VPN 连接

最佳实践

腾讯云

文档目录

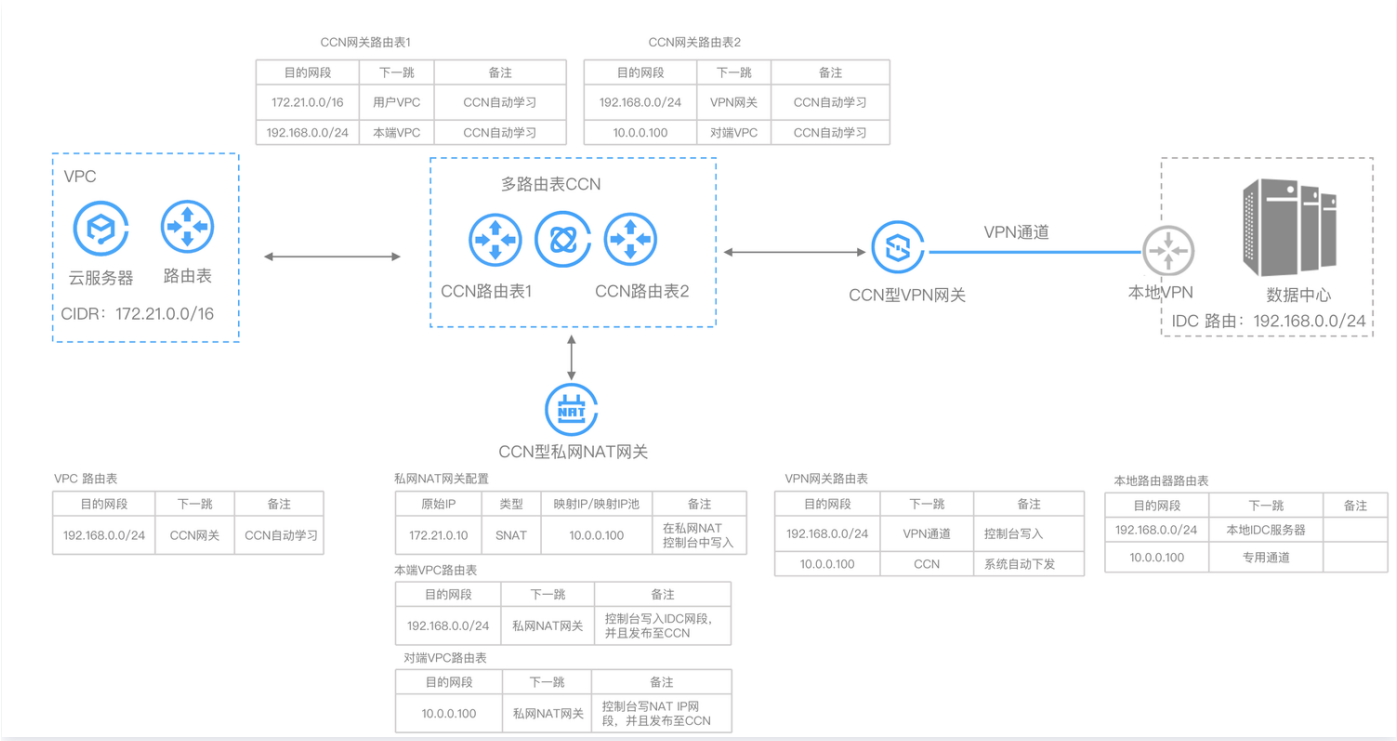
最佳实践
IPsec VPN
通过 VPN + CCN + NAT 解决 IDC 访问与云上资源网段冲突

最近更新时间：2024-01-24 11:57:12

使用 VPN 打通 IDC/第三方云商和腾讯云进行资源互访，通常会出现 IP 冲突问题，重新规划网段耗时耗力。本文指导您通过 VPN + CCN 多路由表 + 私有 NAT 网关解决该问题。

业务场景

用户使用 VPN 打通腾讯云和客户远程 IDC /第三方云商，实现资源访问，同时期望指定访问 IP 地址并无 IP 冲突，可以通过私网 VPN + NAT + CCN 方案来实现。



操作流程

1. 创建支持多路由表的 CCN 实例，并绑定 VPC 实例。
2. 创建 CCN 型私网 NAT 实例，并完成规则设置。
3. 配置本端/对端 VPC 路由，并发布到 CCN。
4. 配置 NAT IP 映射规则。
5. 创建 CCN 型 VPN 网关及其资源，并关联与 CCN 实例。

