ALIBABA CLOUD

Alibaba Cloud

云防火墙

网络流量分析

文档版本：20220420

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 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 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 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 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.概述 05
2.主动外联活动 06
3.互联网访问活动 14
4.VPC访问活动 16
5.全量活动搜索 17
6.智能策略下发 19

1.概述

通过网络流量分析，您可以实时查看主机上发生的入侵事件、网络活动、流量趋势、入侵防御阻断访问和主机主动外联活动等，实现全网流量的可视化。

云防火墙提供以下网络流量分析功能：

- 主动外联活动
- 互联网访问活动
- VPC访问活动
- 失陷感知
- 入侵防御
- 全量活动搜索

> **说明** 您需要先开启云防火墙开关，网络流量分析各模块才会展示出相关的分析数据。如何开启云防火墙开关，请参见开启防火墙。

2.主动外联活动

网络资产开启云防火墙开关后，主动外联活动页面向您实时展示主机的主动外联数据，帮助您及时发现可疑主机。本文介绍了主动外联活动页面展示的信息和支持的操作。

概述

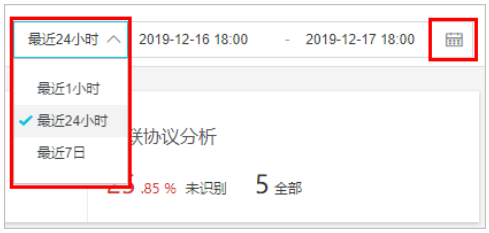
为网站资产开启云防火墙开关后，您可以在云防火墙控制台的**网络流量分析 > 主动外联活动**页面，查看以下流量分析数据：

- 外联数据统计
- 外联明细
- 可视分析

> **注意** 您必须先开启云防火墙开关，**主动外联活动**页面才会展示相应的流量分析数据。关于如何开启云防火墙开关，请参见开启防火墙。

您可以使用右上角的时间选择器设置要查看的时间范围。您可以直接选择查看**最近1小时**、**最近24小时**、**最近7日**的数据，或者自定义时间范围。自定义时间范围时，您可以选择查看任意7天内的数据。

> **说明** 选择的时间范围如果超过7天，会弹出警告，提示您选择7天以内的时间。



外联数据统计

外联数据统计模块位于**主动外联活动**页面上方，为您展示以下统计数据：

- **外联域名**：存在风险的外联域名的数量和全部外联域名的数量。

  单击该区域可以跳转到**外联明细**下的外联域名记录，查看详细信息。
- **外联目的IP**：存在风险的外联目的IP的数量和全部外联目的IP的数量。

  单击该区域可以跳转到**外联明细**下的外联目的IP记录，查看详细信息。
- **外联资产**：发起有风险外联的资产的数量和发起外联的全部资产的数量。

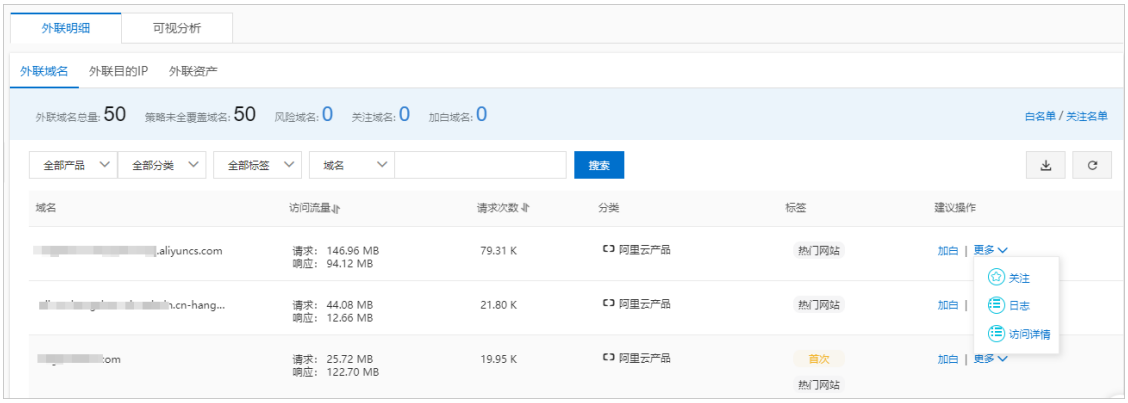
  单击该区域可以跳转到**外联明细**下的外联资产记录，查看详细信息。
- **外联协议分析**：外联协议分析结果，包括未识别协议的外联的占比和外联中用到的全部协议的数量。

