ALIBABA CLOUD

阿里云

云防火墙

防火墙开关

文档版本：20220706

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.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公网IP资产开启或关闭互联网边界防火墙。本文介绍了如何开启或关闭互联网边界防火墙。

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，才能通过云防火墙检测和分析公网IP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。

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，关于不同云防火墙版本拥有不同的公网IP配额限制的信息，请参见功能特性。您可以通过扩充带宽规格来增加默认公网IP配额，相关操作，请参见升级与变配。

操作步骤

1. 登录云防火墙控制台。在左侧导航栏，选择**防火墙开关 > 防火墙开关**。
2. 在**互联网边界防火墙**页签，按照如下维度开启或者关闭互联网边界防火墙。
   - 为所有公网IP资产开启或关闭互联网边界防火墙

     根据**公网IP**、**按地域分类**、**资产类型**三个维度，单击**开启保护**或**关闭保护**，一键开启或关闭有公网IP资产的互联网边界防火墙。
   - 为单个或多个公网IP资产开启或关闭互联网边界防火墙
     a. 在**IPv4**或者**IPv6**页签的公网IP列表中，定位到目标IP。

        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/UID**搜索目标资产。

     b. 单击右侧**操作**列的**开启保护**或**关闭保护**，为其开启或关闭互联网边界防火墙。
   - 为新增资产开启或关闭互联网边界防火墙

     新增资产自动保护开关默认是关闭状态。如果您开启**新增资产自动保护**开关，在当前阿里云账号下新增公网IP资产，新增的公网IP资产将自动开启互联网边界防火墙。

相关操作

您还可以根据业务需要，执行如下操作：

- 升级规格

  单击**规格升级**，升级云防火墙版本或者升级配置规格。具体信息，请参见升级与变配。
- 查看未保护、已保护的IPv6、IPv4个数

  i. 单击…，查看未保护、已保护的IPv6、IPv4个数。

  ii. 单击IPv6、IPv4的个数，页面下方的公网IP资产列表会为您展示对应的数据信息。

  例如单击未保护的IPv6个数，页面下方的公网IP资产列表为您展示未保护的IPv6的资产详细信息。
- 同步资产

  单击**同步资产**，系统为您同步资产信息，整个过程预计需要1~2分钟。

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）。

相关文档

- 互联网边界（内外双向流量）
- 互联网边界防火墙常见问题

2.VPC边界防火墙

2.1. VPC边界防火墙限制说明

本文介绍在开启VPC边界防火墙时，需要您注意的限制条件及处理建议。

通用限制

限制项	处理建议
每个地域最多支持19个VPC实例和1个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（即新增一个实例名称为Cloud_Firewall_VPC的VPC。关于如何查看该VPC的详细信息，请参见查看专有网络）。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，您需要修改VPC配额的上限，具体操作，请参见管理配额。 **注意** 如果VPC配额上限已无法修改，请咨询云防火墙钉钉群售后人员。

云企业网相关限制

限制项	处理建议
在云企业网中存在跨账号开通的VPC时，如果跨账号开通的VPC未获得云防火墙的授权或您的云防火墙版本不是旗舰版，您将无法创建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。具体操作，请参见授权云防火墙访问云资源。 • 需要升级到云防火墙旗舰版。具体操作，请参见升级。
云企业网中的VPC所在的地域都需要是VPC边界防火墙支持的地域，否则会导致无法为该云企业网开启VPC边界防火墙。	云企业网中的VPC所在的地域都是VPC边界防火墙支持的地域。相关内容，请参见VPC边界防火墙支持的地域。
如果您是在2021年05月01日之前开通了VPC边界防火墙，并且您的网络拓扑中存在公网私用的地址段，开启VPC边界防火墙后，您的服务器对SLB和RDS的访问将会中断。 **注意** 2021年05月01日及之后开通VPC边界防火墙的用户无此限制。	建议按标准规划您的网络，避免出现公网私用的情况。
云企业网中发布的路由数最大为100。	建议您减少发布的路由数，并将路由数减少到100条以内。如有需要，请联系云防火墙钉群售后人员。
开启VPC边界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，超过数量限制则无法再为您开启VPC边界防火墙。VPC实例自定义路由的最大数量为400。	增加VPC的配额。 您需要修改当前账号下VPC路由表的自定义路由配额，具体操作，请参见管理配额。

限制项	处理建议
在云企业网中开启VPC边界防火墙时，如果VPC中存在自定义路由表且绑定了vSwitch，不支持开通VPC边界防火墙。	您可以删除相关的自定义路由表或vSwitch解除绑定自定义路由表。
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间的互访流量 • CCN间的互访流量 • VBR与CCN间的互访流量	如果您需要进一步咨询，请联系云防火墙钉钉群售后人员。
SLB和RDS等云服务在开启或关闭VPC边界防火墙过程中，会出现长连接失效问题。	• 在开启或关闭VPC边界防火墙的过程前，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。
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）。	无。
在云企业网中开启VPC边界防火墙时，支持添加的网络实例数量为15个。	建议您使用云企业网转发路由器。相关信息，请咨询云防火墙钉钉群售后人员。
为云企业网创建VPC边界防火墙时，该云企业网中不能存在**策略行为**设置为**拒绝**类型的路由策略（系统默认生产的优先级为5000拒绝类型路由策略除外），否则将会导致业务中断。	建议您删除相关路由策略，或咨询云防火墙钉钉群售后人员。
开启VPC边界防火墙后，如果增加或者删除云企业网的路由策略，云防火墙需要15~30分钟的时间完成路由学习。	建议您等待云防火墙路由学习完成后观察路由策略生效情况，或通过云防火墙钉钉群咨询售后人员。
单专线云企业网用户使用防火墙时，开墙或者网络割接时可能会造成流量中断。	建议开墙或者网络割接前，先通过云防火墙钉钉群咨询售后人员。

云企业网转发路由器相关限制

限制项	处理建议
在云企业网中开启VPC边界防火墙时， 转发路由器支持添加的网络实例（包含VPC、VBR和CCN）在每个地域数量最多为100个。 **说明** 转发路由器支持添加的VPC中，包含了开启VPC边界防火墙时自动新增的VPC（即新增一个实例名称为Cloud_Firewall_VPC的VPC。关于如何查看该VPC的详细信息，请参见查看专有网络）。	无。

限制项	处理建议
转发路由器存在如下限制： • 如果已创建的VPC边界防火墙使用的是**自动模式**， 创建VPC边界防火墙后，需要联系售后服务人员将自动新增的VPC（名称是Cloud_Firewall_VPC）加入白名单之后，才能开启VPC边界防火墙。 • 如果已创建的VPC边界防火墙使用的是**手动模式**，需要联系售后服务将该VPC加入白名单之后，才能开启VPC边界防火墙。	如果您需要将VPC加入白名单，请联系钉钉群售后人员。

高速通道相关限制

限制项	处理建议
在高速通道中开启VPC边界防火墙，不支持防护VPC跨地域、跨账号及VPC与VBR间的互访流量。	如果需要防护VPC跨地域、跨账号或VPC与VBR间的互访流量，建议您改为组云企业网组网。相关信息，请咨询产品钉钉群售后人员。
开启VPC边界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，超过数量限制则无法再为您开启VPC边界防火墙。VPC实例自定义路由的最大数量为400。	增加VPC的配额。 您需要修改当前账号下VPC路由表的自定义路由配额，具体操作，请参见管理配额。
在高速通道中不支持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，或者联系产品钉钉群售后人员。
开启VPC边界防火墙后，如果增加或者删除高速通道的VPC路由表信息，云防火墙需要15~30分钟的时间完成路由学习。	建议您等待云防火墙路由学习完成后观察路由表生效情况，或通过云防火墙钉钉群咨询售后人员。

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、VPC和本地数据中心之间的流量。如果VPC已通过高速通道连接，或者同属于一个云企业网，您可以在高速通道或云企业网下创建VPC边界防火墙，实现控制VPC间的访问流量。本文介绍如何创建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之间的网络互联。详细操作，请参见高速通道同账号VPC互联、云企业网同地域VPC互联。

为云企业网创建VPC边界防火墙：已实现云企业网VPC互联。

版本支持说明

云防火墙企业版、旗舰版支持VPC边界防火墙，高级版不支持。

注意事项

您在云防火墙控制台创建VPC边界防火墙后，云防火墙会在专有网络VPC中自动为您创建以下资源：

- VPC资源：名称为 `Cloud_Firewall_VPC` 。

不要把其他业务资源加入到Cloud_Firewall_VPC中。不要手动修改和删除此VPC内的网络资源。

- 交换机资源：名称为 `Cloud_Firewall_VSWITCH` ，其网段为10.219.219.216/29。

  网络规划时请避开使用VPC边界防火墙交换机的网段10.219.219.216/29，防止因为网段冲突导致跨VPC互访流量不通。

- 自定义路由表条目：备注信息为 `Created by cloud firewall. Do not modify or delete it.` 。
- 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，导致短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。

为云企业网创建VPC边界防火墙

云防火墙支持云企业网中的跨账号VPC流量防护，即当两个不同阿里云账号下VPC通过云企业网互通时，您仍可以使用云防火去为防护连通的VPC流量。在使用云防火墙防护跨账号VPC前，您需要授权云防火墙访问云资源，具体操作，请参见授权云防火墙访问云资源。