前提条件

- 已开启 CCN 多路由表，如需开通，请 提交工单 。
- 已开启私网 NAT 网关特性，如需开通，请 提交工单 。

操作步骤

步骤一：创建 CCN 实例，并关联业务 VPC

1. 登录 云联网控制台，单击**新建**，并关联业务 VPC，详情可参见 新建云联网实例 。

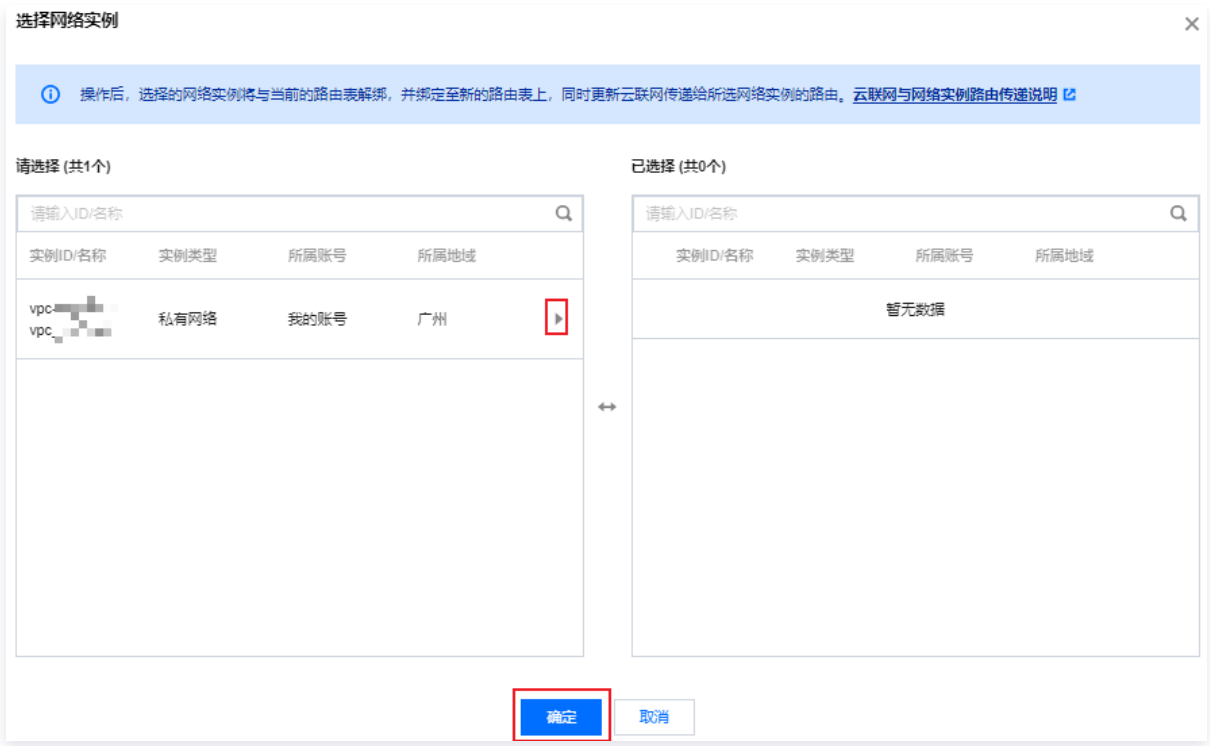
2. 在 CCN 实例列表页面，单击已创建好的**云联网 ID**，然后在 CCN 实例详情页的**路由表**页签，单击**新建路由表**创建两个 CCN 路由表。

