ALIBABA CLOUD

# Alibaba Cloud

## 云防火墙

## 常见问题

文档版本：20220513

阿里云

# 法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

# 通用约定

| 格式 | 说明 | 样例 |
| --- | --- | --- |
| 危险 | 该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。 | 危险<br>重置操作将丢失用户配置数据。 |
| 警告 | 该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。 | 警告<br>重启操作将导致业务中断，恢复业务时间约十分钟。 |
| 注意 | 用于警示信息、补充说明等，是用户必须了解的内容。 | 注意<br>权重设置为0，该服务器不会再接受新请求。 |
| 说明 | 用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。 | 说明<br>您也可以通过按Ctrl+A选中全部文件。 |
| > | 多级菜单递进。 | 单击**设置**> **网络**> **设置网络类型**。 |
| **粗体** | 表示按键、菜单、页面名称等UI元素。 | 在**结果确认**页面，单击**确定**。 |
| `Courier字体` | 命令或代码。 | 执行 `cd /d C:/window` 命令，进入Windows系统文件夹。 |
| *斜体* | 表示参数、变量。 | `bae log list --instanceid` *Instance_ID* |
| [] 或者 [a\|b] | 表示可选项，至多选择一个。 | `ipconfig [-all\|-t]` |
| {} 或者 {a\|b} | 表示必选项，至多选择一个。 | `switch {active\|stand}` |

# 目录

1.与其它云产品的关系 05
2.云防火墙支持的带宽问题 06
3.云防火墙和安全组有什么差异? 07
4.云防火墙授权相关问题 08
5.流量分析相关问题 09
6.访问控制策略相关问题 13
7.互联网边界防火墙常见问题 15
8.VPC边界防火墙相关问题 17
9.日志相关问题 18
10.流量不通时如何排查? 19
11.云防火墙防护流量时的规则匹配顺序 21
12.为什么当前账号无法开启云防火墙? 22
13.为什么有来自阿里云的ICMP周期性探测报文? 24

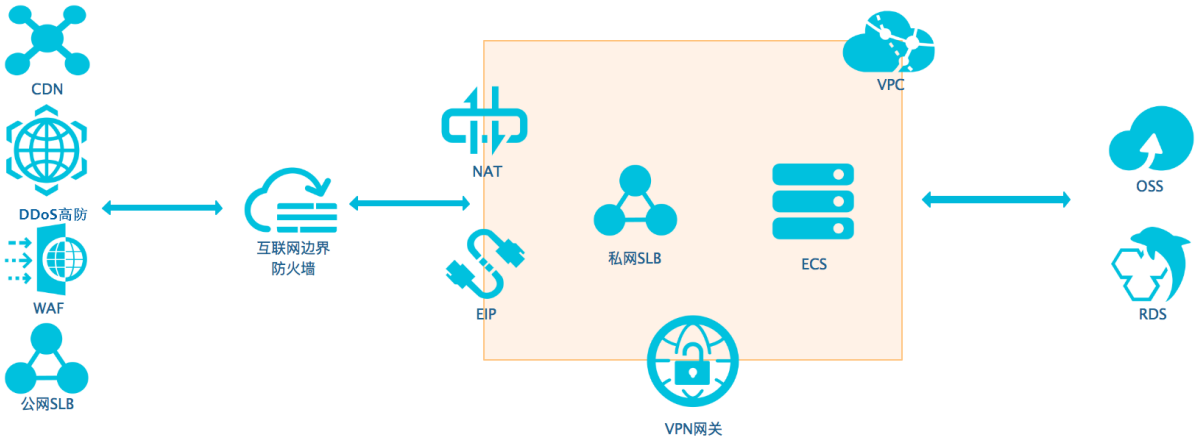
# 1.与其它云产品的关系

## 云防火墙在阿里云网络中的位置

云防火墙有3个控制单元：

- 互联网边界防火墙：部署于EIP的前面（即EIP出互联网方向的第一个防护节点），对公网EIP进行控制（高级版、企业版和旗舰版）。
- VPC边界防火墙：部署于VPC和VPC间的边界，对ECS的私网地址进行控制（企业版和旗舰版）。
- 主机防火墙：即安全组，对ECS实例间的入流量和出流量进行控制（企业版和旗舰版）。

下图展示了部分阿里云产品（包括云防火墙）的逻辑关系。




## 同WAF、DDoS高防等安全产品同时使用

与Web应用防火墙（WAF）、DDoS高防等安全产品同时使用如上图所示。云防火墙防护的是WAF和DDoS高防的源站IP。

## 与CDN产品同时使用

与CDN同时使用时，云防火墙防护的是CDN的源站IP。

## 与OSS、RDS同时使用

目前云防火墙不支持阿里云OSS、RDS。

默认情况下，RDS实例被设置为不允许任何IP（即白名单为127.0.0.1）访问，包括内网访问和外网访问。您可以通过RDS控制台的**数据安全性**页面或者API来添加白名单。白名单的更新无需重启RDS实例，因此不会影响您的业务。

如果您使用的是在ECS上自建的RDS数据库，则可以通过VPC边界防火墙来实现对自建RDS的防护。

# 2.云防火墙支持的带宽问题

## 云防火墙提供的防护带宽流量是多少？

云防火墙可以对您公网方向的流量和VPC之间的流量进行防护，您可根据需要扩展防护流量带宽。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：

- 公网方向的流量：高级版默认10 Mbps/月，企业版默认50 Mbps/月，旗舰版默认200 Mbps/月。
- VPC间流量：高级版不提供防护，企业版默认100 Mbps/月，旗舰版默认1 Gbps/月。