> **注意**
>
> - 是否支持VPC边界防火墙功能取决于云企业网所属的阿里云账号是否有购买云防火墙付费版，与该云企业网下加入的VPC实例所属的阿里云账号是否有购买云防火墙无关。
>
>   例如，使用账号A创建了云企业网和VPC_1，使用账号B创建了VPC_2，VPC_1和VPC_2通过账号A的云企业网实现网络互通，此时您可以使用账号A购买云防火墙付费版，用于防护VPC_1和VPC_2的流量。
>
> - 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（即VPC-IDC）、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。

1. 登录云防火墙控制台，在左侧导航栏，选择**防火墙开关 > 防火墙开关**。
2. 在**防火墙开关**页面，单击**VPC边界防火墙**页签。
3. 在**VPC边界防火墙**页签，单击**云企业网**。
4. 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**。

   云防火墙可以对通过云企业网转发路由器TR（即VPC边界防火墙页面的企业版）连接的VPC间流量进行管控。

   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。

5. 在**创建VPC边界防火墙**对话框，完成VPC边界防火墙配置。

   当云企业网为基础版时，支持诊断是否满足一键开启VPC边界防火墙的条件。您可以在检测完成后，在**诊断记录**面板查看诊断结果。

   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
名称	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，建议您根据业务的实际情况输入具有意义的名称，并保证名称的唯一性。

配置项	说明
路由模式	经过云防火墙的流量的转发路由模式，仅云企业网TR企业版需要选择路由模式。支持以下选项： ○ 自动模式：自动路由模式，由云防火墙来自动分配VPC边界防火墙所属的VPC和Vswitch网段。 ○ 手动模式：在自定义网络规划时，可通过手动模式，自主分配VPC边界防火墙所属的VPC和Vswitch网段，不改变现有网络框架。 **注意** 手动模式下，您还需要选择该云企业网实例连接的VPC网络和使用的交换机。选择了手动模式，需要在云防火墙实例到期前及时续费，否则会导致云防火墙服务不可用时该VPC边界防火墙引流失败，从而引起对应网络中断。
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。
IPS防御能力	选择要开启的入侵防御策略，可选项： ○ **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。

6. 单击**提交**并确认提交，完成VPC边界防火墙的创建。
7. 单击防火墙开关。

   开启VPC边界防火墙开关后，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。

为高速通道创建VPC边界防火墙

说明 高速通道连接VPC模式下，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、VPC和VBR间的互访流量。

1. 登录云防火墙控制台。在左侧导航栏，选择**防火墙开关 > 防火墙开关**。
2. 在**防火墙开关**页面，单击**VPC边界防火墙**页签。

3. 在**VPC边界防火墙**页面，单击**高速通道**页签。
4. 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。
5. 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
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： ○ **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。

6. 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。

防护VPC和本地数据中心（IDC）间的流量

VPC边界防火墙支持对VPC和VBR之间的流量（即VPC到本地数据中心之间的流量）进行防护。使用云企业网连接VPC和本地数据中心的情况下，该云企业网的VPC边界防火墙开启后，会自动对该VPC和VBR之间的流量开启防护，无需为云企业网VBR单独创建和开启VPC防火墙。

登录云防火墙控制台，在**防火墙开关**页面，您可以在**VPC防火墙**页签的**云企业网**列表中，查看到云企业网VBR的防护信息。

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边界防火墙实例。
- 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**访问控制 > 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

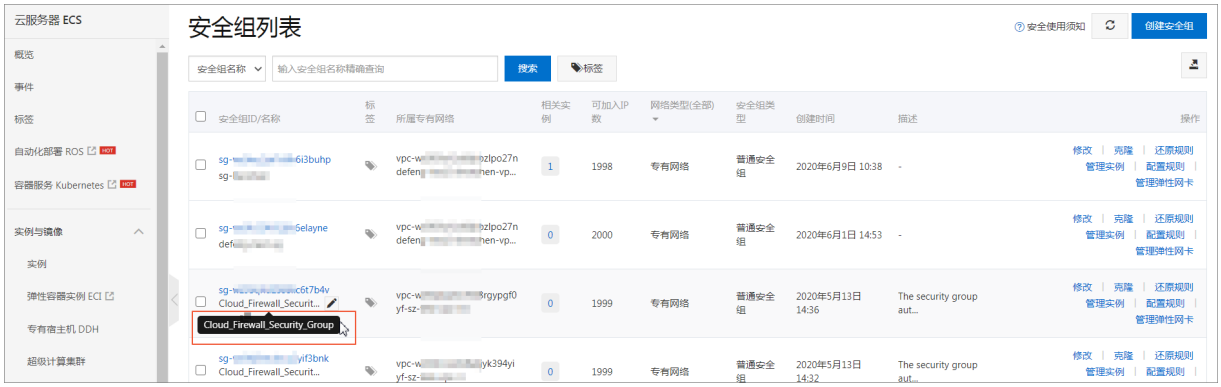
- 已购买了云企业网或高速通道实例，并且已使用云企业网或高速通道完成了两个VPC之间的网络互连。详细操作请参见同账号VPC互连。
- 已创建VPC边界防火墙。您必须先完成创建VPC边界防火墙，才能开启或关闭VPC边界防火墙开关。更多信息，请参见创建VPC边界防火墙。

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。

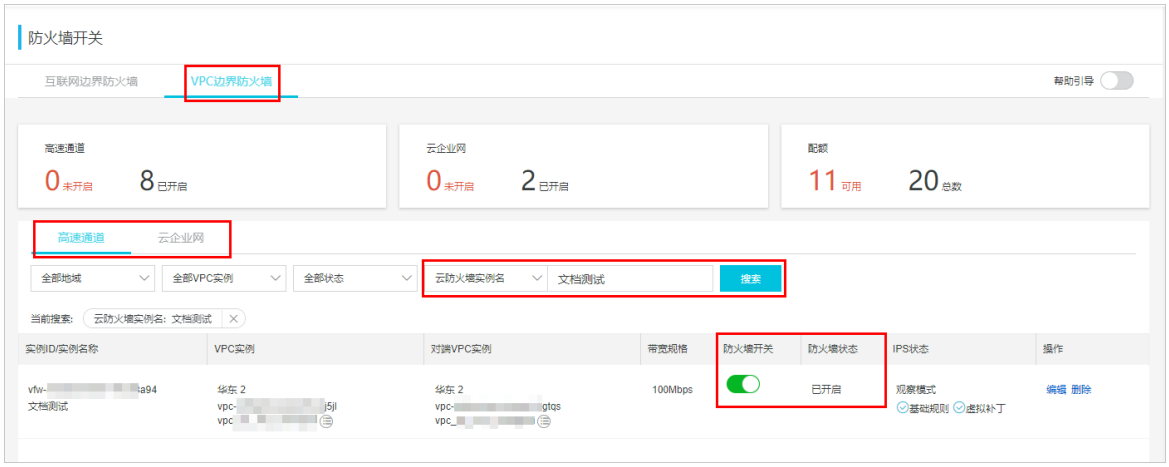


操作步骤

1. 登录云防火墙控制台。

2. 在左侧导航栏，选择**防火墙开关 > 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。

2.4. 防护云企业网TR连接的VPC之间的所有流量

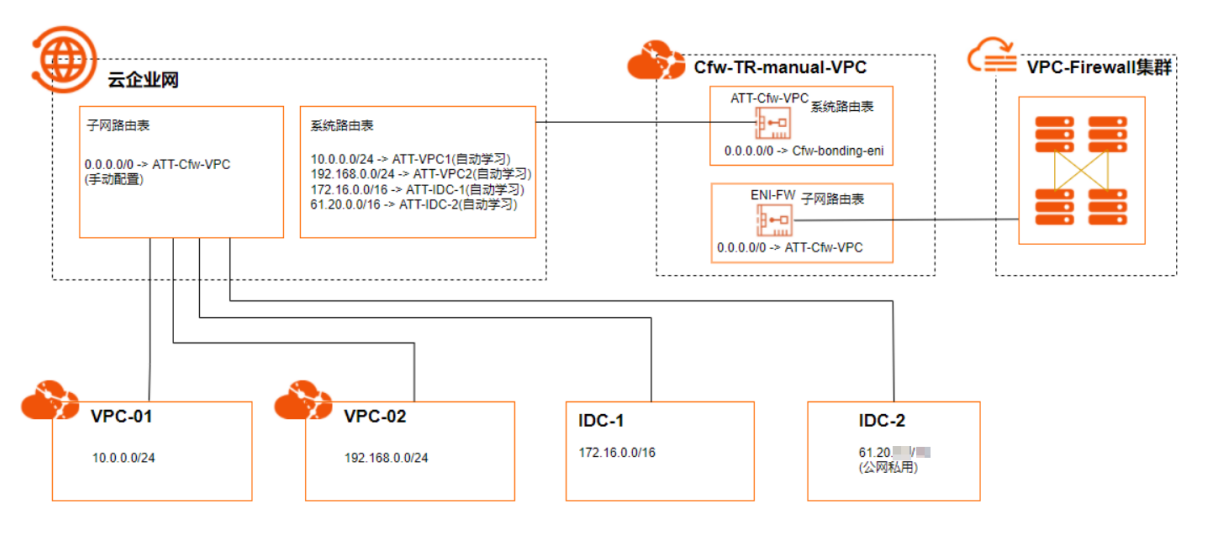
当您使用了转发路由器TR（Transit Router），可以手动配置转发路由器与VPC边界防火墙之间的互访路由，实现VPC边界防火墙对转发路由器连接的VPC之间的所有流量进行防护。本文介绍了如何连通转发路由器与VPC边界防火墙之间的网络。

