ALIBABA CLOUD

阿里云

云防火墙

防火墙开关

文档版本：20201207

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.开启或关闭互联网边界防火墙

互联网边界防火墙帮助您检测互联网和云上公网IP资产间的通信流量。开通云防火墙服务后，您可以为阿里云账号下的指定公网IP资产开启或关闭互联网边界防火墙。只有为资产开启互联网边界防火墙后，您才可以使用云防火墙分析和控制云上主机的互联网访问流量。

前提条件

公网IP配额未超过限制。公网IP配额指支持开启互联网边界防火墙的公网IP数量，不同云防火墙实例版本拥有不同的公网IP配额限制，具体请参见功能特性。您可以通过扩展实例的带宽规格来增加默认公网IP配额。更多信息，请参见续费与升级。

背景信息

云防火墙所有的防护能力是建立在防火墙开关开启后。开启互联网边界防火墙开关后，公网IP流量才能通过云防火墙进行检测和分析。

开启互联网边界防火墙开关之后，只是流量经过云防火墙，访问控制策略默认为**放行**，因此不会对您的业务有任何影响。如果您需要对部分流量进行精细化的访问控制，在开启互联网边界防火墙开关后，您还需配置访问控制策略，具体请参见互联网边界防火墙（内外双向流量）。

> **说明** 建议您开启阿里云账号下所有的互联网边界防火墙。

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**互联网边界防火墙**页签下，为指定的公网IP资产开启或关闭互联网边界防火墙。您可以为当前阿里云账号下的所有公网IP资产一键开启或关闭互联网边界防火墙，或者为指定的单个或多个公网IP资产开启或关闭互联网边界防火墙。

   > **说明** 云防火墙服务开通后，互联网边界防火墙开关默认全部关闭。建议您为所有资产开启互联网边界防火墙。开启后只是流量经过防火墙，策略默认为**放行**，因此对业务不会有任何影响。

   您可以在**互联网边界防火墙**页面进行以下操作：

   - 为所有资产开启或关闭互联网边界防火墙
     a. 在**公网IP**统计数据框，单击**批量操作**。

b. 在**批量操作**对话框，单击**全部开启**或者**全部关闭**，为所有资产开启或关闭互联网边界防火墙。

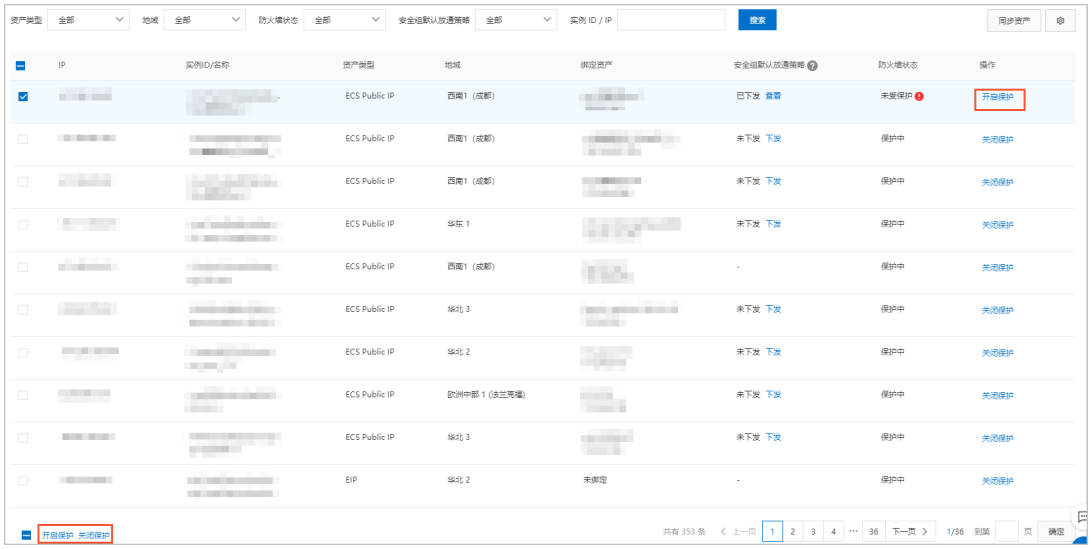
您还可以选择**新增资产**下的**自动开启保护**，则在当前阿里云账号下新增公网IP资产时，新增的公网IP资产将自动开启互联网边界防火墙。

