云防火墙

常见问题

文档版本	13
发布日期	2025-01-03

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

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 云防火墙支持的 QPS、新建/并发连接数大小是多少?

云防火墙作为SaaS化服务，不受传统硬件防火墙在新建连接数、并发连接数以及QPS等方面的限制，衡量云防火墙性能的唯一标准是实际的防护带宽大小。

防护带宽定义如下：

- 防护带宽：所有经过云防火墙防护的业务带宽。
- 互联网边界防护带宽：所有经过云防火墙防护的EIP的流量总和最大值，按照入云流量（入流量）或出云流量（出流量）的最大值取值。
- VPC边界防护带宽：所有经过云防火墙防护的VPC的流量总和最大值。

1.3 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**使用CFW跨账号防护EIP资源**。
- VPC边界跨账号防护需在配置企业路由器时添加VPC连接时，将当前账号A的企业路由器共享至其它账号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**使用CFW跨账号防护VPC资源**。

1.4 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。

1.5 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。

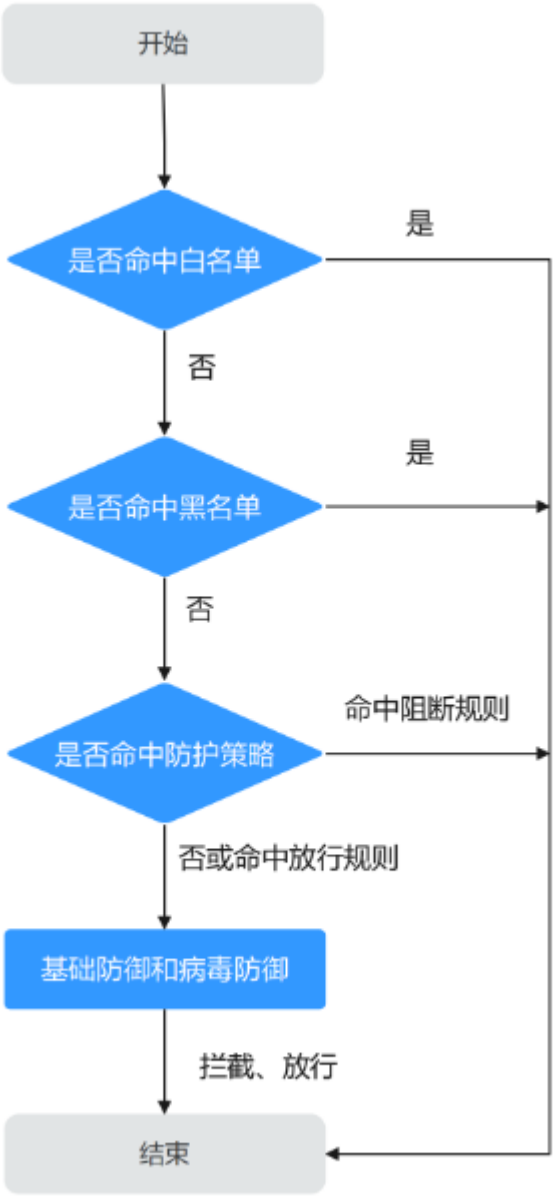
1.6 云防火墙支持哪些维度的访问控制?

云防火墙当前支持基于五元组、IP地址组、服务组、域名、应用、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**。

1.7 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**。

1.8 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

- 如果购买了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**。

1.9 云防火墙支持防护其它企业项目下的资源吗?

支持，CFW支持防护当前区域、当前账号下所有的云资源（EIP、VPC、NAT网关）。

开通企业管理功能，并在购买CFW时选择了企业项目，CFW的账单会归属到该项目下，不影响资源防护。

企业通过企业项目管理业务时如何规划云防火墙的方案示例请参见**使用CFW防护企业资源**。

1.10 云防火墙日志默认存储多长时间?