> **说明**
> 请确保您已开启 CCN 多路由表功能，如未开启，请 提交工单 开通。

3. 将业务 VPC 添加至 CCN 网路由表1。

   3.1 在左侧 CCN 路由表列表中选择路由表1，单击**绑定实例**将业务 VPC 实例绑定。

3.2 在**路由接收策略**页签，单击**添加网络实例**，然后在**选择网络实例**页面，选择业务 VPC 实例并单击**确定**。



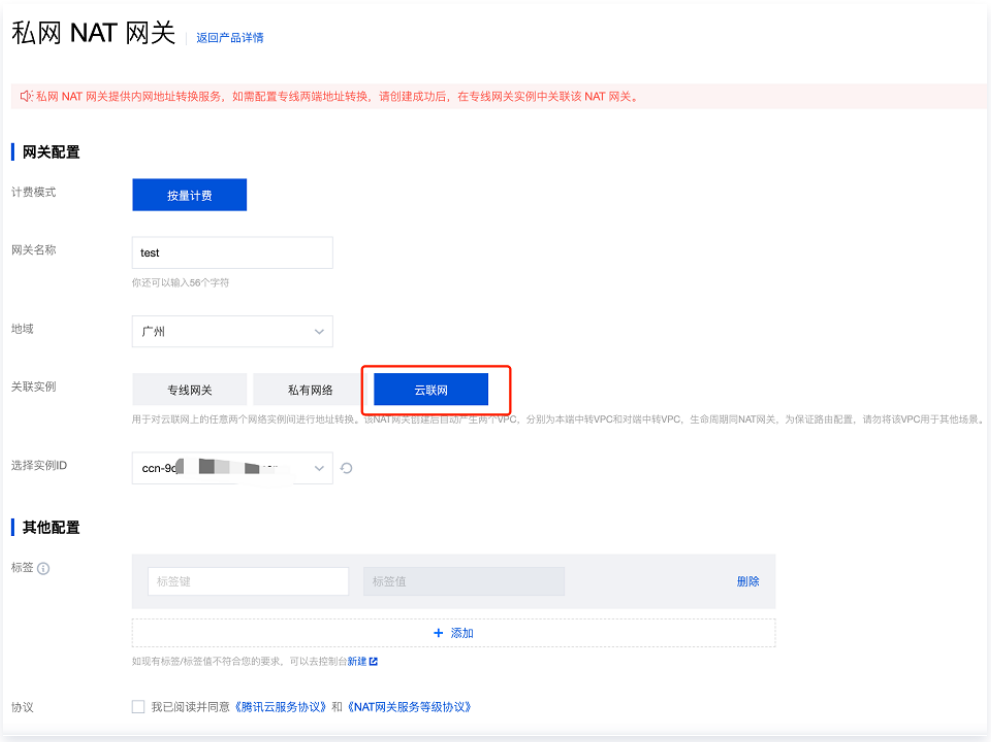
添加完成如下：

步骤二：创建 CCN 型私网 NAT，并添加至 CCN 多路由表。

本步骤您需要在 NAT 侧创建 CCN 型私网 NAT 实例，并将私网 NAT 的附属 VPC 关联到云联网多路由表中。

1. 登录 私网 NAT 网关控制台，在页面上方选择地域和私有网络后，单击**新建**。
2. 在私网 NAT 购买页依据界面提示完成创建。创建成功后，自动展示本端 VPC 实例和对端 VPC 实例。