  单击该区域可以跳转到**可视分析**模块，查看IP流量统计和外联协议分析的详细信息。

外联明细

外联明细页签下包含**外联域名**、**外联目的IP**和**外联资产**列表，您可以单击对应页签，查看相关的外联明细。不同外联明细的具体说明如下：

- **外联域名**



每条记录包含以下信息：外联**域名**、**访问流量**、**请求次数**、**分类**、**标签**、**建议操作**。**分类**和**标签**是云防火墙根据外联域名的公网信息添加的网站属性，供您参考。关于标签的详细介绍，请参见网络流量分析相关问题。

您可以单击列表右上角的

图标，将外联域名列表（CSV格式）下载到本地计算机进行查看和分析。

您可以在外联域名列表中执行以下操作：

- **加白**：单击某个域名记录下的**加白**，将当前外联域名添加到**白名单**的**目的域名**记录中。

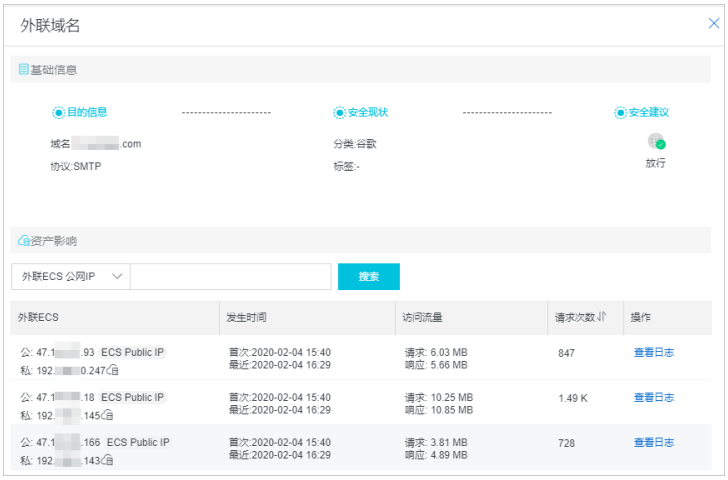
  加白后如何取消：您可以单击右上角的**白名单**，并在**目的域名**记录中**取消加白**。

- **关注**：选择某个域名记录下的**更多 > 关注**，将当前外联域名添加到**关注名单**的**目的域名**记录中。

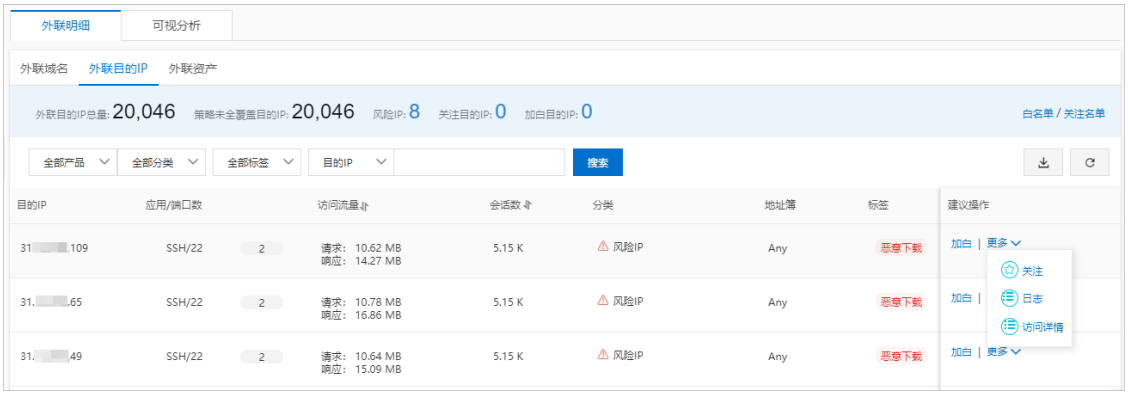
  关注后如何取消：您可以单击右上角的**关注名单**，并在**目的域名**记录中**取消关注**。

