阿里云
云防火墙

工具

文档版本：20200624

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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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。
	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。
	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。	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 策略回滚

互联网边界防火墙访问控制策略（内外双向）支持备份及回滚功能，以保障您的云防火墙访问控制策略能够及时恢复到正常状态。

背景信息

阿里云云防火墙企业版和旗舰版支持策略回滚，高级版不支持策略回滚。

每个阿里云账号最多只保留12次策略备份记录。当前策略备份记录超过12次后无法再新增备份，如果您需要再次新增策略备份，请先删除历史备份记录再进行新增。删除历史备份的操作请参见相关操作。您每日策略备份的次数没有限制。

策略回滚会直接替换您当前正在使用的访问控制策略，为了保证您云防火墙访问控制策略的正常使用，建议您按以下步骤进行操作：

1. 备份当前您正在使用中的访问控制策略。
2. 选择业务低谷期，关闭您所有的防火墙开关。
3. 策略回滚成功后，逐步开启您所有的防火墙开关并验证业务访问是否正常。

说明：

策略回滚仅适用于互联网边界防火墙，不适用于VPC边界防火墙和主机边界防火墙。

策略备份

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**工具箱**。

3. 在**工具箱**页面，单击**立即备份**。

4. 在**策略备份与回滚**页面，单击**新增备份**。

5. 在**备份策略**对话框中，输入备份策略的描述信息，单击**确定**新增策略备份。

策略备份的参数解释请参见下表。

参数	说明
备份时间	创建互联网边界防火墙访问控制策略（内外双向）备份的时间。
描述	创建互联网边界防火墙访问控制策略（内外双向）备份时，您输入的策略备份的描述信息。 **说明:** 备份策略描述的最大输入长度不超过256个字符。回滚策略时，需要通过此处的描述信息和备份时间来判断您需要选择哪条备份记录进行回滚，因此请认真填写备份描述，以便于后续可以区分这些备份记录。

参数	说明
策略数量	当前阿里云登录账号创建的互联网边界防火墙的访问控制策略（内外双向）数量。

您可以在**策略备份与回滚**页面，查看新增的策略备份信息。

策略回滚

互联网边界防火墙进行访问控制策略（内外双向）回滚前，请您先创建策略备份。

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**工具箱**。
3. 在**工具箱**页面，单击**立即备份**。

4. 在**策略备份与回滚**页面定位到需要回滚的备份策略，单击**使用备份**，确认后回滚策略备份。

说明：

- 策略回滚操作秒级完成。
- 如果您的策略数量太多或者多人同时在进行策略回滚操作，可能会出现超时，请避免多人同时对当前云账号的策略进行回滚。如果策略回滚超时，系统会进行提示，请您按照提示进行处理即可。
- 如果策略回滚失败，您当前账号下在使用的访问控制策略将保持不变。

相关操作

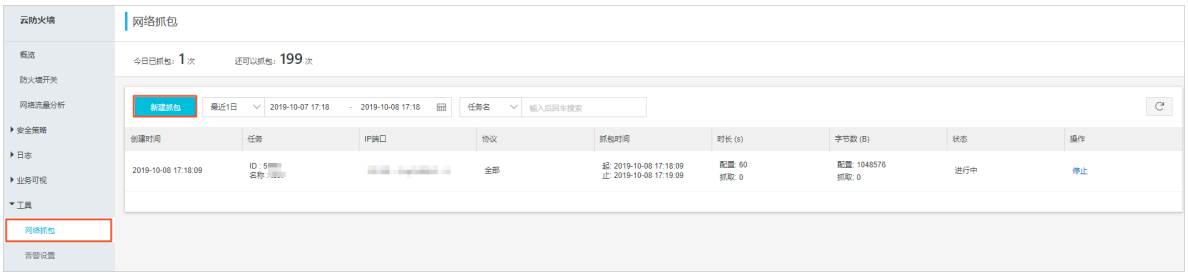
如果您需要删除历史策略备份，在**策略备份与回滚**页面，定位到需要删除的策略备份，单击**删除备份**即可。

