阿里云
云防火墙

安全策略

文档版本：20190920

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。	 **说明:** 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。
*## *	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 访问控制策略总览

您可在云防火墙中配置访问控制策略，限制主机对内、外双向的访问控制，有效降低您资产被入侵的风险。

不同版本可配置的访问控制策略数量限制说明

云防火墙不同版本可配置不同数量的访问控制策略：

- 高级版： 内-外流量和外-内流量各可配置1000条。
- 企业版： 内-外流量和外-内流量各可配置2000条。
- 旗舰版 ： 内-外流量和外-内流量各可配置5000条。

> 说明:
> 云防火墙支持对域名进行访问控制。对域名配置访问控制策略后，访问该域名的所有流量都将受到该条策略的控制（放行、拒绝或观察）。

主机边界防火墙（ECS实例间）策略数量限制说明

默认情况下，您最多可创建100个主机边界防火墙策略组和100条策略（也就是在ECS安全组创建并同步到云防火墙的策略数量和在云防火墙主机边界防火墙侧创建的策略数加起来不超过100条）。

> 说明:
> 如果当前策略数量上限无法满足您的需求，建议您及时清理无需使用的策略或提交工单，申请阿里云技术支持。

访问控制策略相关操作参考文档

- #unique_4
- #unique_5
- #unique_6

2 互联网边界防火墙访问控制（内外双向流量）

云防火墙支持对互联网边界防火墙的访问控制。您可在云防火墙中配置访问控制策略，限制主机对内、外双向的未授权访问。

前提条件

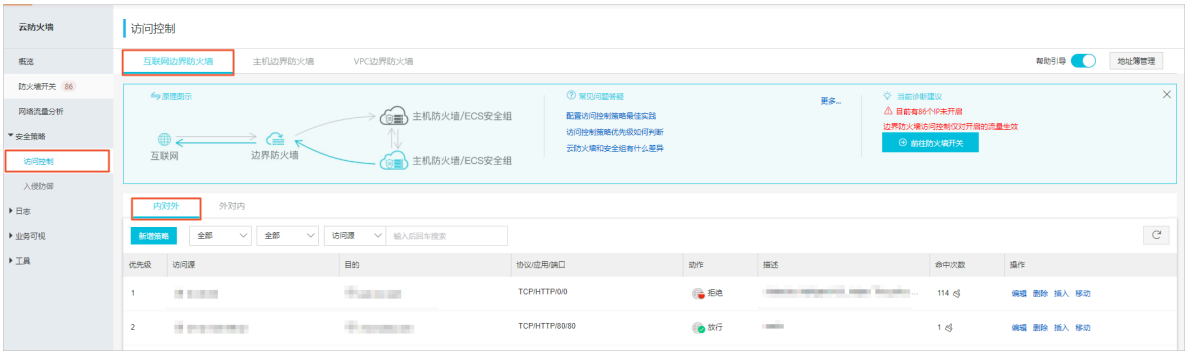
配置互联网边界防火墙策略前，请确认需要进行访问控制的实例互联网边界防火墙开关已开启，否则策略将不会生效。

背景信息

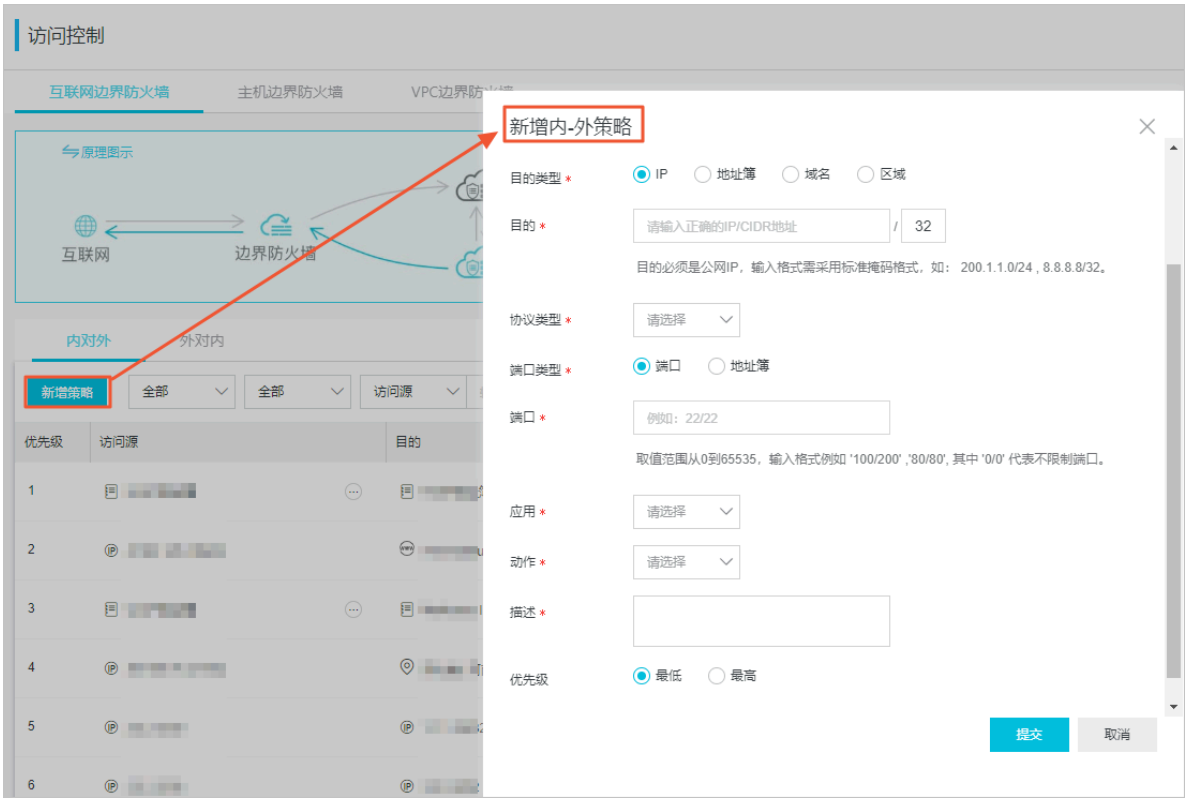
互联网边界防火墙支持内对外（用户内网访问外部互联网）和外对内（外部互联网访问用户的内部网络）流量的访问控制。