- **日志**：选择某个域名记录下的**更多 > 日志**，可以跳转到**日志审计**下的**流量日志**审计页面，查看相关的流量日志记录。更多信息，请参见日志审计。

- **访问详情**：选择某个域名记录下的**更多 > 访问详情**，可以查看当前外联域名的访问详情，例如，外联该域名的ECS实例、外联发生时间、访问流量、请求次数等。外联域名的访问详情如下图所示。



- **外联目的IP**



每条记录包括以下信息：**目的IP**、**应用/端口数**、**访问流量**、**会话数**、**分类**、**地址簿**、**标签**、**建议操作**。**分类**和**标签**是云防火墙根据外联域名的公网信息添加的网站属性，供您参考。关于标签的详细介绍，请参见网络流量分析相关问题。**地址簿**表示收录当前目的IP的地址簿。

您可以单击列表右上角的

图标，将外联目的IP列表（CSV格式）下载到本地计算机进行查看和分析。

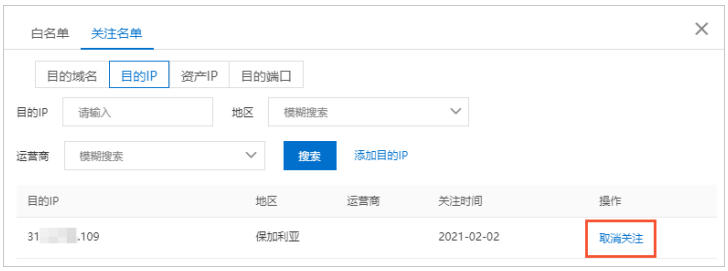
您可以在外联目的IP列表中执行以下操作：

- **加白**：单击某个目的IP记录下的**加白**，将当前外联目的IP添加到**白名单**的**目的IP**记录中。

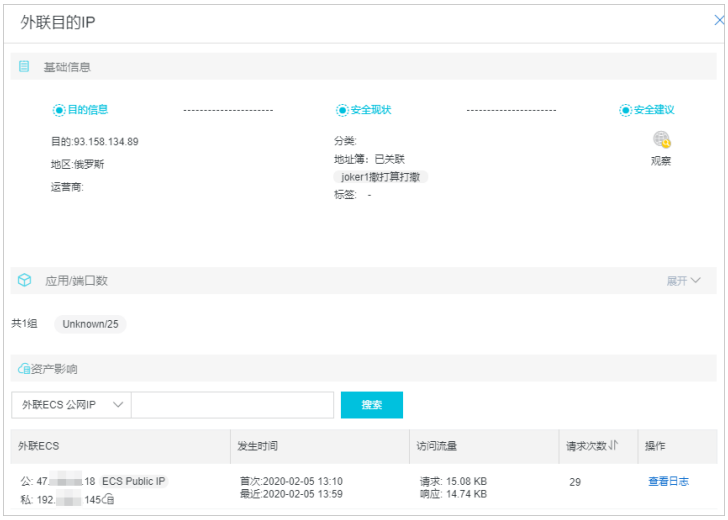
  加白后如何取消：您可以单击右上角的**白名单**，并在**目的IP**记录中**取消加白**。