2 网络抓包

本文主要介绍如何创建网络抓包任务。您可通过网络抓包功能分析目标发送数据包的安全性，从而识别出网络通信的安全风险。

操作步骤

1. 登录云防火墙控制台。
2. 定位到**工具** > **网络抓包**。
3. 单击**新建抓包**。



4. 在**新建抓包任务**对话框，配置任务参数。

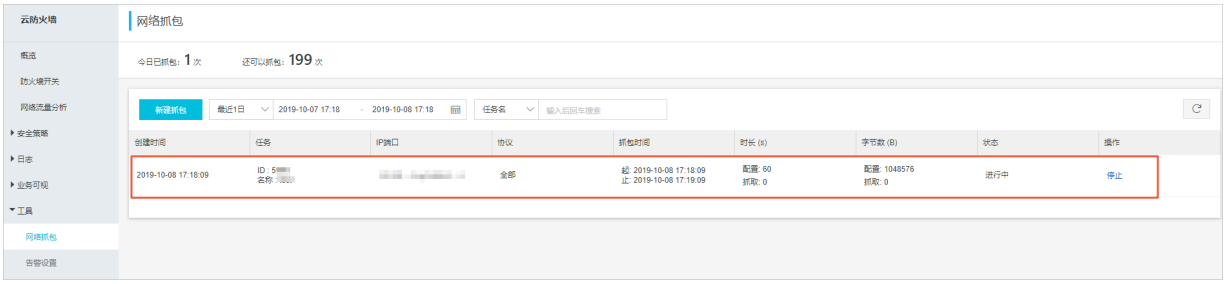
参数	说明
任务名	设置抓包任务名称，建议使用任务用途等信息，方便管理任务。
最大字节数	抓取数据包的最大字节数，如果数据包超过该字节数，则丢弃。
时间限制	抓包的最长时间。单位：秒。
协议	抓包的协议类型，可选全部、TCP、UDP和ICMP。
IP配置类型	选择IP配置类型。 • IP：配置过滤的IP地址，只抓取包含该IP的数据包。 • IP对：配置过滤的IP地址对，只抓取包含该地址对的数据包。
IP	设置过滤的IP。
端口	设置过滤的端口。
对端IP	设置对端的IP。 **说明：** 仅在**IP配置类型**设置为IP对时需要配置。

参数	说明
对端端口	设置对端的端口。 **说明:** 仅在**IP配置类型**设置为IP对时需要配置。

5. 单击**确定**。

预期结果

您可在**工具 > 网络抓包**页面，查看到创建的抓包任务、任务的状态等。


云防火墙
概览
防火墙开关
网络流量分析
安全策略
日志
业务可视
工具
网络抓包
告警设置
网络抓包
今日已抓包：1 次
还可以抓包：199 次
新建抓包
最近1日
2019-10-07 17:18
2019-10-08 17:18
任务名
输入后回车搜索
创建时间
任务
IP|端口
协议
抓包时间
时长 (s)
字节数 (B)
状态
操作
2019-10-08 17:18:09
ID：5
名称：
全部
起: 2019-10-08 17:18:09
止: 2019-10-08 17:19:09
配置: 60
抓取: 0
配置: 1048576
抓取: 0
进行中
停止

3 互联网边界防火墙-严格模式

互联网边界防火墙-严格模式针对命中了访问控制策略，但应用类型未被云防火墙识别（Unknown）的流量提供一键拦截。云防火墙根据应用报文特征识别会话流量的应用类型，在应用类型识别失败时，默认直接放行会话流量。如果您想丢弃未知应用类型的会话流量，建议您开启严格模式。

前提条件

已创建了互联网边界防火墙的访问控制策略。具体请参见#unique_6。

背景信息

互联网边界防火墙-严格模式仅对命中了已配置访问控制策略（无论访问控制策略的动作是放行、拒绝、观察）的流量生效。如果流量未命中访问控制策略，即使其应用类型未被云防火墙识别，仍然会被放行。

开启或关闭严格模式

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**工具箱**。

3. 在**工具箱**页面，开启或关闭**互联网边界防火墙-严格模式**。

   下述步骤以关闭状态下的**互联网边界防火墙-严格模式**为例进行说明：

   a. 在**严格模式**区域，单击严格模式开关。

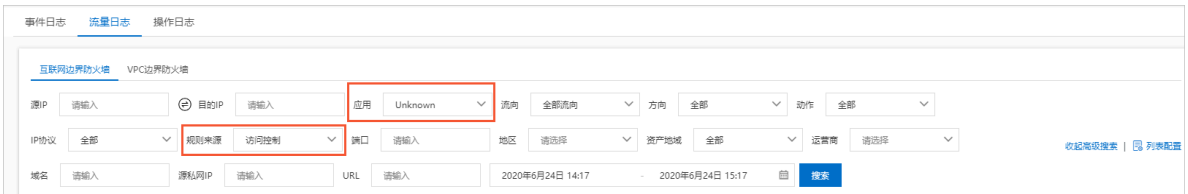
   b. 在**高级设置**对话框中，再次单击严格模式开关。

   c. 单击**提交**，确认后开启**互联网边界防火墙-严格模式**。

   开启严格模式后，命中互联网边界防火墙访问控制策略且应用类型未被识别的流量均被丢弃。您可以通过**日志审计**查看严格模式丢弃的流量记录。

查看严格模式丢弃的流量记录

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**日志** > **日志审计**。
3. 在**流量日志** > **互联网边界防火墙**页签，展开高级搜索，将**应用**设置为**Unknown**、**规则来源**设置为**访问控制**，并单击**搜索**。



4. 查看严格模式丢弃的流量记录（**规则名**为**unknown_app_deny_all**），例如时间、源IP、目的IP、目的端口等。

如果您发现严格模式误丢弃了正常的流量，建议您在请求报文中添加必要的应用协议信息，或者关闭严格模式。