC（专属云）上是否支持使用云防火墙防护?

如果专属云（Dedicated Cloud，DEC）所在的Region上已支持云防火墙，则可以使用云防火墙防护DEC的资源。

说明

- 云防火墙支持的区域请参见**功能总览**。
- 购买云防火墙服务时，需要先切换到DEC项目下，再进行购买。

2 区域与可用区

2.1 什么是区域和可用区?

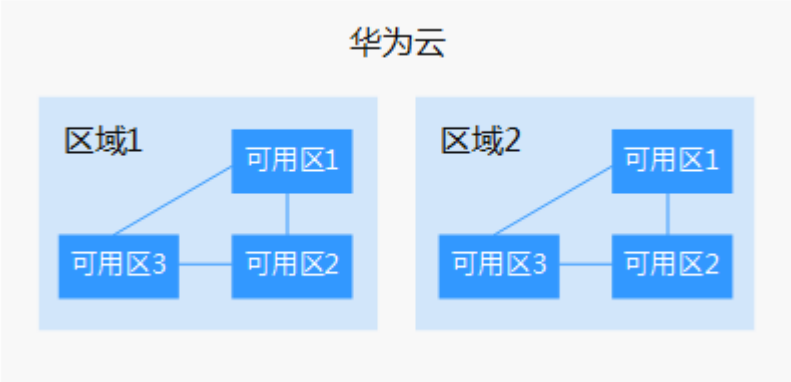
什么是区域、可用区?

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图2-1阐明了区域和可用区之间的关系。

图 2-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

2.2 云防火墙是否支持跨云或跨区域使用?

云防火墙支持哪些区域?

云防火墙及各功能支持的区域请参见**功能总览**。

云防火墙是否支持跨区域使用?

云防火墙不支持跨区域使用。选择区域后，购买的云防火墙仅支持当前区域使用。

说明

如您选择的区域提示无法购买CFW，您可通过VPC的**网络ACL**+VPC的**安全组**的方式进行防护。

云防火墙支持跨云使用吗?

云防火墙不支持跨云使用。目前仅支持对部署在华为云的业务提供防护，对于部署在非华为云的业务，无法提供防护。

3 功能类

3.1 通过日志功能可以查看哪些信息?

您可以通过“日志查询”页面，查看攻击事件日志、访问控制日志和流量日志。

- 攻击事件日志：IPS检测到的流量的危险等级、受影响的端口、命中的规则、攻击事件类型等信息，出现误拦截时您可以修改IPS防护动作。
- 访问控制日志：命中访问控制策略的所有流量。
- 流量日志：查看通过防火墙的所有流量记录。

3.2 云防火墙支持哪些维度的访问控制?

云防火墙当前支持基于五元组、IP地址组、服务组、域名、黑名单、白名单设置ACL访问控制策略；也支持基于IPS（intrusion prevention system，入侵防御系统）设置访问控制。IPS支持观察模式和阻断模式，当您选择阻断模式时，云防火墙根据IPS规则检测出符合攻击特征的流量进行阻断。具体配置步骤请参考**配置访问控制策略**。

3.3 配置阻断 IP 的防护规则需要注意哪些?

配置阻断IP的防护规则需注意以下几点：

1. 建议优先配置精准的IP（如192.168.10.5），减少网段配置，避免误拦截。
2. 对于反向代理IP（如内容分发网络（CDN）、DDoS高防、Web应用防火墙（WAF）的回源IP），请谨慎配置阻断的防护规则，建议配置放行的防护规则或白名单。
3. 对于正向代理IP（如公司出口IP），影响范围较大，请谨慎配置阻断的防护规则。
4. 配置“地域”防护时，需考虑公网IP可能更换地址的情况。

3.4 云防火墙攻击日志，为什么显示还未纳入防护的 EIP?

云防火墙会将所有受到攻击的EIP信息做收集，以便您更好的配置防御策略。

4 故障排查类

4.1 业务流量异常如何排查 CFW 侧防护?

