ALIBABA CLOUD

Alibaba Cloud

云防火墙

工具箱

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.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。
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

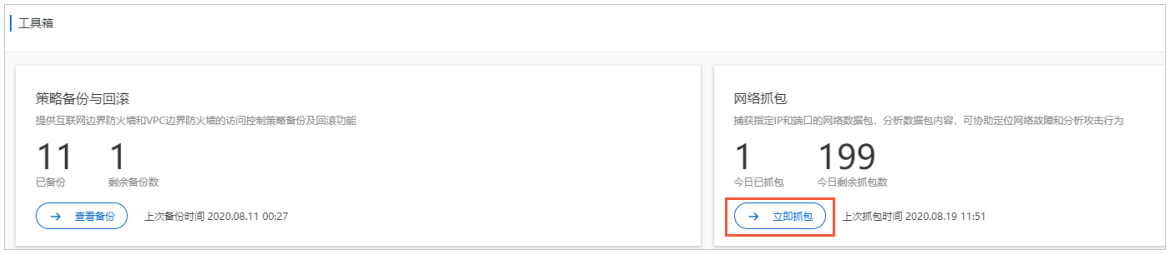
本文主要介绍如何创建网络抓包任务。通过网络抓包功能捕获指定IP和端口的网络数据包、分析数据包内容，帮助您定位网络故障和分析攻击行为，从而识别出网络通信的安全风险。

限制说明

云防火墙企业版和旗舰版支持网络抓包，基础版和高级版不支持网络抓包。每个云账号拥有200次/天的抓包次数额度。

操作步骤

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，单击立即抓包。



4. 在网络抓包页面，单击新建抓包任务。

5. 在新建抓包任务对话框，配置任务参数，单击确定。

参数	说明
任务名	设置抓包任务名称。建议您输入任务目的等信息。
最大字节数	设置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。
时长（s）	设置抓包的最长时间。单位：秒。
协议	设置抓包的协议类型。可选项： ○ *全部* ○ *TCP* ○ *UDP* ○ *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。仅支持输入1个IP地址。 ○ *IP对*：配置过滤的IP地址对（即某个IP及其对端IP），只抓取包含该地址对的数据包。仅支持输入1个IP地址对。
IP	设置过滤的IP。
端口	设置过滤的端口。

参数	说明
对端IP	设置对端的IP。 说明 仅在IP配置类型设置为IP对时，需要配置该项。
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，需要配置该项。

执行结果

您可在网络抓包页面，查看新建的抓包任务和任务状态信息。

3.安全组配置检查

安全组规则设置不当可能会引起严重的安全事故。安全组配置检查功能为您检查ECS服务器安全组中存在高危风险的规则，并提供修复建议，帮助您更安全高效地使用安全组功能。本文介绍如何在云防火墙控制台使用安全组配置检查功能。

背景信息

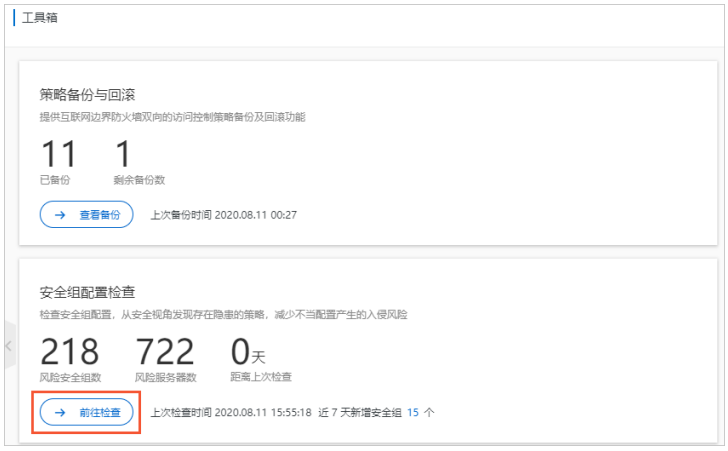
云防火墙高级版、企业版和旗舰版均支持安全组配置检查功能。

安全组是一种虚拟防火墙，仅适用于阿里云ECS服务器。安全组配置检查功能支持对普通安全组和企业级安全组进行安全检查。安全组相关信息请参见安全组概述。

安全组配置检查支持的检查项请参见安全组配置检查项列表。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏单击工具箱。
3. 在工具箱页面的安全组配置检查区域，单击前往检查。



4. （可选）在安全组配置检查页面单击获取最新检查结果。安全组检查预计需要1~5分钟，请您耐心等待。

> **说明** 此处获取的最新检查结果只是针对安全规则的静态分析得出，可能无法覆盖全部的端口风险情况。您可以在互联网访问活动页面查看端口相关的全部检查结果，了解端口的实际暴露情况。