内对外流量访问控制

1. 登录云防火墙控制台。
2. 单击导航栏的安全策略 > 访问控制 > 互联网边界防火墙 > 内对外。



3. 在 内对外tab页面左上角单击新增策略按钮，打开新增内-外策略对话框。



4. 创建内对外访问控制策略。

a. 创建第一条内对外策略，先对可信的源IP进行放行。

A. 依照表格中序号配置规则参数。

序号	参数名称	参数配置
1	源类型	可选择IP或地址簿。 · IP：仅支持单个IP地址段。 · 地址簿：是您预先配置的IP地址簿，是多个IP地址段的组合，便于您在策略配置时对多个IP地址进行限制。
2	访问源	设置访问流量的来源地址。本操作步骤中访问源代表允许访问外部互联网的内网IP地址。 · 选择IP作为源类型时，该访问源一定要设置成网段，如：1.1.1.1/32。 · 选择地址簿作为源类型时，您可单击从地址簿中选择按钮，选择源IP地址簿作为访问源。

序号	参数名称	参数配置
3	目的类型	可选择IP、地址簿、域名或区域。 说明: 目的区域已支持全部国内区域（中国23个省、4个直辖市、5个自治区以及2个特别行政区），以及全部国际区域（全球7个洲）。
4	目的	设置接收流量的目的地址。本操作步骤中目的代表允许某个内网IP地址访问的外部互联网地址。
5	协议类型	设置该内到外访问流量的协议类型，可选择TCP、UDP、ICMP或ANY。不确定具体协议类型时可选择ANY。
6	端口类型	可选择端口或地址簿。 · 端口：仅支持一个端口范围。 · 地址簿：是指您预先配置的端口地址簿，是多个端口的组合，便于您在策略配置时对多个端口进行限制。
7	端口	设置需要放开或限制的端口。可根据端口类型的配置项，手动输入单个端口号，或者单击从地址簿中选择，选择预先配置的端口地址簿。
8	应用	设置该内到外访问流量的应用类型。 说明: 目的类型选择域名时，应用可选择HTTP、HTTPS、SMTP或SMTPS。
9	动作	设置允许或拒绝该流量通过互联网边界防火墙。本操作步骤中选择放行。
10	描述	输入该策略的备注内容，便于您后续查看时能快速区分每条策略的目的。
11	优先级	选择该策略的优先级，默认为最低。

B. 单击提交完成访问控制策略的创建。

说明:

最新创建的策略会展示在访问控制策略列表最后一页的最后一列中。

b. 创建第二条内对外访问控制策略，拒绝其它所有访问源去访问外部互联网。

将访问源地址设置为`0.0.0.0/0`，动作设置为拒绝，禁止所有未授权的访问。其他访问控制参数配置可参考上一步。

c. 确定第一条可信源放行策略的优先级高于第二条所有访问源拒绝策略的优先级。

说明:

默认情况下，云防火墙按照访问控制策略创建的先后顺序为策略分配优先级，新创建策略的优先级低于已有策略的优先级。有关策略优先级的详细内容，参见#unique_8。

有关策略配置参数的详细说明，参见访问控制策略参数表。

外对内流量访问控制

1. 登录云防火墙控制台。
2. 单击导航栏的安全策略 > 访问控制 > 互联网边界防火墙 > 外对内。
3. 在 外对内tab页面左上角单击新增策略按钮，打开新增外-内策略对话框。
4. 创建第一条外对内访问控制策略，先对可信的外部源IP进行放行。

   访问源设置为可信的IP地址段或选择预先配置的可信IP地址簿，动作设置为放行。其他访问控制可参考内对外流量访问控制中的配置。

   说明:

   外对内流量的访问控制策略中，如果源类型选择了地址簿，那么访问源可选择IP地址簿或云地址簿类型；目的地址簿仅可选择IP地址簿类型。
5. 创建第二条外对内访问控制策略，拒绝其它所有访问源去访问内部网络。

   将访问源地址设置为`0.0.0.0/0`，动作设置为拒绝，禁止所有未授权的访问。
6. 确定第一条可信源放行策略的优先级高于第二条所有访问源拒绝策略的优先级。

查看访问控制策略是否已生效

访问控制策略配置完成后，默认情况下策略立即生效。但如果策略参数配置不当，或者互联网边界防火墙未开，可能会导致您的策略配置不生效。

您可在访问控制策略列表中定位到该新增的策略，并单击命中次数，跳转到流量日志页面，查看策略是否生效。流量日志页面规则名一栏如果显示出该策略的名称，表示该策略已生效。