详细内容，请参见云防火墙功能与计费表。

## 哪些流量会占用云防火墙的防护带宽？

公网互访流量会占用云防火墙防护带宽，VPC间互访流量不占用云防火墙防护带宽。例如：某个EIP遭受了DDoS攻击，无论云防火墙是否成功拦截了这些攻击行为，由于这些流量属于公网方向的互访流量，都会计算到云防火墙防护的带宽里。

## 业务流量超出云防火墙支持的带宽规格怎么办？

如果您的业务实际流量超出云防火墙提供的防护带宽，云防火墙将只对防护带宽范围内的流量提供防护。对于超出防护带宽的流量，云防火墙默认不提供防护。业务实际流量超过防护带宽时，您必须扩充防护带宽规格。关于扩充防护带宽的详细内容，请参见升级与变配。

当您的业务流量超出云防火墙提供的防护带宽时，为您提供以下建议：

- 关注云防火墙控制台**概览**页面的流量趋势数据和**网络流量分析 > VPC访问活动**页面的VPC网络流量信息，及时了解流量变化情况。结合云防火墙的日志数据，定位异常IP并排除风险。
- 您的业务流量超出云防火墙提供的防护带宽后，云防火墙向您发送邮件通知。请您及时查看邮件，根据邮件信息进行相应的处理。

> **说明** 预计您会在业务流量超出云防火墙防护带宽后的第二天收到邮件通知。

# 3.云防火墙和安全组有什么差异？

安全组是ECS提供的虚拟主机防火墙，对ECS实例间的流量进行访问控制。

云防火墙是互联网边界防火墙、VPC边界防火墙、主机边界防火墙的统称，为您提供互联网边界、VPC网络边界、ECS实例间的三重防护。

云防火墙的主机边界防火墙底层使用了安全组的能力。您既可以在云防火墙控制台**访问控制 > 主机边界防火墙**处配置策略，也可以在ECS控制台**安全组**页面配置策略，两者配置自动保持同步。

## 云防火墙相对安全组的独有功能

- 支持应用级别的访问控制。例如：可以管控HTTP协议流量，其HTTP服务可以运行在任意端口。
- 支持域名级别的访问控制。例如：可以配置只允许所有ECS到**.aliyun.com*的请求。
- 提供入侵防御功能，支持对常见的系统漏洞和暴力破解进行防护。
- 访问控制策略支持观察模式。
- 提供完整的流量日志，并支持对流量进行实时分析。

## 云防火墙相对安全组的增强功能

云防火墙相对安全组提供了一些增强功能：

- 策略组在未设置放行策略的情况下，该策略组中的ECS实例之间无法互通。

  > **说明** 如果新增策略组之后，又删除了该策略组中的全部策略，这种情况也属于该策略组未添加任何策略。

- 通过提供不限数量的VPC边界访问控制策略（提工单可申请扩展），减少配置不必要的主机防火墙策略（即ECS安全组规则），可以有效解决ECS安全组规则存在数量上限的问题。

# 4.云防火墙授权相关问题

## 为什么使用云防火墙需要授权？

您授权云防火墙访问当前阿里云账号下的云资产（即您的ECS实例列表、VPC实例列表、SLB实例列表等云资产信息）后，才能在云防火墙控制台看到云资产的流量请求和响应情况，以及云资产之间的私网业务访问情况，并根据这些数据的分析结果配置访问控制策略。

您只有使用阿里云账号或拥有管理访问控制权限（AliyunRAMFullAccess）的RAM用户身份，才能授权云防火墙访问云资源。关于授权的具体操作，请参见授权云防火墙访问云资源。

## 为云企业网创建VPC边界防火墙时，为什么提示未授权？

如果您的阿里云账号下的云企业网中，存在另一个账号开通的专有网络VPC，需要先授权云防火墙访问该VPC所属阿里云账号下的云资产。

针对此场景，如果您未完成对该VPC所属阿里云账号的授权，为该VPC创建VPC边界防火墙时，页面会提示**存在未授权的网络实例，不允许创建**。

# 5.流量分析相关问题

## 流量分析中Unknown应用类型占比较大，是产品无法识别外网的具体请求吗？

应用显示为Unknown可能存在以下原因。

- 来自互联网入方向的流量很大时，该类流量大部分不是标准协议，因此无法识别为已知协议。
- 网络流量可能被目的服务器阻断，发送大量的rst回包。这类包会记录到出方向或入方向的流量中，如果数量较大，则相应的Unknown占比也较大。

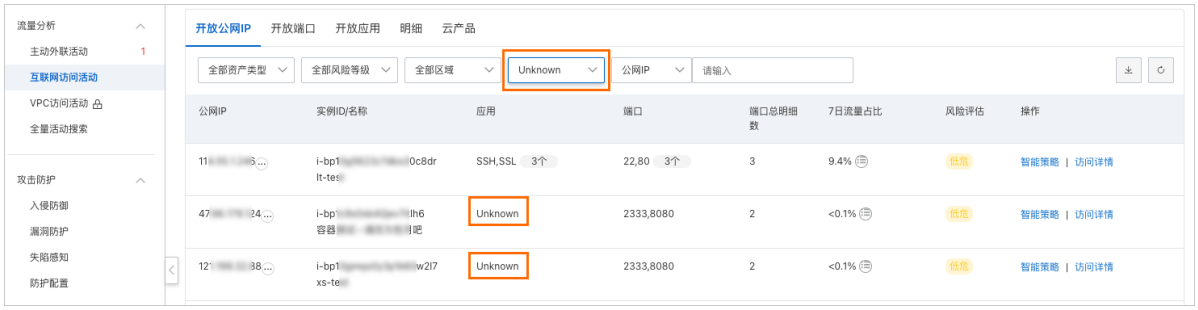
> **说明** 您可以在云防火墙控制台的左侧导航栏选择**日志分析 > 日志审计**，然后单击**事件日志**或**流量日志**页签，观察Unknown流量的具体来源与用途，判断出方向或入方向流量是否存在异常情况。