> **说明**
> 请确保已开启私网 NAT 功能，如未开启，请 提交工单 开通。



3. 在 云联网控制台 找到步骤一中创建的 CCN 实例，并在其详情页的**路由表**页签，将 NAT 实例的本端 VPC 绑定到 CCN 实例的路由表1中。

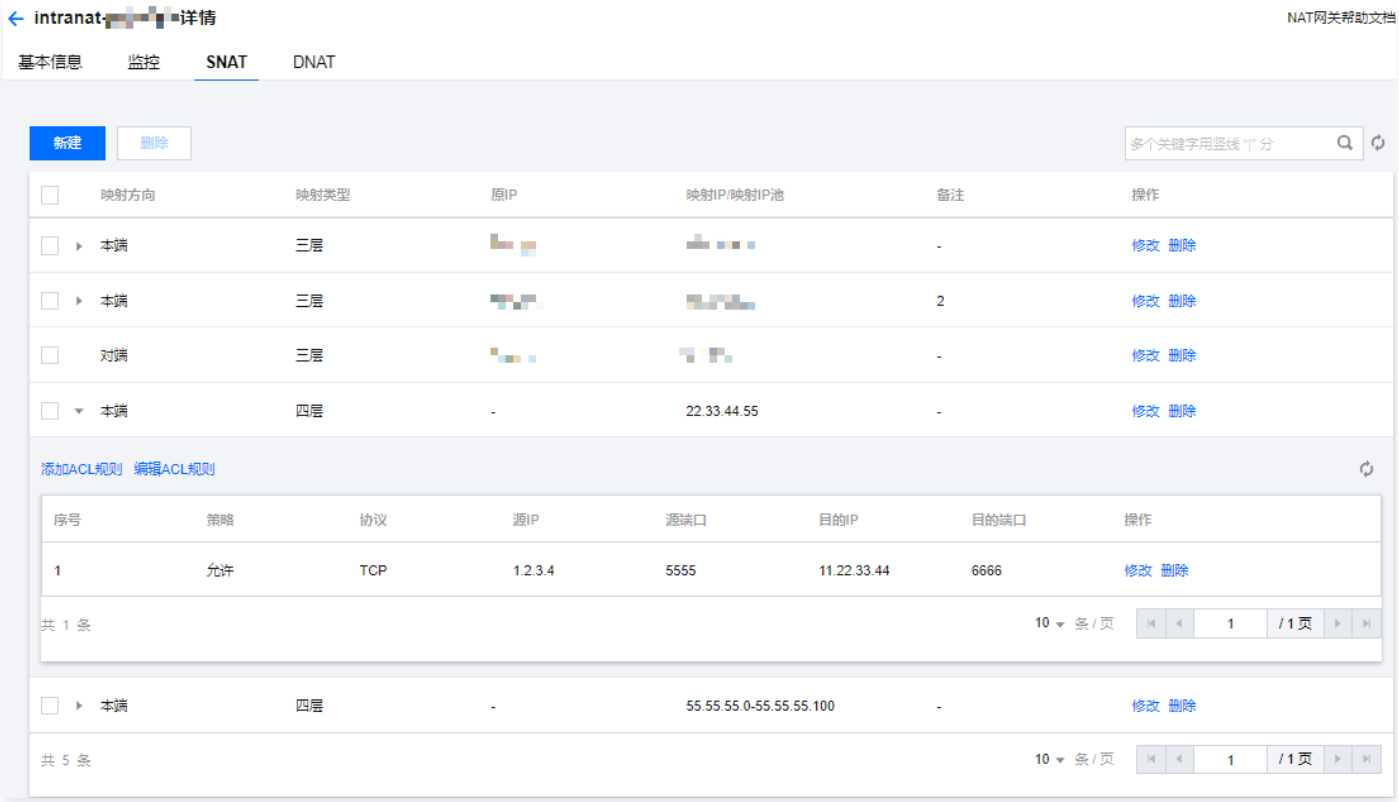
4. 在 CCN 路由表1中设置路由接收策略，详情请参见 步骤一的步骤3 。

5. 同理，将 NAT 实例的对端 VPC 绑定到 CCN 实例的路由表2中，并配置路由接收策略。

步骤三：配置 IP 映射规则

1. 在 私网 NAT 网关 实例详情页，单击 步骤二 中创建的私网 NAT 实例 ID，然后在其详情页单击 SNAT。
2. 在 SNAT 页签中，单击**新建**依据界面提示进行配置。本处以本端四层规则为例。

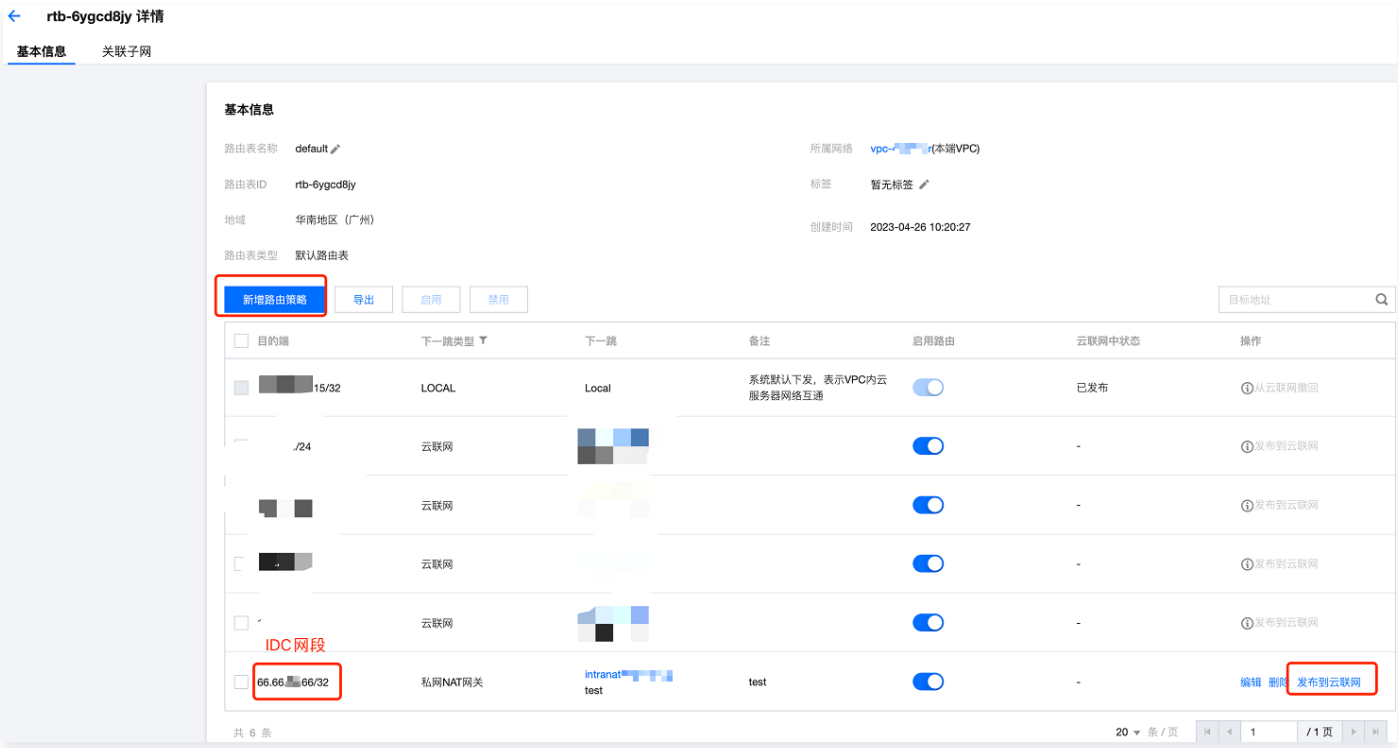
> **说明：**
> 当映射类型为四层时，必须配置添加 ACL 规则，详情可参见 规则概述 或者 提交工单 咨询。