- 为单个或多个资产开启或关闭互联网边界防火墙

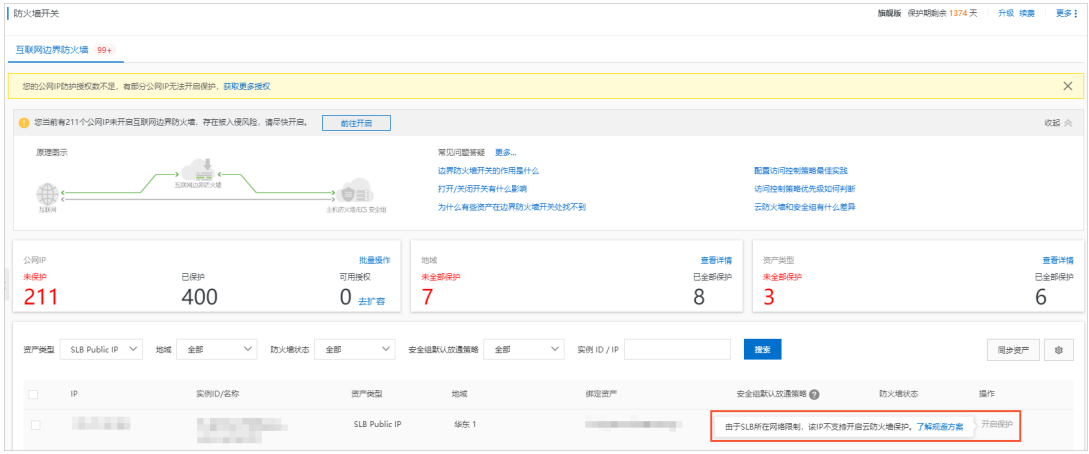
a. 在页面下方的资产列表中，定位到要操作的公网IP资产。

您可以通过**资产类型**、**地域**、**防火墙状态**过滤资产列表，或者使用**实例ID/IP**搜索目标资产。

b. 选择要操作的资产，单击资产列表下方的**开启保护**或**关闭保护**，为其开启或关闭互联网边界防火墙。您还可以直接单击某个资产操作列下的**开启保护**或**关闭保护**，单独为其开启或关闭互联网边界防火墙。



由于SLB公网的限制，部分资产IP无法开启边界防火墙开关（开启保护开关不可点击，并提示**由于SLB所在网络限制，该IP不支持开启云防火墙保护**）。这种情况下，建议您使用其他安全产品防护您的SLB公网IP，例如Web应用防火墙等。



执行结果

开启或关闭互联网边界防火墙后，**防火墙状态**更新为**保护中**（表示互联网边界防火墙的防护已生效）或**未受保护**（表示互联网边界防火墙的防护已关闭）。防火墙状态更新可能需要数秒时间，请耐心等待。