前提条件

1. 已在云企业网控制台创建了云企业网实例，且创建了两个专有网络VPC（本文中分别以`VPC-01`和`VPC-02`为例）。具体操作，请参见创建云企业网实例。
2. 已在专有网络控制台手动创建了VPC边界防火墙的VPC实例（本文中以Cfw-TR-manual-VPC为例），且为该VPC实例创建了3个交换机（其中2个交换机提供给TR网络实例连接使用，可用区与TR网络实例连接的主备可用区保持一致。本文示例中命名分别为TR-Vswitch-01和TR-VSwitch-02，1个交换机提供给创建VPC边界防火墙的时候使用，本文示例中命名为Cfw-Vswitch）。

3. 已在专有网络控制台为Cfw-TR-manual-VPC创建自定义路由表（本文中以VPC-CFW-RouteTable为例）。

示意图如下：



适用对象

云防火墙可以防护通过云企业网转发路由器连接的网络实例之间的流量，网络实例包括VPC、VBR、CCN。

本文仅针对VPC边界防火墙手动引流模式的配置，适用于对多个VPC（相同地域）之间互访流量的防护。

步骤一：在转发路由器中添加防火墙VPC的网络实例连接

本步骤建立VPC实例（Cfw-TR-manual-VPC）与转发路由器企业版之间的连接。

1. 登录云企业网管理控制台。
2. 在**云企业网实例**页面，定位到需要引流到云防火墙VPC边界防火墙的云企业网实例，并单击实例ID。
3. 在该云企业网实例页面**基本信息**页签，单击**操作**列的**创建网络实例连接**或单击页面上方VPC基础信息右侧的 ⊕ 图标。
4. 在**连接网络实例**页面，设置Cfw-TR-manual-VPC和转发路由器之间的连接信息。

   以下是创建网络连接实例时，关键的配置项说明。

配置项	如何设置
实例类型	通过云企业网连接的网络实例的类型。此处选择专有网络（VPC）。
地域	通过云企业网连接的网络实例的地址。此处需要与创建Cfw-TR-manual-VPC时指定的地域保持一致。
网络实例	通过云企业网连接的网络实例。此处选择Cfw-TR-manual-VPC的实例ID。
交换机	网络连接实例可绑定的交换机。**主交换机**选择**TR-Vswitch-01**，**备交换机**为**TR-VSwitch-02**。

   其他配置项的说明，请参见使用企业版转发路由器创建VPC连接。

步骤二：为两个VPC创建云企业网网络实例连接

您需要为VPC-01和VPC-02分别创建网络实例连接，将两个VPC加载到该云企业网中。

相关内容，请参见使用企业版转发路由器创建VPC连接。

步骤三：创建VPC边界防火墙

本步骤为Cfw-TR-manual-VPC创建VPC边界防火墙。

在云防火墙控制台**防火墙开关 > 防火墙开关**页面的**VPC边界防火墙**页签，单击**云企业网**定位到网络实例Cfw-TR-manual-VPC，单击**操作**列**创建**。创建该VPC边界防火墙时，**路由模式**选择**手动**、**专有网络**选择**Cfw-TR-manual-VPC**、交换机选择**Cfw-Vswitch**。相关内容，请参见为云企业网创建VPC边界防火墙。

> **说明** 完成此步骤后，您会拥有1个弹性网卡（在ECS控制台的**网络与安全 > 弹性网卡**页面，系统默认分配名称为cfw-bonding-eni的网卡）。

步骤四：为VPC-01和VPC-02创建路由

本步骤为云企业网和VPC边界防火墙之间的流量创建路由。

1. 登录云企业网管理控制台。
2. 在**云企业网实例**页面，定位到需要引流到云防火墙VPC边界防火墙的云企业网实例，并单击实例ID。
3. 在该云企业网实例页面的转发路由器列表，单击**路由表**列下的数字，打开**转发路由器路由表**页签。
4. 单击**转发路由器路由表**页签左侧的**创建路由表**。在**创建路由表**对话框，配置路由表的信息。

   转发路由器选择默认的路由器。本文示例中路由表名称设置为Cfw-TR-RouteTable。

   新增的路由表Cfw-TR-RouteTable用于转发VPC-01和VPC-02到VPC边界防火墙Cfw-TR-manual-VPC之间的流量。
5. 定位到Cfw-TR-RouteTable路由表，单击**创建路由条目**。在**添加路由条目**对话框，配置路由条目的信息。

   配置项说明：

   - **目的地址**：选择默认地址段`0.0.0.0/0`。
   - **是否为黑洞路由**：选择默认选项`否`。
   - **下一跳连接**：选择防火墙VPC实例Cfw-TR-manual-VPC。

   本操作完成后，来自云企业网自定义路由表Cfw-TR-RouteTable的流量会默认指向VPC防火墙。
6. 在**转发路由器路由表**页签，单击左侧路由表列表中的系统路由表，然后在**路由表详情**页签，单击**关联转发**。
7. 在**关联转发**页签，删除下一跳为VPC-01和VPC-02的关联转发。然后在**转发路由器路由表**页签，单击左侧路由表列表中Cfw-TR-RouteTable路由表。
8. 在**路由表详情**页面，单击**关联转发**，然后单击**创建关联转发**。
9. 在**添加关联转发**页面，**关联转发**选择VPC-01和VPC-02，单击**确定**保存该关联转发设置。

   本操作完成后，两个VPC的流量关联转发到Cfw-TR-RouteTable。
10. 在**转发路由器**页面，单击左侧路由器列表中的系统路由表。
11. 在系统路由表的**路由表详情**页签中，单击**路由学习**页签。
12. 在**路由学习**页签，创建两条路由学习，**关联连接**分别选择VPC-01和VPC-02。

    本操作会为系统路由表创建路由学习，自动同步VPC-01和VPC-02的路由。

路由学习创建完成后，您可以在**路由条目页签**查看自动学习的路由信息。

13. 在当前的系统路由表的**路由表详情**页面，单击**关联转发**页签。
14. 在**关联转发**页签，单击**创建关联转发**。
15. 在**添加关联转发**对话框，选择**Cfw-TR-manual-VPC**。

本步骤完成后，云企业网路由配置完成，流量牵引到VPC边界防火墙的VPC实例上。

步骤五：添加VPC路由表到VPC边界防火墙

本步骤将防火墙VPC实例的路由引流到VPC边界防火墙上。

1. 登录专有网络管理控制台。
2. 在**路由表**页面，打开路由表**VPC-CFW-RouteTable**，在**已绑定交换机**页签，单击**绑定交换机**。其中**交换机**选择**Cfw-Vswitch**。然后单击**确定**。
3. 在**路由条目列表**页签，选择**自定义路由条目**页签。单击**添加路由条目**，配置路由条目信息。

   关键配置项说明：

   - **目标网段**：选择**0.0.0.0/0**。
   - **下一跳类型**：选择**转发路由器**。
   - **转发路由器**：选择默认项，即VPC防火墙的网络实例连接。

   本操作完成后，VPC边界防火墙出方向的流量会通过子网路由表转发到云企业网转发路由器TR。
4. 在路由表列表页面，选择防火墙VPC实例 的系统路由表。
5. 在**路由条目**列表，单击**自定义**页签。
6. 单击**添加自定义路由条目**，配置路由条目信息。

   关键配置项说明：

   - **目标网段**：选择**0.0.0.0/0**。
   - **下一跳类型**：选择**辅助弹性网卡**。
   - **辅助弹性网卡**：选择**Cfw-bonding-eni**。
7. 在**自定义**页签，单击其他自定义路由条目**操作**列**删除**，删除其他自定义路由条目。

   本步骤完成后，来自防火墙VPC实例的流量会牵引到云防火墙实例上。

步骤六：验证转发配置是否成功

您可以在流量日志功能查看是否有来自该云企业网的流量日志。如果有相关流量日志，代表转发配置成功。具体步骤，请参见流量日志。

2.5. 防护云企业网TR连接的VPC之间的部分流量

当您使用了转发路由器TR（Transit Router），可以手动配置转发路由器与VPC边界防火墙之间的互访路由，实现VPC边界防火墙对转发路由器连接的VPC、VBR之间的部分流量进行防护。本文介绍了如何连通转发路由器与VPC边界防火墙之间的网络。

