私有网络

安全

产品文档

腾讯云

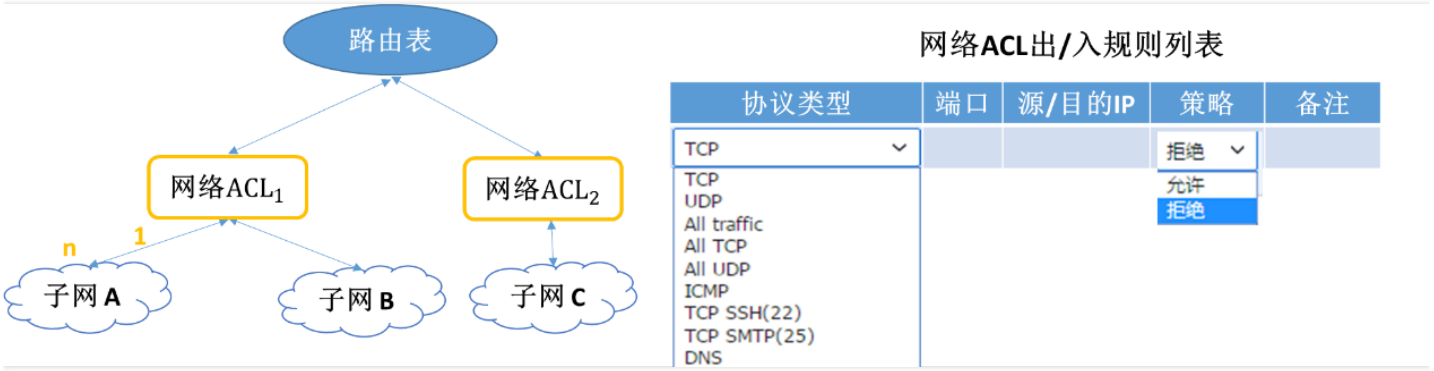
文档目录

安全
网络ACL

最近更新时间：2018-05-29 10:16:25

基本概念

网络访问控制列表（Access Control List，ACL）是一个子网级别无状态的可选安全层，用于控制进出子网的数据流，可以精确到协议和端口粒度。如下图所示，其规则与安全组相似。但由于网络 ACL 无状态的特性，即使设置入站规则允许某些访问，如果没有设置相应的出站规则会导致无法响应访问。



使用场景

用户可以为具有相同网络流量控制的子网关联同一个网络 ACL，通过设置出站和入站允许规则，对进出子网的流量进行精确控制。例如，您在腾讯云私有网关内托管多层 Web 应用，创建了不同子网分别部署 Web 层、逻辑层和数据层服务，通过网络 ACL 您可以控制这三个子网之间的访问：Web 层子网和数据库层子网无法相互访问，只有逻辑层可以访问 Web 层和数据层子网。

ACL规则

ACL 规则是网络 ACL 的组成部分。当您在网络 ACL 中添加或删除规则时，更改也会自动应用到与其相关联的子网。
网络 ACL 规则包括以下四个组成部分：

- 协议类型，如 TCP、UDP 和 HTTP 等。
- 目的端口或端口范围。
- 源数据（入站）或目标数据（出站）的 IP 或者 IP 范围（以 CIDR 表示）。
- 策略：允许或拒绝。

腾讯云根据与子网关联的 ACL 入站/出站规则评估数据包，判断数据包是否允许流向/流出子网。

规则优先级

网络 ACL 规则的应用顺序保持由规则第一条（列表顶端）开始应用至最后一条（列表末尾）。若有规则/部分规则冲突，默认应用 ***位置更前*** 的规则。
例如，需要允许所有源 IP 对云服务器所有端口进行访问，同时唯一拒绝源 IP 为 `192.168.200.11/24` 的机器 HTTP 访问 80 端口。则可按以下方式设置：