后续步骤

- 概述
- 互联网边界防火墙（内外双向流量）

相关文档

- 边界防火墙开关的作用是什么？

2.VPC边界防火墙

2.1. VPC边界防火墙限制说明

本文档主要介绍了在开启VPC边界防火墙时，需要您注意的限制条件。

限制项	描述	处理建议
VPC数量限制	在云企业网（同地域下）中开启VPC边界防火墙，默认支持6个VPC， 最多可扩展到20个VPC。 **说明** 云防火墙计划在2020年第四季度增加可支持的VPC数量。	无。
	每个地域最多支持19个VPC实例和1个云防火墙VPC边界防火墙（即VPC边界防火墙会占用1个配额）。开启VPC边界防火墙后，每个地域会自动新增一个VPC（您可以前往专有网络管理控制台**专有网络**页面查看实例名称为Cloud_Firewall_VPC的新增VPC）。VPC配额不足的情况下，您将无法开启VPC边界防火墙。	如果配额已满，您需要前往专有网络管理控制台**配额管理**页面修改VPC配额的上限。如果VPC配额上限已无法修改，请提交工单或咨询钉钉群售后人员。
	已开启VPC边界防火墙的VPC数量和地域数量的总和小于等于32个（未开启VPC边界防火墙不影响）。 **说明** 云防火墙计划在2020年第四季度增加可支持的VPC数量。	无
VPC自定义路由条目限制	开启VPC防火墙会为用户添加自定义路由，由于每个用户VPC路由表中自定义路由的数量存在限制，VPC自定义路由数量为最大值时，您无法再开启VPC边界防火墙。相关内容请参见添加自定义路由条目。	增加VPC的配额。 您可以前往专有网络管理控制台**配额管理**页面，修改当前账号下VPC路由表的自定义路由配额。 **说明** 请不要删除和修改云防火墙自动添加的自定义路由，否则会导致VPC边界防火墙到ECS的入方向流量无法受到VPC边界防火墙的防护。
云企业网（CEN）相关	云企业网下存在跨账号开通的VPC时，如果跨账号开通的VPC未获得云防火墙的授权，将无法为该云企业网创建VPC边界防火墙。	您需要用对应账号登录云防火墙完成授权后，再开启VPC边界防火墙。有关授权的详细操作请参见云企业网创建VPC边界防火墙。
	云企业网中的所有地域都需要是VPC防火墙支持的地域，否则会导致无法开启该云企业网的VPC边界防火墙。	无。

限制项	描述	处理建议
	VPC防火墙用户在云企业网中不可以发布32位网段的路由。如果有32位网段的路由，开启VPC边界防火墙后，会导致对此网段的网络访问中断。	建议您先将网段掩码长度修改为小于等于30后，再开启VPC边界防火墙。
非VPC间流量	以下非VPC间互访流量不经过云防火墙，因此无法受到云防火墙的防护： • VBR互访流量 • CCN互访流量 • VBR与CCN	如需进一步咨询请提交工单或联系产品钉钉群售后人员。
SLB和RDS相关	SLB服务和RDS等云服务在开启或关闭VPC边界防火墙过程中，会出现业务原有的长连接失效问题。如果您的SLB后端服务器存在自定义转发规则（自定义SNAT或DNAT、路由转发），SLB的健康检查报文以及流量进行跨VPC访问。 **说明** 计划于2020年第四季度针对该问题进行优化升级。	建议如下： • 在开启或关闭防火墙的过程前，暂时设置SLB的健康检查为本VPC后端，避免健康检查抖动。 • 在客户端增加连接保活以及重连机制。
	如果在您的拓扑中，存在公网私用的地址段，开启防火墙后，对SLB和RDS的访问将会中断。 **说明** 计划于2021年第一季度针对该问题进行优化升级。	建议按标准规划您的网络，避免公网私用。

2.2. 创建VPC边界防火墙

VPC边界防火墙帮助您检测和管控两个VPC间的通信流量。如果您的VPC已通过高速通道连接，或者同属于一个云企业网，则您可以在高速通道或云企业网下创建VPC边界防火墙。创建并开启VPC边界防火墙后，您才可以使用云防火墙分析和控制VPC间的访问流量。

