ALIBABA CLOUD

Alibaba Cloud

云防火墙
快速入门

文档版本：20200925

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}`

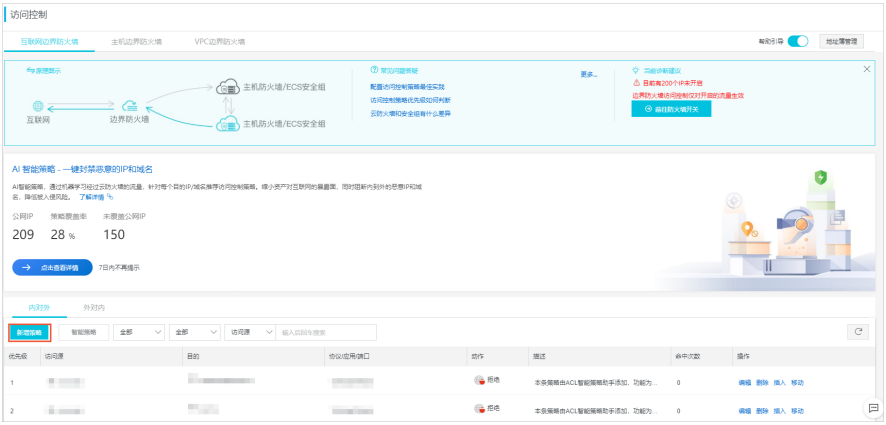
目录

1.教程概览

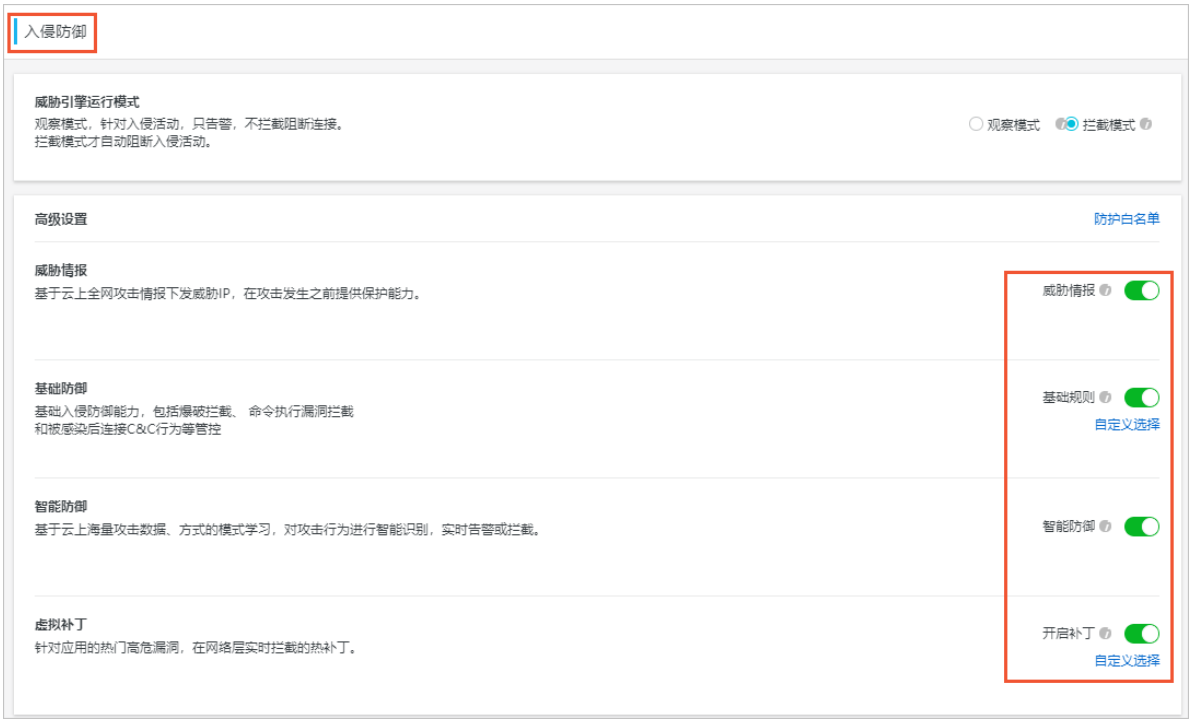
本文档介绍了如何使用阿里云云防火墙控制台来快速完成基本的操作。

您可以通过云防火墙控制台进行以下操作：

- 在云防火墙控制台**防火墙开关**页面开启防火墙。更多信息请参见开启防火墙。
- 在**安全策略 > 访问控制**页面，单击**新增策略**配置访问控制策略。更多信息请参见配置访问控制策略。