当您的业务流量异常，可能被CFW中断时，可按照本节内容排查故障。

定位方式

步骤1 关闭CFW的防护。

- EIP流量故障：关闭CFW对业务中断的EIP的防护，请参见**关闭EIP防护**。
- SNAT或VPC间访问不通：关闭VPC边界防火墙的防护，请参见**关闭VPC边界防火墙**。

步骤2 观察业务情况。

- 业务恢复正常，请参见**排查思路**。
- 业务仍未恢复，说明非CFW造成的流量中断，可参考常见的故障原因：
  - 网络故障：路由配置错误，网元故障。
  - 策略拦截：其他安全服务、网络ACL或安全组配置错误导致的误拦截。

  若您需要华为云协助排查，可**提交工单**。

----结束

排查思路

步骤1 在**访问控制日志**中，搜索被阻断IP/域名的日志记录。

- 如有记录，可单击“规则”列跳转至匹配到的阻断策略，后续操作见**场景一：防护策略配置错误**。
- 如无记录，执行**步骤2**。

步骤2 在**攻击事件日志**中，搜索被阻断IP/域名的日志记录。

- 如有记录，可复制“规则ID”列信息，后续操作见**场景二：IPS等入侵防御功能的误拦截**。
- 如无记录，执行**步骤3**。

步骤3 弹性公网IP管理中关闭了EIP的防护或VPC边界防火墙管理中关闭了防护后，业务恢复正常，则建议您关闭防火墙防护并**提交工单**咨询。

步骤4 （可选）为了监测防火墙状态，迅速把握异常情况，推荐您进行如下配置：

- 在云防火墙控制台配置告警通知，请参见**告警通知**。
- 在云监控控制台配置CFW告警规则，配置方式请参见**设置监控告警规则**，支持的监控指标请参见**CFW监控指标说明**。

----结束

场景一：防护策略配置错误

可能原因

在访问控制策略中配置了阻断规则，或将正常的业务加入了黑名单，此时CFW会阻断相关会话，导致业务受损。

解决方案

- 阻断的是黑名单：
  - 删除该条黑名单策略。
  - 增加一条该IP/域名的白名单策略（白名单优先黑名单匹配，增加后黑名单策略失效，该流量将直接放行）。
- 阻断的是防护规则：
  - 在**访问规则列表**中搜索相关IP/域名的阻断策略，将阻断该IP/域名策略停用。
  - 修改对应的阻断策略的匹配条件，移除该IP/域名信息。
  - 添加一条“动作”为“放行”用于放通该IP/域名的防护规则，优先级高于其他“阻断”规则，添加防护规则请参见**添加防护规则**。

案例

处理流程：发现故障 -> 关闭防护 -> 查看日志 -> 修改策略 -> 恢复防护 -> 确认日志

某公司的网络运维人员发现一台云服务器无法通过绑定的EIP：xx.xx.xx.94访问公网。

防火墙管理员做了以下措施：

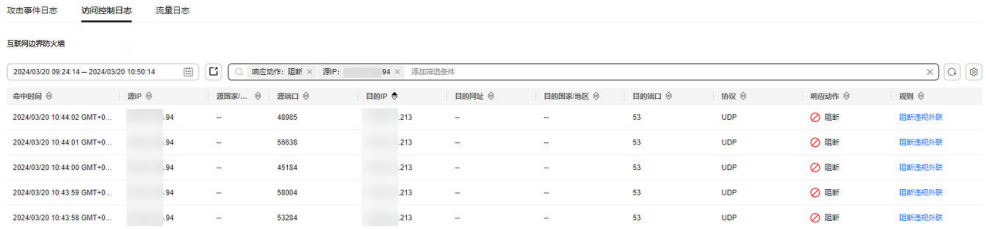
步骤1 为优先保证问题定位期间该IP可以正常外联，防火墙管理员登录云防火墙控制台，进入“资产管理 > 弹性公网IP管理”，关闭了该EIP的防护。

防火墙在关闭期间不再处理该EIP的流量，不展示相关日志。

图 4-1 弹性公网 IP 列表

步骤2 在“日志审计 > 日志查询”的“访问控制日志”页签中筛选出了“访问源”IP为xx.xx.xx.94的阻断日志，发现一条规则名为“阻断违规外联”的阻断规则，阻断了该IP访问外网的流量。