前提条件

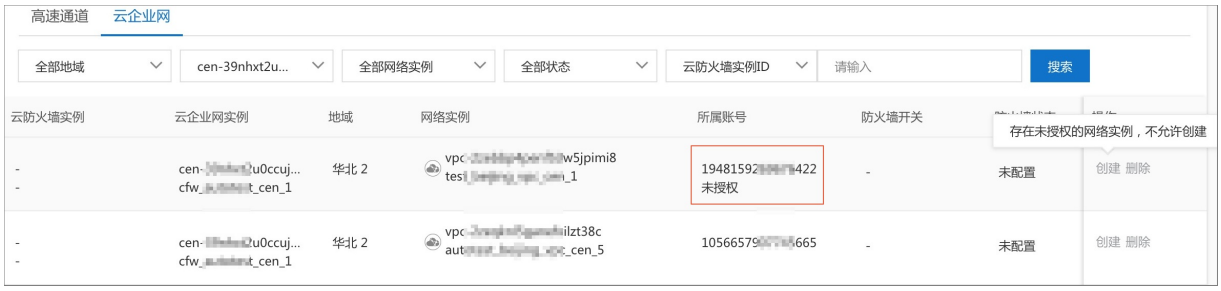
已购买了云企业网或高速通道实例，并且已使用云企业网或高速通道完成了两个VPC之间的网络互连。详细操作请参见同账号VPC互连。

背景信息

云防火墙企业版、旗舰版支持VPC边界防火墙。VPC边界防火墙只能在已相互连接的VPC之间创建。两个VPC可通过高速通道或者云企业网实现连接。

云企业网创建VPC边界防火墙

云防火墙支持云企业网连通模式下跨账号VPC防护。跨账号是指当前云账号下云企业网中存在另一个账号开通的专有网络VPC，这两个分属于不同云账号的VPC通过云企业网连通。云企业网下存在跨账号开通的VPC时，需要先授权云防火墙访问这两个账号下的云资产。未完成授权的情况下，您将无法为该云企业网创建VPC边界防火墙，云防火墙控制台的**防火墙开关 > VPC防火墙 > 云企业网**页面会提示**存在未授权的网络实例，不允许创建**。



您需要执行以下步骤完成授权操作：

1. 使用未授权的账号登录云防火墙控制台。
2. 在云防火墙欢迎页面完成新手引导。

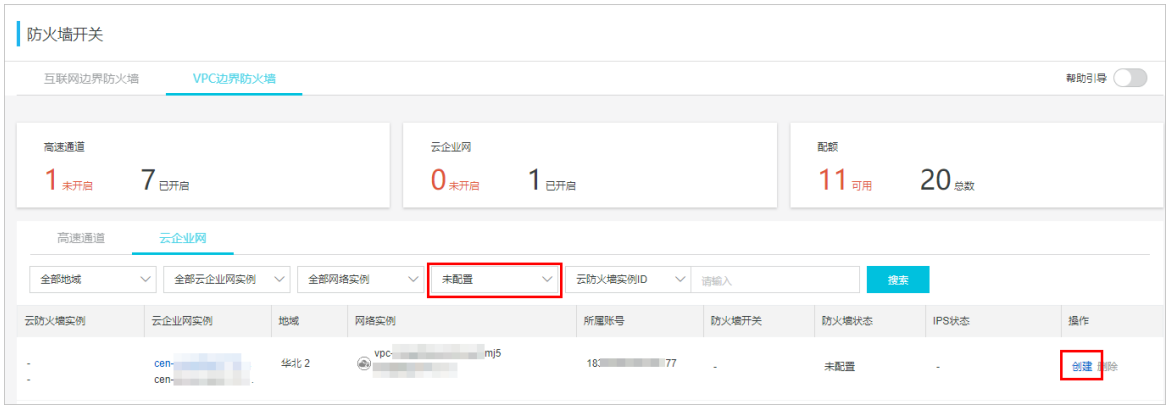
3. 在**云资产访问授权**页面单击**同意授权**。

> **说明** 云企业网连通VPC模式下，有以下注意事项：
>
> - VPC边界防火墙支持VPC跨地域、跨账号。跨账号VPC防护允许除当前操作账号外，其他的账号下VPC未开通云防火墙付费版（即高级版、企业版或旗舰版）。
> - 同一个云企业网同地域可开启VPC边界防火墙的VPC数量最大规格是10个，如需增加规格，请提交工单。
> - VPC边界防火墙支持防护VPC和VPC互访、VPC和VBR互访、VPC和CCN互访流量，不支持防护VBR和VBR互访、CCN和CCN互访、CCN和VBR互访流量。