协议类型	端口	源IP	策略
HTTP	80	192.168.200.11/24	拒绝
ALL	ALL	0.0.0.0/0	允许

临时端口范围

临时端口是客户端发起请求时配置的端口，设置网络 ACL 出站规则时需注意这点。由于网络 ACL 无状态的特性，即使设置入站规则允许某些访问，如果没有设置相应的出站规则会导致无法响应访问。

例如：某客户端向 VPC 内某子网中主机发起请求，该子网关联了网络 ACL。客户端默认配置的端口属于临时端口范围。如果网络 ACL 出站规则中没有设置允许对应临时端口的流量，那么客户端的请求将无法返回。根据客户端的操作系统不同，临时端口范围也随之不同。

- 许多 Linux 内核使用端口 32768-61000
- Windows Server 2003 使用端口 1025-5000
- Windows Server 2008 使用端口 49152-65535

因此，如果一项来自 Internet 上的 Windows XP 客户端的请求访问您的 VPC 内某子网的 Web 服务器，该子网关联了网络 ACL，则您的网络 ACL 必须有相应的出站规则，允许目标端口为 1025-5000 的数据流通过。

安全组与网络ACL的区别

安全组	网络ACL
CVM 实例级别的流量控制（第一防御层）	子网级别的流量控制（第二防御层）
支持允许规则和拒绝规则	支持允许规则和拒绝规则
有状态：返回数据流会被自动允许，不受任何规则的影响	无状态：返回数据流必须被规则明确允许
只有在启动 CVM 实例的同时指定安全组、或稍后将安全组与实例关联的情况下，操作才会被应用到实例	自动应用到关联子网内的所有 CVM 实例（备份防御层，若CVM 实例为绑定安全组，这里可以做备份防御）

使用约束

关于网络 ACL 您需要了解：

- 一个网络 ACL 可以绑定多个子网，但一个子网同一时间只能绑定一个网络 ACL。
- 网络 ACL 有单独的入站和出站规则，每条规则包括协议类型、端口、源/目的 IP，策略（拒绝/允许）和备注。
- 每个新建网络 ACL 最初都为关闭状态（不允许任何数据流），直至您添加规则为止。
- 网络 ACL 没有任何状态，对允许入站数据流的响应会随着出站数据流规则的变化而改变（反之亦然），亦即您需要分别对请求和响应数据流设置规则。
- 网络 ACL 对所关联子网内的 CVM 实例之间的互访不产生影响。

资源	限制（个）
每个私有网络内网络ACL数	50
每个网络ACL中规则数	入站方向：20条，出站方向：20条
每个子网关联的网络ACL个数	1
每个网络ACL关联的子网个数	无限制

计费方式

网络 ACL 服务免费。有关私有网络的其他服务费用，可以参考 VPC 所有服务计费总览

操作指南

创建网络 ACL

1) 登录腾讯云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】-【网络 ACL】选项卡。
2) 单击【新建】按钮，在新建网络 ACL 弹出框中输入名称、选择所属的私有网络，单击确定完成。

查看网络 ACL 列表

1) 登录腾讯云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】-【网络 ACL】选项卡。
2) 在顶部选择地域及私有网络，即可查看属于此私有网络的网络 ACL 列表。

增加网络 ACL 规则

1) 登录腾讯云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】-【网络 ACL】选项卡。
2) 在列表中单击要修改的网络 ACL 的 ID，进入网络 ACL 详情页。
3) 单击【入站规则】或【出站规则】选项卡，在规则列表旁单击【编辑】按钮，在编辑状态下单击【新增一行】按钮。
4) 新增的规则会默认加入规则列表的 ***首行***，选择协议类型并输入端口、源 IP/目的 IP和策略，单击【保存】按钮。新增的规则即会显示在 ACL 规则列表中。

删除网络 ACL 规则

1) 登录腾讯云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】-【网络 ACL】选项卡。
2) 在列表中单击要修改的网络 ACL 的 ID，进入网络 ACL 详情页。
3) 单击【入站规则】或【出站规则】选项卡，在规则列表旁单击【编辑】按钮，在编辑状态下单击 ACL 规则后方的【删除】按钮。
4) 此时本条 ACL 规则置灰。若本次删除属于误操作，则可通过单击【恢复删除】按钮将其恢复。
5) 单击【保存】按钮，保存上述操作。