云防火墙支持免费查询和导出7天内的日志记录，请参见**日志查询**。

将单个或者多个日志记录至LTS中，支持查看1~365天的日志记录，请参见**日志管理**。

说明

LTS按流量单独计费。有关LTS的计费详情，请参见**LTS价格详情**。

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?

通常使用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 故障排查

3.1 业务流量异常怎么办?

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。

问题描述

业务流量异常，例如：

- EIP无法访问公网
- 无法访问某个服务器

排查思路

图 3-1 业务流量异常排查思路

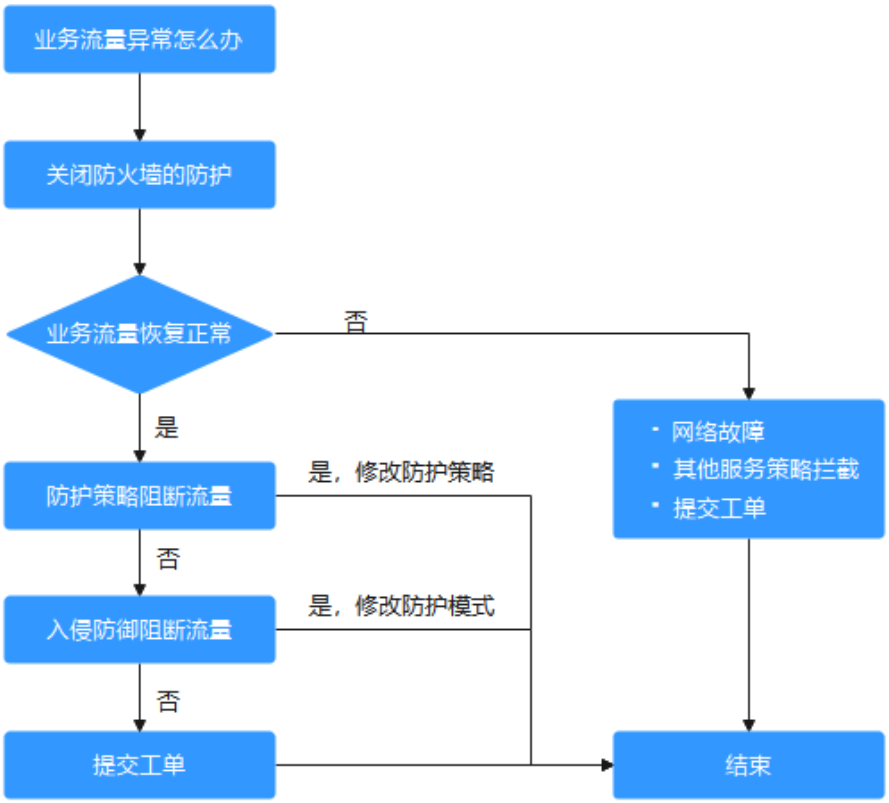


表 3-1 业务流量异常排查思路

序号	可能原因	处理措施
1	非CFW造成的流量中断	解决方法请参考**原因一：非CFW造成的流量中断**
2	防护策略阻断流量	解决方法请参考**原因二：防护策略阻断流量**
3	入侵防御阻断流量	解决方法请参考**原因三：入侵防御阻断流量**

原因一：非 CFW 造成的流量中断

可以在云防火墙控制台，关闭防护，观察业务情况，如果业务仍未恢复，说明非CFW造成的流量中断。

关闭防护的方式如下：

- 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**。

如果业务仍未恢复，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：其它安全服务、网络ACL或安全组配置错误导致的误拦截。

如果您需要华为云协助排查，可**提交工单**。

原因二：防护策略阻断流量

可能是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。

您可以采取以下措施：

在**访问控制日志**中，搜索被阻断IP/域名的日志记录

- 如果无记录，请参见**表3-1**原因三。
- 如果有记录，单击“规则”列跳转至匹配到的阻断策略。
  - 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：
    - 在访问控制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，优先级高于其它“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：