步骤四：配置及发布 VPC 至 CCN 的路由策略

本步骤您需要在 VPC 侧配置本端/对端的 VPC 路由，并发布到云联网。

1. 登录 私有网络控制台，找到业务 VPC 并单击 **VPC实例**。
2. 在 VPC 实例详情页面，单击**路由表**，在本端 VPC 默认路由表的基本信息页，单击新增路由策略。
3. 在新增路由页面，配置目的端是 IDC 网段、下一跳类型为私网 NAT 网关。并且发布到云联网。

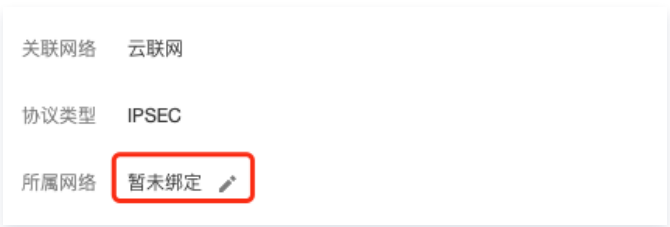


4. 同理，对端 VPC 默认路由表添加条目如下，目的端为 步骤三里的步骤2 中创建的 NAT 规则映射 IP 路由，下一跳为私网 NAT 网关，然后发布到云联网。

步骤五：创建 CCN 型 VPN 网关及其资源，并关联至 CCN 多路由表。

1. 登录 私有网络控制台，在左侧导航栏，单击 VPN 连接 > VPN 网关，选择地域和私有网络后，单击新建，关联网络选择“云联网”，依据界面提示，完成创建 CCN 型 VPN 网关。详细操作可参考 创建 VPN 网关 。

2. 在 VPN 网关详情页绑定 步骤一 创建的 CCN 实例。



3. 在 CCN 实例 > 路由表页签，将 VPN 网关加入云联网路由表2中，并绑定 VPN 网关实例，同时设置路由接收策略，详细操作可参考 步骤一中的步骤3 。

4. 在 VPN 侧 创建对端网关 和 创建 VPN 通道 。
5. （可选）发布路由至 CCN，仅当 VPN 通道为 SPD 策略型时，需要在 VPN 网关手动将路由发布至 CCN。
6. 在用户 IDC 侧配置防火墙或者本地 VPN。

通过专线接入（BGP路由）和 VPN 连接（静态路由）实现混合云主备冗余通信（自动切换）

最近更新时间：2024-04-23 16:00:01

当用户业务分别部署于云下数据中心和云上 VPC 中时，可通过专线接入或 VPN 连接实现云上云下业务互通，为提升业务高可用性，可同时创建专线接入和 VPN 连接服务，结合 CCN 配置两条链路为主备链路，来实现冗余通信。

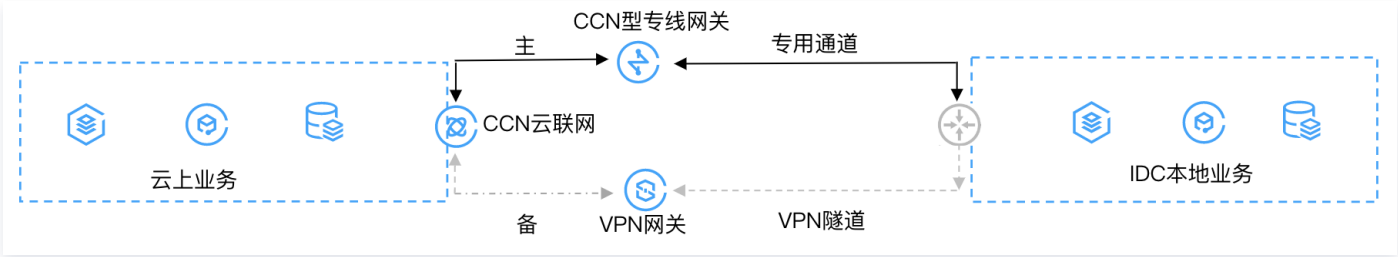
说明

- 路由优先级功能目前处于内测中，如有需要，请 在线咨询 。
- 暂不支持控制台修改路由优先级，如需调整，请 在线咨询 。
- 配置主备路由时，专线网段掩码长度须大于 VPN 网段掩码长度。

业务场景

如下图所示，用户在 VPC 和 IDC 中部署了业务，为了实现云上与云下业务交互，用户需要部署网络连接服务来实现业务互通，为实现高可用通信，故障时业务自动切换，部署方案如下：

- 专线接入（主）：本地 IDC 通过物理专线，接入CCN型的专线网关实现云下云上业务通信。在物理专线链路正常时，本地 IDC 与 VPC 之间所有的通信流量都通过物理专线进行转发。
- VPN 连接（备）：本地 IDC 与云上 VPC 通过建立 CCN 型 VPN 安全隧道来实现云上云下业务通信，当专线链路出现异常时，自动将流量切换至该链路，确保业务可用性。