> 注：ACL规则的删除必须保存后才会生效。

子网关联网络 ACL

1) 登录腾讯云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】-【网络ACL】选项卡。
2) 单击需要关联的网络 ACL 的 ID，进入网络 ACL 详情页。
3) 单击【基本信息】选项卡，在关联子网部分单击【新增关联】按钮。
4) 在关联子网弹出框中，选择需要关联的本私有网络下的子网，单击【确定】按钮，即可成功关联网络 ACL 与子网。

子网解关联网络 ACL

1) 登录腾讯云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】-【网络 ACL】选项卡。
2) 单击需要解关联的网络 ACL 的 ID，进入网络 ACL 详情页。
3) 单击【基本信息】选项卡，在关联子网列表中需要解关联的子网项后单击【解绑】按钮；或勾选所有需要解绑的子网，单击【批量解绑】按钮，即可解绑该子网与网络 ACL。

删除网络 ACL

1) 登录腾讯云控制台单击导航条【私有网络】，进入私有网络控制台，左侧选择【安全】-【网络ACL】选项卡。
2) 单击需要删除的网络 ACL 的【删除】按钮，在确认删除弹出框中单击【确定】，即可删除本网络 ACL 及本网络 ACL 的所有规则。
3) 若【删除】按钮置灰，则表示本网络 ACL 正与子网相关联，您需要先解除这些关联后才能进行删除操作。

API 概览

您可以使用 API 操作来设置和管理网络 ACL 相关接口，有关 VPC API的更多功能可以查看 VPC 所有 API 概览。

接口功能	Action ID	功能描述
创建VPC网络ACL	CreateNetworkAcl	创建安全防火墙。
删除网络ACL	DeleteNetworkAcl	删除指定安全防火墙。
修改网络ACL名称	ModifyNetworkAcl	修改安全防火墙名称。
查询网络ACL列表	DescribeNetworkAcl	查询vpc安全防火墙列表。
设置网络ACL规则	ModifyNetworkAclEntry	设置安全防火墙网络规则。
网络ACL绑定子网	CreateSubnetAclRule	安全防火墙绑定子网。
网络ACL解绑子网	DeteleSubnetAclRule	安全防火墙和子网解绑。

访问控制

概述

最近更新时间：2018-06-19 11:32:03

如果您中使用到了私有网络（VPC）、云服务器、数据库等服务，这些服务由不同的人管理，但都共享您的云账号密钥，将存在以下问题：

- 您的密钥由多人共享，泄密风险高；
- 您无法限制其它人的访问权限，易产生误操作造成安全风险。

访问控制（CAM）用于管理腾讯云账户下资源访问权限，通过CAM，您可以通过身份管理和策略管理控制哪些子账号有哪些资源的操作权限。

例如，您的账户下有多个VPC分布部署不同项目的服务，为了加强网络安全控制，您可以给项目A的网络管理员绑定一个授权策略，该策略规定：只有该网络管理员可操作项目A所在的VPC资源。

如果您不需要对子账户进行VPC相关资源的访问控制，您可以跳过此章节。跳过这些部分并不影响您对文档中其余部分的理解和使用.