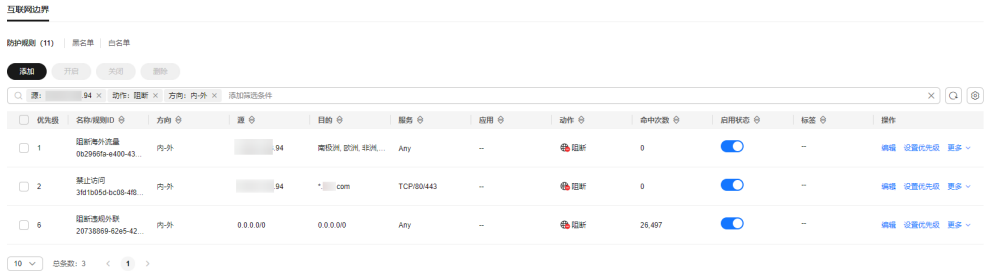
图 4-2 筛选访问控制日志



步骤3 在访问控制策略列表中搜索“源：xx.xx.xx.94，动作：阻断，方向：内-外，启用状态：启用”，发现有3条包含该IP且在生效中的策略。

其中包含了“阻断违规外联”这条策略，根据“命中次数”列，可知已有大量会话被阻断。

图 4-3 搜索防护规则



注意

图 搜索防护规则除了第二条防护规则配置错误以外，源IP包含xx.xx.xx.94的有效策略中，优先级最高的一条“名称”为“禁止访问”，以及最低的一条“名称”为“阻断访问海外流量”，这两条策略仍会生效，需要排查这两条策略是否有拦截正常业务的风险。

经过团队内部核对，因该IP有访问可疑IP的行为，某位管理员针对该IP配置了阻断的防护规则，但“目的”配置错误，误将所有外联流量都阻断了（**图 搜索防护规则**中第二条防护规则）。

步骤4 管理员将目的地址修改为了需要阻断访问的特定IP地址后，在云防火墙控制台“资产管理 > 弹性公网IP管理”中重新开启了该EIP的防护。恢复防护后该EIP的流量被云防火墙转发。

步骤5 管理员在流量日志中查看到了该IP相关的外联日志，确认业务已恢复。

----结束

场景二：IPS 等入侵防御功能的误拦截

解决方案

- 在对应的模块（如IPS）中将动作设为观察，具体防护模块请参见**配置入侵防御策略**。
- 将不需要防火墙防护的IP添加到白名单，配置白名单请参见**添加黑/白名单**。

案例

处理流程：发现故障 -> 修改防护状态 -> 查看日志 -> 确认业务 -> 修改策略 -> 恢复防护状态 -> 确认日志

某公司的运维人员发现无法访问IP地址为xx.xx.xx.90的服务器的某种业务，疑似是由于防火墙拦截造成。

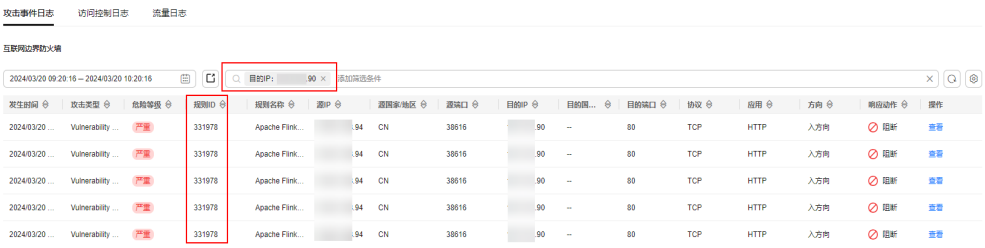
防火墙管理员做了以下措施：

步骤1 为优先保证业务恢复，防火墙管理员登录云防火墙控制台，进入“攻击防御 > 入侵防御”，将“防护模式”由“严格模式-拦截”改为“观察模式”。

在此期间，防火墙不再拦截攻击流量，只记录到攻击日志。

步骤2 在“日志审计 > 日志查询”的“攻击事件日志”中筛选出了访问目的IP为xx.xx.xx.90的日志，发现“规则ID”为“331978”的IPS规则，阻断了该流量。