您可以在云防火墙控制台以下页面看到Unknown数据。

- **互联网访问活动**

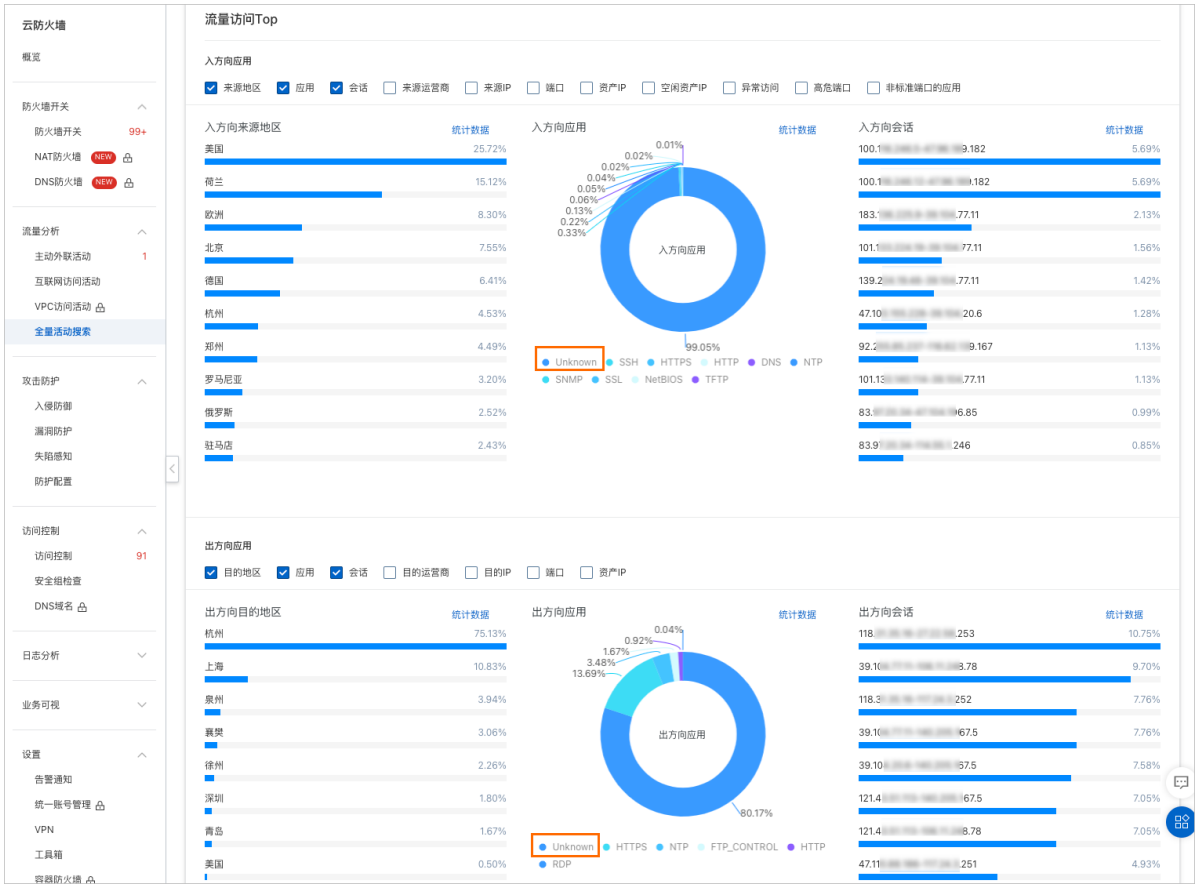
  在左侧导航栏，选择**流量分析 > 互联网访问活动**。在下方列表的应用类型下拉菜单，选择Unknown。