- **关注**：选择某个目的IP记录下的**更多 > 关注**，将当前外联目的IP添加到**关注名单**的**目的IP**记录中。

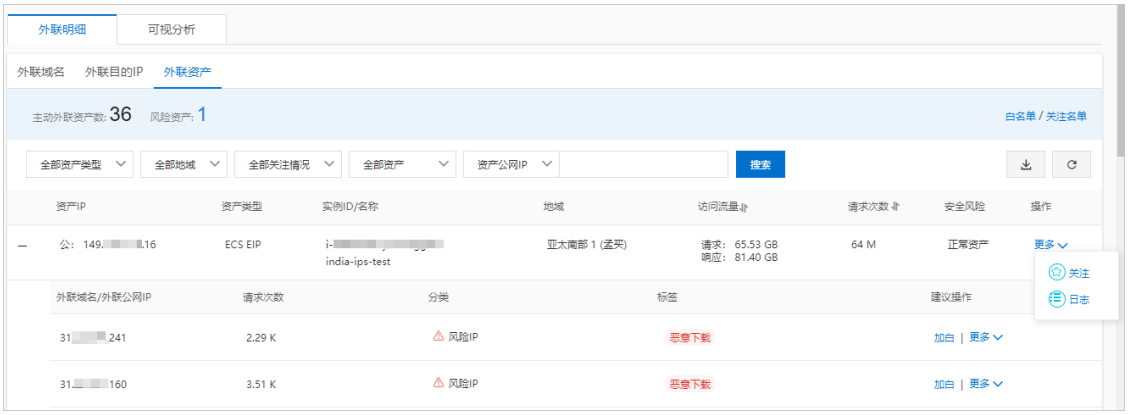
  关注后如何取消：您可以单击右上角的**关注名单**，并在**目的IP**记录中**取消关注**。



- **日志**：选择某个目的IP记录下的**更多 > 日志**，可以跳转到**日志审计**下的**流量日志**审计页面，查看当前目的IP的流量日志记录。更多信息，请参见日志审计。
- **访问详情**：选择某个目的IP记录下的**更多 > 访问详情**，可以查看当前外联目的IP的访问详情，例如，外联该IP的ECS实例、外联发生时间、访问流量、请求次数等信息。外联目的IP的访问详情如下图所示。



- **外联资产**



每条记录包括以下信息：**资产IP**、**资产类型**、**实例ID/名称**、**地域**、**访问流量**、**请求次数**、**安全风险**、**操作**。**安全风险**是云防火墙根据外联记录为当前资产添加的安全状态属性，供您参考。

您可以单击列表右上角的

图标，将外联资产列表（CSV格式）下载到本地计算机进行查看和分析。

您可以对资产IP记录执行以下操作：

- **关注**：选择某个资产IP记录下的**更多 > 关注**，将当前资产IP添加到**关注名单**的**资产IP**记录中。

  关注后如何取消：您可以单击右上角的**关注名单**，并在**资产IP**记录中**取消关注**。

- **日志**：选择某个资产IP记录下的**更多 > 日志**，可以跳转到**日志审计**下的**流量日志**审计页面，查看当前资产IP（即发起外联的源IP）的流量日志记录。更多信息，请参见日志审计。
- 查看资产IP的外联明细：单击某个资产IP记录前的

  +

  图标，可以查看当前资产的外联明细。

  资产外联明细包括以下信息：**外联域名/外联公网IP**、**请求次数**、**分类**、**标签**、**建议操作**。**分类**和**标签**是云防火墙根据外联域名的公网信息添加的网站属性，供您参考。关于标签的详细介绍，请参见网络流量分析相关问题。

  您可以对资产外联明细执行以下操作：

  - **加白**：单击某个外联域名或公网IP记录下的**加白**，将当前外联域名或公网IP添加到**白名单**的**目的域名**或**目的IP**记录中。

    加白后如何取消：您可以单击右上角的**白名单**，并在**目的域名**或**目的IP**记录中**取消加白**。

  - **关注**：选择某个外联域名或公网IP记录下的**更多 > 关注**，将当前外联域名或公网IP添加到**关注名单**的**目的域名**或**目的IP**记录中。