CAM 基本概念

根账户通过给子账户绑定策略实现授权，策略设置可精确到**[API，资源，用户/用户组，允许/拒绝，条件]**维度。

1、 账户

- **根账号**：腾讯云资源归属、资源使用计量计费的基本主体，可登录腾讯云服务。
- **子账号**：由根账号创建账号，有确定的身份ID和身份凭证，且能登录到腾讯云控制台。根账号可以创建多个子账号(用户)。**子账号默认不拥有资源，必须由所属根账号进行授权。**
- **身份凭证**：包括登录凭证和访问证书两种，**登录凭证**是指用户登录名和密码，**访问证书**是指云API密钥(SecretId和SecretKey)。

2、资源与权限

- **资源**：资源是云服务中被操作的对象，如一个云服务器实例，COS存储桶，VPC实例等。
- **权限**：权限是指允许或拒绝某些用户执行某些操作。默认情况下，**根账号拥有其名下所有资源的访问权限**，而**子账号没有根账号下任何资源的访问权限。**
- **策略**：策略是定义和描述一条或多条权限的语法规范。**根账号**通过将**策略关联**到用户/用户组完成授权。
  单击查看更多CAM介绍

相关文档

目标	链接
了解策略和用户之间关系	策略管理
了解策略的基本结构	策略语法
了解还有哪些产品支持CAM	支持CAM的云服务列表

VPC访问控制策略示例

最近更新时间：2018-08-24 15:53:59

VPC 的全读写策略

以下策略允许用户创建和管理 VPC。可向一组网络管理员关联此策略。Action 元素指定所有VPC相关API。

```
{
"version": "2.0",
"statement": [
{
"action": [
"name/vpc:*"
],
"resource": "*",
"effect": "allow"
}
]
}
```

VPC 的只读策略

以下策略允许用户查询您的 VPC 及相关资源。但用户无法创建、更新或删除它们。
在控制台，操作一个资源的前提是可以查看该资源，所以建议您为用户开通VPC全读权限。

```
{
"version": "2.0",
"statement": [
{
"action": [
"name/vpc:Describe*",
"name/vpc:Inquiry*",
"name/vpc:Get*"
],
"resource": "*",
"effect": "allow"
}
]
}
```

只允许某子账号管理某VPC A及部署在A的网络资源,但不允许该用户管理其它VPC

以下策略允许用户看到所有VPC，但只能操作VPC A（假设A的Id是vpc-d08sl2zr）及 A下的网络资源（如子网、路由表等，不包括云服务器、数据库等）。
该版本不支持***只让用户看到A***,后续版本会支持

```
{
"version": "2.0",
"statement": [
{
"action": "name/vpc:*",
"resource": "*",
"effect": "allow",
"condition": {
"string_equal_if_exist": {
"vpc:vpc": [
"vpc-d08sl2zr"
],
"vpc:accepter_vpc": [
"vpc-d08sl2zr"
],
"vpc:requester_vpc": [
"vpc-d08sl2zr"
]
}
}
}
}
```

```
]
}
```

允许用户管理VPC,但是不允许用户操作路由表

以下策略允许用户读写VPC及其相关资源，但是不允许用户对路由表进行相关操作。

```
{
"version": "2.0",
"statement": [
{
"action": [
"name/vpc:*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"name/vpc:AssociateRouteTable",
"name/vpc:CreateRoute",
"name/vpc:CreateRouteTable",
"name/vpc:DeleteRoute",
"name/vpc:DeleteRouteTable",
"name/vpc:ModifyRouteTableAttribute"
],
"resource": "*",
"effect": "deny"
}
]
}
```

允许用户管理VPN资源

该策略允许用户查看所有VPC资源，但只允许其对VPN进行增、删、改、查操作。

```
{
"version": "2.0",
"statement": [
{
"action": [
"name/vpc:Describe*",
"name/vpc:Inquiry*",
"name/vpc:Get*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"name/vpc:*Vpn*",
"name/vpc:*UserGw*"
],
"resource": "*",
"effect": "allow"
}
]
}
```