  筛选后，您可以查看Unknown应用类型的互联网访问活动。




- **全量活动搜索**

  在左侧导航栏，选择**流量分析 > 全量活动搜索**。在**流量访问Top**区域，您可以查看入方向和出方向应用中的Unknown应用类型。




- **日志审计**

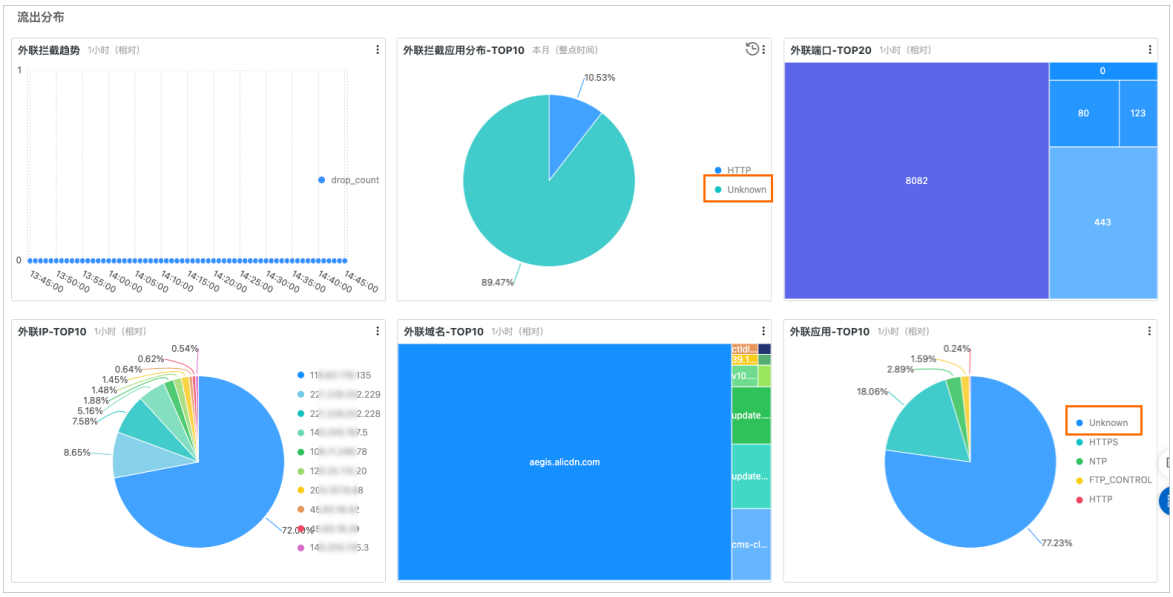
  在左侧导航栏，选择**日志分析 > 日志审计**，然后选择**事件日志**或**流量日志**页面的**互联网边界防火墙**或**VPC边界防火墙**页签。在日志列表的**应用**列，查看**Unknown**应用类型。

- **日志分析**

  在左侧导航栏，选择**日志分析 > 日志分析 > 报表**。在**流入分布**和**流出分布**区域，您可以查看入方向和出方向Top 10应用和拦截应用中的**Unknown**应用类型。

  - 流入分布

- 流出分布




> **说明** 单击每个功能区域右上角的 ⋮ 图标，您可以进行调整时间范围、下载图表数据、下载图表等操作。

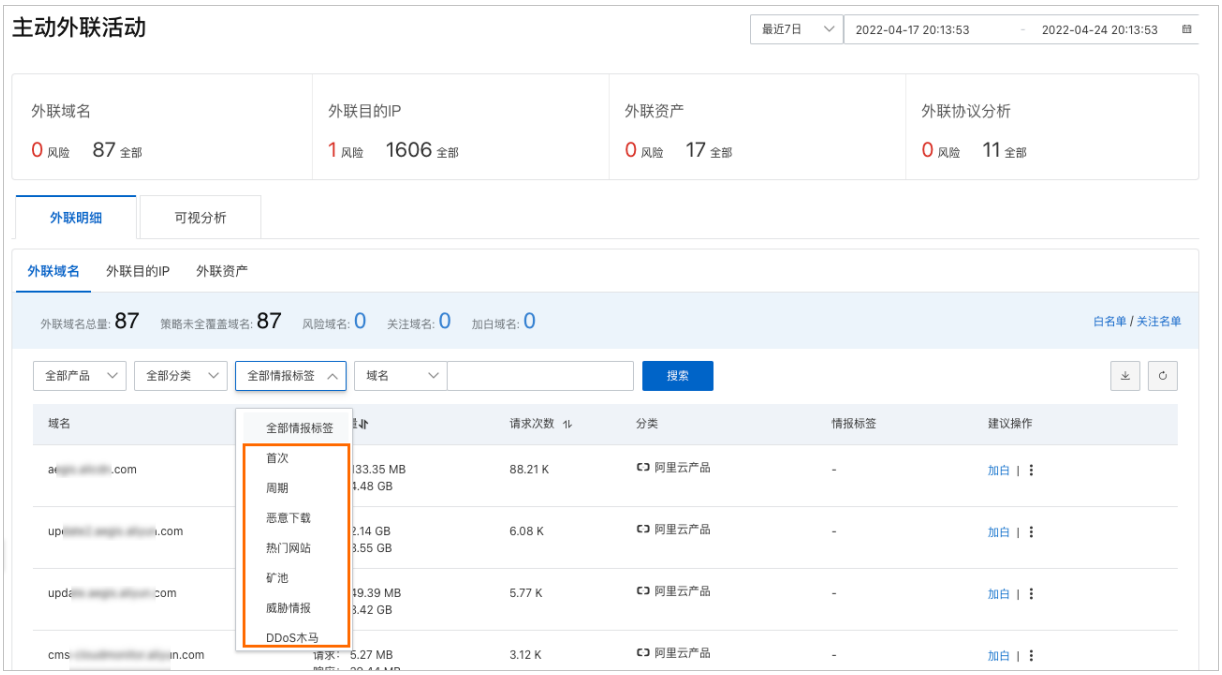
## 流量分析的全量活动搜索结果中流量访问Top中为什么出现很多未知运营商？

来自中国以外地区的流量的入方向地区只展示国家名称，如果入方向存在很多来自中国以外的流量，运营商会被标识为未知。

您可在云防火墙控制台的左侧导航栏选择**日志分析 > 日志审计 > 流量日志**，观察具体IP对应的地区与运营商。

## 主动外联活动中会展示域名的标签，这些标签代表什么？

标签是云防火墙根据外联域名或目的IP的公网信息自动添加的属性，包括：**首次**、**周期**、**恶意下载**、**热门网站**、**矿池**、**威胁情报**、**DDoS木马**。