前提条件

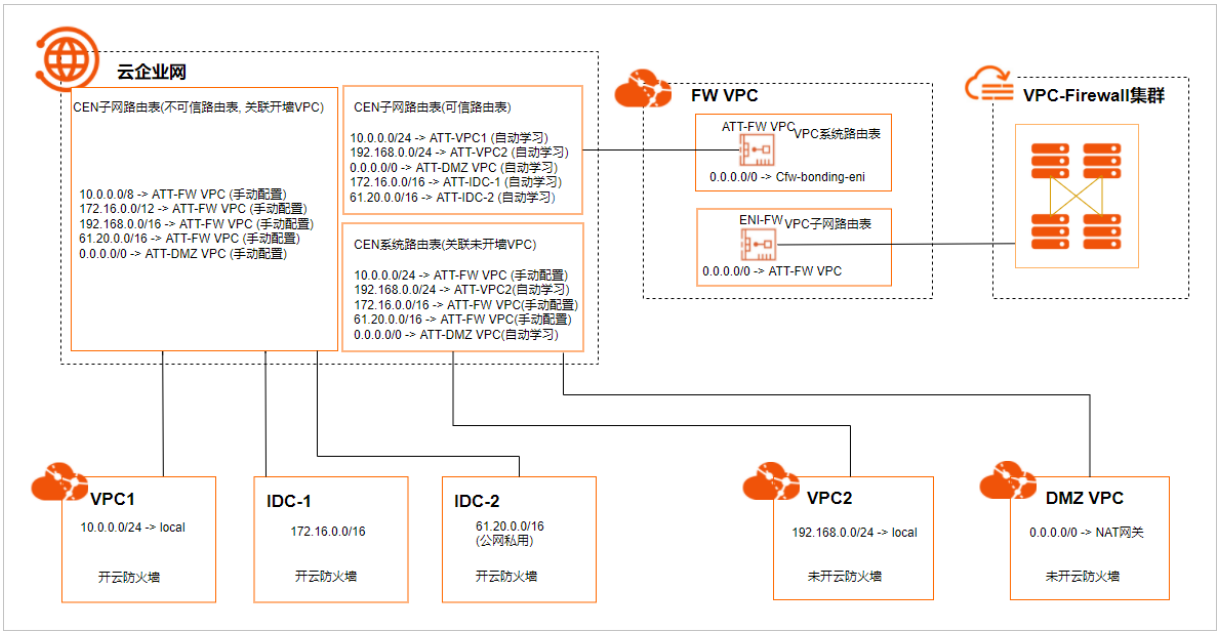
1. 已在云企业网控制台创建了云企业网实例，且创建了3个专有网络VPC（本文分别以VPC1、VPC2、DMZ

VPC为例）和2个VBR（本文分别以IDC-1、IDC-2为例）。具体操作，请参见创建云企业网实例。

2. 已在专有网络控制台手动创建了VPC边界防火墙的VPC实例（本文以FW VPC为例），且为该VPC实例创建了3个交换机（其中2个交换机提供给TR网络实例连接使用，可用区与TR网络实例连接的主备可用区保持一致。本文示例中命名分别为TR-Vswitch-01和TR-VSwitch-02，1个交换机提供给创建VPC边界防火墙的时候使用，本文示例中命名为Cfw-Vswitch）。
3. 已在专有网络控制台为Cfw-TR-manual-VPC创建自定义路由表（本文中以VPC-CFW-RouteTable为例）。

示例中VPC1、IDC-1、IDC-2和其他VPC之间互访的流量受云防火墙保护。VPC2和DMZ VPC互访的流量，不受云防火墙保护。任意VPC、IDC访问0.0.0.0/0默认路由的流量，不受云防火墙保护。

示意图如下：



适用对象

云防火墙可以防护通过转发路由器连接的网络实例之间的流量，网络实例包括VPC、VBR、CCN。

本文仅针对VPC边界防火墙手动引流模式的配置，适用于对多个VPC（相同地域）之间互访流量的防护。

步骤一：在转发路由器中添加防火墙VPC的网络实例连接

本步骤建立VPC实例（FW VPC）与转发路由器企业版之间的连接。

1. 登录云企业网管理控制台。
2. 在**云企业网实例**页面，定位到需要引流到云防火墙VPC边界防火墙的云企业网实例，并单击实例ID。

3. 在该云企业网实例页面**基本信息**页签中，单击**操作**列的**创建网络实例连接**或单击页面上方VPC基础信息右侧的 ⊕ 图标。

4. 在**连接网络实例**页面，设置FW VPC和转发路由器之间的连接信息。

   以下是创建网络连接实例时，关键的配置项说明。

配置项	如何设置
实例类型	通过云企业网连接的网络实例的类型。此处选择**专有网络（VPC）**。
地域	通过云企业网连接的网络实例的地址。此处需要与创建FW VPC时指定的地域保持一致。
网络实例	通过云企业网连接的网络实例。此处选择**FW VPC**的实例ID。
交换机	网络连接实例可绑定的交换机。设置**主交换机**为TR-Vswitch-01，**备交换机**为TR-VSwitch-02。

   其他配置项的说明，请参见使用企业版转发路由器创建VPC连接。

步骤二：为VPC、VBR创建云企业网网络实例连接

您需要为VPC1、VPC2、DMZ VPC及IDC-1、IDC-2分别创建网络实例连接，并将创建的VPC和VBR加载到该云企业网中。

具体操作，请参见使用企业版转发路由器创建VPC连接。

步骤三：创建VPC边界防火墙

本步骤为FW VPC创建VPC边界防火墙。

在云防火墙控制台**防火墙开关**页面的**VPC边界防火墙**页签，单击**云企业网**定位到网络实例FW VPC，单击**操作**列**创建**。创建该VPC边界防火墙时，设置**路由模式**为**手动**、**专有网络**为FW VPC、**交换机**为Cfw-Vswitch。

具体操作，请参见为云企业网创建VPC边界防火墙。

> **说明** 完成此步骤后，您会拥有1个弹性网卡（在ECS控制台的**网络与安全** > **弹性网卡**页面，系统默认分配名称为cfw-bonding-eni的网卡）。

步骤四：为VPC1、VPC2、DMZ VPC创建路由

本步骤为云企业网和VPC边界防火墙之间的流量创建路由。

1. 登录云企业网管理控制台。
2. 在**云企业网实例**页面，定位到需要引流到云防火墙VPC边界防火墙的云企业网实例，并单击实例ID。

3. 在该云企业网实例页面的**转发路由器**列表，单击**路由表**列下的数字。

4. 创建路由表Cfw-Untrust-RouteTable和Cfw-Trust-RouteTable。
   i. 在**转发路由器路由表**页签，单击**创建路由表**。
   ii. 在**创建路由表**对话框，配置路由表Cfw-Untrust-RouteTable和Cfw-Trust-RouteTable。

   转发路由器：选择默认的路由器。

   > 说明
   > - 路由表Cfw-Untrust-RouteTable：用于转发VPC1、IDC-1、IDC-2的流量到FW VPC。
   > - 路由表Cfw-Trust-RouteTable：用于转发FW VPC流量到VPC1、VPC2、DMZ VPC、IDC-1、IDC-2。

5. 配置路由表Cfw-Trust-RouteTable。

   为路由表Cfw-Trust-RouteTable自动同步VPC1、VPC2、DMZ VPC、IDC-1、IDC-2的路由，并将FW VPC的流量关联转发到Cfw-Trust-RouteTable。
   i. 单击已创建的Cfw-Trust-RouteTable路由表，在右侧区域，单击**路由学习**。
   ii. 在**路由学习**页签，单击**创建路由学习**。
   iii. 在**添加路由学习**对话框，关联连接分别选择**VPC1**、**VPC2**、**DMZ VPC**、**IDC-1**、**IDC-2**。然后单击**确定**。
   路由学习创建完成后，您可以在**路由条目**页签中看到自动学习的路由信息。
   iv. 在**转发路由器路由表**页签，单击左侧路由表列表中的系统路由表，然后在**路由表详情**页签，单击**关联转发**。
   v. 在**关联转发**页签，删除下一跳为FW VPC的关联转发。
   vi. 单击已创建的Cfw-Trust-RouteTable路由表，在**关联转发**页签，单击**创建关联转发**。
   vii. 在**添加关联转发**页面，在**关联转发**下拉框，选择**FW VPC**。然后单击**确定**。

6. 配置路由表Cfw-Untrust-RouteTable。

   将云企业网自定义路由表Cfw-Untrust-RouteTable的流量会默认指向VPC防火墙。
   i. 单击已创建的Cfw-Untrust-RouteTable路由表，在右侧区域，单击**路由条目**。
   ii. 在**路由条目**页签，单击**创建路由条目**。
   iii. 在**添加路由条目**对话框，配置路由条目的信息。

   配置项说明：
   - **目的地址CIDR**：选择默认地址段**10.0.0.0/8**。
   - **是否为黑洞路由**：选择默认选项**否**。
   - **下一跳连接**：选择防火墙VPC实例（FW VPC）。

iv. 重复上述步骤，新增如下网段路由。

- 新增172.16.0.0/12网段路由，下一跳到防火墙VPC实例（FW VPC）。
- 新增192.168.0.0/16的网段路由，下一跳到防火墙VPC实例（FW VPC）。
- 新增61.20.0.0/16的网段路由，下一跳到防火墙VPC实例（FW VPC）。
- 新增0.0.0.0/0的网段路由，下一跳到DMZ VPC。