VPC API操作支持的资源级权限

最近更新时间：2018-06-19 11:34:34

在CAM中，可对私有网络资源进行以下API操作的授权， 具体API支持的资源和条件的对应关系如下：

重要：在表格中没有出现VPC API不支持资源级权限，但您可向用户授予使用不在该列表中的VPC API，但是必须为策略语句的资源元素指定： *。

API 操作	资源	条件	备注
AcceptVpcPeeringConnection	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示域。
	对等连接资源 qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:region vpc:requester_vpc	vpc:accepter_v VPC，取值为接 vpc:requester_ 起方VPC，取值 VPC； vpc:region表示域。
	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId(接收方vpcId)	vpc:region	vpc:region表示域。
AcceptVpcPeeringConnectionEx	对等连接资源 qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:accepter_vpc_region vpc:requester_vpc vpc:requester_vpc_region	vpc:accepter_v VPC，取值为接 vpc:accepter_v 表示接收方地域 vpc:requester_ 起方VPC，取值 VPC； vpc:requester_ 表示发起方地域
	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示域。
AddVpnConnEx	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示域。
	vpn网关资源 qcs::vpc:$region:$account:vpngw/* qcs::vpc:$region:$account:vpngw/$vpnGwId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
	对端网关资源 qcs::vpc:$region:$account:cgw/*	vpc:region	vpc:region表示域。
	vpn通道资源 qcs::vpc:$region:$account:vpnx/*	vpc:vpc vpc:vpngw vpc:region	vpc:vpc表示开发 vpc:vpngw表示 的vpn网关 vpc:region表示域。
AssignPrivateIpAddresses	弹性网卡资源 qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc:vpc表示开发 vpc:subnet表示 的子网 vpc:region表示域。
AssociateVip	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:vpc vpc:region
AssociateRouteTable	子网资源 qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。

	路由表资源 qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
AttachClassicLinkVpc	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示 域。
	云服务器资源 qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region	cvm:region表示 所在地域。
AttachNetworkInterface	弹性网卡资源 qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc:vpc表示开发 vpc:subnet表示 的子网 vpc:region表示 域。
	云服务器资源 qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region	cvm:region表示 所在地域 。
CreateAndAttachNetworkInterface	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示 域。
	云服务器资源 qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region	cvm:region表示 所在地域 。
	弹性网卡资源 qcs::vpc:$region:$account:eni/*	vpc:vpc vpc:subnet vpc:region	vpc:vpc表示开发 vpc:subnet表示 的子网 vpc:region表示 域。
CreateDirectConnectGateway	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示 域。
	专线网关资源 qcs::vpc:$region:$account:dcg/*	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreateLocalDestinationIPPortTranslationNatRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreateLocalIPTranslationAclRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreateLocalIPTranslationNatRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreateLocalSourceIPPortTranslationAclRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreateLocalSourceIPPortTranslationNatRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreatePeerIPTranslationNatRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreateNatGateway	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示 域。

	nat网关资源 qcs::vpc:$region:$account:nat/*	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreateNetworkAcl	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示 域。
	网络acl资源 qcs::vpc:$region:$account:acl/*	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreateNetworkInterface	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示 域。
	子网资源 qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
	弹性网卡资源 qcs::vpc:$region:$account:eni/*	vpc:vpc vpc:subnet vpc:region	vpc:vpc表示开发 vpc:subnet表示 网 vpc:region表示 域。
CreateRoute	路由表资源 qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreateRouteTable	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示 域。
	路由表资源 qcs::vpc:$region:$account:rtb/*	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreateSubnet	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示 域。
	子网网关资源 qcs::vpc:$region:$account:subnet/*	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreateSubnetAclRule	网络acl资源 qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
	子网网关资源 qcs::vpc:$region:$account:subnet/*	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
CreateVpcPeeringConnection	vpc资源(发起方) qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示 域。
	对等连接资源 qcs::vpc:$region:$account:pcx/*	vpc:accepter_vpc vpc:requester_vpc vpc:region	vpc:accepter_v VPC，取值为接 vpc:requester_ 起方VPC，取值 VPC； vpc:region表示 域。
CreateVpcPeeringConnectionEx	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示 域。
	对等连接资源	vpc:accepter_vpc	vpc:accepter_v

