阿里云
云防火墙

快速入门

文档版本：20190122

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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **注意:** 您也可以通过按**Ctrl** + **A**选中全部文件。
>	多级菜单递进。	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。	单击 **确定**。
`courier 字体`	命令。	执行 `cd /d C:/windows` 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。	`swich` *`{stand | slave}`*

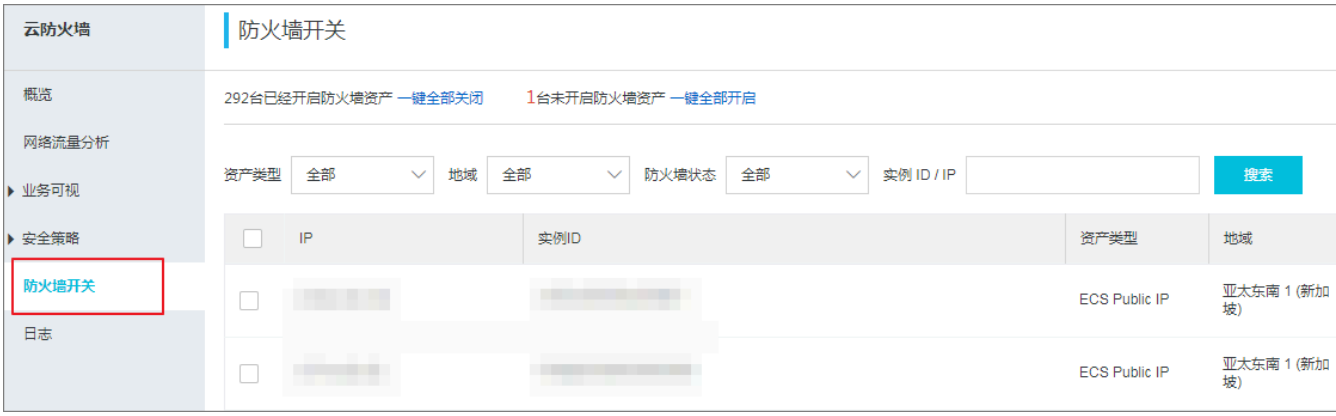
目录

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。



- 在访问控制页面单击右上角新增策略配置访问控制策略。

- 在入侵防御页面配置入侵防御策略。

- 在网络流量分析页面查看网络流量。可查看主动外联活动、入侵检测、IPS阻断分析和全量活动搜索等信息。

2 开启防火墙

云防火墙服务开通后，防火墙默认设置是**未启用**状态。您可以在**防火墙开关**页面一键开启全部防火墙或针对某些资产的防火墙单独进行开启或关闭。云防火墙开启无需进行复杂的网络配置，开启后即可使用。

操作步骤

1. 登录云防火墙控制台。
2. 在导航栏单击**防火墙开关**打开防火墙开关页面。
3. 在防火墙开关页面点击**一键全部开启**开启所有的防火墙，或在资产列表中勾选需要开启的防火墙并单击**开启保护**按钮打开对应资产的防火墙。

注意:

您也可以通过**一键全部关闭**来关闭所有的防火墙。建议全部开启防护。

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

3 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**访问控制**页面单击右上角**新增策略**打开新增策略对话框。

在新增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。
- 目的端口：数据接收方地址的端口。
- 应用：某协议类型下，该访问控制策略支持的应用。
- 动作：可选**放行**或**拒绝**。
- 描述：其他需要备注的信息。

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**可在**地址簿管理**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。

注意:

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**。

4 配置入侵防御策略

云防火墙内置了威胁检测引擎（IPS）实现入侵防御的功能，实时拦截入侵行为。

操作步骤

1. 单击**观察模式**监控恶意流量并进行告警，或单击**拦截模式**对恶意流量进行拦截。

   注意:

   云防火墙服务开通后，威胁检测引擎默认开启**观察模式**。

2. 在**基础防御**模块单击**基础规则**按钮开启/关闭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。
3. 点击**威胁情报**按钮开启/关闭全网威胁情报。
4. 在**虚拟补丁**模块单击**开启补丁**开启/关闭热门高危漏洞的免安装补丁。

注意:

入侵防御设置完成后，您可在**网络流量分析-阻断活动**页面中查看不同入侵防御动作的详情。

5 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，实现全网应用的可视化。

主动外联活动

主动外联活动页面实时为您展示主动外联TOP主机和TOP域名以及IP地址，帮助您及时发现可疑主机。

操作步骤

1. 登录云防火墙控制台。
2. 单击导航栏网络流量分析 > 主动外联活动。
   - 在网络流量展示页面单击主动外联活动，查看1小时、1天、7天、1个月内和自定义时间范围内的主动外联活动情况。
   - 在主动外联资产模块单击查看更多。
   - 您可打开主动外联资产列表，在搜索栏对资产信息进行搜索，查看资产的主动外联总次数、发送流量和接收流量。
   - 单击已关注，查看已关注的IP地址或添加/关注其他进行主动外联的资产IP。

     注意:
     被关注的IP地址将会纳入云防火墙的流量监控。被取消关注的资产IP将从主动外联资产列表中移除。
   - 单击已忽略页面，查看被设置为忽略状态的IP地址或将其他进行主动外联的资产IP设置为忽略或取消忽略。

     注意:
     被忽略的IP地址将不再纳入主动外联资产检测范围内。

入侵检测

入侵检测页面实时为您展示由威胁检测引擎检测到的威胁活动、趋势和详细信息。

操作步骤

1. 登录云防火墙控制台。

2. 单击导航栏网络流量分析 > 入侵检测打开入侵检测页面。

   - 在入侵检测页面可查看近6个月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内。
   - 单击详情查看入侵事件列表中入侵事件的详细信息及安全建议。

IPS阻断分析

IPS阻断分析页面实时为您展示1小时、1天、7天、1个月内或自定义时间范围内的IPS阻断活动情况。

操作步骤

1. 登录云防火墙控制台。
2. 单击导航栏网络流量分析网络流量分析 > IPS阻断分析。

   - 在IPS阻断分析页面单击页面查看1小时、1天、7天、1个月内或自定义时间范围内的阻断活动情况。
   - 在方向模块中单击入方向或出方向，显示入方向/出方向被阻断的流量分布区域及对应的百分比。
   - 在动作模块中单击详情查看该时间的详细信息和事件描述。
   - 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IPS阻断来源类型、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/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。

操作步骤

1. 登录云防火墙控制台。
2. 单击导航栏网络流量分析 > 全量活动搜索。

   - 在网络流量展示页面，单击全量活动搜索，查看15分钟、1小时、4小时、1天、7天或自定义时间范围内的全部威胁活动情况和趋势图。

注意:

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/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/出方向来源地区及占比数据、不同应用的占比数据、TOP 10会话地址及其占比数据等。

6 异常事件处理

云防火墙对于未处理的异常事件保留30天。您可通过云防火墙控制台网络流量分析页面查看异常活动趋势和威胁事件详情并进行处理。