> **说明:**
> 如果删除策略，之前配置的放行/拒绝策略会失效，请谨慎删除。

访问控制策略参数表

规则参数	参数选项说明
源类型	访问源地址的类型，可选择IP或地址簿类型。 · IP地址：访问源地址类型为IP地址，需手动输入IP地址段。 · 地址簿：访问源设置需从您预先配置的址簿中选择。 您可以将多个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。
访问源	发送流量的IP/CIDR地址。 **说明:** 访问源只支持配置一个网段，例如：1.1.1.1/32。 如果源类型选择的是地址簿，需要从地址簿列表中选择一个地址簿作为访问源。 **说明:** · 内对外流量：源类型只可选择IP地址簿类型，目的地址簿可选择IP地址簿、域名地址簿或云地址簿类型。 · 外对内流量：源类型可选择IP地址簿或云地址簿类型，目的地址簿仅可选择IP地址簿类型。
目的类型	· IP地址：访问目的设置为IP地址。 · 地址簿：访问目的从地址簿中选择一组IP地址。 · 域名：策略目的设置为某一个域名。域名配置支持泛域名，如`*.aliyun.com`。 **说明:** - 只有内对外流量策略目的类型支持配置IP地址、域名或区域。 - 对于HTTP Header中没有Host字段或HTTPS请求没有SNI的流量默认放行。

规则参数	参数选项说明
目的	访问目的需要设置为网段；只可配置一个网段。 如果目的类型选择的是域名，可以配置为域名或泛域名。 说明: · 内对外流量：访问源如果选择地址簿，只可选择IP地址簿类型；目的地址簿可选择IP地址簿、域名地址簿或云地址簿类型。 · 外对内流量：源类型可选择IP地址簿或云地址簿类型，目的地址簿仅可选择IP地址簿类型。
协议类型	· ANY：任何协议。 · TCP协议。 · UDP协议。 · ICMP协议。
目的端口	支持配置端口范围；0/0代表任意端口。 说明: 协议选择为ICMP，目的端口配置不生效。协议选择为ANY，对于ICMP流量做访问控制，目的端口配置不生效。
应用	当前支持配置的应用有： ANY、HTTP、HTTPS、Mamcache、MongoDB、MQTT、MySQL、RDP、Redis、 协议选择TCP时，支持配置不同的应用类型；如选择其他类型协议，应用类型只能设置为ANY。 说明: 识别应用依赖应用报文特征（协议识别不依据端口）；应用识别失败时，该会话流量会被放行。
动作	允许或拒绝该流量通过互联网边界防火墙。 · 放行：允许访问。 · 拒绝：禁止访问，并且不会提供任何形式的通知信息。 · 观察：设置为观察模式后仍允许源到目的的访问。观察一段时间后可根据需要调整为放行或拒绝。
描述	对访问控制策略进行描述或备注。输入该策略的备注内容，便于您后续查看时能快速区分每条策略的目的。

规则参数	参数选项说明
优先级	设置访问控制策略的优先级。默认优先级为最低。 · 最低：指访问控制策略生效的顺序最低，最后生效。 · 最高：指访问控制策略生效的顺序最高，最先生效。

3 主机边界防火墙访问控制（ECS实例间）

云防火墙支持对主机边界防火墙（即ECS实例间访问流量）的访问控制。您可在云防火墙中配置访问控制策略，限制ECS实例间的未授权访问。

主机边界防火墙底层使用了安全组的能力，您在云防火墙主机边界防火墙页面配置的访问控制策略会自动同步到ECS安全组中。

> 说明:
> 在主机边界防火墙策略列表中，选择来源为自定义类型，单击搜索，您将能看到您在主机边界防火墙页面配置的所有策略组信息。

主机边界防火墙的优势

- 支持策略的批量发布。
- 支持策略组初始模板。

  模板类型可选：

  - `default-accept-login`：默认放行入方向所有流量的22和3389端口。
  - `default-drop-all`：默认拒绝该策略组中的所有流量。
  - `default-accept-all`：默认放行该策略组中的所有流量。
- 同应用组配合，自动创建安全组。

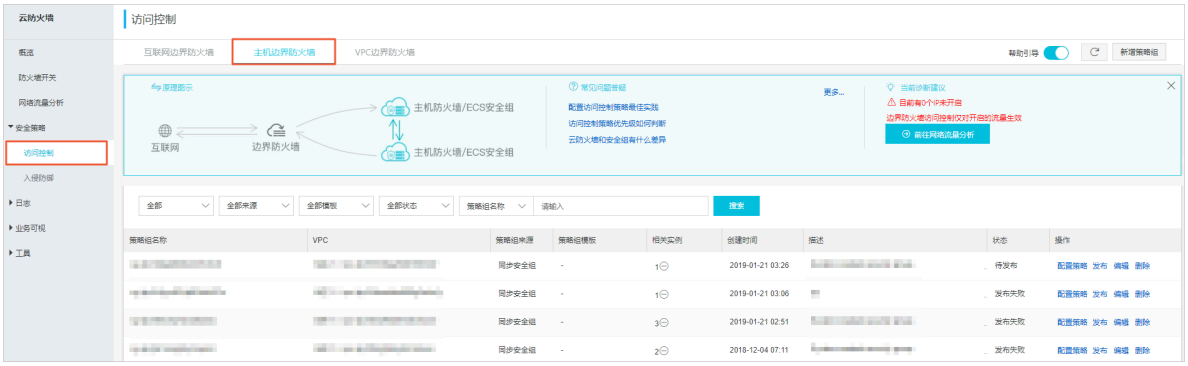
> 说明:
> 默认情况下，您最多可创建100个策略组和100条策略（也就是在ECS安全组创建并同步到云防火墙的策略数量和在云防火墙主机边界防火墙侧创建的策略数加起来不超过100条）。如果当前策略数量上限无法满足您的需求，建议您及时清理无需使用的策略或提交工单，申请阿里云技术支持。