    关注后如何取消：您可以单击右上角的**关注名单**，并在**目的域名**或**目的IP**记录中**取消关注**。

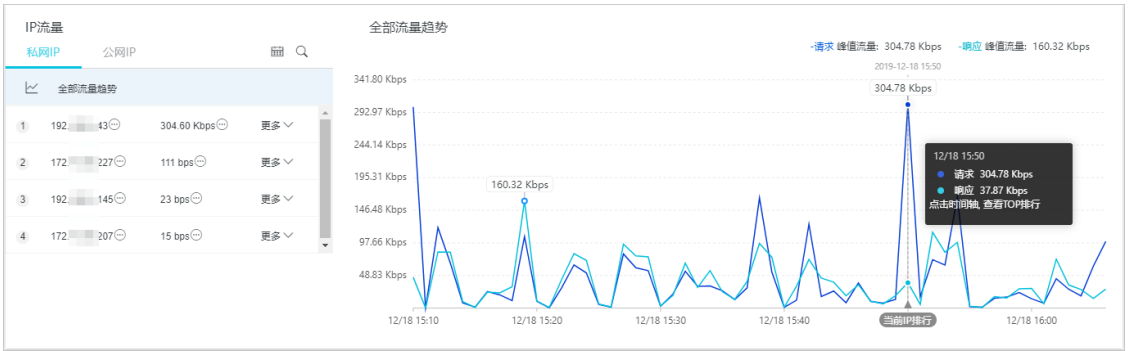
  - **日志**：选择某个外联域名或公网IP记录下的**更多 > 日志**，可以跳转到**日志审计**下的**流量日志**审计页面，查看相关的流量日志记录。更多信息，请参见日志审计。

可视分析

可视分析页签从上到下包含**IP流量统计**和**外联协议分析**两个模块，具体说明如下：

- **IP流量统计**

  IP流量统计模块包括左侧的**IP流量**排序表和右侧的**全部流量趋势**图。排序表和趋势图支持联动操作。



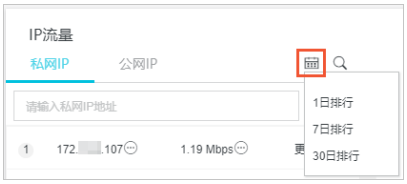
  IP流量表：展示某一时刻所有私网IP或公网IP的响应流量大小排序，按照响应流量从高到低排序。

  - 单击**私网IP**或**公网IP**页签，切换展示私网IP、公网IP流量排序。

- 单击**全部流量趋势**图横轴上任意时刻，刷新IP流量表，查看当前时刻的IP流量排序。
- 单击某个IP地址后的**更多 > 查看日志**，跳转到**日志审计**下的**流量日志**审计页面，查看指定IP地址的流量日志记录。更多信息，请参见日志审计。

全部流量趋势图：实时展示全部或者指定的网络资产上的总请求和响应峰值流量趋势。光标悬置在图上任意时刻，展示当前时刻的请求和响应峰值流量。

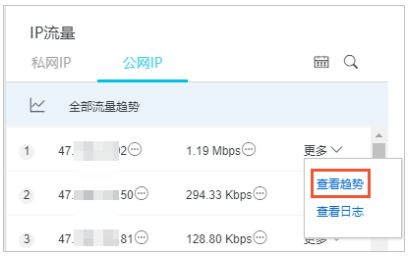
- 设置时间范围：默认展示近7日的数据。使用**IP流量**表右上角的时间选择器，可以设置要查看的时间范围。



支持设置的时间范围包括：

  - **1日排行**：展示近1日的数据。
  - **7日排行**：展示近7日的数据。
  - **30日排行**：展示近30日的数据。

- 设置数据范围：默认展示全部开启防护的网络资产的总流量趋势。使用**IP流量**表可以设置展示指定资产的流量趋势，操作方法如下：
  - 在IP流量表中单击任意一个IP，或者选择某个IP下的**更多 > 查看趋势**，刷新全部流量趋势图，查看指定IP的流量趋势。



- 使用IP流量表右上角的IP搜索工具，指定一个公网IP或私网IP，刷新全部流量趋势图，查看指定IP的流量趋势。

> **说明** 执行该操作后，IP流量表不再显示IP排序数据。

设置数据范围后，全部流量趋势图上方显示设置的过滤条件。

- **外联协议分析**

外联协议分析模块包括左侧的**应用占比**饼状图和右侧的**外联协议详情**表。

应用占比图：展示外联活动中使用的不同应用协议的分布占比。

外联协议详情表：展示外联活动中使用的应用协议的详情。您可以在**操作**列，单击某个应用的**日志**，跳转到**流量日志**审计页面，查看指定应用的流量日志记录。