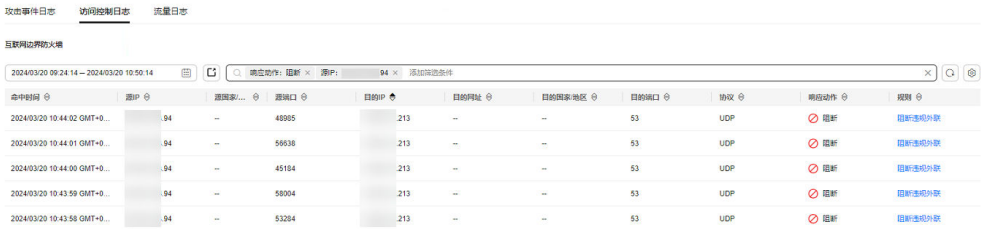
步骤1 为优先保证问题定位期间该IP可以正常外联，防火墙管理员登录云防火墙控制台，进入“资产管理 > 弹性公网IP管理”，关闭了该EIP的防护。

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 3-2 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。

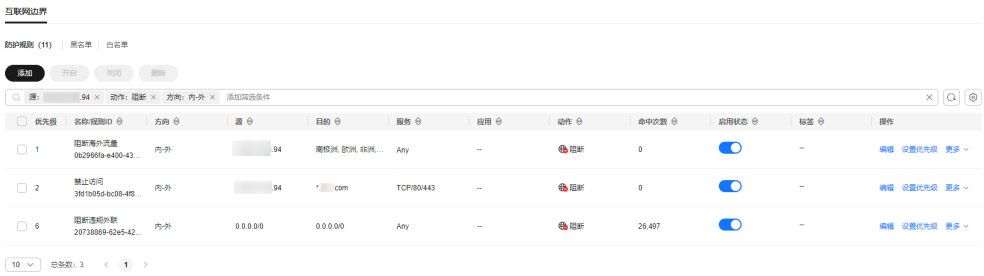
图 3-3 筛选访问控制日志



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 3-4 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

原因三：入侵防御阻断流量

IPS等入侵防御功能防护模式设置粒度过细，阻断了正常流量。

您可以采取以下措施：

在**攻击事件日志**中，搜索被阻断IP/域名的日志记录。

- 如果无记录，请**提交工单**排查问题。
- 如果有记录，参考以下两种方式处理：
  - 可复制“规则ID”列信息，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。

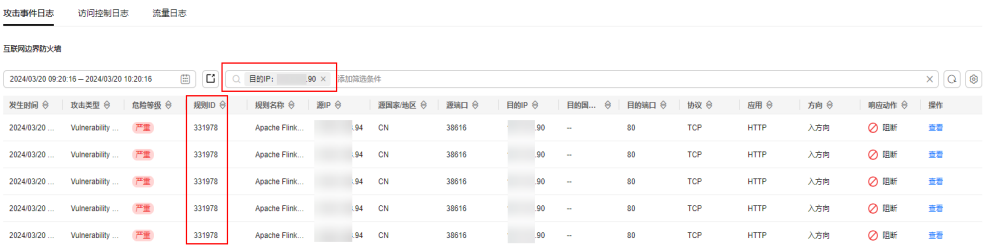
防火墙管理员做了以下措施：

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 3-5 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 3-6 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

提交工单

如果上述方法均不能解决您的疑问，请**提交工单**寻求更多帮助。

3.2 流量日志和攻击日志信息不全怎么办?

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。

3.3 防护规则没有生效怎么办?

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 在左侧导航栏中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

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 3-7 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?

云防火墙防护EIP时设置的防护策略是根据“弹性公网IP管理列表”执行的，如果您已开启全局（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是否开启防护，具体操作请参见**开启弹性公网IP防护**。

3.4 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 在左侧导航栏中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

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 3-8 规则 ID

攻击事件类型	危险等级	规则ID	命中规则名称
Vulnerability ...	高	336842	Simple HTT...

步骤6 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

3.5 为什么访问控制日志页面数据为空?

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**。

3.6 为什么使用 NAT64 转换的 IP 地址被阻断了?