操作步骤

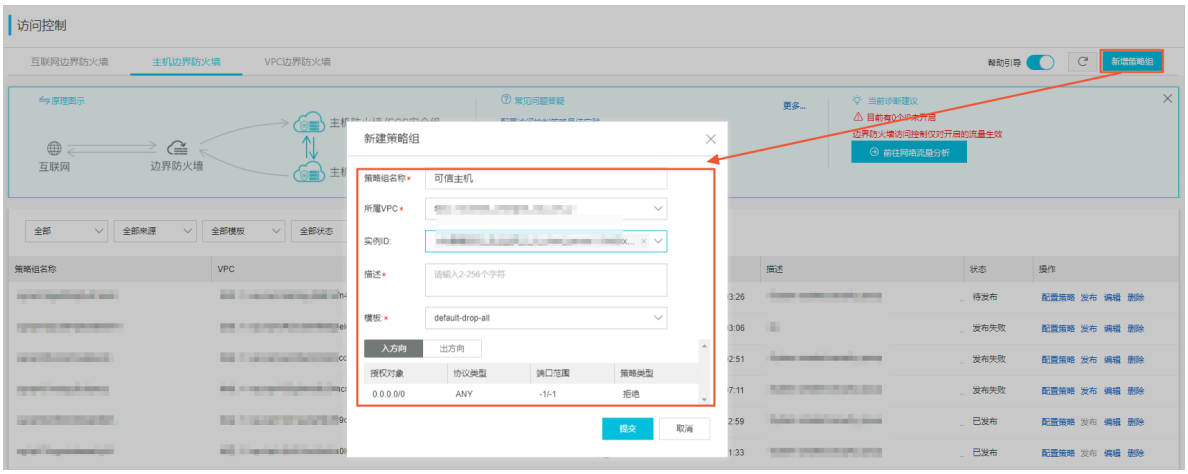
配置主机间访问控制策略时，您需先新建策略组，然后在该策略组中配置对应的入方向或出方向访问控制策略。

1. 登录云防火墙控制台。

2. 单击导航栏的安全策略 > 访问控制 > 主机边界防火墙。



3. 单击右上角新建策略组，在新建策略组对话框中配置策略组。



策略组配置项说明如下。

配置项名称	配置项描述	配置方法
策略组名称	策略组的自定义名称。字符长度限制范围为1-128。	手动输入策略组名称，便于您后续识别该策略组。
所属VPC	该策略组应用的VPC网络。	单击所属VPC下拉框并选择该策略组应用的VPC。 说明: 您只可选择一个所属VPC。
实例ID	该所属VPC网络下的实例ID。	单击实例ID下拉框并选择该VPC网络下的实例IP。 说明: 实例ID支持多选。
描述	该策略组的备注信息。字符长度限制范围为2-256。	手动输入描述内容，便于您后续识别该策略组。

配置项名称	配置项描述	配置方法
模板	该策略组允许或拒绝流量通过的模板。	单击模板下拉框并选择模板类型。模板类型可选： · default-accept-login：默认放行入方向所有流量的22和3389端口。 · default-drop-all：默认拒绝该策略组中的所有流量。 · default-accept-all：默认放行该策略组中的所有流量。