相关文档

- 开启防火墙
- 网络流量分析相关问题
- 智能策略下发

- 地址簿管理

3.互联网访问活动

云防火墙的互联网访问活动页面为您展示资产入方向正常流量和异常流量的概览信息，包括入方向流量的开放应用、开放端口、开放公网IP地址和入方向流量访问的云产品信息。

前提条件

您必须先开启互联网边界防火墙开关，**互联网访问活动**页面才会展示对应的流量分析数据。

关于如何开启互联网边界防火墙开关，请参见开启防火墙。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**流量分析 > 互联网访问活动**。
3. 在**互联网访问活动**页面右上角，设置查询时间范围。

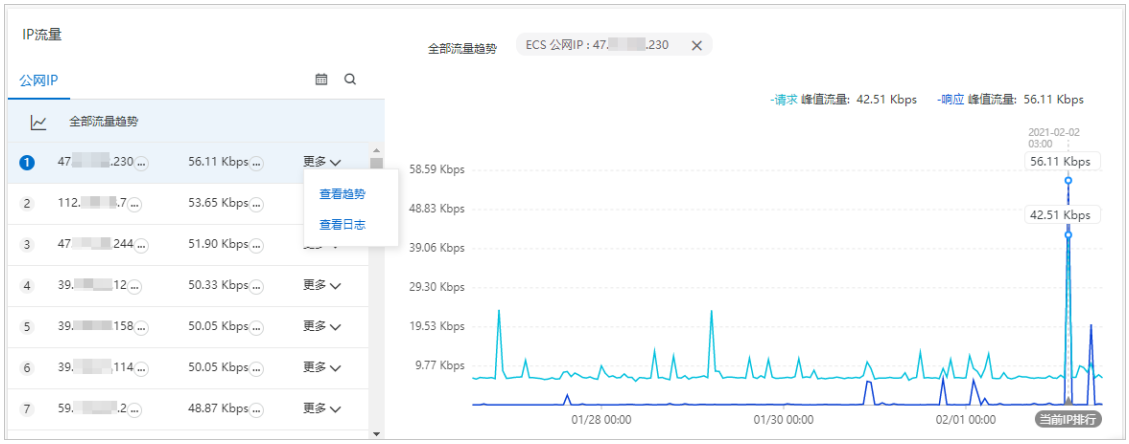
   您可以直接从下拉列表中选择以下时间范围：**最近1日**、**最近7日**、**最近30日**，也可以自定义查询指定时间段的数据。

4. 查看满足条件的互联网访问活动数据。

   您可以查看以下数据：

   - 互联网访问活动的概览信息：包括**开放公网IP**的总数量和对应的风险项数量、**开放端口**的总数量和对应的风险项数量、**开放应用**的总数量和对应的风险项数量、入流量访问的**云产品**的**公网IP**的风险项数量和**开放端口**的总数量。

   - **IP流量**排行表和**全部流量趋势**图：



- **IP流量**排行表：展示某一时刻所有公网IP的流量大小排序，按照流量从高到低排序。统计时刻在**全部流量趋势**图中体现，即横轴上的**当前IP排行**点。

  您可以在**IP流量**排行表中执行以下操作：

  - 选择某个目标公网IP后的**更多 > 查看趋势**，可以在**全部流量趋势**图中查看该公网IP的流量趋势信息。
  - 选择某个目标公网IP后的**更多 > 查看日志**，可以跳转到**日志审计**下的**流量日志**页面。您可以在流量日志中查看到所有互联网入方向流量的详细数据。更多信息，请参见日志审计。

- **全部流量趋势图**：实时展示所有资产上的总请求和响应流量峰值。

- 互联网访问活动详情：包括**开放公网IP**、**开放端口**、**开放应用**、资产**明细**，以及互联网流量访问的**云产品**的详细记录。

  您可以单击列表右上方的

  图标，将对应列表（CSV格式）下载到本地计算机进行查看和分析。

4.VPC访问活动

云防火墙的VPC访问活动模块为您展示VPC专有网络之间的流量信息，帮助您实时获取VPC网络流量信息，及时发现和排查异常流量，从而更快地发现和检测出攻击。VPC访问活动页面中展示的信息包括VPC间流量访问TOP排行、VPC间会话TOP排行、流量访问的开放端口和资产信息等。