如果您的VPC是通过云企业网连接，请参考以下步骤创建VPC边界防火墙。

> **说明** 创建、开启、关闭或删除VPC边界防火墙时，会自动修改您的VPC路由表中的自定义路由，导致在一个极短的时间内会出现网络中断。如果需要批量操作或频繁开关VPC边界防火墙，为不影响您的业务，建议在业务流量较小的低峰期进行。

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，单击**VPC边界防火墙**页签。
4. 在**VPC边界防火墙**页签，单击**云企业网**。
5. 定位到需要创建VPC防火墙的云企业网实例，单击操作列下的**创建**。如果云企业网实例过多，您可以在列表上方使用地域、云企业网实例、网络实例、云防火墙配置状态过滤列表。例如，您可以将状态设置为**未配置**并单击**搜索**，查询所有未配置云防火墙的云企业网实例。



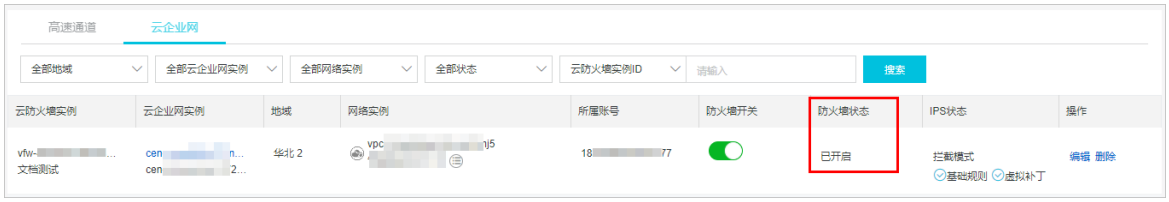
6. 在**创建VPC边界防火墙**对话框，完成VPC边界防火墙配置。

   以下表格介绍了云企业网连通模式下VPC边界防火墙的配置。

配置项	说明
实例名	定义VPC边界防火墙的名称。该名称用于识别VPC边界防火墙实例，建议您输入具有业务意义的名称，并保证名称的唯一性。
对等互通方式	确认互通方式。对等互通方式指VPC之间或VPC与本地数据中心之间的通信方式，此处固定为**云企业网**，无需您手动设置。
网络实例	确认地域和网络实例，并选择要防护的**目标网段**。 单击**目标网段**右侧的**新增目标网段**，可添加多个网段。
IPS防御模式	选择入侵防御模块（IPS）的工作模式，可选项： ○ **观察模式**：开启观察模式后，可对恶意流量进行监控并告警。 ○ **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。 **说明** 此设置将应用于同一云企业网下的所有VPC。

配置项	说明
入侵防御	选择要开启的入侵防御策略，可选项： ○ **观察模式**（对命中入侵防御规则的流量进行观察，不对流量进行拦截）或**拦截模式**（对命中入侵防御规则的流量进行拦截）。两种模式只能选择一种。 ○ **基础规则**：开启后可为您的资产提供基础的防护能力，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。 ○ **虚拟补丁**：开启后可实时防御热门的高危应用漏洞。 **说明** 此设置将应用于同一云企业网下的所有VPC。
开启VPC防火墙开关	开启开关，则云企业网到已配置的目标网段的流量会受到云防火墙的保护。如果您无需自动开启VPC防火墙开关，关闭该开关即可。

7. 单击**提交**并确认提交。VPC边界防火墙创建完成。若您在VPC边界防火墙配置中选择开启VPC边界防火墙，则VPC边界防火墙在开启中，请耐心等待。当VPC边界防火墙的**防火墙状态**变更为**已开启**，则VPC边界防火墙正式生效。