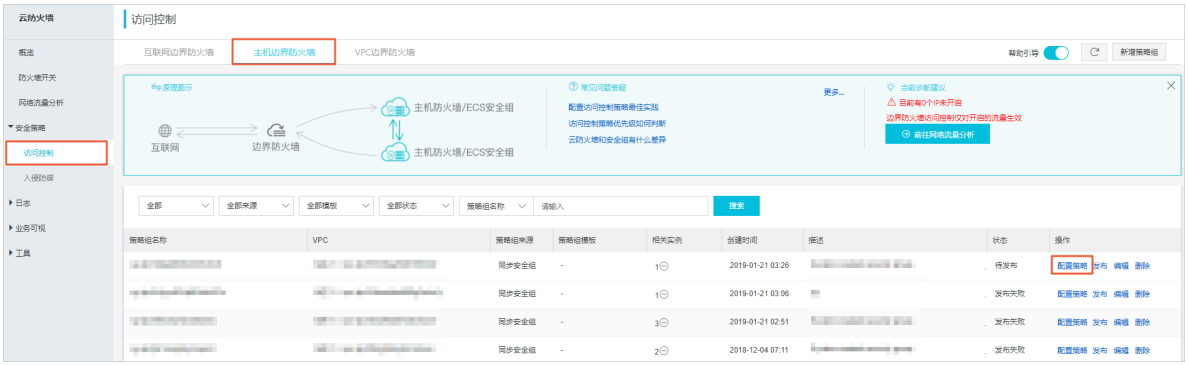
4. 单击提交，完成策略组的创建。

   策略组创建完成后，您可在主机边界防火墙页面的策略组列表中找到该策略组，可对策略组配置策略、发布策略、编辑策略组或删除策略组。

   > 说明：
   > 策略组支持修改和删除。策略组修改仅限修改实例和描述信息；策略组删除后，该策略中组的主机访问控制策略也将被自动删除并失效，请谨慎操作。

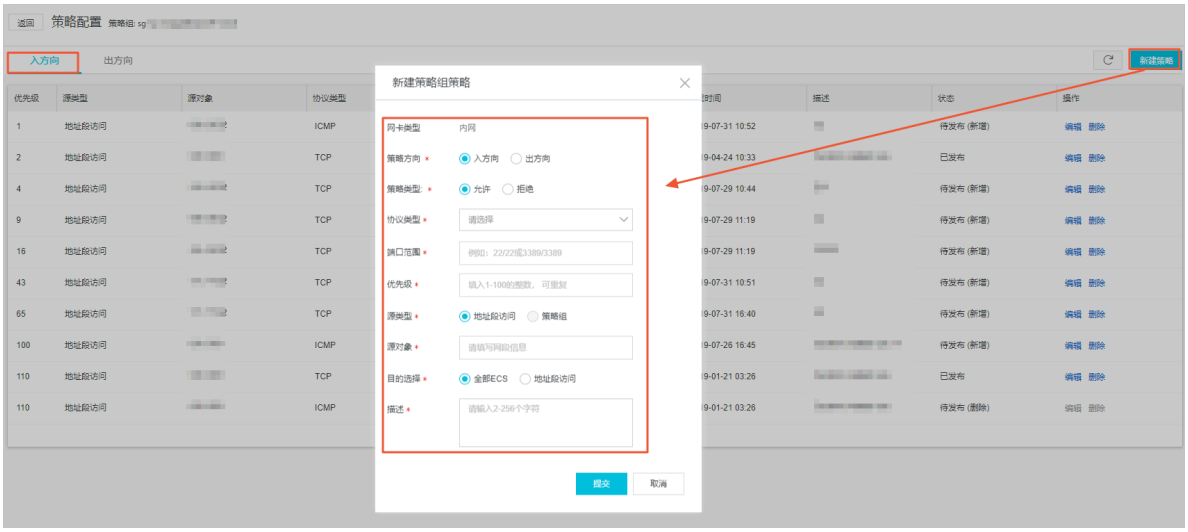
5. 单击策略组操作栏的配置策略，将主机访问控制策略添加到该策略组中。

   > 说明：
   > 策略组中支持添加多条主机访问控制策略。默认情况下，您最多可创建100个策略组和100条策略。如果当前策略数量上限无法满足您的需求，建议您及时清理无需使用的策略或提交工单，申请阿里云技术支持。



6. 在策略配置页面选择入方向或出方向，并单击右上角新建策略。

7. 在新建策略组策略对话框中完成策略项配置。



策略配置说明如下。

策略配置项名称	配置项描述	配置方法
网卡类型	该策略应用的网络类型。	系统默认配置为内网表示内网间的访问流量。
策略方向	该策略控制的流量方向。	可选项： · 入方向：从其它ECS访问本机。 · 出方向：从本机访问其它ECS。
策略类型	允许或拒绝该流量通过主机防火墙。	可选项： · 允许：允许该内网间流量通过。 · 拒绝：不允许该内网间流量通过。
协议类型	该访问流量的协议类型。	单击协议类型下拉框并选择对应的类型。可选项： · TCP · UDP · ICMP · ANY：表示任何协议类型。不确定该访问流量的类型时可选择ANY。
端口范围	该策略限制或放行某个访问流量所经过的目的端口。	手动输入端口的地址范围。例如：22/22。

策略配置项名称	配置项描述	配置方法
优先级	该策略生效的优先级。	手动输入优先级。  说明: 主机访问控制策略优先级范围为1-100，优先级可重复。策略优先级相同时，拒绝策略优先生效。优先级相同的策略，如果都是放行类型，那这两条策略将同时生效。
源类型	该策略限制的访问源的类型。	可选项: · 地址段访问：该策略的访问源为地址段。 · 策略组：该策略的访问源类型为策略组访问，表示访问源为该策略组中的多个实例地址。  说明: 在ECS安全组中创建的策略，您将无法选择策略组作为源类型，只允许选择地址段访问源类型。
源对象	该策略访问源地址，为单个地址段或者策略组中的多个实例地址。	根据选择的源类型配置源对象。 · 源类型选择地址段访问时，需手动输入访问源地址段。仅支持单个地址段。 · 源类型选择策略组时，单击源对象下拉框并选择策略组，表示访问源为策略组中的多个实例地址。  说明: 只允许选择单个策略组作为源对象。
目的选择	表示访问流量的目的地址。	可选项: · 全部ECS：该策略将应用到您的所有ECS中。 · 地址段访问：手动输入IP/ICDR地址段。策略将应用到该地址接收的流量中。
描述	该策略的备注信息，用于区分策略的目的。	需手动输入描述信息。字符范围为2-256。