图 4-4 筛选攻击事件日志



步骤3 通过查看“详情 > 攻击payload”和**抓包**，确认该业务为正常业务。于是管理员参考了**修改基础防御规则动作**，在“基础防御”页签的列表中筛选出了“规则ID”为“331978”的规则。

图 4-5 筛选“331978”的规则

步骤4 将“操作”设置为“观察”，该IPS规则将不再拦截匹配到特征的流量，只做日志记录。

步骤5 完成规则设置后，管理员将“防护模式”调回了“严格模式-拦截”，并在“基础防御”页签中确认“规则ID”为“331978”的规则，“当前动作”仍为“观察”。

步骤6 管理员在攻击事件日志中确认，业务会话命中该规则后，“响应动作”为“放行”，确认业务已恢复。

----结束

4.2 流量分析页面发现流量日志和攻击日志不全怎么办?

CFW只记录云防火墙开启阶段的用户流量日志和攻击日志，如果反复开启、关闭云防火墙，会导致关闭期间的日志无法记录。

因此，建议您避免反复执行开启、关闭CFW的操作。

4.3 配置了策略为什么没有生效?

配置了仅放行几条 EIP 的规则，为什么所有流量都能通过?

云防火墙开启EIP防护后，访问控制策略默认状态为放行。如您希望仅放行几条EIP，您需配置阻断全部流量的防护规则，并设为优先级最低，可按如下步骤进行：

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

步骤4 （可选）当前账号下仅存在单个防火墙实例时，自动进入防火墙详情页面，存在多个防火墙实例时，单击防火墙列表“操作”列的“查看”，进入防火墙详情页面。

步骤5 在左侧导航栏中，选择“访问控制 > 访问策略管理”，进入“访问策略管理”页面，选择“互联网边界”或“VPC边界”页签。

步骤6 配置全局阻断规则。单击“添加”按钮，在弹出的“添加防护规则”对话框中，填写参数如图 拦截所有流量所示，其余参数可根据您的部署进行填写。

图 4-6 拦截所有流量

说明

建议您添加完所有规则后再开启“启用状态”。

步骤7 配置放行规则。添加防护规则请参见添加防护规则。

步骤8 将步骤6中全局阻断规则的“优先级”置为最低，具体操作请参见**设置优先级**。

步骤9 启用所有规则。建议先开启“放行”规则，后开启“阻断”规则。

----结束

配置了全局阻断，为什么没有放行的 IP 还是能通过?

云防火墙中设置的防护策略是根据“弹性公网IP管理列表”执行的，若您已开启全局（0.0.0.0/0）阻断，但仍有未配置“放行”策略的EIP通过，需检查该IP是否在列表中，若不在，需进行资产同步操作，具体操作请参见**开启弹性公网IP防护**。

4.4 IPS 拦截了正常业务如何处理?

如果确认拦截的为正常业务流量，您可按照以下两种方式处理：

- 查询拦截该业务流量的规则ID，并在IPS规则库中修改对应规则的防护动作，操作步骤请参见**查询命中规则及修改防护动作**。
- 降低IPS防护模式的拦截程度，IPS防护模式说明请参见**配置入侵防御策略**。

查询命中规则及修改防护动作

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 在左侧导航树中，单击左上方的 ，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

步骤4 （可选）当前账号下仅存在单个防火墙实例时，自动进入防火墙详情页面，存在多个防火墙实例时，单击防火墙列表“操作”列的“查看”，进入防火墙详情页面。

步骤5 在左侧导航树中，选择“日志审计 > 日志查询”。进入“攻击事件日志”页面，记录拦截该业务流量的“规则ID”。

图 4-7 规则 ID

步骤6 在左侧导航栏中，选择“攻击防御 > 入侵防御” 。单击“基础防御”中的“查看生效中的规则”，进入“基础防御规则”页面。

步骤7 在搜索框中输入“规则ID”搜索，并在“操作”修改为“观察”或“禁用”。

- 观察：修改为“观察”状态，修改后防火墙对匹配当前防御规则的流量，记录至日志中，不做拦截。
- 禁用：修改为“禁用”状态，修改后防火墙对匹配当前防御规则的流量，不记录、不拦截。

----结束

4.5 访问控制日志没有数据怎么办?