前提条件

- 用户本地 IDC 网关设备具有 IPsec VPN 功能，可同时作为用户侧 VPN 网关设备，与云侧 VPN 设备建立 IPsec 隧道通信。
- 用户 IDC 侧网关设备已配置静态 IP。
- 已创建 CCN 实例，并开启了 ECMP 和路由重叠特性，详情联系 在线支持 。
- 专线侧已开启动态 BGP 传递特性，详情请联系 在线支持 。

操作步骤

步骤一：配置 IDC 通过专线接入上云

1. 登录 专线接入控制台，单击左侧导航栏的物理专线，单击**新建**，创建物理专线，详情可参见 申请接入物理专线 。
2. 单击左侧导航栏的专线网关，单击**新建**，创建 CCN 型专线网关，创建完成后在其详情发布指向 CCN 的网段，详细操作可参见 创建专线网关 、发布网段至云联网 。
3. 单击左侧导航栏的**专用通道** > **独享专用通道**，单击**新建**，创建独享专用通道，此处需要配置通道名称、选择专线类型、已创建的专线网关、腾讯云侧和用户侧的互联 IP、路由方式选择静态路由、填写 IDC 通信网段等，配置完成后下载配置指引并在 IDC 设备完成配置。详细操作可参见 独享专用通道 。

说明

更多详细配置可参考 IDC 通过云联网上云 。

步骤二：配置 IDC 通过 VPN 连接上云

1. 登录 VPN 网关控制台，单击**新建**，创建 CCN 型 VPN 网关可参见 创建 VPN 网关，创建完成后，在其详情页关联 CCN 实例，详细操作可参见 绑定云联网实例 。
2. 单击左侧导航栏的对端网关，配置对端网关（即 IDC 侧 VPN 网关的逻辑对象），填写 IDC 侧 VPN 网关的公网 IP 地址，例如202.xx.xx.5。详细操作可参见 创建对端网关 。
3. 单击左侧导航栏的 VPN 通道，单击**新建**，创建 VPN 通道，请页面引导配置 SPD 策略、IKE、IPsec 等参数。详细配置信息可参见 创建 VPN 通道 。
   在 IDC 本地网关设备上配置 VPN 通道信息，此处配置需要和 步骤3 中的 VPN 通道信息一致，否则 VPN 隧道无法正常连通。
   在网关的路由表页签配置指向对端网关的路由。

> **说明**
> 更多详细配置请参考 建立 IDC 到云联网的连接 。

步骤三：配置告警

为及时发现探测链路异常，可配置告警策略。当检测到链路异常时，告警信息将通过电子邮件和短信等形式发送到您，帮助您提前预警风险。

1. 登录腾讯云可观测平台的 告警策略控制台 。
2. 单击**新建**，填写策略名称、策略类型选择私有网络/网络探测，告警对象选择具体的网络探测实例，配置触发条件和告警通知等信息，并单击**完成**即可。

步骤四：切换主备路由

当收到专线网关主路径的网络探测异常告警时，自动会将您的流量切换至 VPN 网关备份路由上。

通过专线接入和 VPN 连接实现混合云主备冗余通信（手动切换）

最近更新时间：2023-06-06 15:34:43

当用户业务分别部署于云下数据中心和云上 VPC 中时，可通过专线接入或 VPN 连接实现云上云下业务互通，为提升业务高可用性，可同时创建专线接入和 VPN 连接服务，结合 VPC 路由优先级功能，配置两条链路为主备链路，来实现冗余通信。本文指导您如何配置专线和 VPC 主备链路来实现云上云下混合通信。

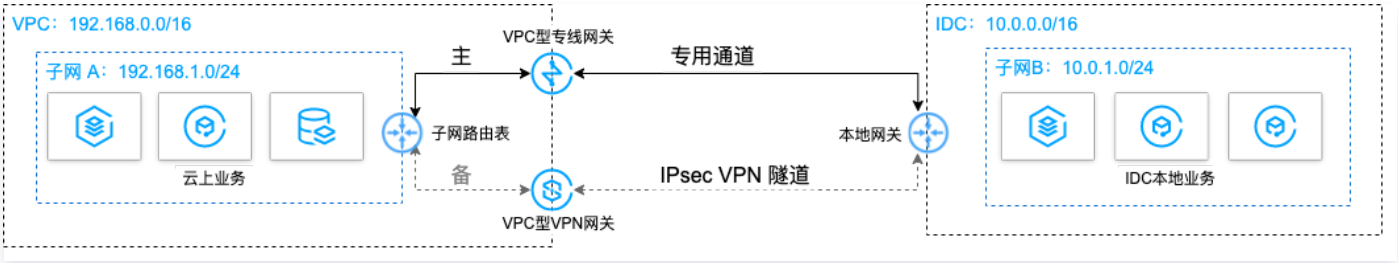
说明

- 路由优先级功能目前处于内测中，如有需要，请 在线咨询 。
- VPC 路由表中根据不同的下一跳类型定义了不同的优先级，目前默认路由优先级为：云联网 > 专线网关 > VPN 网关 > 其他。
- 暂不支持控制台修改路由优先级，如需调整，请 在线咨询 。
- 当故障发生后您需要在 VPC 手动切换路由，当前暂不支持自动切换。