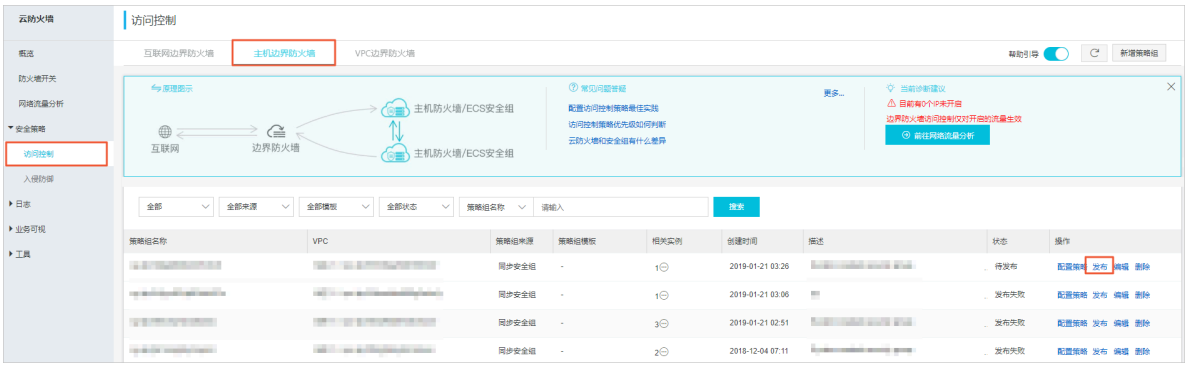
8. 单击提交，完成策略的创建。

   您可策略配置页面的入方向或出方向策略列表中，查看、编辑或删除已创建的策略。

说明：

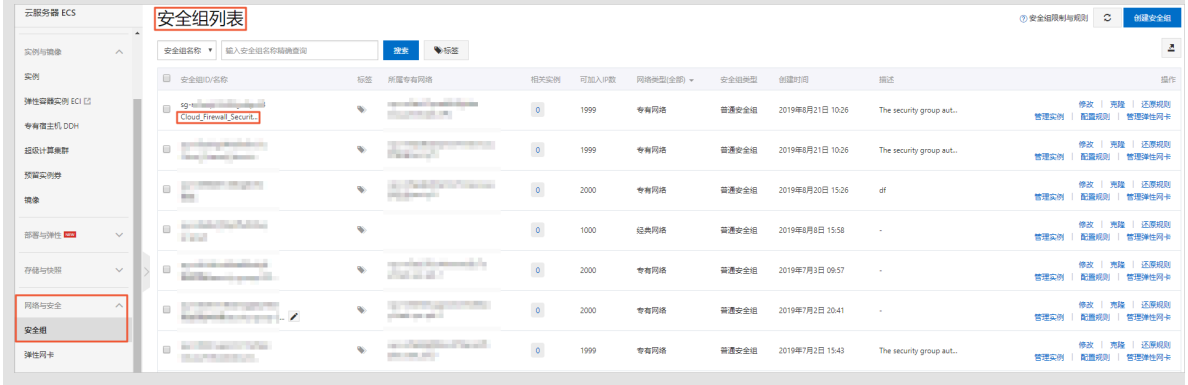
策略删除后，该策略中对应流量的访问控制将失效，请谨慎删除。策略删除后，该策略的记录仍会保留在策略列表中，但您无法再对其执行任何操作。