说明 开启VPC边界防火墙后会自动添加名称为Cloud_Firewall_Security_Group的安全组和放行策略，用于放行到VPC边界防火墙的流量，请不要删除和修改此安全组和策略。

高速通道创建VPC边界防火墙

高速通道连接VPC模式下，有以下注意事项：

- VPC边界防火墙支持防护同地域的VPC和VPC互访流量，不支持防护VPC跨地域、跨账号的互访流量。
- VPC边界防火墙不支持防护VPC和VBR互访流量。

如果您的VPC是通过高速通道连接，请参考以下步骤创建VPC边界防火墙。

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，单击**VPC边界防火墙**页签。
4. 在**VPC边界防火墙**页面，单击**高速通道**页签。
5. 定位到需要创建VPC防火墙的高速通道实例，单击操作列下的**创建**。如果高速通道实例过多，您可以在列表上方使用地域、VPC实例、云防火墙配置状态过滤列表。例如，您可以将状态设置为**未配置**并单击**搜索**，查询所有未配置VPC边界防火墙的高速通道实例。
6. 在**创建VPC边界防火墙**对话框，完成VPC边界防火墙配置。配置描述如下。

配置项	说明

配置项	说明
实例名	定义VPC边界防火墙的名称。该名称用于识别VPC边界防火墙实例，建议您使用具有业务意义的名称，并保证名称的唯一性。
对等互通方式	确认互通方式。对等互通方式指VPC之间或VPC与本地数据中心之间的通信方式，此处固定为**高速通道**，无需您手动设置。
VPC	确认VPC地域和VPC实例，选择要防护的**路由表**，并填写**目标网段**。 ○ 路由表 创建VPC时，系统会为您自动创建一张默认的路由表，用于为专有网络添加系统路由来管理专有网络的流量。VPC支持按需创建多个路由表。详细介绍请参见路由表概述。 在云防火墙控制台创建VPC边界防火墙时，云防火墙自动读取您的VPC路由表信息。高速通道支持多个路由表，因此您在高速通道下创建VPC边界防火墙时可看到多个路由表，并可以选择需要防护的VPC路由表。 ○ 目标网段 在路由表下拉列表中选中某个路由时，目标网段会自动展示该路由表的默认目标网段。如果您需要防护其它网段，可手动修改目标网段。支持添加多个网段，多个网段间用英文逗号隔开。
对端VPC	确认对端VPC地域和VPC实例，选择要防护的**路由表**，并填写**目标网段**。关于路由表和目标网段的描述，请参见**VPC**的配置说明。
入侵防御	选择要开启的入侵防御策略，可选项： ○ **观察模式**（对命中入侵防御规则的流量进行观察，不对流量进行拦截）或**拦截模式**（对命中入侵防御规则的流量进行拦截）。两种模式只能选择一种。 ○ **基础规则**：开启后可为您的资产提供基础的防护能力，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。 ○ **虚拟补丁**：开启后可实时防御热门的高危应用漏洞。 ○
开启VPC边界防火墙	开启开关，则在创建VPC边界防火墙后，自动开启VPC边界防火墙开关。如果您无需自动开启VPC开关，关闭该开关即可。

7. 单击**提交**并确认提交。VPC边界防火墙创建完成。若您在VPC边界防火墙配置中选择开启VPC边界防火墙，则VPC边界防火墙在开启中，请耐心等待。当VPC边界防火墙的**防火墙状态**变更为**已开启**，则VPC边界防火墙正式生效。

后续步骤

VPC边界防火墙创建成功后，您可以根据需要执行以下操作：

- 在**VPC边界防火墙**页面**编辑**或者**删除**已创建的VPC边界防护墙实例。
- 在**VPC边界防火墙**页面开启或关闭VPC边界防火墙。更多信息，请参见开启或关闭VPC边界防火墙。
- 在**安全策略 > 访问控制**页面设置VPC边界防火墙策略，控制VPC间的访问活动。更多信息，请参见VPC边界防火墙。