7. 配置系统路由表。

i. 在**转发路由器路由表**页签，单击左侧路由表列表中的系统路由表，然后在右侧区域，单击**路由学习**。

ii. 在**路由学习**页签，删除VPC1、IDC-1、FW VPC、IDC-2的路由学习。
该操作后，您的系统路由表只保留VPC2和DMZ VPC的路由学习。配置完成后，您可以在路由条目页签中看到自动学习的路由信息。

iii. 在**路由条目**页签，单击**创建路由条目**。

iv. 在**添加路由条目**对话框，新增如下网段路由。

- 新增10.0.0.0/24（VPC1）网段路由，下一跳到防火墙VPC实例（FW VPC）。
- 新增172.16.0.0/12（IDC-1）的网段路由，下一跳到防火墙VPC实例（FW VPC）。
- 新增61.20.0.0/16（IDC-2）的网段路由，下一跳到防火墙VPC实例（FW VPC）。

v. 在**关联转发**页签，删除下一跳为**VPC1**、**IDC-1**、**IDC-2**的关联转发。

8. 配置**Cfw-Untrust-RouteTable**路由表。

将VPC1、IDC-1、IDC-2的流量关联转发到**Cfw-Untrust-RouteTable**。

i. 单击已创建的**Cfw-Untrust-RouteTable**路由表，在右侧区域，单击**关联转发**。

ii. 在**关联转发**页签，单击**创建关联转发**。

iii. 在**添加关联转发**对话框，在**关联转发**下拉框，选择**VPC1**、**IDC-1**、**IDC-2**。然后单击**确定**。

本步骤完成后，云企业网路由配置完成，流量牵引到VPC边界防火墙的VPC实例上。

步骤五：添加VPC路由表到VPC边界防火墙

本步骤将防火墙VPC实例的路由引流到VPC边界防火墙上。

1. 登录专有网络管理控制台。在左侧导航栏，单击**路由表**。
2. 在**路由表**页面，打开路由表**VPC-CFW-RouteTable**，在**已绑定交换机**页签，单击**绑定交换机**。其中**交换机**选择**Cfw-Vswitch**。然后单击**确定**。
3. 在**路由条目列表**的**自定义路由条目**页签，单击**添加路由条目**，配置路由条目信息。

关键配置项说明：

- **目标网段**：选择 `0.0.0.0/0` 。
- **下一跳类型**：选择 **转发路由器** 。
- **转发路由器**：选择默认项，即VPC防火墙的网络实例连接。

本操作完成后，VPC边界防火墙出方向的流量会通过子网路由表转发到转发路由器。

4. 在路由表列表页面，选择防火墙VPC实例（FW VPC）的系统路由表。
5. 在**路由条目**列表，单击**自定义路由条目**页签。
6. 单击**添加路由条目**，配置路由条目信息。

关键配置项说明：

- **目标网段**：选择0.0.0.0/0。
- **下一跳类型**：选择辅助弹性网卡。
- **辅助弹性网卡**：选择Cfw-bonding-eni。

7. 在**自定义路由条目**页签，单击其他自定义路由条目**操作**列**删除**，删除其他自定义路由条目。

   本步骤完成后，来自防火墙VPC实例的流量会牵引到云防火墙实例上。

步骤六：验证转发配置是否成功

您可以在流量日志功能查看是否有来自该云企业网的流量日志。如果有相关流量日志，代表转发配置成功。例如：

- VPC1与VPC2之间能够访问正常，且有流量日志。
- VPC2与DMZ VPC之间能够访问正常，但是无流量日志。

具体步骤，请参见流量日志。

2.6. 防护云企业网TR跨地域场景的VPC之间的流量

当您使用了转发路由器TR（Transit Router）连通跨地域网络实例时，您可以手动配置转发路由器与VPC边界防火墙之间的互访路由，实现VPC边界防火墙对网络实例之间的流量进行防护。本文介绍了如何防护跨地域场景的转发路由器中网络实例与VPC边界防火墙之间的全部流量。

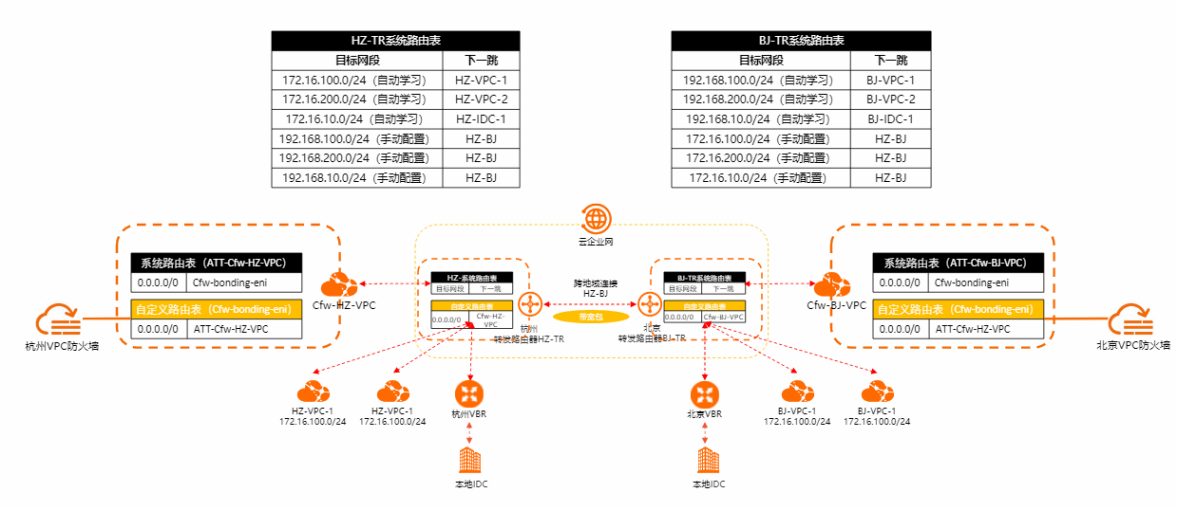
场景示例

云防火墙可以防护连接到转发路由器的网络实例之间的通信流量，网络实例包括专有网络VPC（Virtual Private Cloud）、边界路由器VBR（Virtual Border Router）、云连接网CCN（Cloud Connect Network）。本文以跨地域VPC互通为例，介绍如何防护转发路由器连接的2个VPC实例互访流量，如下图场景所示。

> **说明** 本文仅针对VPC边界防火墙手动引流模式的配置，适用于对多个VPC（跨地域）之间互访流量的防护。

某企业在阿里云华东1（杭州）地域部署2个VPC实例（HZ-VPC-1、HZ-VPC-2），在华北2（北京）地域部署2个VPC实例（BJ-VPC-1、BJ-VPC-2），并且使用云企业网的转发路由器创建跨地域连接，实现华东1（杭州）地域和华北2（北京）地域的VPC互通。同时，该企业分别在华东1（杭州）和华北2（北京）地域各部署1个边界路由器VBR实例（HZ-IDC-1和BJ-IDC-1），实现云上和云下资源互访。

为了保障VPC之间流量互访安全，该企业计划通过云防火墙的VPC边界防火墙来检测和管控2个VPC间的通信流量。



前提条件

- 您已创建一个云企业实例。具体操作，请参见创建云企业网实例。
- 您已在华东1（杭州）和华北2（北京）地域，创建了业务需使用的专有网络VPC和边界路由器VBR，并建立了VPC、VBR与云企业网网络实例连接，且为华东1（杭州）和华北2（北京）地域创建跨地域网络连接。
  - 华东1（杭州）：专有网络VPC（HZ-VPC-1、HZ-VPC-2）和边界路由器VBR（HZ-IDC-1）。
  - 华北2（北京）：专有网络VPC（BJ-VPC-1、BJ-VPC-2）和边界路由器VBR（BJ-IDC-1）。
- 您已在华东1（杭州）和华北2（北京）地域，分别创建了防火墙的VPC实例（Cfw-HZ-VPC、Cfw-BJ-VPC），并在各自的VPC实例下创建了交换机和自定义路由表。具体操作，请参见创建VPC连接、创建和管理专有网络、创建和管理路由表。

  如下表所示：

地域	云防火墙VPC	交换机&可用区	云防火墙VPC的自定义路由表
华东1（杭州）	Cfw-HZ-VPC	HZ-TR-vSwitch-1 供TR网络实例连接使用，可用区与TR网络实例连接的主可用区保持一致。本示例中华东1（杭州）的主可用区需选择H。	HZ-VPC-CFW-RouteTable
		HZ-TR-vSwitch-2 供TR网络实例连接使用，可用区与TR网络实例连接的备可用区保持一致。本示例中华东1（杭州）的备可用区需选择I。	
		HZ-Cfw-vSwitch 供VPC边界防火墙使用。	

地域	云防火墙VPC	交换机&可用区	云防火墙VPC的自定义路由表
华北2（北京）	Cfw-BJ-VPC	BJ-TR-vSwitch-1 供TR网络实例连接使用，可用区与TR网络实例连接的主可用区保持一致。本示例中华北2（北京）的主可用区需选择H。	BJ-VPC-CFW-RouteTable
		BJ-TR-vSwitch-2 供TR网络实例连接使用，可用区与TR网络实例连接的备可用区保持一致。本示例中华北2（北京）的备可用区需选择G。	
		BJ-Cfw-vSwitch 供VPC边界防火墙使用。	