业务场景

如下图所示，用户在 VPC 和 IDC 中部署了业务，为了实现云上与云下业务交互，用户需要部署网络连接服务来实现业务互通，为实现高可用通信，部署方案如下：

- 专线接入（主）：本地 IDC 通过物理专线，接入 VPC 的专线网关实现云下云上业务通信。在物理专线链路正常时，本地 IDC 与 VPC 之间所有的通信流量都通过物理专线进行转发。
- VPN 连接（备）：本地 IDC 与云上 VPC 通过建立 VPN 安全隧道来实现云上云下业务通信，当专线链路出现异常时，可将流量切换至该链路，确保业务可用性。



前提条件

- 用户本地 IDC 网关设备具有 IPsec VPN 功能，可同时作为用户侧 VPN 网关设备，与 VPC 侧 VPN 设备建立 IPsec 隧道通信。
- 用户 IDC 侧网关设备已配置静态 IP。
- 数据准备如下：

配置项			示例值
网络配置	VPC 信息	子网 CIDR	192.168.1.0/24
		VPN 网关公网 IP	203.xx.xx.82
	IDC 信息	子网 CIDR	10.0.1.0/24
		网关公网 IP	202.xx.xx.5

操作流程

1. 配置 IDC 通过专线接入上云
2. 配置 IDC 通过VPN连接上云

3. 配置网络探测
4. 配置告警
5. 切换主备路由

操作步骤

步骤一： 配置 IDC 通过专线接入上云

1. 登录 专线接入控制台，单击左侧导航栏的**物理专线**创建物理专线。
2. 单击左侧导航栏的**专线网关**创建专线网关，本例选择接入私有网络，标准型的专线网关，如果 IDC 和 VPC 通信网段冲突也可以选择 NAT 型。
3. 单击左侧导航栏的**独享专用通道**创建专用通道，此处需要配置通道名称、选择专线类型、已创建的专线网关、腾讯云侧和用户侧的互联 IP、路由方式选择静态路由、填写 IDC 通信网段等，配置完成后下载配置指引并在 IDC 设备完成配置。
4. 在 VPC 通信子网关联的路由表中配置下一跳为专线网关、目的端为 IDC 通信网段的路由策略。

> **说明**
> 更多详细配置可参考 专线接入快速入门 。

步骤二：配置 IDC 通过 VPN 连接上云

1. 登录 VPN 网关控制台 ，单击**新建**创建 VPN 网关，本例关联网络选择私有网络。
2. 单击左侧导航栏的**对端网关**，配置对端网关（即 IDC 侧 VPN 网关的逻辑对象），填写 IDC 侧 VPN 网关的公网 IP 地址，例如202.xx.xx.5。
3. 单击左侧导航栏的 **VPN 通道**，请配置 SPD 策略、IKE、IPsec 等配置。
4. 在 IDC 本地网关设备上配置 VPN 通道信息，此处配置需要和步骤3中的 VPN 通道信息一致，否则 VPN 隧道无法正常连通。
5. 在 VPC 通信子网关联的路由表中配置下一跳为 VPN 网关、目的端为 IDC 通信网段的路由策略。

> **说明**
> 更多详细配置请参考 建立 VPC 到 IDC 的连接（路由表） 。

步骤三：配置网络探测

> **说明**
> 如上两步配置完成后，VPC 去往 IDC 已经有两条路径，即下一跳为专线网关和 VPN 网关，根据路由默认优先级：专线网关 > VPN 网关，则专线网关为主路径，VPN 网关为备路径。

为了解主备路径的连接质量，需要分别配置两条路径的网络探测，实时监控到网络连接的时延、丢包率等关键指标，以探测主备路由的可用性。

1. 登录 网络探测控制台 。
2. 单击**新建**，创建网络探测，填写网络探测名称，选择私有网络、子网、探测目的IP，并指定源端下一跳路由，如专线网关。
3. 请再次执行 步骤2 ，指定源端下一跳路由为 VPN 网关。配置完成后，即可查看专线接入和 VPN 连接主备路径的网络探测时延和丢包率。

> **说明**
> 更多详细配置请参考 网络探测 。

步骤四：配置告警

为及时发现探测链路异常，可配置告警策略。当检测到链路异常时，告警信息将通过电子邮件和短信等形式发送到您，帮助您提前预警风险。

1. 登录腾讯云可观测平台下的 告警策略控制台 。
2. 单击**新建**，填写策略名称、策略类型选择**私有网络/网络探测**，告警对象选择具体的网络探测实例，配置触发条件和告警通知等信息，并单击**完成**即可。