如果VPC边界防火墙已开启，您可以在**网络流量分析 > VPC访问活动**页面查看VPC间访问流量的数据统计和分析结果。更多信息，请参见VPC访问活动。

2.3. 开启或关闭VPC边界防火墙

VPC边界防火墙能够检测和统计已连通的VPC间的通信流量数据，帮助您发现和排查异常攻击。您可以在云防火墙控制台开启或关闭VPC边界防火墙。

前提条件

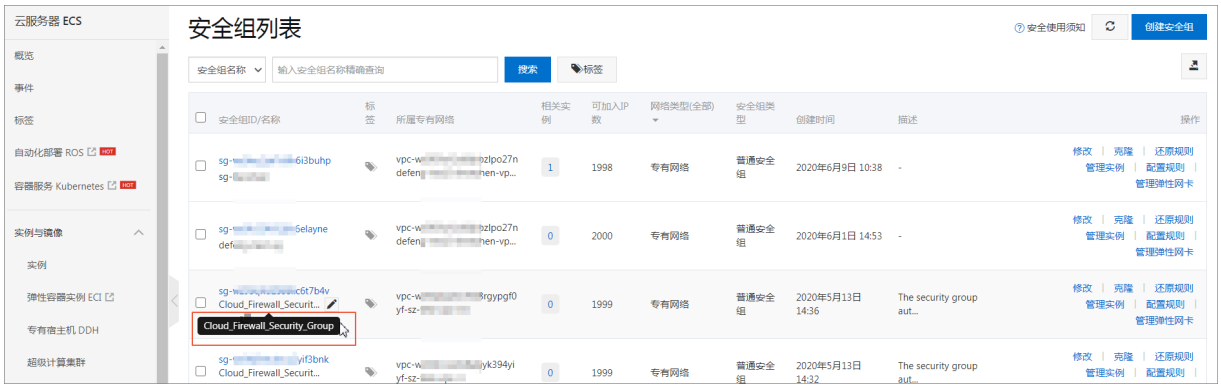
- 已购买了云企业网或高速通道实例，并且已使用云企业网或高速通道完成了两个VPC之间的网络互连。详细操作请参见同账号VPC互连。
- 已创建VPC边界防火墙。您必须先完成创建VPC边界防火墙，才能开启或关闭VPC边界防火墙开关。更多信息，请参见创建VPC边界防火墙。

背景信息

只有开启VPC边界防火墙后，您才可以在**网络流量分析 > VPC访问活动**页面查看VPC网络间的相互访问流量。

开启VPC边界防火墙后，ECS控制台**网络与安全 > 安全组**页面会自动添加名称为Cloud_Firewall_Security_Group的安全组和放行策略（即**授权策略**），用于放行VPC边界防火墙到ECS的入方向流量。

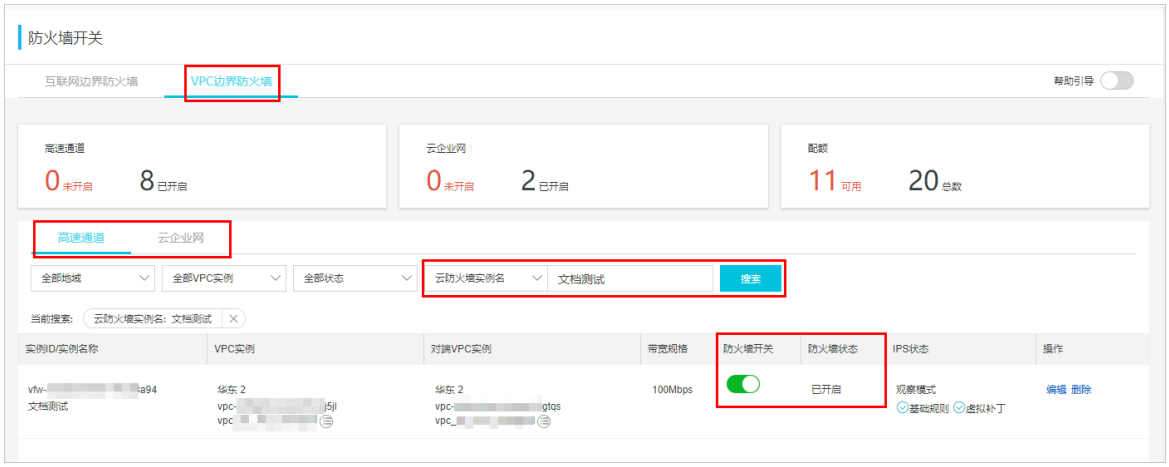
> **说明** Cloud_Firewall_Security_Group的安全组和放行策略不可以删除，否则会导致VPC边界防火墙到ECS的入方向流量无法受到VPC边界防火墙的防护。