- 在**安全策略 > 入侵防御**页面配置入侵防御策略。更多信息请参见配置入侵防御策略。



- 在**网络流量分析**模块查看网络流量。可查看主动外联活动、失陷感知、IPS拦截记录和全量活动搜索等信息。更多信息请参见查看网络流量。


云防火墙
主动外联活动
外联域名
0 风险 236 全部
外联目的IP
1 风险 606 全部
外联资产
1 风险 24 全部
外联协议分析
8 .59 % 未识别 6 全部
IP流量
私网IP
公网IP
全部流量趋势
390.63 Kbps
341.80 Kbps
292.97 Kbps
244.14 Kbps
195.31 Kbps
146.48 Kbps
97.66 Kbps
48.83 Kbps
138.42 Kbps
364.64 Kbps
04/16 10:06
04/16 10:16
04/16 10:26
04/16 10:36
04/16 10:46

2.开启防火墙

云防火墙服务开通后，防火墙开关默认关闭。您可以在**防火墙开关**页面开启或关闭防火墙开关。开启云防火墙无需进行复杂的网络配置，开启后即可使用。

限制说明

云防火墙企业版、旗舰版支持VPC边界防火墙，基础版（即免费版本）和高级版不支持VPC边界防火墙。具体请参见产品版本与使用限制。

开启VPC边界防火墙时，需要您关注的注意事项请参见VPC边界防火墙限制说明。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**防火墙开关**。
3. 在**防火墙开关**页面开启防火墙开关。

> **说明** 由于仅云防火墙企业版和旗舰版支持VPC边界防火墙，如果您开通的是云防火墙基础版（即免费版本）或高级版，您在**防火墙开关**页面将无法看到**VPC边界防火墙**页签。

您可以开启**互联网边界防火墙**或**VPC边界防火墙**。

- **互联网边界防火墙**
  a. 在**防火墙开关**页面，单击**互联网边界防火墙**。
  b. 在**互联网边界防火墙**页面，执行以下操作。
     - 单击**批量操作**，在提示页面单击**全部开启**，开启所有的**互联网边界防火墙**。
     - 在防火墙列表中选择需要开启的**互联网边界防火墙**，单击左下角的**开启保护**。
- **VPC边界防火墙**
  a. 在**防火墙开关**页面，单击**VPC边界防火墙**。
  b. 在**VPC边界防火墙**页面，定位到需要开启保护的防火墙，在**防火墙开关**列表下开启防火墙开关。

您可通过筛选**资产类型**、**地域**以及**防火墙状态**来搜索并查看指定资产的防火墙开启状态。

3.开启云防火墙入侵防御拦截模式

云防火墙内置了威胁检测引擎（IPS）实现入侵防御的功能，可实时拦截入侵行为。

云防火墙 安全策略 入侵防御 威胁检测引擎 实时拦截入侵

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**安全策略 > 入侵防御**。
3. 对**威胁引擎运行模式**进行以下配置。
   - 选择**拦截模式**对恶意流量进行拦截。

     > **说明** 云防火墙服务开通后，威胁检测引擎默认开启**观察模式**。开启**观察模式**只会对恶意流量进行监控和告警，不会对恶意流量进行拦截。

   - 开启**威胁情报**，实时接收全网威胁情报。
   - 在**基础防御模块**单击**自定义选择**打开内置的基础入侵防御规则，包括爆破拦截、命令执行漏洞拦截等。
   - 在**虚拟补丁模块**选择**开启补丁**，免安装更新热门高危漏洞补丁。

     > **说明** 入侵防御设置完成后，您可在**网络流量分析 > IPS拦截记录**页面中查看不同入侵防御动作的详情。

4.查看网络流量分析

通过网络流量分析，您可以实时查看主机上发生的威胁事件、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。

云防火墙 网络流量分析

背景信息

网络流量分析是配置访问控制策略的基础。建议您在配置访问控制策略前全面了解您资产的网络流量情况。

主动外联活动

主动外联活动页面主要展示ECS（包括SNAT IP）主动对外请求流量大小、IP地址、端口、域名等信息，帮助您及时发现可疑主机。

您可根据**主动外联活动**的数据配置访问控制策略。

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，查看您资产最近1小时、最近24小时、最近7日内或自定义时间范围内的主动外联活动情况。 详细操作说明参见主动外联活动。