前提条件

您必须先开启VPC边界防火墙开关，**VPC访问活动**页面才会展示对应的流量分析数据。

关于如何开启VPC边界防火墙开关，请参见开启防火墙。

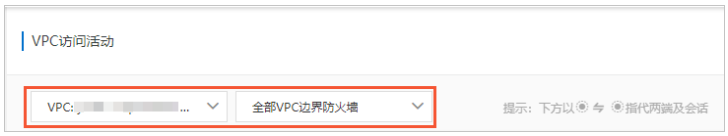
操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**流量分析 > VPC访问活动**。
3. 在**VPC访问活动**页面右上角，设置查询时间范围。

   您可以直接从下拉列表中选择以下时间范围：**最近1小时**、**最近24小时**、**最近7日**，也可以自定义查询最近7日范围内任何时间段的数据。

4. 在**VPC访问活动**页面上方，设置要查看的目标VPC和已开启的VPC边界防火墙。

5. 查看满足条件的VPC访问活动数据。

   您可以查看以下数据：

   - **VPC间流量**：查看VPC专有网络入方向、出方向流量的峰值和均值数据，及对应的入方向、出方向流量数据趋势。
   - **流量Top排行**：查看流量排名前10、20或50的流量数据和相关信息，包括流量的IP地址、流入和流出数据。
   - **VPC间会话TOP排行**：查看VPC间会话的流量排行数据和相关信息，包括流量排行、IP会话、IP会话数、流量和端口数据。

     在**VPC间会话TOP排行**列表中，单击**查看占比**栏的**查看**，可以查看该会话中端口占比的详细数据。
   - **开放端口占比**：查看所有开放端口占比信息。
   - **开放端口和资产明细**：查看VPC间流量日志详情列表，包括VPC间流量访问的开放端口和资产的基本信息。

     您可以单击列表右上方的

     图标，将VPC开放端口、VPC资产列表（CSV格式）下载到本地计算机进行查看和分析。

5.全量活动搜索

全量活动搜索页面为您实时展示云防火墙保护范围内所有主机的全部流量访问趋势数据、入方向或出方向TOP应用访问的来源地区及其占比数据、TOP会话地址及其占比数据等。

前提条件

您需要先开启云防火墙开关，**全量活动搜索**页面才会展示出相关的分析数据。如何开启云防火墙开关，请参见开启防火墙。

操作步骤

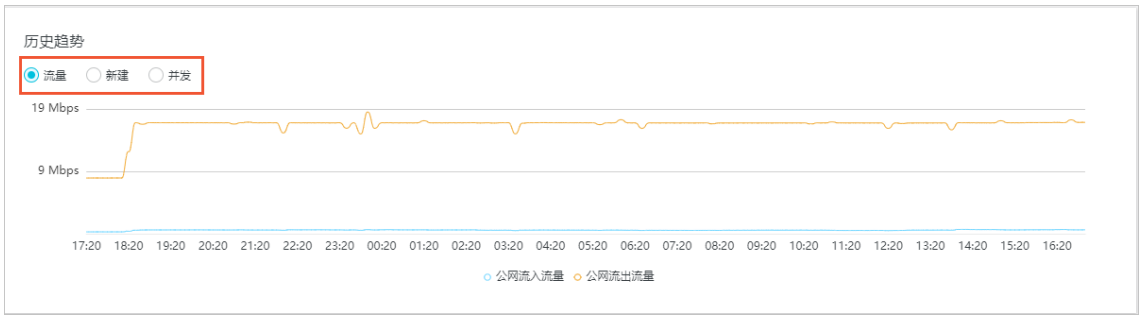
1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**流量分析 > 全量活动搜索**。
3. 在**全量活动搜索**页面，查看15分钟、1小时、4小时、1天、1周内或自定义时间范围内的全部威胁活动情况和趋势图。