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，如果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**。

3.7 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"
            ]
        }
    ]
}
```

3.8 配置 LTS 日志时提示权限不足怎么办?

在“日志管理”页面，完成日志配置后，提示“您的权限不足”，此时需要添加“LTS FullAccess”权限。

问题描述

“日志管理”页面，提示“您的权限不足”。

问题原因

“日志管理”页面，是将日志转储到云日志服务（Log Tank Service，简称LTS）中，此页面的所有操作，需要调用LTS服务的接口，依赖LTS服务权限。

解决方法

由主账号给子账号添加“LTS FullAccess”权限，授权操作请参见**授权IAM用户使用云日志服务LTS**

4 网络流量

4.1 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。

4.2 云防火墙数据流量怎么统计?

云防火墙流量统计分为两种形式：

- 基于流量统计数据。

  在“总览”页面的“流量趋势”模块中查看；数据信息实时更新。
- 基于会话统计数据，流量在会话结束的瞬间时刻统计。
  - 在“日志审计 > 日志查询 > 流量日志”页面查看；数据信息是会话创建到结束期间的整体流量；在会话连接期间，数据不会上报，连接结束后才会上报。
  - 在“流量分析”下的任意页面查看；数据信息是流量日志中在该时间结束会话的流字节数的平均值。

4.3 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：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：标准版不提供基础防护流量，专业版默认200 Mbps。

说明

如果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**。

4.4 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，可能出现限流、随机丢包、自动Bypass等现象，导致您的部分业务在一定时间内不可用、卡顿、延迟等。

如果出现这种情况，您需要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。

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**。

4.5 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：

- “总览”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，在会话连接期间，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。

4.6 如何验证 HTTP/HTTPS 的出方向域名防护规则的有效性?

可按照以下操作步骤验证有效性：

步骤1 发送HTTP或HTTPS请求。

- 方式一：使用curl命令，例如：