访问控制日志展示的是ACL防护策略匹配到的流量，您需要配置ACL策略才能查看访问控制日志。

- 添加防护规则请参见**添加防护规则**。
- 通过云防火墙的所有流量记录请查看**流量日志**。
- 攻击事件记录请查看**攻击事件日志**。

4.6 NAT64 防护策略配置需要注意哪些?

防火墙无法防护NAT64转换前的真实源IP，如果您开启了弹性公网IP的IPv6转换功能，NAT64会将源IP转换成198.19.0.0/16的网段进行ACL访问控制。

使用IPv6访问时建议放行预定义地址组中“NAT64转换地址组”，设置后198.19.0.0/16网段中的IP均会被放行，若其中有您需要阻断的IP地址，请使用黑名单或阻断策略。

- IPv6转换功能请参见**IPv6转换**。
- NAT64转换地址组请参见**NAT64转换地址组**。
- 设置黑名单请参见**添加黑/白名单**。
- 设置阻断策略请参见**添加防护规则**。

4.7 系统策略授权企业项目后，为什么部分权限会失效?

CFW部分功能依赖于弹性云服务器（Elastic Cloud Server, ECS）、虚拟私有云（Virtual Private Cloud, VPC）等云服务，因这些云服务中部分功能不支持企业项目，将“CFW FullAccess” 和“CFW ReadOnlyAccess”两个系统策略授权到企业项目维度后会造成部分权限失效。

所以需要使用华为云账户自行创建两条系统策略，具体创建步骤请参见：**创建自定义策略**。

- CFW依赖的云服务中不支持企业项目的功能需要按照以下内容添加权限，其中云日志服务（Log Tank Service，简称LTS）在CFW页面操作时需授权LTS服务全部权限。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpc:quotas:list",
                "vpc:publicipTags:get"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ecs:availabilityZones:list"
            ]
        },
        {
```

```
            "Effect": "Allow",
            "Action": [
                "lts:groups:list",
                "lts:groups:get",
            ]
        }
    ]
}
```

- CFW依赖全局服务的权限：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "eps:resources:list"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "tms:predefineTags:list"
            ]
        }
    ]
}
```


5 网络流量类

5.1 云防火墙数据流量怎么统计?

目前云防火墙是基于会话的流量统计，在连接期间，数据不会上报，须连接结束后才会上报。

说明

- 流量的大小是基于从会话创建到结束期间该会话的整体流量。
- Internet互联网边界包括两个方向的流量，即从互联网访问服务的流量（入流量）和业务主动外联访问的流量（出流量）。

5.2 业务流量超过防护带宽怎么办?

如果您的实际业务流量超过已购买的防护带宽流量，可能会出现丢包现象，建议您及时根据实际业务情况购买扩展包来提供足够的防护带宽。

当您的业务流量持续超过可防护流量峰值时，云防火墙会将超出限额部分的流量进行bypass处理，被bypass的流量将无法被云防火墙防护。

购买扩展包请参见**变更扩展包**。

说明

云防火墙支持设置流量超额预警，当业务流量达到已购买带宽规格的一定比例时，将发送告警通知，设置告警通知请参见**告警通知**。

5.3 云防火墙提供的防护带宽是多少?

云防火墙为您提供互联网边界和VPC之间的防护，您可根据需要扩展防护带宽。根据您购买的服务版本的不同，云防火墙提供不同规格的防护带宽：

- 互联网方向：基础版默认10 Mbps（不可扩容），标准版默认10 Mbps，专业版默认50 Mbps。

  说明

  互联网方向的防护带宽按照入流量或出流量的最大值取值。

- VPC间防护：基础版、标准版不提供基础防护流量，专业版默认200 Mbps。

说明

若您的实际流量超过限额，需购买扩展包，请参见操作步骤**变更扩展包**。

5.4 流量趋势模块和流量分析页面展示的流量有什么区别?