	qcs::vpc:$region:$account:pcx/*	vpc:accepter_vpc_region vpc:requester_vpc vpc:requester_vpc_region	VPC，取值为接 vpc:accepter_v 表示接收方地域 vpc:requester_ 起方VPC，取值 VPC； vpc:requester_ 表示发起方地域
DeleteDirectConnectGateway	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
DeleteLocalDestinationIPPortTranslationNatRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
DeleteLocalIPTranslationAclRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
DeleteLocalIPTranslationNatRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
DeleteLocalSourceIPPortTranslationAclRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
DeletePeerIPTranslationNatRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
DeleteLocalSourceIPPortTranslationNatRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
DeleteNatGateway	nat网关资源 qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/$natId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
DeleteNetworkAcl	网络acl资源 qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
DeleteNetworkInterface	弹性网卡资源 qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc:vpc表示开发 vpc:subnet表示 的子网 vpc:region表示 域。
DeleteRoute	路由表资源 qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
DeleteRouteTable	路由表资源 qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
DeleteSubnet	子网资源 qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
DeleteUserGw	对端网关资源 qcs::vpc:$region:$account:cgw/* qcs::vpc:$region:$account:cgw/$userGwId	vpc:region	vpc:region表示 域。
DeleteVpc	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region vpc:vpc	vpc:region表示 域。

DeleteVpcPeeringConnection	对等连接资源 qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:region vpc:requester_vpc	vpc:accepter_v VPC，取值为接 vpc:requester_ 起方VPC，取值 VPC； vpc:region表示 域。
DeleteVpcPeeringConnectionEx	对等连接资源 qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:accepter_vpc_region vpc:requester_vpc vpc:requester_vpc_region	vpc:accepter_v VPC，取值为接 vpc:accepter_v 表示接收方地域 vpc:requester_ 起方VPC，取值 VPC； vpc:requester_ 表示发起方地域
DeleteVpnConn	vpn通道资源 qcs::vpc:$region:$account:vpnx/* qcs::vpc:$region:$account:vpnx/$vpnConnId	vpc:vpc vpc:vpngw vpc:usergw vpc:region	vpc:vpc表示开发 vpc:vpngw表示 的网关 vpc:usergw表示 的对端网关 vpc:region表示 域。
DetachClassicLinkVpc	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region vpc:vpc	vpc:region表示 域。
	云服务器资源 qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region	cvm:region表示 所在地域 。
DetachNetworkInterface	云服务器资源 qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region	cvm:region表示 所在地域 。
	弹性网卡资源 qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc:vpc表示开发 vpc:subnet表示 的子网 vpc:region表示 域。
DeteleSubnetAclRule	子网资源 qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
	网络acl资源 qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
EipBindNatGateway	nat网关资源 qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/$natId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
EipUnBindNatGateway	nat网关资源 qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/$natId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
EnableVpcPeeringConnection	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示 域。
	对等连接资源 qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:region vpc:requester_vpc	vpc:accepter_v VPC，取值为接 vpc:requester_ 起方VPC，取值 VPC；

			vpc:region表示域。
EnableVpcPeeringConnectionEx	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示域。
	对等连接资源 qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:accepter_vpc_region vpc:requester_vpc vpc:requester_vpc_region	vpc:accepter_v VPC，取值为接 vpc:accepter_v 表示接收方地域 vpc:requester_ 起方VPC，取值 VPC； vpc:requester_ 表示发起方地域
MigrateNetworkInterface	弹性网卡资源 qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc:vpc表示开发 vpc:subnet表示 的子网 vpc:region表示域。
	云服务器资源 qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId(迁移前后的都需要授权)	cvm:region	cvm:region表示所在地域 。
MigratePrivateIpAddress	弹性网卡资源 qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc:vpc表示开发 vpc:subnet表示 的子网 vpc:region表示域。
ModifyDirectConnectGateway	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
ModifyLocalDestinationIPPortTranslationNatRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
ModifyLocalIPTranslationAclRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
ModifyLocalIPTranslationNatRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
ModifyLocalSourceIPPortTranslationAclRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
ModifyPeerIPTranslationNatRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
ModifyLocalSourceIPPortTranslationNatRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
ModifyNatGateway	nat网关资源 qcs::vpc:$region:$account:nat/* qcs::vpc:$region:$account:nat/nat-dc7cdf	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
ModifyNetworkAcl	网络acl资源 qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
ModifyNetworkAclEntry	网络acl资源	vpc:vpc	vpc:vpc表示开发

