

ALIBABA CLOUD

Alibaba Cloud

云防火墙
网络流量分析

文档版本：20201014

 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。
<code>Courier</code> 字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
<i>斜体</i>	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录


1.概述	05
2.主动外联活动	06
3.互联网访问活动	10
4.VPC访问活动	11
5.失陷感知	12
6.IPS拦截记录	13
7.全量活动搜索	15
8.智能策略下发	16

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](#)
- [IPS拦截记录](#)
- [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说明和相关操作。

概述

网络流量分析 > 主动外联活动页面从上到下分为以下四个模块，您可以单击模块名称查看各模块展示的信息说明和相关操作。

- 外联数据统计
- IP流量统计
- 外联协议分析
- 外联活动记录

 **说明** 您需要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。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。可以直接选择查看最近1小时、最近24小时、最近7日的的数据，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。选择的时间范围若超过7天，则会弹出警告。

时间选择器

外联数据统计

外联数据统计模块展示以下统计数据。

- **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外联协议分析模块，查看详细信息。

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，跳转到流量日志审计页面，查看指定IP地址的流量日志记录。

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，或者单击某个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。

 **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。

外联活动记录

外联活动记录包括外联域名列表、外联目的IP列表和外联资产列表。单击外联域名、外联目的IP、外联资产页签，查看对应记录。

- **外联域名**

每条记录包括以下信息：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：**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。

有关标签的详细介绍，请参见[网络流量分析相关问题](#)。

- 建议操作：包括以下操作。

- 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。您可以单击右上角的白名单/关注名单，并在目的域名记录中取消加白。



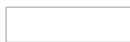
- 关注：单击某个域名记录下的更多 > 关注，将当前外联域名添加到关注名单的目的域名记录中。
- 取消关注：如果您想要取消某个外联域名的关注，您可以单击该域名记录下的更多 > 取消关注。或者您也可以单击右上角的白名单/关注名单，并在目的域名记录中取消关注。





- 日志：跳转到流量日志审计页面，查看相关的流量日志记录。
- 访问详情：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：云防火墙根据外联目的IP的公网信息添加的属性，供您参考。
有关标签的详细介绍，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。
 - 建议操作：包括以下操作。
 - 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。您可以单击右上角的白名单/关注名单，并在目的IP记录中取消加白。
- 
- 关注：单击某个目的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。
 - 取消关注：如果您想要取消某个目的IP的关注，您可以单击该目的IP记录下的更多 > 取消关注。或者您也可以单击右上角的白名单/关注名单，并在目的IP记录中取消关注。
- 
- 日志：跳转到流量日志审计页面，查看当前目的IP的流量日志记录。
 - 访问详情：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。
- 支持的操作包括：
 - 关注：将当前资产IP添加到白名单/关注名单的资产IP记录中。您可以单击右上角的白名单/关注名单，并在资产IP记录中取消关注。
 - 日志：跳转到流量日志审计页面，查看当前资产IP（即发起外联的源IP）的流量日志记录。

展开一条资产记录，展示当前资产的外联记录。资产外联记录包括以下信息：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：云防火墙根据外联域名或公网IP的公网信息添加的属性，供您参考。
有关标签的详细介绍，请参见[网络流量分析相关问题](#)。
- 建议操作：包括以下操作。
 - 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。您可以单击右上角的白名单/关注名单，并在目的域名或目的IP记录中取消加白。
 - 关注：单击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。
 - 取消关注：如果您想要取消某个外联域名或公网IP的关注，您可以单击该域名或公网IP记录下的更多 > 取消关注。或者您也可以单击右上角的白名单/关注名单，并在目的域名或目的IP记录中取消关注。
 - 日志：跳转到流量日志审计页面，查看相关的流量日志记录。

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

云防火墙互联网访问活动页面展示您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

您需要先开启云防火墙开关，互联网访问活动页面才会展示相应的流量分析数据。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. 在左侧导航栏单击网络流量分析 > 互联网访问活动。
3. 您在互联网访问活动页面可以进行以下操作。
 - 查看互联网访问活动的概览信息，包括开放应用、开放端口、开放公网IP、入流量访问的云产品公网IP和开放端口总数量和对应的风险项数量。



- 查看IP流量排行表和全部流量趋势图。IP流量排行列表展示某时刻所有公网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。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。



在IP流量排行表，单击指定目标公网IP行更多下的查看日志可跳转到流量日志页面，您可在流量日志中查看所有互联网入方向流量的详细信息。

在IP流量排行表，单击指定目标公网IP行更多下的查看趋势可在全部流量趋势图处查看该公网IP的流量趋势图。

- 查看互联网访问活动详情，您可查看开放公网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信息。



相关文档

[云防火墙支持防护的范围](#)

4.VPC访问活动

云防火墙VPC访问活动模块展示您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。

背景信息

云防火墙提供的VPC防火墙可以有效防御异常流量，VPC防火墙捕获到的所有VPC间流量信息都会展示在VPC访问活动页面。

 **说明** 您需要先开启VPC边界防火墙开关，VPC访问活动页面才会展示相应的流量分析数据。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. 在左侧导航栏单击网络流量分析 > VPC访问活动。
3. 选择待查看的目标VPC网络区域，展示VPC网络间的流量信息。

选择VPC

在VPC访问活动页面，可以进行以下操作。

- 查看VPC专有网络入方向、出方向流量的峰值和均值数据，并查看选择时间范围内对应的入方向、出方向流量数据。
- 查看流量排名前10、20或50位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。
- 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，可展示该会话中端口占比的详细数据。
- 查看所有开放端口占比信息。
- 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。