互联网访问活动

互联网访问活动页面为您展示ECS对外提供的服务情况和来自互联网对服务访问情况的分析，包括开放的端口、应用、IP地址，帮助您区分正常访问流量和扫描。您可以根据互联网活动页面提供的数据和信息对**内对外**访问控制策略进行配置。

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，查看您资产的开放公网IP、开放端口、开放应用等详细信息。

VPC访问活动

VPC访问活动页面为您实时展示VPC专有网络之间的流量信息，帮助您及时发现和排查异常流量，从而更快地发现和检测出攻击。

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. 在**VPC访问活动**页面，查看VPC间流量访问、VPC间会话TOP排行、流量访问的开放端口和资产等信息。

失陷感知

失陷感知页面为您展示资产被扫描和入侵的情况。支持对入侵检测事件进行一键防御。

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，您可以执行忽略、查看入侵事件详情等操作。

   您可以根据需要进行以下操作：

   - 查看指定时间段内的威胁活动情况和威胁事件的详细信息。

- 可通过筛选威胁分类、处理状态和检测时间定位到相关威胁事件。
- 单击**忽略**，被忽略的IP地址将不再纳入入侵检测范围。
- 单击**详情**，查看入侵事件列表中入侵事件详情及后续建议。

IPS拦截记录

IPS拦截记录页面实时为您展示1小时、1天、7天、1个月内或自定义时间范围内入侵防御模块的拦截情况，包括入侵来源区域、入侵应用分布和详细的事件日志。

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 > IPS拦截记录**。
3. 在**IPS拦截记录**页面，您可以查看拦截数据的详细信息。

   您可以根据需要进行以下操作：

   - 在**IPS拦截记录**页面查看1小时、1天、7天、1个月内或自定义时间范围内的拦截活动情况。
   - 在**阻断数据**模块中单击**入方向**或**出方向**，显示入方向或出方向被阻断的流量分布区域及对应的百分比。
   - 在**详细数据**模块中单击**详情**查看该事件的详细信息。
   - 在阻断事件列表中可查看阻断目的IP地址、被阻断的应用以及阻断来源。
   - 在阻断事件列表中，可通过筛选判断来源类型、方向、防御状态、检测时间以及源IP搜索相关阻断事件的详细信息。

全量活动搜索

全量活动搜索为您实时展示外部请求IP或资产IP的流量情况。

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，您可以进行查看流量访问信息等操作。

   您可以根据需要进行以下操作：

   - 查看15分钟、1小时、4小时、1天、1周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**右侧图标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。
   - 在**流量访问TOP**模块，您可查看TOP 10流量访问活动的入方向来源地区及应用占比数据、出方向应用及应用占比数据、TOP 10会话地址等信息。

5.配置访问控制策略

云防火墙访问控制策略可限制主机对外开放的端口和对外部进行访问，从而降低入侵风险。云防火墙支持对内-外流量、内-内流量和外-内流量的访问进行精准控制。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，单击**安全策略 > 访问控制**。
3. 在**互联网边界防火墙**页签单击**新增策略**。

4. 在**新增内-外策略**对话框中配置策略参数。

- 源类型：可选择IP地址或者地址簿作为访问源。
- 访问源：数据发送方地址。择IP地址为源类型后，需要在**访问源**一栏输入IP/CIDR地址。
- 目的类型：数据接收方的类型。
- 目的：数据接收方地址。
- 协议类型：支持TCP、UDP、ICMP三种协议。
- 端口类型：可选择端口或地址簿。
- 端口：设置需要放开或限制的端口。
- 应用：某协议类型下，选择该访问控制策略支持的应用。
- 动作：可选**放行**、**观察**或**拒绝**。
- 描述：其他需要备注的信息。
- 优先级：选择该策略的优先级，默认为最后。

您可以将一组IP设置成一个地址簿，方便您在配置访问控制规则时简化规则配置。单击**地址簿管理**可在对应地址薄页面新增、编辑或删除策略地址信息。

您还可在访问控制列表中针对单个策略进行编辑、删除和移动排序。

> **说明** 除开放有必要的主动外联访问，建议您将其他内-外流量全部设置为**拒绝**。

5. 单击**提交**。