```
curl -k "https://www.example.com"
```

- 方式二：使用浏览器访问域名。

注意

请勿使用telnet命令进行域名测试。

使用telnet命令对域名和端口进行测试时（例如telnet www.example.com 80），只会生成TCP握手流量，并不会模拟完整的HTTP或HTTPS请求，此时应用类型识别为Unknown，不会被HTTP或HTTPS应用策略命中。

步骤2 进入云防火墙管理控制台，查看防护规则的命中次数和日志记录，如果有新增，说明规则生效，如果无新增，请及时修改防护规则。

1. 在“访问控制 > 访问策略管理”的“防护规则”页签中，查看规则的“命中次数”。
2. 在“日志审计 > 日志查询”的“访问控制日志”页签中，查看该规则的防护记录。

----结束

4.7 如何获取攻击者的真实 IP 地址?

流量经过反向代理后，源IP被转换为回源IP，此时如果受到外部攻击，CFW无法通过源IP获取到攻击者的真实IP地址，您可通过攻击事件日志中的X-Forwarded-For字段查询真实IP地址。

查看 X-Forwarded-For

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 在左侧导航栏中，单击左上方的，选择“安全与合规 > 云防火墙”，进入云防火墙的总览页面。

步骤4 （可选）切换防火墙实例：在页面左上角的下拉框中切换防火墙。

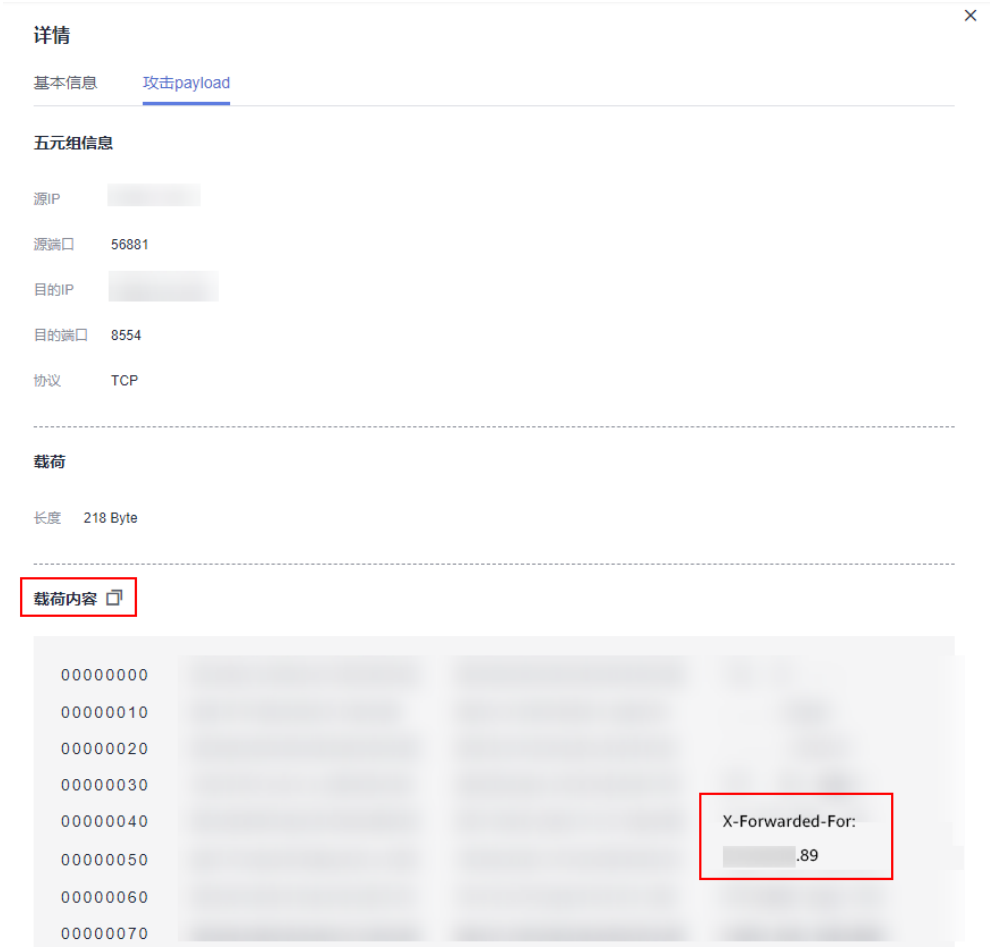
步骤5 在左侧导航树中，选择“日志审计 > 日志查询”。进入“攻击事件日志”页面，在对应事件的“操作”列，单击“查看”。

图 4-1 查看攻击事件日志详情

步骤6 在“详情”中，切换至“攻击payload”页签，获取X-Forwarded-For字段。

- 方法一：在“载荷内容”中查看X-Forwarded-For（从客户端到最后一个代理服务器的所有地址IP）。

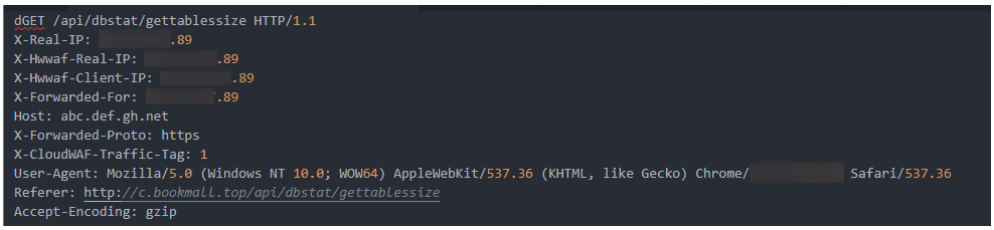
图 4-2 载荷内容中 X-Forwarded-For



- 方法二：复制“载荷内容”，通过Base64工具，获得解码结果：
  - X-Forwarded-For：从客户端到最后一个代理服务器的所有地址IP

  例如，通过**图 Base64解码结果**可得真实客户端的IP为xx.xx.xx.89，只经过云模式WAF的一层代理。

图 4-3 Base64 解码结果示例



----结束

4.8 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**。