两个模块流量数据的统计方式不同：

- “概览”页面的“流量趋势”模块基于流量统计数据，数据信息实时更新；展示的内容为入方向流量、出方向流量、VPC间流量信息。
- “流量分析”页面基于会话统计数据，在连接期间，数据不会上报，连接结束后才会上报。
  - 入云流量：入云方向的会话。
  - 出云流量：出云方向的会话。
  - VPC间访问：VPC间的会话。

5.5 收到流量超限预警如何处理?

适用场景

配置告警通知后收到了邮件或短信形式的流量超限预警，说明您的实际业务流量已达到设置的阈值，即将超过可防护流量峰值。

处理方式

如果您的实际业务流量超过已购买的可防护流量峰值，可能会出现丢包现象，建议您：

- 购买扩展包来提供足够的防护流量，购买扩展包请参见**变更扩展包**。
- 及时减少防护对象，关闭EIP防护请参见**关闭EIP防护**。

如果您的业务流量持续超过可防护流量峰值，则云防火墙会将超出限额部分的流量进行bypass处理，被bypass的流量将无法被云防火墙防护。

6 API 类

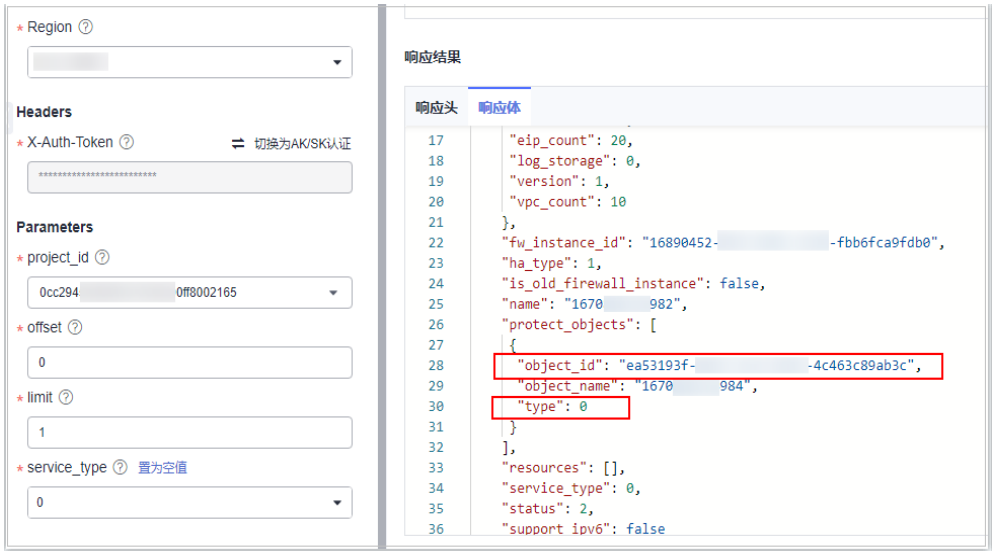
6.1 什么是 Object_Id?

Object_Id防护对象id，是创建云防火墙后用于区分互联网边界防护和VPC边界防护的标志id。

可通过调用**查询防火墙实例**获取。

- type为0：Object_Id为互联网边界防护对象Id。
- type为1：Object_Id为VPC边界防护对象Id。

图 6-1 Object_Id 和 type



6.2 什么是 Firewall_Instance_Id?