- **首次**：云防火墙第一次发现该外联活动。

- **周期**：您的资产对该域名或目的IP存在周期性的外联活动。
- **恶意下载**、**矿池**、**威胁情报**：云防火墙检测出的存在威胁的外联活动。请您及时排查此类标签对应的外联活动是否存在误报，如果确认是恶意行为，建议您配置访问控制策略进行管控。详细内容请参见互联网边界（内外双向流量）。
- **热门网站**：您的服务器或您的业务经常访问的域名。
- **DDoS木马**：云防火墙检测出的存在DDoS攻击威胁的外联活动。

# 6.访问控制策略相关问题

## 配置了应用为HTTP或者HTTPS的内对外域名访问控制策略后，如何验证策略的有效性？

请勿使用telnet命令进行域名测试，建议使用curl命令或浏览器访问域名进行测试。例如 `curl -k "https://www.aliyundoc.com"` ，然后查看命中策略的次数和日志审计信息。

## 访问控制策略优先级如何判断？

访问控制策略优先级决定了策略生效的顺序，优先级由云防火墙自动分配。默认情况下，优先级数字越小策略的优先级越高，优先级数字越大策略的优先级越低。您也可以手动调整策略的优先级。相关内容，请参见修改云防火墙访问控制策略的优先级。

如果您设置了多条访问控制策略，访问流量进入**云防火墙**后，会根据策略的优先级按顺序匹配生效的策略。当某个访问流量匹配到一条策略后，云防火墙不再继续匹配其他策略。如果符合放行策略则对流量进行放行，如果触发拒绝策略则拒绝流量通过云防火墙。

- 互联网边界防火墙（内对外流量或外对内流量），优先级数字越小优先级越高，越大优先级越低。

  > **注意** 互联网边界防火墙中策略的优先级是唯一的。

- 主机边界防火墙（内-内流量）优先级和安全组一致，优先级数字小的优先级越高，数字越大优先级越低。

  主机防火墙优先级范围为1~100，优先级可以重复。优先级相同时，动作设置为**拒绝**的策略优先生效。

## 主机边界防火墙策略组规格达到上限，该怎么办？

默认情况下，您最多可以创建100个策略组和100条策略，即在ECS安全组创建并同步到云防火墙的策略数量和在云防火墙主机边界防火墙创建的策略数量加起来不超过100条。如果当前策略数量上限无法满足您的需求，建议您及时清理无需使用的策略，或提交工单申请阿里云技术支持。

## 普通策略组和企业策略组有什么区别？

主机边界防火墙（ECS实例间）访问控制的策略组分为普通策略组和企业策略组。

- 普通策略组对应于ECS的普通安全组，是一种虚拟防火墙，具备状态检测和数据包过滤功能，用于在云端划分安全域。您可以通过配置策略组策略，允许或拒绝策略组内的ECS实例的入流量、出流量。
- 企业策略组对应于ECS的企业安全组，是一种全新的策略组类型，相比原有的普通策略组，大幅提升了组内容纳实例数量，不再限制组内私网IP数量，规则配置方式更加简洁便于维护，适用于对整体规模和运维效率有较高需求的企业级用户。

下表描述了普通策略组和企业策略组的功能差异。

| 功能 | 普通策略组 | 企业策略组 |
| --- | --- | --- |
| 支持专有网络VPC | 是 | 是 |
| 支持设置规则优先级 | 是 | 否 |
| 支持授权给其他策略组 | 是 | 否 |
| 能容纳的私网IP地址数量 | 2000 | 65536 |
| 默认支持同一个策略组内ECS实例互通 | 否。普通策略组出方向默认允许所有访问，入方向上需要您添加访问规则。 | 否。需要您添加出方向和入方向的访问规则。 |

## 安全组放通时单击下发按钮返回失败的提示

表明该IP所关联的安全组不支持默认放通，原因如下：

- 企业安全组不支持安全组放通功能，并且您如果在同一个VPC网络中存在企业安全组，则该VPC所属的安全组也不支持默认放通功能。相关信息，请参见企业安全组。
- 目前，安全组放通只支持ECS Public IP和ECS EIP这两类资产的互联网方向（外到内）流量，公网SLB等不支持开启。
- 为更好地保护您的资产安全，对于未开启云防火墙开关的IP，不建议执行默认放通。对于已放通的IP，不建议关闭云防火墙的防护开关，否则会存在公网IP暴露的风险。

## 安全组默认放通策略下发状态，提示“配置冲突不可调整”

安全组默认放通策略为**配置冲突不可调整**时，说明相同VPC下的某个安全组的规则占用了可调整的优先级。

ECS所属VPC中，其他ECS有安全组与云防火墙要调整的优先级冲突时，需要确保该VPC下所有ECS安全组优先级不存在冲突的情况下，才可使用一键下发的功能。

## 安全组放通一键下发功能不可使用（置灰）

原因是存在还未解决冲突的安全组。对该IP所在的ECS实例关联的安全组中，只要存在配置冲突，都必须先解决冲突后才能下发默认放通策略。相关内容请参考安全组默认放通。

## 一键下发失败（报错）

待放通安全组规则规格超出限制，需要手动调整规则。

默认情况下，您最多可以创建100个策略组和100条策略，即在ECS安全组创建并同步到云防火墙的策略数量和在云防火墙主机边界防火墙创建的策略数量加起来不超过100条。如果当前策略数量上限无法满足您的需求，建议您及时清理无需使用的策略，或提交工单申请阿里云技术支持。