9. 在主机防火墙页面定位到需要生效的策略组，并单击右侧操作栏的发布，使策略生效并同步到ECS安全组。



说明：

策略发布后才会生效并同步到ECS安全组。您可在ECS控制台安全组 > 安全组列表页面，查看您在云防火墙主机边界防火墙页面创建、并同步到安全组中的访问控制策略。



主机边界防火墙配置视频教程

主机边界防火墙和ECS安全组的区别

云防火墙的主机边界防火墙可对ECS实例间的访问流量进行控制。

有关主机边界防火墙和ECS安全组的区别，参见#unique_10

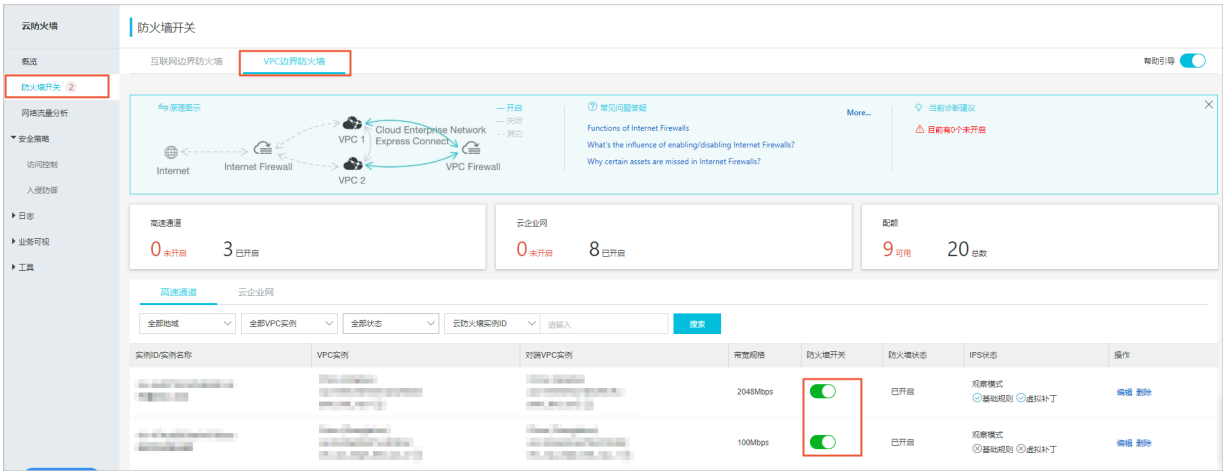
4 VPC边界防火墙访问控制

本文档介绍了VPC边界防火墙的访问控制操作。

前提条件

VPC边界防火墙默认不存在。因此在创建VPC访问控制策略前，必须需先创建并开启相应的VPC边界防火墙。

VPC边界防火墙开关开启后，访问控制策略才能生效。



背景信息

云防火墙支持对VPC边界防火墙的访问控制。VPC边界防火墙用于检测和控制两个VPC间的通信流量。

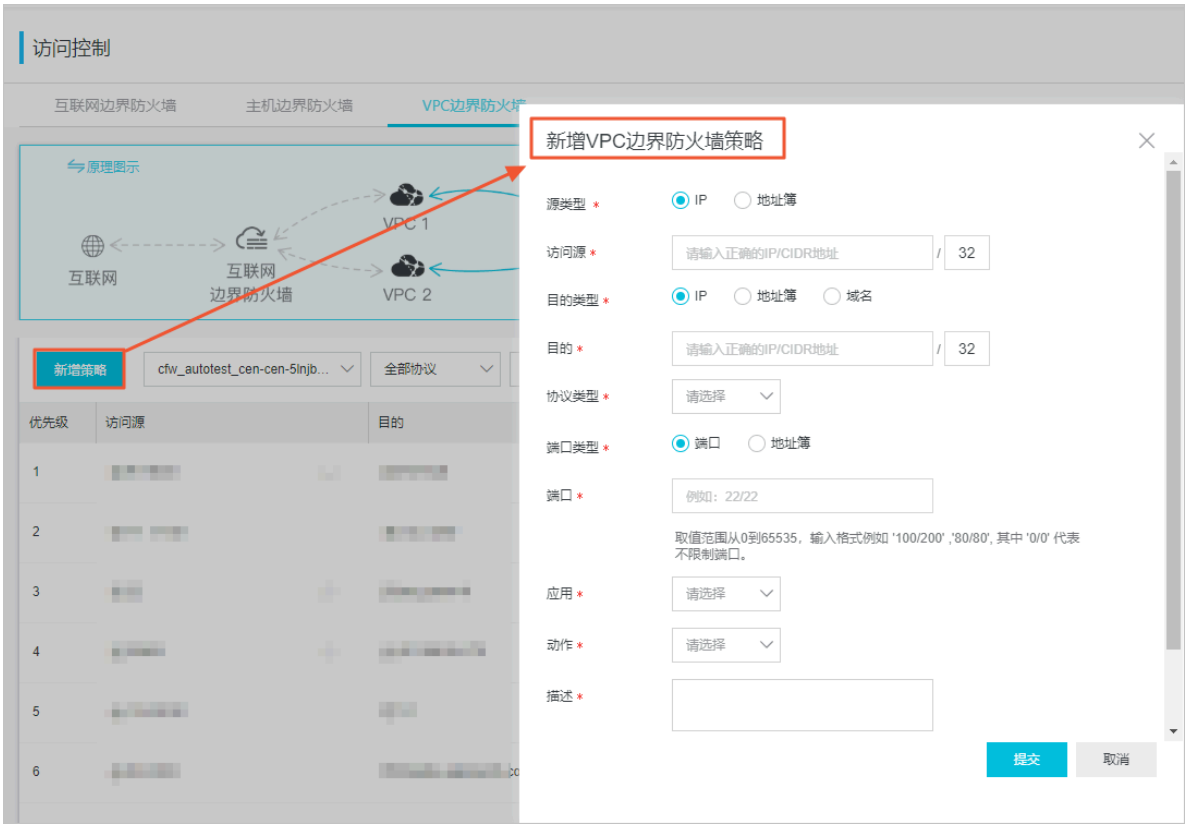
访问控制策略配置原理

VPC边界防火墙默认放行所有流量，您在对VPC间流量进行管控时，需要对不可信的流量进行拒绝；或者先对可信源进行放通，再拒绝任意地址的访问。

操作步骤

1. 登录云防火墙控制台。
2. 单击导航栏的安全策略 > 访问控制 > VPC边界防火墙。

3. 单击新增策略按钮。
4. 在新增VPC边界防火墙策略对话框中，配置访问控制策略。



您可根据您的业务需要，选择适合的VPC边界防火墙策略配置方式。

- 对非可信流量拒绝通过。
- 先创建对可信源进行放行的策略，再创建一条拒绝其他所有访问的策略。策略配置完成后，确认放行策略的优先级高于拒绝策略的优先级。有关优先级的详细内容，参见#unique_8。

关于访问控制策略配置项详细说明，参见本文配置项说明表。

> **说明:**
> VPC边界防火墙默认对所有地址放通。

配置项说明表

规则参数	参数选项说明
源类型	访问源地址的类型，可选择IP或地址簿类型。 · IP地址：访问源地址类型为IP地址，需手动输入IP地址段。 · 地址簿：访问源设置需从您预先配置的址簿中选择。 您可以将多个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。
访问源	发送流量的IP/CIDR地址。 说明: 访问源只支持配置一个网段，例如：1.1.1.1/32。 如果源类型选择的是地址簿，需要从地址簿列表中选择一个地址簿作为访问源。
目的类型	· IP地址：访问目的设置为IP地址。 · 地址簿：访问目的从地址簿中选择一组IP地址。 · 域名：策略目的设置为某一个域名。域名配置支持泛域名，例如：*.aliyun.com。 说明: 对于HTTP Header中没有Host字段或HTTPS请求没有SNI的流量默认放行。
目的	访问目的需要设置为网段；只可配置一个网段。 如果目的类型选择的是域名，可以配置为域名或泛域名，例如：*.aliyun.com。
协议类型	· ANY：任何协议。 · TCP协议。 · UDP协议。 · ICMP协议。
目的端口	支持配置端口范围；0/0代表任意端口。 说明: 协议选择为ICMP，目的端口配置不生效。协议选择为ANY，对于ICMP流量做访问控制，目的端口配置不生效。

规则参数	参数选项说明
应用	当前支持配置的应用有： ANY、HTTP、HTTPS、Mamcache、MongoDB、MQTT、MySQL、RDP、Redis、 协议选择TCP时，支持配置不同的应用类型；如选择其他类型协议，应用类型只能设置为ANY。 说明: 识别应用依赖应用报文的特征（协议识别不依据端口）；应用识别失败时，该会话流量会被放行。
动作	允许或拒绝该流量通过互联网边界防火墙。 · 放行：允许访问。 · 拒绝：禁止访问，并且不会提供任何形式的通知信息。 · 观察：设置为观察模式后仍允许源到目的的访问。观察一段时间后可根据需要调整为放行或拒绝。
描述	对访问控制策略进行描述或备注。输入该策略的备注内容，便于您后续查看时能快速区分每条策略的目的。
优先级	设置访问控制策略的优先级。默认优先级为最低。 · 最低：指访问控制策略生效的顺序最低，最后生效。 · 最高：指访问控制策略生效的顺序最高，最先生效。