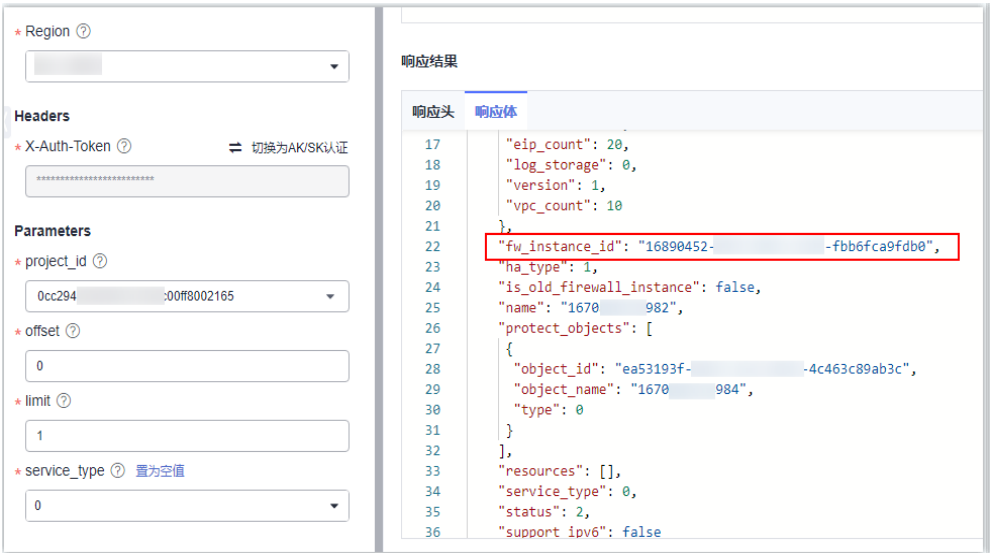
Firewall_Instance_Id防火墙实例id，是创建云防火墙后用于标志防火墙由系统自动生成的标志id。

- 默认情况下，fw_instance_Id为空时，返回账号下第一个墙的信息；fw_instance_Id非空时，返回与fw_instance_Id对应墙的信息。

- 若object_Id非空，默认返回object_Id对应墙的信息；填写时object_Id需要属于fw_instance_Id对应的墙。

可通过调用**查询防火墙实例**获取。

图 6-2 Firewall_Instance_Id



7 计费类

7.1 云防火墙如何收费和计费?

云防火墙支持包年/包月（预付费）计费方式，详细信息请参见**产品价格详情**。

其中基础版不支持扩容，标准版支持扩容防护公网IP数和互联网边界流量峰值。

专业版支持扩容防护公网IP数、互联网边界流量峰值和防护VPC数。

- 有关CFW详细的计费说明，请参见**计费说明**。
- 有关CFW各版本差异，请参见**服务版本差异**。

7.2 云防火墙如何变更版本规格?

云防火墙不支持基础版升级，支持标准版升级到专业版，不支持专业版变更到标准版。如需更换基础版或降低版本规格，需退订当前版本后再进行购买。

有关退订CFW的详细操作，请参见**如何退订云防火墙?** 。

升级版本操作步骤

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

步骤4 （可选）当前账号下仅存在单个防火墙实例时，自动进入防火墙详情页面，存在多个防火墙实例时，单击防火墙列表“操作”列的“查看”，进入防火墙详情页面。

步骤5 在页面左上角，单击“升级到专业版”，进入“购买云防火墙”页面。

步骤6 确认版本规格后，单击“立即购买”。

步骤7 确认订单详情，阅读并勾选“我已阅读并同意《华为云防火墙服务声明》”，单击右下角“去支付”。

步骤8 在“付款”页面，选择付款方式进行付款。

----结束

7.3 如何为云防火墙续费?

该任务指导用户如何在云防火墙即将到期时进行续费。续费后，用户可以继续使用云防火墙。

- 购买的服务版本到期前，系统会以短信或邮件的形式提醒您服务即将到期，并提醒您续费。
- 购买的服务版本到期后，如果没有按时续费，公有云平台提供一定的保留期。
  保留期的时长由“客户等级”来定，详细信息请参见**保留期**。

  说明

  为了防止造成不必要的损失，请您及时续费。

操作步骤

步骤1 **登录管理控制台**。

步骤2 单击管理控制台左上角的，选择区域。

步骤3 在左侧导航树中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的概览页面。

步骤4 在界面右上角，单击“续费”。

步骤5 在“续费管理”界面，根据页面提示完成续费。

详细续费操作请参见**续费管理**。

----结束

7.4 如何退订云防火墙?