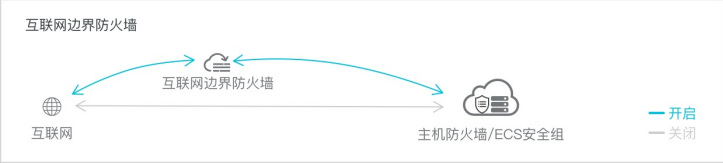
# 7.互联网边界防火墙常见问题

## 互联网边界防火墙的作用是什么？

对于未开启互联网边界防火墙的公网IP资产，网络流量不会经过互联网边界防火墙，只经过主机防火墙（即安全组），最终到达您的ECS实例。

对于开启了互联网边界防火墙的公网IP资产，流量经过边界防火墙检测和过滤后，再经过主机防火墙，最终到达您的ECS实例。如果仅开启互联网边界防火墙开关、未配置云防火墙的访问控制策略也未设置入侵防御策略，云防火墙将仅对该流量进行检测和告警、不会进行拦截。

互联网边界防火墙开关开启或关闭时网络流量路径如下图所示：




## 开启互联网边界防火墙开关是否会对网络流量产生影响？

购买了云防火墙，互联网边界防火墙开关默认全部开启。如果未进行任何策略配置，您业务的访问流量仅经过云防火墙，云防火墙不会对流量进行任何处理。

## 关闭互联网边界防火墙开关有什么影响？

互联网边界防火墙页面如下图所示：

关闭互联网边界防火墙开关可能会产生以下影响：

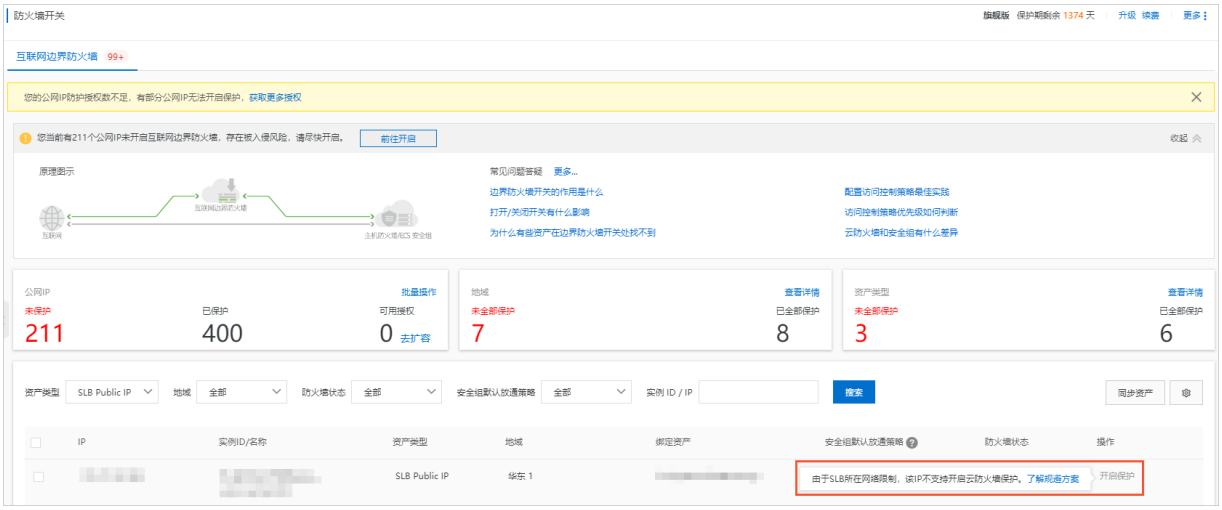
- **网络流量分析** > **互联网访问活动**页面中，网络流量分析部分图表可能无数据。
- 如果配置了**内对外**或**外对内**访问控制策略，关闭互联网边界防火墙开关将会使该主机对应的访问控制策略失效，表现为该访问控制策略的**命中次数**保持不变。
- 所有流量将不会经过云防火墙，入侵防御功能将会失效。
- **日志分析** > **日志审计**页面中的**流量日志**页签，将不会显示防火墙开关关闭后的流量数据。
- 所有流量将不会经过云防火墙，网络抓包抓取不到开关关闭后的流量数据，**设置** > **工具箱**页面中的**网络抓包**模块也不会展示对应IP的报文信息。详细内容，请参见网络抓包。

相关操作，请参见互联网边界防火墙。

## 为什么无法开启互联网边界防火墙开关？

**现象描述**

云防火墙控制台互联网边界防火墙列表中，部分资产无法开启边界防火墙保护（**开启保护**开关不可操作，并提示**由于SLB所在网络限制，该IP所在网络不支持开启防火墙保护**）。




**问题原因**

该SLB资产只有私网IP，不支持开启云防火墙保护，因此部分资产无法开启互联网边界防火墙。

**解决方法**

对于资产只有私网SLB的情况，建议您采用私网SLB加EIP的方案（相关信息，请参见绑定和管理EIP），将流量牵引到云防火墙上进行防护。

## 互联网边界防火墙支持防护哪些公网IP类型？

云防火墙支持以下类型的公网IP引流，即可以对您以下类型的公网资产提供防护：

- ENI EIP（支持绑定到专有网络类型的ECS实例、专有网络类型的私网SLB实例、弹性网卡和NAT网关上）
- Nat PublicIP（ECS系统分配的公网IP）
- SLB EIP（绑定到专有网络SLB的EIP）
- 堡垒机

# 8.VPC边界防火墙相关问题

## 开启防火墙开关是否对网络流量会产生影响？

无论是开启互联网边界防火墙和VPC边界防火墙都不会对网络流量产生任何影响。

开启VPC边界防火墙开关之前，需要评估以下限制：目前，开启或关闭VPC边界防火墙操作会触发长连接重置。如果您的VPC内正在使用内网SLB，您在开启VPC边界防火墙前需要检查您的应用程序是否支持TCP自动重传机制，并关注应用连接状态，避免未配置重传机制导致的连接中断。