	qcs::vpc:$region:$account:acl/* qcs::vpc:$region:$account:acl/$networkAclId	vpc:region	vpc:region表示域。
ModifyNetworkInterface	弹性网卡资源 qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc:vpc表示开发 vpc:subnet表示 的子网 vpc:region表示域。
ModifyPrivateIpAddress	弹性网卡资源 qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc:vpc表示开发 vpc:subnet表示 的子网 vpc:region表示域。
ModifyRouteTableAttribute	路由表资源 qcs::vpc:$region:$account:rtb/* qcs::vpc:$region:$account:rtb/$routeTableId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
ModifySubnetAttribute	子网资源 qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
ModifyUserGw	对端网关资源 qcs::vpc:$region:$account:cgw/* qcs::vpc:$region:$account:cgw/$userGwId	vpc:region	vpc:region表示域。
ModifyVpcAttribute	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:Region	vpc:region表示域。
ModifyVpcPeeringConnection	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示域。
	对等连接资源 qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:region vpc:requester_vpc	vpc:accepter_v VPC，取值为接 vpc:requester_ 起方VPC，取值 VPC； vpc:region表示域。
ModifyVpcPeeringConnectionEx	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示域。
	对等连接资源 qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:accepter_vpc_region vpc:requester_vpc vpc:requester_vpc_region	vpc:accepter_v VPC，取值为接 vpc:accepter_v 表示接收方地域 vpc:requester_ 起方VPC，取值 VPC； vpc:requester_ 表示发起方地域
ModifyVpnConnEx	vpn通道资源 qcs::vpc:$region:$account:vpnx/* qcs::vpc:$region:$account:vpnx/$vpnConnId	vpc:vpc vpc:vpngw vpc:usergw vpc:region	vpc:vpc表示开发 vpc:vpngw表示 的网关 vpc:usergw表示 的对端网关 vpc:region表示域。
ModifyVpnGw	vpn网关资源 qcs::vpc:$region:$account:vpngw/* qcs::vpc:$region:$account:vpngw/$vpnGwId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示域。
RejectVpcPeeringConnection	vpc资源 qcs::vpc:$region:$account:vpc/*	vpc:region	vpc:region表示域。

	qcs::vpc:$region:$account:vpc/$vpcId		
	对等连接资源 qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:region vpc:requester_vpc	vpc:accepter_v VPC，取值为接 vpc:requester_ 起方VPC，取值 VPC； vpc:region表示 域。
RejectVpcPeeringConnectionEx	vpc资源 qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	vpc:region	vpc:region表示 域。
	对等连接资源 qcs::vpc:$region:$account:pcx/* qcs::vpc:$region:$account:pcx/$peeringConnectionId	vpc:accepter_vpc vpc:accepter_vpc_region vpc:requester_vpc vpc:requester_vpc_region	vpc:accepter_v VPC，取值为接 vpc:accepter_v 表示接收方地域 vpc:requester_ 起方VPC，取值 VPC； vpc:requester_ 表示发起方地域
ResetVpnConnSA	vpn通道资源 qcs::vpc:$region:$account:vpnx/* qcs::vpc:$region:$account:vpnx/$vpnConnId	vpc:vpc vpc:vpngw vpc:usergw vpc:region	vpc:vpc表示开发 vpc:vpngw表示 的网关 vpc:usergw表示 的对端网关 vpc:region表示 域。
SetLocalIPTranslationAclRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
SetLocalSourceIPPortTranslationAclRule	专线网关资源 qcs::vpc:$region:$account:dcg/* qcs::vpc:$region:$account:dcg/$directConnectGatewayId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
SetSSLVpnDomain	vpn网关资源 qcs::vpc:$region:$account:vpngw/* qcs::vpc:$region:$account:vpngw/$vpnGwId	vpc:vpc vpc:region	vpc:vpc表示开发 vpc:region表示 域。
UnassignPrivateIpAddresses	弹性网卡资源 qcs::vpc:$region:$account:eni/* qcs::vpc:$region:$account:eni/$networkInterfaceId	vpc:vpc vpc:subnet vpc:region	vpc:vpc表示开发 vpc:subnet表示 的子网 vpc:region表示 域。