5 设置/修改访问控制策略的优先级

云防火墙中配置的每条访问控制策略都会自动分配一个默认的优先级。您可通过移动功能修改访问控制策略的优先级。

背景信息

策略优先级是指访问控制策略生效的顺序。云防火墙每条访问控制策略拥有唯一优先级，1代表最高优先级。

优先级数字从1开始顺序递增，优先级数字越小，优先级越高。

云防火墙不同版本可配置不同数量的访问策略，因此不同版本的优先级范围也不同。

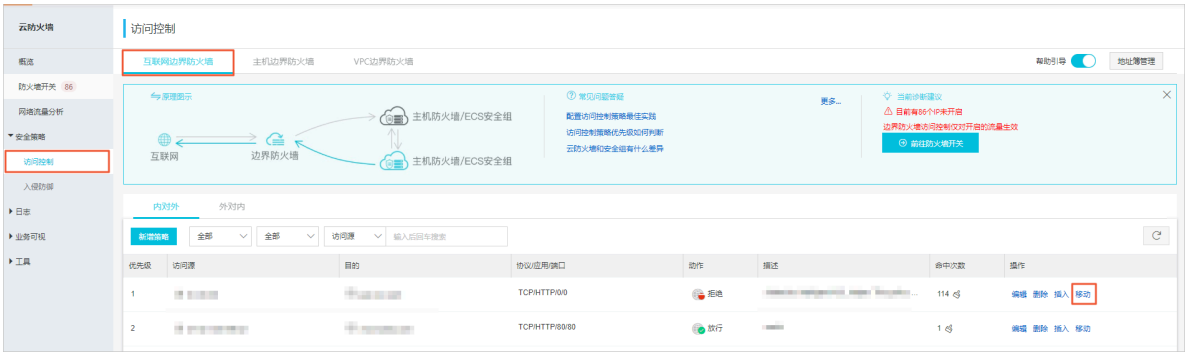
- 高级版：可配置1000条访问控制策略。策略优先级范围为1-1000。
- 企业版：可配置2000条访问控制策略。策略优先级范围为1-2000。
- 旗舰版：可配置5000条访问控制策略。策略优先级范围为1-5000。

说明:

新增的策略默认为最低优先级（优先级最大数值）。

操作步骤

1. 登录云防火墙控制台。
2. 单击导航栏的安全策略 > 访问控制，选择互联网边界防火墙页面。
3. 在互联网边界防火墙页面的内对外或外对内流量列表中，定位到需要修改优先级的访问控制策略，并单击最右侧操作栏中的移动按钮。



4. 在移动优先级对话框中修改优先级参数。

5. 单击确定完成优先级修改。

说明:

策略优先级修改后，该策略原优先级之后的策略优先级都将相应依次递减。

6 入侵防御策略

云防火墙内置了威胁检测引擎，可对互联网上的恶意流量入侵活动和常规攻击行为进行实时阻断和拦截，并提供精准的威胁检测虚拟补丁，智能阻断入侵风险。

背景信息

您可以通过云防火墙提供的入侵防御功能对威胁引擎的运行模式进行设置，并可根据业务需要对基础防御和虚拟定义进行自定义配置，更精准地识别和阻断入侵风险。

威胁引擎运行模式

威胁引擎可选择以下两种模式：

- 观察模式：开启观察模式后，可对恶意流量进行监控并告警。

  说明：

  云防火墙服务开通后，入侵防御功能默认开启为观察模式。

- 拦截模式：开启拦截模式后，可对恶意流量进行拦截，阻断入侵活动。

高级设置

云防火墙入侵防御功能提供高级设置功能，支持您对入侵防御白名单、威胁情报、基础防御和虚拟补丁进行自定义设置，为您提供更精准的入侵防御体系。

- 防护白名单：

  云防火墙入侵防御模块不会对防护白名单中的流量进行拦截，加入到防护白名单的源/目的IP会被云防火墙视为可信流量并放行。

- 虚拟情报：

  威胁情报可将阿里云全网检测到的恶意IP同步到云防火墙，如：恶意访问源、扫描源、爆破源等，并对其进行精准拦截。开启后可提前感知全网威胁源。

- 基础防御：

  基础防御可提供基础的入侵防御能力，包括爆破拦截、命令执行漏洞拦截、以及对被感染后连接C&C（命令控制）的行为进行管控。开启后可为您的资产提供基础的防护能力。

- 虚拟补丁：

  虚拟补丁无需在系统上进行安装，开启后可实时防护热门的应用高危漏洞。

操作步骤

1. 登录云防火墙控制台。
2. 单击导航栏的安全策略 > 入侵防御。
3. 在 入侵防御页面可执行以下操作，对您的网络安全提供防护。

- 在威胁引擎运行模式中选择观察模式或拦截模式。

  
  说明:
  云防火墙服务开通后，入侵防御功能默认开启为观察模式。只有开启拦截模式后，威胁情报、基础防御和虚拟补丁模块才会开启相应的威胁拦截，如未开启拦截模式，入侵防御模块将只会各类威胁和恶意流量进行监控。

- 在高级设置模块中单击防护白名单，将您确定为可信的流量添加到白名单中。设置防护白名单后，云防火墙入侵防御功能将对白名单中的流量地址放行。

  您可将内外双向流量的可信源源IP地址、目的IP地址或地址簿配置到防护白名单中。

- 设置 威胁情报开关状态。开启后，云防火墙可扫描侦查威胁情报，并提供中控情报阻断。

  
  说明:
  建议开启威胁情报。

- 设置 基础防御开关状态。开启后，云防火墙可为您的资产提供爆破拦截、命令执行漏洞拦截等基础防御能力。

  
  说明:
  建议开启基础防御规则。

  在基础防御设置中单击右侧的自定义选择，打开基础防御-自定义选择对话框，可对单个或部分基础防御规则进行自定义设置。

- 设置虚拟补丁开关状态。开启后，云防火墙可为您的资产提供实时、免安装热门漏洞防护。

  
  说明:
  虚拟补丁关闭后将无法实时自动更新。建议开启所有的虚拟补丁。

  在虚拟补丁设置中单击右侧的自定义选择，打开虚拟补丁-自定义选择对话框，可对单个或部分基础虚拟补丁规则进行自定义设置。