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，单击**VPC边界防火墙**页签。
4. 在**VPC边界防火墙**页面，根据VPC的网络连通类型，单击**高速通道**或**云企业网**页签。
5. 定位到要操作的云防火墙实例，开启或关闭其**防火墙开关**。如果云防火墙实例过多，建议您使用列表上

方的筛选和搜索功能，快速定位到要操作的云防火墙或VPC实例。



6. 等待云防火墙开启或关闭完成，该过程一般需要数秒。

执行结果

- 开启防火墙开关后，**防火墙状态**变为**开启中**，等到状态更新为**已开启**，则表示成功开启VPC边界防火墙。
- 关闭防火墙开关后，**防火墙状态**变为**关闭中**，等到状态更新为**未开启**，则表示成功关闭VPC边界防火墙。

后续步骤

开启VPC边界防火墙开关后，当您的VPC网络中出现互访流量时，您可以在**网络流量分析 > VPC访问活动**页面查看VPC访问流量的数据统计和分析结果。关于VPC访问流量的更多信息，请参见VPC访问活动。

3.安全正向代理

云防火墙提供安全正向代理，对NAT网关出公网的流量进行防护。NAT网关访问互联网的流量会先经过云防火墙安全正向代理。

背景信息

安全正向代理是一种虚拟化的防火墙，创建并开启安全正向代理后，经过NAT网关的互联网流量会自动切换到云防火墙安全正向代理，实现对内网访问互联网的流量进行访问控制和防护。

版本支持说明

正向代理支持的版本为企业版、旗舰版。

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 > 安全正向代理**。
3. 在**安全正向代理**页面，单击**创建安全正向代理**。
4. 在**创建安全正向代理**对话框中，完成参数配置。

配置项	说明
名称	自定义正向代理规则的名称。可输入中文、英文、特殊字符。
Region	正向代理支持的地域。目前，支持华北2（北京）、华东1（杭州）、华东2（上海）、华南1（深圳）。
VPC	需要防护的NAT网关所在的VPC。
VPC网段	需要防护的NAT网关所在的VPC网段。
NAT网关	NAT网关访问公网的路由。选择路由后，原有的路由会被关闭，流量会经过安全正向代理转发。

创建正向代理后，安全正向代理防火墙默认开启。此时，流量会经由安全正向代理转发。

您还可以在**安全正向代理**页面，对已创建的正向代理进行修改和删除、下载已创建的正向代理数据列表。

相关操作

- 查看NAT网关公网IP访问情况

  在互联网访问活动页面的开放公网IP列表中，您可以查看到经过正向代理的NAT EIP访问情况。相关内容，请参见互联网访问活动。

- 查看哪些NAT EIP资产有主动外联的记录

  在**主动外联**页面的**外联明细 > 外联资产**列表中，您可以查看NAT EIP资产进行主动外联活动的情况。相关内容，请参见主动外联活动。

- 查看NAT EIP资产的流量日志

  在**日志审计**页面的**流量日志**列表中，您可以搜索并查看NAT EIP资产所有相关流量的日志记录。相关内容，请参见流量日志。