5. 失陷感知

云防火墙失陷感知页面实时为您展示由威胁检测引擎检测到的入侵活动及其详细信息。

前提条件

您需要先开启互联网边界防火墙开关，失陷感知页面才会采集到相关入侵事件的信息。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. 在左侧导航栏单击网络流量分析 > 失陷感知。
3. 在失陷感知页面查看入侵事件详细信息。




在失陷感知页面，根据需要执行以下操作：

- 您可在入侵事件列表中查看入侵事件的详细信息，包括风险级别、受影响资产IP和处理状态等信息。
- 可通过筛选风险级别、处理状态、检测时间范围或输入实例IP搜索单个入侵事件。
- 如果您判断入侵事件为正常活动，可单击该事件操作栏的忽略。

 **说明** 标记为忽略的入侵事件将从入侵事件列表中移除，云防火墙后续不会再对该事件进行告警。

- 查看事件详情。定位到需要查看的事件，单击操作栏的详情，查看入侵事件的详细信息和对应的安全建议。

 **说明** 一键防御开关不对单个事件进行控制。开启或关闭一键防御将会开启或关闭整个云防火墙的入侵防御功能。

6. IPS拦截记录

云防火墙IPS拦截记录页面为您实时展示云防火墙拦截流量的源区域、目的IP、阻断应用、阻断来源和阻断事件详情等信息。本文介绍了IPS拦截页面展示的信息和相关操作。

前提条件

您需要先在入侵防御开关页面开启基础规则开关，云防火墙才能拦截这些流量并展示在IPS拦截记录中。



概述

云防火墙网络流量分析 > IPS拦截记录页面为您展示了互联网拦截和VPC拦截的流量数据的详细信息，您可切换到互联网拦截或VPC拦截页签查看对应事件详情。

IPS拦截页面

互联网拦截页面

在互联网拦截页面，您可查看最近1小时、1天、7天、1个月内和自定义时间范围内出方向或入方向的阻断活动情况。可设置的自定义时间范围为3个月内。

IPS拦截记录页面

互联网拦截页面具体包含以下模块：

- **被阻断的源区域TOP：**展示了被云防火墙IPS功能阻断的出方向或入方向流量的来源或目的区域。

被阻断的源区域TOP

- **阻断目的IP：**展示了被云防火墙IPS功能阻断的出方向或入方向流量的目的IP地址信息。

阻断目的IP

单击阻断目的IP地址右侧的查看日志可跳转到云防火墙日志审计页面。您可在日志列表中查看该目的IP地址的目的端口、应用类型、动作等详细信息。

- **被阻断的应用TOP：**展示了被云防火墙IPS功能阻断的出方向或入方向流量占比前5的应用类型。

被阻断的应用TOP

- **阻断来源TOP：**展示了云防火墙各个IPS功能模块阻断的流量占比。

阻断来源TOP

- **详细数据：**展示了所有阻断事件的详细信息，包括事件的风险级别、事件数量、源IP地址和目的IP地址等信息。



在详细数据模块，您可以根据需要执行以下操作：

- 在搜索栏通过筛选风险级别、判断来源、方向和时间范围等定位到具体事件。
- 单击动作栏的详情可打开阻断事件的详情页面，查看事件描述等详细信息。

事件详情

VPC拦截页面

VPC拦截页面展示了云防火墙拦截到的VPC网络之间的异常事件信息。您可以查看指定时间段内VPC拦截事件的名称、风险级别、攻击类型等详细信息。

在**VPC拦截**页签，您可根据需要执行以下操作：

- 选择风险级别、防御状态、攻击类型和时间等条件后，单击**搜索**，查看符合设定条件的事件信息。
- 定位到目标事件，单击**动作**栏下的**详情**，查看当前事件的事件描述、规则ID、防御状态等详细信息。

VPC拦截事件详情

相关文档

- [云防火墙支持防护的范围](#)
- [入侵防御开关](#)

7. 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. 在左侧导航栏单击网络流量分析 > 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。

全量搜索活动选择时间

 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。

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。

历史趋势

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。

 说明 趋势图显示15分钟、1小时、4小时、1天、7天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

[云防火墙支持防护的范围](#)

8. 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. 在左侧导航栏单击网络流量分析 > 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。

开放公网IP

4. 定位到目标公网IP，单击最右侧操作栏下智能策略。

智能策略页面为您展示了当前云防火墙针对该公网IP的防护为您推荐智能策略，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。

理由

- 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。您可在安全策略 > 访问控制 > 互联网边界防火墙 > 外对内页面，查看到您已下发的智能策略。

□

 **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。

您可对下发的策略进行编辑、删除、插入和移动。

蠕虫防御

当用户的主机遭受蠕虫攻击时，会受蠕虫恶意代码的控制，对恶意网站的域名发出请求。若云防火墙检测到您的主机发起了外联请求，会为您推荐配置策略，禁止主机对恶意域名的外联访问，防止主机下载恶意程序，遭受被控制或恶意挖矿的风险。

1. 登录[云防火墙控制台](#)。
2. 在左侧导航栏单击网络流量分析 > 主动外联活动。
3. 在主动外联活动页面，单击外联域名模块。跳转到外联域名列表。

4. 定位到目标外联域名，单击建议操作栏下智能策略。



智能策略页面为您展示了当前云防火墙针对该IP外联情况为您推荐智能策略，即对于主机外联的拒绝策略。



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。

您可查看到用户主机曾对恶意源发起过很多次的恶意请求。



- 单击下发策略 > 提交后，云防火墙推荐的该智能防护策略将会即时生效。您可在安全策略 > 访问控制 > 互联网边界防火墙 > 内对外页面，查看到您已下发的智能策略。



 **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。

您可对下发的策略进行编辑、删除、插入和移动。