## 开启VPC边界防火墙后，ECS安全组规则是否会受到影响？

不会。

开启VPC边界防火墙后会自动添加名称为Cloud_Firewall_Security_Group的安全组和放行策略，用于放行到VPC边界防火墙的流量。

开启VPC边界防火墙后自动创建的安全组仅对该VPC之间的流量进行管控，您原来已创建的ECS安全组规则仍然生效并不受影响。因此，无需您对ECS安全组规则做任何迁移或修改。

## VPC边界防火墙存在哪些限制？

请参见VPC边界防火墙限制说明。

# 9.日志相关问题

本文档主要介绍了云防火墙日志相关的常见问题。

## 云防火墙的流量日志是否支持导出到第三方系统？

支持。云防火墙高级版、企业版和旗舰版支持日志分析功能，并已同步阿里云日志服务（SLS）。目前云防火墙日志分析功能支持查看并导出**互联网流量日志**和**VPC流量日志**。

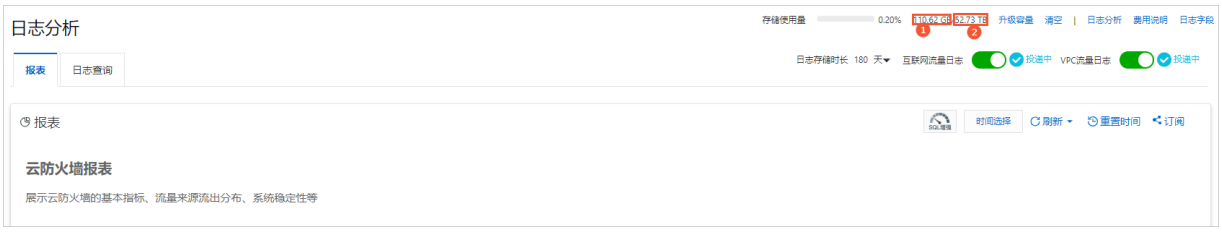
您可通过日志分析功能将导出的流量日志文件接入到您的业务系统中，如您的安全运维中心等。

> **说明** 互联网流量日志包括漏洞风险等级和访问控制规则命中结果等数据。

相关操作，请参见将云防火墙流量日志导入第三方系统。

## 如何查看云防火墙日志存储剩余容量？

如果您已经购买了云防火墙高级版、企业版或旗舰版，并开通了日志存储容量（即日志分析服务）。您可以在云防火墙控制台的**日志分析 > 日志分析**页面的右上角，查看日志分析的存储使用量（下图中标注①）和剩余可用容量（下图中标注②）。




> **说明** 由于云防火墙基础版和免费试用版不支持日志分析功能，控制台将不会展示日志存储容量。

## 为什么在云防火墙控制台看不到日志存储容量？

云防火墙基础版和免费试用版不支持日志分析功能。如果您使用的是云防火墙基础版或免费试用版，控制台将不会展示日志存储容量。如何开通云防火墙服务的日志分析功能，请参见开通日志分析服务。