- 您已将云防火墙VPC（Cfw-HZ-VPC、Cfw-BJ-VPC）的实例ID加入白名单，便于后续为其创建VPC边界防火墙。

  将云防火墙VPC的实例ID加入白名单的操作需要通过售后人员完成。

  > **注意** 如果您需要使用该功能，请联系云防火墙售后人员开启白名单。未开启白名单的情况下，在云防火墙控制台的**VPC边界防火墙**页面，无法为云企业网TR实例创建VPC边界防火墙，并提示您先申请加入白名单。

配置流程

步骤一：建立云防火墙VPC实例与云企业网TR的连接

分别将华东1（杭州）云防火墙VPC实例、华北2（北京）云防火墙VPC实例加入TR。

1. 登录云企业网管理控制台。
2. 在**云企业网实例**页面，单击需要被云防火墙防护的云企业网实例。
3. 在该云企业网实例**基本信息**的**转发路由器**页签，单击**操作**列的**创建网络实例连接**。
4. 在**连接网络实例**页面，设置华东1（杭州）云防火墙VPC实例、华北2（北京）云防火墙VPC实例和转发路由器之间的连接信息。然后单击**确定创建**。

   以下是创建网络连接实例时，关键的配置项说明：

配置项	说明	华东1（杭州）VPC防火墙实例配置示例值	华北2（北京）VPC防火墙实例配置示例值
实例类型	通过转发路由器连接的网络实例的类型。	**专有网络（VPC）**	**专有网络（VPC）**

配置项	说明	华东1（杭州）VPC防火墙实例配置示例值	华北2（北京）VPC防火墙实例配置示例值
地域	选择连接到转发路由器的网络实例所属的地域。	**华东1（杭州）**	**华北2（北京）**
网络实例	通过转发路由器连接的网络实例。	**Cfw-HZ-VPC**的实例ID。	**Cfw-BJ-VPC**的实例ID。
交换机	网络连接实例可绑定的交换机。	○ **主交换机**：HZ-TR-vSwitch-1 ○ **备交换机**：HZ-TR-vSwitch-2	○ **主交换机**：BJ-TR-vSwitch-1 ○ **备交换机**：BJ-TR-vSwitch-2

其他配置项的说明，请参见使用企业版转发路由器创建VPC连接。

步骤二：创建VPC边界防火墙

为华东1（杭州）云防火墙、华北2（北京）云防火墙VPC实例创建VPC边界防火墙。

1. 登录云防火墙控制台。在左侧导航栏，选择**防火墙开关 > 防火墙开关**。
2. 在**防火墙开关**页面，**VPC边界防火墙**的**云企业网**页签，分别定位到华东1（杭州）的防火墙VPC（Cfw-HZ-VPC）和华北2（北京）的防火墙VPC（Cfw-BJ-VPC），然后单击**操作**列**创建**。

   以下是创建VPC边界防火墙时，关键的配置项说明：

配置项	说明	华东1（杭州）VPC防火墙实例配置示例值	华北2（北京）VPC防火墙实例配置示例值
路由模式	经过云防火墙的流量的转发路由模式。	**手动**	**手动**
专有网络	建立云防火墙所在的专有网络。	**Cfw-HZ-VPC**	**Cfw-BJ-VPC**
交换机	绑定云防火墙网卡所在的交换机。	**HZ-Cfw-vSwitch**	**BJ-Cfw-vSwitch**

   其他配置项的说明，请参见为云企业网创建VPC边界防火墙。

   完成此步骤后，华东1（杭州）云防火墙VPC实例和华北2（北京）云防火墙VPC实例分别拥有1个弹性网卡（**cfw-bonding-eni**）。

   您可以在云防火墙控制台，对应的云防火墙VPC实例的详情页面，查看分配的弹性网卡实例ID。

步骤三：为杭州地域的云防火墙VPC配置路由表

将华东1（杭州）云防火墙VPC实例的流量引流到VPC边界防火墙。

1. 登录专有网络管理控制台，并切换地域为**华东1（杭州）**。在左侧导航栏，单击**路由表**。
2. 在**路由表**页面，配置华东1（杭州）云防火墙VPC（Cfw-HZ-VPC）的路由表。

   按照如下网络规划配置：

   i. 在**路由表**页面，单击**创建路由表**。创建自定义路由表。

ii. 单击该路由表，在路由表详情页的**已绑定交换机**页签，单击**绑定交换机**。为自定义路由表和系统路由表绑定交换机。

iii. 在该路由表详情页**路由条目列表**的**自定义路由条目**页签，单击**添加路由条目**。为自定义路由表和系统路由表创建路由条目。

具体操作，请参见创建和管理路由表。

按照如下网络规划配置：

配置目的	路由表	交换机	路由条目
将VPC边界防火墙出方向的流量，通过自定义路由表转发到转发路由器。	自定义路由表：HZ-VPC-CFW-RouteTable	HZ-Cfw-vSwitch	关键配置项说明： ○ **目标网段**：选择**0.0.0.0/0**。 ○ **下一跳类型**：选择**转发路由器**。 ○ **转发路由器**：选择默认项，即VPC防火墙的网络实例连接。
将华东1（杭州）云防火墙VPC实例的流量，通过系统路由表引流到VPC边界防火墙。	系统路由表	○ HZ-TR-vSwitch-1 ○ HZ-TR-vSwitch-2	您需要在待配置的路由表详情页的**自定义路由条目**页签下创建路由条目。 关键配置项说明： ○ **目标网段**：选择**0.0.0.0/0**。 ○ **下一跳类型**：选择**辅助弹性网卡**。 ○ **辅助弹性网卡**：选择**Cfw-bonding-eni**。

3. 在华东1（杭州）云防火墙VPC（Cfw-HZ-VPC）系统路由表的**自定义路由条目**页签，单击其他自定义路由条目**操作**列**删除**，删除其他自定义路由条目，只保留上一步配置的**0.0.0.0/0**默认路由。

步骤四：为北京地域的云防火墙VPC配置路由表

将华北2（北京）云防火墙VPC实例的流量引流到VPC边界防火墙。

1. 登录专有网络管理控制台，并切换地域为**华北2（北京）**。在左侧导航栏，单击**路由表**。
2. 在**路由表**页面，配置华北2（北京）云防火墙VPC（Cfw-BJ-VPC）的路由表。

i. 在**路由表**页面，单击**创建路由表**。创建自定义路由表。

ii. 单击该路由表，在路由表详情页的**已绑定交换机**页签，单击**绑定交换机**。为自定义路由表和系统路由表绑定交换机。

iii. 在该路由表详情页**路由条目列表**的**自定义路由条目**页签，单击**添加路由条目**。为自定义路由表和系统路由表创建路由条目。

具体操作，请参见创建和管理路由表。

按照如下网络规划配置：

配置目的	路由表	交换机	路由条目
将VPC边界防火墙出方向的流量，通过自定义路由表转发到转发路由器。	自定义路由表：BJ-VPC-CFW-RouteTable	BJ-Cfw-vSwitch	关键配置项说明： ○ **目标网段**：选择**0.0.0.0/0**。 ○ **下一跳类型**：选择**转发路由器**。 ○ **转发路由器**：选择默认项，即VPC防火墙的网络实例连接。
将华北2（北京）云防火墙VPC实例的流量，通过系统路由表引流到VPC边界防火墙。	系统路由表	○ BJ-TR-vSwitch-1 ○ BJ-TR-vSwitch-2	关键配置项说明： ○ **目标网段**：选择**0.0.0.0/0**。 ○ **下一跳类型**：选择**辅助弹性网卡**。 ○ **辅助弹性网卡**：选择**Cfw-bonding-eni**。

3. 在华北2（北京）云防火墙VPC（Cfw-BJ-VPC）的系统路由表的**自定义路由条目**页签，单击其他自定义路由条目**操作**列**删除**，删除其他自定义路由条目，只保留上一步配置的**0.0.0.0/0**默认路由。

步骤五：为杭州地域的转发路由器配置路由表

本步骤为华东1（杭州）地域网络实例（HZ-VPC-1、HZ-VPC-2、HZ-IDC-1）创建转发路由器自定义路由表（Cfw-HZ-TR-RouteTable），并配置关联转发和路由学习，用于转发华东1（杭州）地域网络实例到华东1（杭州）云防火墙VPC实例（Cfw-HZ-VPC）之间的流量。

本步骤以配置HZ-VPC-1为例，您需要根据如下介绍，分别配置HZ-VPC-1、HZ-VPC-2、HZ-IDC-1。

1. 登录云企业网管理控制台。在左侧导航栏，单击**云企业网实例**。
2. 在**云企业网实例**页面，为华东1（杭州）地域的网络实例（HZ-VPC-1）创建云企业转发路由器自定义路由表，并为此自定义路由表创建路由条目。
   i. 单击网络实例，在**基本信息**页签，单击**创建转发路由器**。创建云企业网转发路由器实例。
   ii. 单击该转发路由器实例，在**转发路由器路由表**页签，单击**创建路由表**。为转发路由器实例创建路由表。
   iii. 单击该路由表，在路由表详情页的**路由条目**页签，单击**创建路由条目**。为自定义路由表创建路由条目。