> **说明** 自定义时间范围不限。

- 单击**条件**下拉框选择对应的查询条件并输入或选择该条件的详细信息，**查询**对应的流量访问活动的历史趋势。单击**重置**清除设置的搜索条件。

> **说明** 单击**增加**可增加一条搜索条件，新增的搜索条件和原有的搜索条件同时生效。您最多可增加两条搜索条件。

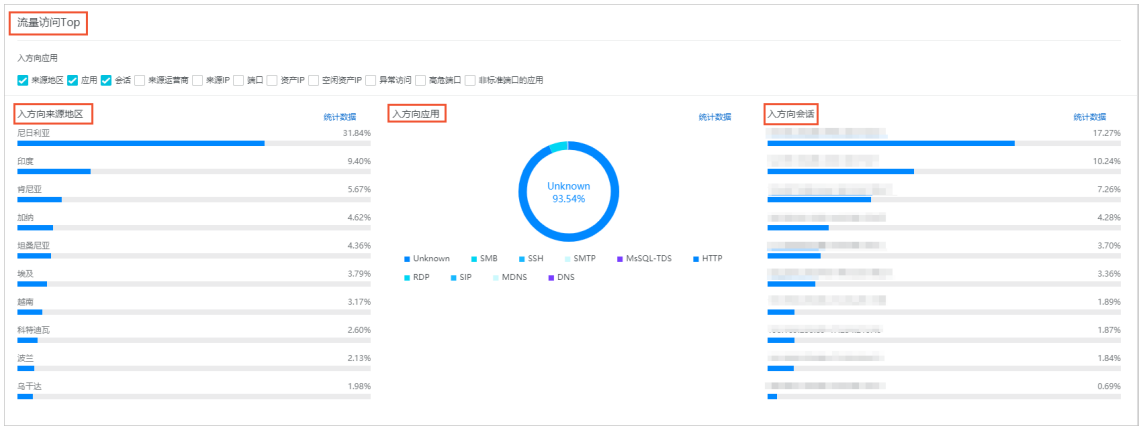
- 在**历史趋势**模块，您可查看选定时间范围内公网流入或流出流量趋势图、新建连接数趋势图以及并发连接数趋势图。



单击**流量**、**新建**或**并发**可对应切换到流量趋势、新建连接数趋势、出入方向并发流量趋势。

> **注意** 趋势图显示15分钟、1小时、4小时、1天、1周内或自定义时间范围内的流量数据。自定义时间范围不限。

- 在**流量访问Top**模块，您可查看出方向或入方向流量访问排名前十的区域、应用类型及其占比数等信息。



- 在**流量访问Top**模块单击**统计数据**打开对应的入方向来源地区、出方向目的地区、入方向或出方向应用等的**统计数据**弹框，查看详细统计数据。
- 单击**填充到条件**可将对应条件自动填充到全量活动搜索条件栏。如下图所示。**历史趋势**和**流量访问Top**模块将显示填充条件的相关趋势图。

相关文档

- 云防火墙可以防护哪些云资产或流量？

6.智能策略下发

云防火墙基于互联网访问和主动外联的智能策略功能，为您提供高危服务隔离（外对内）和蠕虫防御（内对外）模式的安全策略配置，为您推荐更加安全的ACL策略，帮助您防御网络和主机的安全威胁。

高危服务隔离

云防火墙的**智能策略**功能会根据互联网访问检测的安全威胁，为您提供最佳的ACL策略。例如，如果互联网暴露的IP资产开启了危险性较高的服务（SSH，RDP等），且服务存在被爆破、入侵的风险，**智能策略**会推荐您配置策略，仅放行来自常用登录地区且登录状态正常的互联网请求，拒绝其他登录地区的互联网请求，从而降低网络被攻击的风险。

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**流量分析 > 互联网访问活动**。
3. 在**互联网访问活动**页面，单击**开放公网IP**模块跳转到开放公网IP列表。
4. 定位到目标公网IP，单击最右侧**操作**栏下**智能策略**。

   智能策略面板为您展示了当前云防火墙针对该公网IP的防护为您推荐的智能策略，包括对于用户IP及端口的**放行**和**拒绝**策略。
5. 在**智能策略**页面，选择执行以下操作。
   - 单击**展开**，可查看推荐智能策略的理由。

     您可查看到曾有大量恶意IP尝试访问用户IP的SSH服务。
   - 单击**下发策略 > 提交**后，云防火墙推荐的该智能策略将会即时生效。

     > **说明** 执行**下发策略**前，请确保您已知悉推荐策略的含义，及该策略对业务可能造成的影响。