5. 在检查结果详情区域，查看检测出的安全组风险详细信息。

您可以查看安全组**风险等级**、**检查项**、**风险安全组/服务器数**和**检查项状态**信息。

> **说明** 您可以根据需要开启或关闭检查项状态。

6. 修复高危安全组检查项。
   i. 定位到指定的检查项，单击其操作列下的**修复详情**。您也可以单击**风险安全组/服务器数**下的数字跳转至**安全组修复详情**页面。
   ii. 在**安全组修复详情**页面，定位到需要修复的安全组，单击其操作列下的**去安全组修复**。

您也可以单击**风险安全组ID/名称**下的安全组ID链接跳转至**ECS管理控制台**的**安全组列表**页面，去进行安全组修复。

> **说明** 安全组规则设置不当可能会引起严重的安全事故。**安全组修复详情**页面针对风险安全组提供了**修复建议**，建议您根据**修复建议**尽快修改存在风险的安全组规则。

相关操作

如果您使用的是免费版云防火墙，单击**去安全组修复**，您可以选择**立即升级**或**去安全组手动修复**。

- **立即升级**：购买云防火墙高级版及以上的版本，使用云防火墙提供的**安全组配置检查**功能修复安全组高危规则。云防火墙可统一管理安全组和公网IP访问控制策略，及时缩小安全风险暴露面，提高安全管理效率。推荐您使用该方式。

- **去安全组手动修复：**跳转至ECS管理控制台的**安全组列表**页面，手动修复高危安全组规则。更多信息请参见修改安全组规则。

安全组配置检查项列表

检查项名称	安全风险	修复建议
Linux远程运维端口暴露	22端口允许任意IP访问，关联的Linux服务器可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器22端口的访问。如果业务需要访问服务器22端口，建议您限制可访问该端口的公网IP，或使用堡垒机进行远程运维。更多信息请参见什么是堡垒机。
Windows远程运维端口暴露	3389端口允许任意IP访问，关联的Windows服务器可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器3389端口的访问。如果业务需要访问服务器3389端口，建议您限制可访问该端口的公网IP，或使用堡垒机进行远程运维。更多信息请参见什么是堡垒机。
DB2远程运维端口暴露	50000端口允许任意IP访问，关联的DB2数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器50000端口的访问。
ECS加入的安全组数量过多	ECS实例加入了3个及以上安全组，会增加运维难度，提高错误配置风险。	建议一台ECS实例加入的安全组数量小于等于2个。更多信息请参见安全组概述。
Elasticsearch远程运维端口暴露	9200、9300端口允许任意IP访问，关联的Elasticsearch可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器9200、9300端口的访问。
Hadoop YARN远程运维端口暴露	8088端口允许任意IP访问，关联的Hadoop YRAN可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器8088端口的访问。
Hadoop远程运维端口暴露	50070、50030端口允许任意IP访问，关联的Hadoop可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器50070、50030端口的访问。
MongoDB远程运维端口暴露	27017端口允许任意IP访问，关联的Mongo DB数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器27017端口的访问。
MySQL远程运维端口暴露	3306端口允许任意IP访问，关联的MySQL数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器3306端口的访问。
Oracle远程运维端口暴露	1521端口允许任意IP访问，关联的Oracle数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器1521端口的访问。
PostgreSQL远程运维端口暴露	5432端口允许任意IP访问，关联的PostgreSQL数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器5432端口的访问。
Redis远程运维端口暴露	6379端口允许任意IP访问，关联的Redis数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器6379端口的访问。

检查项名称	安全风险	修复建议
SQL Server远程运维端口暴露	1433端口允许任意IP访问，关联的SQL Sever数据库可能被暴力破解入侵。	建议您在ECS管理控制台的安全组列表页面配置拒绝公网IP对服务器1433端口的访问。
Spark远程运维端口暴露	6066端口允许任意IP访问，关联的Spark可能被暴力破解入侵。	建议您在ECS管理控制台的安全组列表页面配置拒绝公网IP对服务器6066端口的访问。
Splunk远程运维端口暴露	8089、8090端口允许任意IP访问，关联的Splunk可能被暴力破解入侵。	建议您在ECS管理控制台的安全组列表页面配置拒绝公网IP对服务器8089、8090端口的访问。
访问源过度开放	检查到安全组配置为入方向允许任意IP访问任意端口，关联服务器被入侵风险极大。	建议仅开放业务所需端口，并限制访问源IP范围。

4.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。具体请参见互联网边界防火墙（内外双向流量）。

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：
   i. 在**严格模式**区域，单击严格模式开关。

   ii. 在**高级设置**对话框中，再次单击严格模式开关。

   iii. 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。