   具体操作，请参见自定义路由表、转发路由器自定义路由条目。

   按照如下网络规划配置：

配置的目的	路由表	路由条目
创建的路由表用于转发华东1（杭州）地域网络实例到杭州云防火墙VPC实例（Cfw-HZ-VPC）之间的流量。	Cfw-HZ-TR-RouteTable **转发路由器**：选择默认的路由器。	关键的配置项说明： ○ **目的地址CIDR**：选择默认地址段**0.0.0.0/0**。 ○ **是否为黑洞路由**：选择默认选项**否**。 ○ **下一跳连接**：选择防火墙VPC实例**Cfw-HZ-VPC**。

3. 为转发路由器自定义路由表（Cfw-HZ-TR-RouteTable）设置关联转发，并为系统路由表配置路由学

习。

i. 将出云防火墙VPC的流量关联转发到系统路由表。

a. 在**转发路由器路由表**页签，单击系统路由表。

b. 在系统路由表详情页面，单击**关联转发**。

c. 在**关联转发**页签，删除下一跳为**HZ-VPC-1**、**HZ-VPC-2**、**HZ-IDC-1**和**HZ-BJ**的关联转发。

您需要确认**Cfw-HZ-VPC**的关联转发是否存在，如果不存在，需要为其添加关联转发。

具体操作，请参见关联转发。

ii. 将华东1（杭州）地域的网络实例（HZ-VPC-1、HZ-VPC-2、HZ-IDC-1）和跨地域连接的流量关联转发到自定义路由表。

a. 在**转发路由器路由表**页签，单击路由列表中的**Cfw-HZ-TR-RouteTable**路由表。

b. 在路由表详情页面，单击**关联转发**，然后单击**创建关联转发**。

c. 在**添加关联转发**对话框，**关联转发**选择**HZ-VPC-1**、**HZ-VPC-2**、**HZ-IDC-1**和**HZ-BJ**。

具体操作，请参见关联转发。

iii. 为系统路由表配置路由学习。

a. 在**转发路由器路由表**页签，单击左侧路由器列表中的系统路由表。

b. 在系统路由表的路由表详情页面，单击**路由学习**页签。

c. 在**路由学习**页签，删除**HZ-BJ**、**Cfw-HZ-VPC**。

您需要确认已存在三条路由学习，关联连接分别为**HZ-VPC-1**、**HZ-VPC-2**、**HZ-IDC-1**。

具体操作，请参见路由学习。

4. 在**转发路由条目**页签，单击**创建路由条目**，为系统路由表添加静态路由。

配置的目的	路由条目
配置对端地域的静态路由，实现华东1（杭州）和华北2（北京）的网络实例跨地域互通。	关键配置项说明： • **目的地址CIDR**：选择华北2（北京）网络实例的地址段**192.168.100.0/24**（BJ-VPC-1网段）、**192.168.200.0/24**（BJ-VPC-2网段）、**192.168.10.0/24**（BJ-IDC-1网段） • **是否为黑洞路由**：选择默认选项否。 • **下一跳连接**：选择跨地域连接实例**HZ-BJ**。

具体操作，请参见转发路由器自定义路由条目。

> **说明** 为了防止**0.0.0.0/0**的默认路由向IDC传播，可以为HZ-IDC-1单独创建一张自定义路由表，并创建关联转发为HZ-IDC-1。根据业务情况配置云上明细路由，下一跳为Cfw-HZ-VPC。

步骤六：为北京地域的转发路由器配置路由表

本步骤为华北2（北京）地域网络实例（BJ-VPC-1、BJ-VPC-2、BJ-IDC-1）创建转发路由器自定义路由表（Cfw-BJ-TR-RouteTable），并配置关联转发和路由学习，用于转发华北2（北京）地域网络实例到华北2（北京）云防火墙VPC实例（Cfw-BJ-VPC）之间的流量。

本步骤以配置BJ-VPC-1为例，您需要根据如下介绍，分别配置BJ-VPC-1、BJ-VPC-2、BJ-IDC-1。

1. 登录云企业网管理控制台。在左侧导航栏，单击**云企业网实例**。
2. 在**云企业网实例**页面，按照下表所示，为华北2（北京）地域的网络实例（BJ-VPC-1）创建转发路由器自定义路由表，并为此自定义路由表创建路由条目。
   i. 单击网络实例，在**基本信息**页签，单击**创建转发路由器**。创建云企业网转发路由器实例。
   ii. 单击该转发路由器实例，在**转发路由器路由表**页签，单击**创建路由表**。为转发路由器实例创建路由表。
   iii. 单击该路由表，在路由表详情页的**路由条目**页签，单击**创建路由条目**。为自定义路由表创建路由条目。

   具体操作，请参见创建和管理路由表。

   按照如下网络规划配置：

配置的目的	路由表	路由条目
创建的路由表用于转发华北2（北京）地域网络实例到华北2（北京）云防火墙VPC实例（Cfw-BJ-VPC）之间的流量。	Cfw-BJ-TR-RouteTable **转发路由器**：选择默认的路由器。	关键的配置项说明： ○ **目的地址CIDR**：选择默认地址段0.0.0.0/0。 ○ **是否为黑洞路由**：选择默认选项否。 ○ **下一跳连接**：选择防火墙VPC实例Cfw-BJ-VPC。

3. 为转发路由器自定义路由表（Cfw-BJ-TR-RouteTable）设置关联转发，并为系统路由表配置路由学习。
   i. 将出云防火墙VPC的流量关联转发到系统路由表。
      a. 在**转发路由器路由表**页签，单击系统路由表。
      b. 在系统路由表详情页面，单击**关联转发**。
      c. 在**关联转发**页签，删除下一跳为BJ-VPC-1、BJ-VPC-2、BJ-IDC-1和HZ-BJ的关联转发。

         您需要确认Cfw-BJ-VPC的关联转发是否存在，如果不存在，需要为其添加关联转发。

      具体操作，请参见关联转发。
   ii. 将华北2（北京）地域的网络实例（BJ-VPC-1、BJ-VPC-2、BJ-IDC-1）和跨地域连接的流量关联转发到自定义路由表。
      a. 在**转发路由器路由表**页签，单击路由列表中的Cfw-BJ-TR-RouteTable路由表。
      b. 在路由表详情页面，单击**关联转发**，然后单击**创建关联转发**。
      c. 在**添加关联转发**对话框，**关联转发**选择BJ-VPC-1、BJ-VPC-2、BJ-IDC-1和HZ-BJ。

      具体操作，请参见关联转发。
   iii. 为系统路由表配置路由学习。
      a. 在**转发路由器路由表**页签，单击左侧路由器列表中的系统路由表。
      b. 在系统路由表的路由表详情页面，单击**路由学习**页签。
      c. 在**路由学习**页签，删除HZ-BJ、Cfw-BJ-VPC。

         您需要确认已存在三条路由学习，关联连接分别为BJ-VPC-1、BJ-VPC-2、BJ-IDC-1。

      具体操作，请参见路由学习。
4. 在**转发路由条目**页签，单击**创建路由条目**，为系统路由表添加静态路由。

配置的目的	路由条目
配置对端地域的静态路由，实现华北2（北京）和华东1（杭州）的网络实例跨地域互通。	关键配置项说明： ○ **目的地址CIDR**：选择华东1（杭州）网络实例的地址段**172.16.100.0/24**（HZ-VPC-1网段）、**172.16.200.0/24**（HZ-VPC-2网段）、**172.16.10.0/24**（HZ-IDC-1网段）。 ○ **是否为黑洞路由**：选择默认选项**否**。 ○ **下一跳连接**：选择跨地域连接实例**HZ-BJ**。

具体操作，请参见转发路由器自定义路由条目。

> **说明** 为了防止**0.0.0.0/0**的默认路由向IDC传播，可以为BJ-IDC-1单独创建一张自定义路由表，并创建关联转发为BJ-IDC-1，根据业务情况配置云上明细路由，下一跳为Cfw-BJ-VPC。

步骤七：验证转发配置是否成功

当您的业务有跨VPC访问的私网流量，您可以在日志审计的流量日志的VPC边界防火墙，查看云企业网的跨VPC访问的流量日志。如果有相关流量日志，代表转发配置成功。

具体操作，请参见流量日志。

3.NAT防火墙

云防火墙提供NAT防火墙功能，实现对私网IP访问公网的流量进行访问控制和防护。

前提条件

- 已开通企业版或旗舰版云防火墙服务。

  > 注意 云防火墙企业版默认支持配置2个NAT防火墙实例，旗舰版默认支持配置3个NAT防火墙实例。如果您需要配置更多NAT防火墙实例，请提交工单申请，或者联系产品钉钉群售后人员。