# 10.流量不通时如何排查？

## 问题描述

网络经过云防火墙时，可能会出现以下问题：

- 您无法登录服务器。
- 您无法访问服务器上的服务。
- 您的服务器无法访问外网。

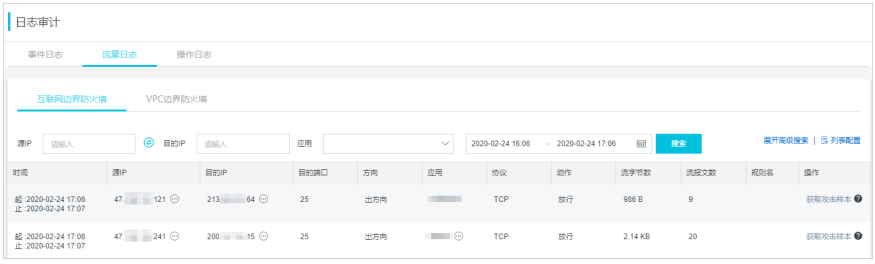
## 互联网边界防火墙排查步骤

1. 确认资产是否开启了互联网边界防火墙。

开启了边界防火墙后，流量才会经过云防火墙。关于如何开启边界防火墙开关，请参见互联网边界防火墙。

> **说明** 如果资产未开启互联网边界防火墙，流量不会经过云防火墙，您需要排查是否存在其他问题，例如：网络不通等。

2. 确认**流量日志**页签是否有相应的流量记录。



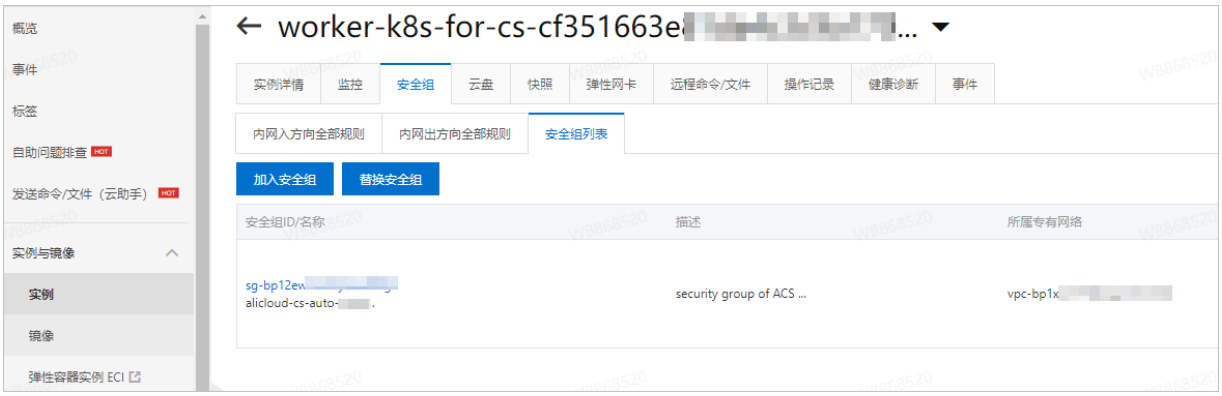

- 如果不存在流量日志，说明流量还未到达防火墙就被丢弃。
- 如果存在流量日志，且动作为**丢弃**，说明流量是在互联网防火墙处被丢弃，在**事件日志**列表中查询对应流量，根据**判断来源**列确认拦截该流量的指令来源。

  - 指令来源为**访问控制**：说明您配置的访问控制策略对该流量进行了拦截。建议您检查对应访问控制策略配置并进行修改。
  - 指令来源为**基础防御**、**虚拟补丁**或**威胁情报**：说明您设置的入侵防御策略对该流量进行了拦截。您可以前往**攻击防护 > 入侵防御**页面，关闭对应的入侵防御策略。

- 如果存在流量日志，动作为**放行**或**观察**，说明流量不是在互联网边界防火墙处被丢弃，需要继续排查主机防火墙（安全组）策略。

## 主机防火墙（安全组）排查步骤

登录ECS控制台的左侧导航栏，选择**实例与镜像 > 实例**，定位到网络不通的ECS实例，在**安全组**页签下的**安全组列表**页签，确认安全组是否放行（**授权策略**设置为**允许**）。




如果上述步骤还不能解决您的问题，请提交工单。

# 11.云防火墙防护流量时的规则匹配顺序

云防火墙防护流量时，有以下规则匹配顺序：

- 如果您未启用访问控制策略或已启用访问控制策略但流量未命中访问控制策略，流量会先匹配**威胁情报**，再匹配**基础防御**、**智能防御**、**虚拟补丁**。

> **注意** 如果流量匹配**威胁情报**时产生拦截动作，不会再匹配其他规则。

- 如果您已启用访问控制策略且流量命中了动作为放行或观察的访问控制策略，流量不再匹配威胁情报规则，会匹配**基础防御**、**智能防御**、**虚拟补丁**。
- 如果您已启用访问控制策略且流量命中了动作为拒绝的访问控制策略，流量不再匹配其他规则。

> **注意** **基础防御**、**智能防御**、**虚拟补丁**规则不分先后顺序，流量都会匹配一遍。

# 12.为什么当前账号无法开启云防火墙？

## 问题描述

使用阿里云账号登录云防火墙控制台，控制台界面上展示**当前账号无法开启云防火墙**。

## 主要原因

有以下两个原因会导致此问题：

- 当前账号为阿里云账号（主账号）且已被其他阿里云账号添加为成员账号进行统一管理。
- 当前账号为RAM用户（子账号）且未完成授权。

## 解决方法

您可以将光标移至控制台界面右上角登录账号头像处，查看**账号ID**。

- 如果**账号ID**是以1开头的一串数字，表示该账号为阿里云账号（主账号）。请您使用统一管理该账号的阿里云账号登录云防火墙控制台，您登录成功后可以为该账号下的云资产开启防护。
- 如果**账号ID**是以2开头的一串数字，表示该账号为RAM用户（子账号）。您需要对该账号进行授权操作：
  i. 登录RAM控制台。相关信息，请参见RAM用户登录阿里云控制台。
  ii. 在左侧导航栏，选择**身份管理 > 用户**。
  iii. 在**用户**页面，单击目标RAM用户**操作**列**添加权限**。
  iv. 在**添加权限**页面，选中createSlr、AliyunYundunCloudFirewallReadOnlyAccess和AliyunYundunCloudFirewallFullAccess。

  > 注意　createSlr是自定义权限策略。相关信息，请参见创建权限策略。

  v. 单击**确认**，完成授权操作。

## 创建权限策略

- 登录RAM控制台。
- 在左侧导航栏，选择**权限管理 > 权限策略**。
- 在**权限策略**页面，单击**创建权限策略**。
- 在**创建权限策略**页面，单击**脚本编辑**。
- 在**脚本编辑**页面，**名称**输入createSlr，完成脚本编辑。

  具体的脚本如下：

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateServiceLinkedRole"
            ],
            "Resource": "acs:ram:*:166032244439****:role/*",
            "Effect": "Deny",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": [
                        "cloudfw.aliyuncs.com"
                    ]
                }
            }
        }
    ],
    "Version": "1"
}
```

**注意** Resource参数的格式为acs:ram:*:阿里云账号（主账号）的UID:role/*。阿里云账号（主账号）的UID表示RAM用户（子账号）所属主账号的UID。

- 单击**确认**，完成安全验证。

# 13.为什么有来自阿里云的ICMP周期性探测报文？

云防火墙为了保障服务质量，会周期性发送ICMP报文进行探测，该类探测不是扫描攻击，不会对业务造成影响。

其访问源IP在云防火墙地址簿云地址簿中的Source address for SLA monitoring中可以查看到，具体日志数据可以通过访问控制中外对内SLA策略命中次数访问详细日志。