参数模板

最近更新时间：2018-06-19 11:35:50

简介

参数模板是一组参数的集合，支持 IP 地址和协议端口两类，可被安全组规则引用，主要用于统一管理安全组规则的 IP 或协议端口组。

参数模板类型：

- IP 地址 (ipm) ：支持单个 IP、CIDR、IP 范围。
- IP 地址组 (ipmg)：多个 IP 地址对象集合。
- 协议端口 (ppm)：支持单个端口、多个端口、连续端口及所有端口，协议支持：TCP、UDP、ICMP、GRE 协议。
- 协议端口组 (ppmg) ：多个协议端口对象集合。

使用场景

参数模板主要用于统一管理 IP/协议端口，常用场景如下：
1、统一管理具有**相同**诉求的 IP/协议端口组
2、统一管理具有**频繁编辑**诉求的 IP/协议端口组
例如：某银行只允许第三方已指定公网 IP 访问某些云服务器。
step1：创建一个 IP 地址对象，将指定公网 IP 加入该 IP 地址对象中。
step2：在这些云服务器绑定的安全组上增加一条规则，允许源地址为该 IP 地址对象的访问。
step3：如果需要增加新的第三方公网 IP 时，只需往该 IP 地址组中增加 IP 即可，无需修改安全组规则或者新建安全组。

如果不使用参数模板功能，则需要重复多次编辑安全组规则，管理麻烦，易遗留、易出错。

使用约束

配额如下表所示，您还可以查看 VPC 其它产品的 使用约束。

实例	配额
IP 地址对象 (ipm)	每个租户上限 1000
IP 地址组对象 (ipmg)	每个租户上限 1000
协议端口对象 (ppm)	每个租户上限 1000
协议端口组对象 (ppmg)	每个租户上限 1000
IP 地址对象 (ipm) 内的 IP 地址成员	每个租户上限 20
IP 地址组对象 (ipmg)内的 IP 地址对象成员 (ipm)	每个租户上限 20
协议端组对象 (ppm)内的协议端口成员	每个租户上限 20
协议端口组对象 (ppmg)内的协议端口对象成员 (ppm)	每个租户上限 20
IP 地址对象 (ipm) 可被多少个 IP 地址组对象 (ipmg)引用	每个租户上限 50
协议端口对象 (ppm)可被多少个协议端口组对象 (ppmg)引用	每个租户上限 50

注：参数模板可被安全组引用，其功能类似于把参数模板展开成多条安全组规则，展开后，每个安全组规则条目数不能超过 512。

计费模式

免费，有关私有网络服务的更多价格信息，可以查看 私有网络价格总览。

操作指南

创建 IP 地址

1) 登录腾讯云控制台单击导航条【私有网络】，进入私有网络控制台，选择【安全】-【参数模板】-【IP地址】
2) 单击【新建】填写IP地址。
3) 单击【完成】，即可完成创建。

创建端口协议

1) 登录腾讯云控制台单击导航条【私有网络】，进入私有网络控制台，选择【安全】-【参数模板】-【端口协议】
2) 单击【新建】填写端口协议。
3) 单击【完成】，即可完成创建。

在安全组中引用参数模板

1) 打开云服务器 CVM 控制台-选择【安全组】。
2) 单击指定安全组 ID，选择入/出规则，在源/目的，端口协议内选择对应的参数模板。