- 创建NAT防火墙2.0，需要拥有地域为华东1（杭州）、可用区为**华东1可用区I**或**华东1可用区K**的增强型NAT网关且已提交工单申请。

  > 注意 NAT防火墙2.0支持SNAT和DNAT两种策略条目。

- 创建NAT防火墙1.0（原安全正向代理），需要拥有满足以下条件的NAT网关：
  - 华东2（上海）、西南1（成都）或中国香港地域的NAT网关，或者华北2（北京）、华东1（杭州）或华南1（深圳）地域的NAT网关且已提交工单申请。
  - 已为NAT网关配置了SNAT条目。相关内容，请参见创建和管理SNAT条目。

    > 注意 NAT防火墙1.0只支持SNAT策略条目，不支持DNAT策略条目。

  - NAT网关所在的VPC支持VPC高级功能。相关内容，请参见VPC高级功能。

  > 注意 每个NAT网关默认最多绑定5个EIP（Elastic IP Address）和1,000条SNAT条目。如果您需要NAT网关绑定更多EIP，请通过钉钉加入阿里云云防火墙问题答疑群聊（群号：33081734）咨询售后人员。

背景信息

NAT防火墙是一种虚拟化的防火墙，创建并开启NAT防火墙后，经过NAT网关的流量会自动切换到云防火墙NAT防火墙。您可以在NAT防火墙页面的NAT防火墙列表的**版本**列，查看NAT防火墙的具体版本。

创建NAT防火墙

创建NAT防火墙时，NAT防火墙1.0会做NAT路由切换，导致20秒左右业务闪断，请在业务低峰期进行操作；NAT防火墙2.0通过服务链技术实现，无需切换路由，有效避免了路由切换造成的业务闪断，开启过程业务无感知，实现秒级开启。

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**防火墙开关 > NAT防火墙**。
3. 在**NAT防火墙**页面，单击NAT防火墙实例列表**操作**列的**创建**。
4. 在**创建NAT防火墙**对话框中，完成以下参数配置。

配置项	说明
名称	自定义NAT防火墙的名称。可输入中文、英文、任意特殊字符。

配置项	说明
交换机	该NAT防火墙所在的交换机（vSwitch）。有以下两种模式可以选择： ○ **自选模式**：云防火墙自动创建交换机并绑定自定义路由表。 ○ **手动模式**：您可以选择已手动创建的交换机。相关信息，请参见在手动模式下创建交换机。 **注意** 只有NAT防火墙1.0才需要设置该参数。
启用状态	是否启用该NAT防火墙。

创建NAT防火墙后，如果已打开NAT防火墙开关，流量会经由NAT防火墙转发。

您还可以在**NAT防火墙**页面，对已创建的NAT防火墙进行修改和删除、下载已创建的NAT防火墙数据列表。

注意 云防火墙服务到期后，如果您未及时续费，您所创建的NAT防火墙将会自动释放，同时流量路由会切换至您原始的由内网访问公网的路由。此时，可能会造成业务短暂中断，请您提前续费确保服务可用。相关内容，请参见操作步骤。

在手动模式下创建交换机

在创建NAT防火墙1.0时，您可以自主创建交换机并绑定自定义路由表，然后选择该交换机来创建NAT防火墙1.0。

1. 在**创建NAT防火墙1.0**对话框，单击**前往VPC控制台手动创建交换机**。
2. 在专有网络控制台的**交换机**页面，单击**创建交换机**。
3. 在**创建交换机**页面，完成参数配置，单击**确认**。

   选择**专有网络**为NAT防火墙1.0所在的VPC，选择**可用区**为NAT网关所在的可用区，确保**IPv4网段**的可用IP数大于NAT网关的SNAT EIP数。相关信息，请参见创建交换机。
4. 在专有网络控制台的**路由表**页面，单击**创建路由表**。
5. 在**创建路由表**页面，完成参数配置，单击**确定**。

   选择**专有网络**为NAT防火墙1.0所在的VPC。相关信息，请参见创建自定义路由表。
6. 在专有网络控制台的**路由表**页面，在路由表列表定位到您自主创建的路由表，单击该路由表的实例ID。
7. 在**路由表基础信息**页面的**已绑定交换机**页签，单击**绑定交换机**，在**绑定交换机**对话框中选择自主创建的交换机，单击**确定**。

注意 路由表不允许添加自定义路由条目，交换机不允许接入ECS、RDS、SLB等云资源。

相关操作

- 查看哪些NAT网关有主动外联的记录

  在**NAT防火墙**页面，单击NAT防火墙**操作**列的⋮图标，再单击**流量分析**跳转到**主动外联活动**页面，您可以在**主动外联活动**页面查看NAT网关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网关的公网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NAT网关的访问情况。相关内容，请参见互联网访问活动。

- 查看NAT网关的流量日志

  在**NAT防火墙**页面，单击NAT防火墙**操作**列的 ⋮ 图标，再单击**日志审计**跳转到**日志审计**页面，在**日志审计**页面，您可以搜索并查看NAT网关所有相关流量的日志记录。

- 创建访问控制策略

  在**NAT防火墙**页面，单击NAT防火墙**操作**列的 ⋮ 图标，再单击**访问控制**跳转到**访问控制**页面，您可以在**访问控制**页面创建访问控制策略。

4.DNS防火墙

云防火墙提供DNS防火墙功能，支持对VPC访问互联网上指定的域名进行精细管控。VPC要访问互联网上的指定域名，必须先通过DNS服务器解析域名对应的IP地址。开启DNS防火墙后，VPC访问互联网域名时会先经过DNS防火墙，实现对VPC访问互联网域名进行访问控制和防护。

前提条件

创建DNS防火墙的VPC需要支持VPC高级功能。相关内容，请参见VPC高级功能。

版本和地域支持说明

云防火墙企业版和旗舰版支持DNS防火墙功能，高级版不支持。

只有华东2（上海）、西南1（成都）和中国香港地域的VPC支持创建DNS防火墙；华北2（北京）、华东1（杭州）和华南1（深圳）地域的VPC需要提交工单申请后，才可以创建DNS防火墙；其他地域暂不支持创建DNS防火墙。

云防火墙企业版默认支持配置2个DNS防火墙，旗舰版默认支持配置3个DNS防火墙。如果您需要配置更多DNS防火墙，请提交工单申请，或者联系产品钉钉群售后人员。

创建DNS防火墙

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**防火墙开关 > DNS防火墙**。
3. 在**DNS防火墙**页面，单击**创建DNS防火墙**。
4. 在**创建DNS防火墙**对话框，请参见下面的参数表，完成以下配置。

配置项	说明
名称	自定义DNS防火墙的名称。可输入中文、英文、任意特殊字符。
全部地域	只有华东2（上海）、西南1（成都）和中国香港地域的VPC支持创建DNS防火墙；华北2（北京）、华东1（杭州）和华南1（深圳）地域的VPC需要提交工单申请后，才可以创建DNS防火墙；其他地域暂不支持创建DNS防火墙。
VPC	该DNS防火墙防护的VPC实例ID。
UID	已选VPC所属的阿里云账号ID。
DNS Server	DNS服务器。当前只支持阿里云DNS服务器。
交换机	该DNS防火墙所在的交换机（vSwitch）。有以下两种模式可以选择： ○ **自选模式**：云防火墙自动创建交换机并绑定自定义路由表。 ○ **手动模式**：您可以选择已手动创建的交换机。相关信息，请参见在手动模式下创建交换机。

开启DNS防火墙开关后，会出现**配置访问控制策略**按钮。

5. 单击**确定**，完成DNS防火墙的创建。
创建DNS防火墙需要2分钟，请耐心等待。创建DNS防火墙后，DNS防火墙默认开启，DNS防火墙的防护已生效。

如果当前阿里云账号下有多个VPC，您可以按照实际需求创建多个DNS防火墙。

在手动模式下创建交换机

您可以自主创建交换机并绑定自定义路由表，然后选择该交换机来创建DNS防火墙。

1. 在**创建DNS防火墙**对话框，单击**前往VPC控制台手动创建交换机**。
2. 在专有网络控制台的**交换机**页面，单击**创建交换机**。
3. 在**创建交换机**页面，完成参数配置，单击**确认**。

   选择**专有网络**为DNS防火墙所在的VPC。相关信息，请参见创建交换机。
4. 在专有网络控制台的**路由表**页面，单击**创建路由表**。
5. 在**创建路由表**页面，完成参数配置，单击**确定**。

   选择**专有网络**为DNS防火墙所在的VPC。相关信息，请参见创建自定义路由表。
6. 在专有网络控制台的**路由表**页面，在路由表列表定位到您自主创建的路由表，单击该路由表的实例ID。
7. 在**路由表基础信息**页面的**已绑定交换机**页签，单击**绑定交换机**，在**绑定交换机**对话框中选择自主创建的交换机，单击**确定**。

> **注意** 路由表不允许添加自定义路由条目，交换机不允许接入ECS、RDS、SLB等云资源。

查看防火墙交换机列表

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**防火墙开关 > DNS防火墙**。
3. 在**DNS防火墙**页面，单击**防火墙交换机列表**。
4. 在**防火墙交换机列表**面板，查看详细信息。
   您可以在防火墙交换机列表面板，查看当前阿里云账号下已创建的DNS防火墙和安全正向代理所在交换机的详细信息。

开启DNS防火墙开关后，您还需要添加DNS域名访问控制策略。更多内容，请参见DNS域名访问控制策略。

相关文档

- 流量日志