该任务指导用户退订包年/包月方式购买的云防火墙。

退订后原CFW配置数据将不能保存且无法找回，建议您退订前导出防护策略，重购后导入防护策略，以便CFW更好的为您防护。有关导入导出策略的详细操作，请参见**批量管理防护规则**。

操作步骤

步骤1 **登录管理控制台**。

步骤2 在界面右上方，单击“费用”，进入“费用中心”界面。

步骤3 在左侧导航树上选择“订单管理 > 退订与退换货 > 云服务退订”。

步骤4 根据页面提示完成退订。

详细退订操作请参见**退订管理**。

----结束

A 修订记录

发布日期	修改说明
2024-04-29	第二十二次正式发布。 新增： **收到流量超限预警如何处理？** 章节。
2024-04-08	第二十一次正式发布。 新增： **资源部署在DEC（专属云）上是否支持使用云防火墙防护？** 章节。
2024-01-15	第二十次正式发布。 新增： • **是否支持同时部署WAF、DDoS高防和CFW？** 章节。 • **业务流量异常如何排查CFW侧防护？** 章节。 • **流量趋势模块和流量分析页面展示的流量有什么区别？** 章节。
2023-12-20	第十九次正式发布。 新增**NAT64防护策略配置需要注意哪些？** 章节。
2023-10-11	第十八次正式发布。 新增： • **云防火墙和安全组、网络ACL的访问控制有什么区别？** 章节。 • **IPS拦截了正常业务如何处理？** 章节。
2023-08-02	第十七次正式发布。 新增： **VPC个数和VPC边界防护流量峰值如何计算？** 章节。

发布日期	修改说明
2023-07-05	第十六次正式发布。 新增： ● **云防火墙的防护顺序是什么？**章节。 ● **访问控制日志没有数据怎么办？**章节。 优化**云防火墙支持跨账号使用吗？**章节，支持跨账号使用。 下线“华为旁路引擎”相关内容： ● “标准版旁路引擎服务停售相关问题”章节。 ● “华为旁路引擎（已下线）版本的访问控制日志中为什么看不见放行规则的记录”章节。 ● “购买华为旁路引擎（已下线），后面可以切换为直路引擎吗？”
2023-05-06	第十五次正式发布。 新增**系统策略授权企业项目后，为什么部分权限会失效？**章节。
2023-01-19	第十四次正式发布。 新增“标准版旁路引擎服务停售相关问题”章节。 新增**API类**章节。
2022-10-28	第十三次正式发布。 修改**云防火墙提供的防护带宽是多少？**防护带宽流量计算方式。
2022-09-27	第十二次正式发布。 新增“华为旁路引擎（已下线）版本的访问控制日志中为什么看不见放行规则的记录”章节。 新增**配置了策略为什么没有生效？**章节。
2022-07-25	第十一次正式发布。 ● 新增**云防火墙提供的防护带宽是多少？**章节。 ● 新增“计费类”及其子章节。
2022-07-21	第十次正式发布。 新增**云防火墙是否支持跨云或跨区域使用？**章节。
2022-04-09	第九次正式发布。 新增以下章节。 ● “购买华为旁路引擎（已下线），后面可以切换为直路引擎吗？” ● QPS高，流量峰值就高吗？ ● **云防火墙攻击日志，为什么显示还未纳入防护的EIP？** ● 4.4.9-Spring Framework远程代码执行漏洞攻击，华为云云防火墙如何启用检测和防御？

发布日期	修改说明
2022-01-11	第八次正式发布。 新增**业务流量超过防护带宽怎么办？**章节。
2021-12-10	第七次正式发布。 新增4.4.8-Apache Log4j 远程代码执行漏洞攻击，华为云云防火墙如何启用检测和防御？章节。
2021-12-08	第六次正式发布。 新增**云防火墙支持线下服务器吗？**章节。
2021-10-25	第五次正式发布。 新增**云防火墙支持哪些维度的访问控制？**章节。
2021-10-12	第四次正式发布。 新增以下章节： • **云防火墙支持跨账号使用吗？** • **云防火墙与Web应用防火墙有什么区别？** • **通过日志功能可以查看哪些信息？**
2021-08-17	第三次正式发布。 新增云防火墙可以跨区域使用吗？章节。
2021-07-29	第二次正式发布。 • 新增**网络流量类**章节。 • 修改**功能类**章节，优化章节内容。
2021-06-30	第一次正式发布。