步骤五：切换主备路由

当收到专线网关主路径的网络探测异常告警时，您需要手动禁用主路由，将流量切换至 VPN 网关备份路由上。

1. 登录 路由表控制台 。
2. 单击 VPC 通信子网关联路由表 ID，进入路由详情页，单击  禁用下一跳到专线网关的主路由，此时 VPC 去往 IDC 的流量将从专线网关切换至 VPN 网关。

建立 IDC 到云联网的连接

最近更新时间：2023-02-03 14:13:45

CCN 型 VPN 网关可以关联至云联网，实现 IDC 与云联网间的加密通信。本文介绍如何将 CCN 型 VPN 网关关联至云联网。

背景信息

CCN 类型的 VPN 网关可以关联至云联网，每个 CCN 型 VPN 网关可以建立多个 VPN 加密通道，每个 VPN 通道可以打通一个本地 IDC。

将 CCN 类型的 VPN 网关关联至云联网步骤如下：

1. 创建 CCN 型 VPN 网关：VPN 网关是云联网建立 VPN 连接的出口网关，与对端网关配合使用。
2. 关联云联网实例：将创建的 CCN 型 VPN 网关与云联网实例关联。
3. 创建对端网关：对端网关是用来记录 IDC 端的 IPsec VPN 网关公网 IP 地址的逻辑对象（IDC 端必须有固定公网 IP），需与腾讯云 VPN 网关配合使用，一个 VPN 网关可与多个对端网关建立加密的 VPN 网络通道。
4. 创建 VPN 通道： VPN 通道支持 IPsec 加密协议，用于保护数据传输的信息安全。
5. 配置 VPN 网关路由：VPN 通道配置成功后，需要配置 VPN 网关至对端网关的路由。
6. IDC本地配置：在 IDC 侧的“本地网关”上配置另一侧（腾讯云侧）的 VPN 通道信息。
7. 启用 IDC 网段：将 SPD 策略中的对端网段加入云联网中。

操作步骤

步骤一：创建 CCN 型 VPN 网关

1. 登录 私有网络控制台 。
2. 在左侧导航栏中选择 **VPN连接** > **VPN网关**。
3. 在顶部导航栏选择**地域**，并在 “VPN 网关”页面单击**新建**。
4. 在弹出的“新建VPN网关”窗口中，填写 VPN 网关名称（如 TomVPNGw），选择关联网络、带宽上限、计费方式，单击**创建**即可。VPN 网关创建完成后，系统随机分配公网 IP，如 `203.195.147.82` 。

> **说明**
> 如需将 CCN 型 VPN 网关新建在指定的可用区下，请提交 工单申请 。

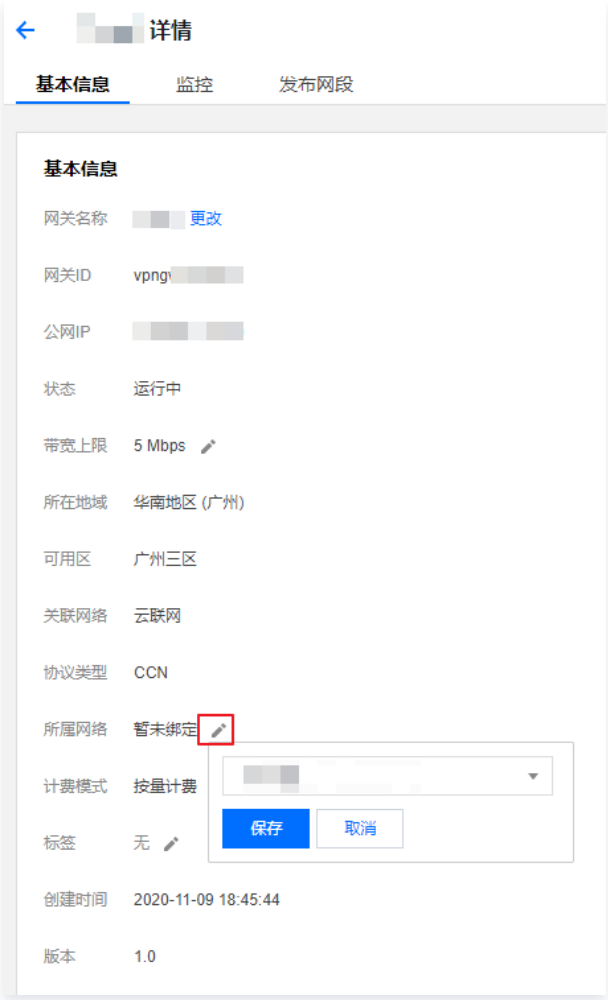
参数名称	参数说明
网关名称	填写 VPN 网关名称，不超过60个字符。
所在地域	展示 VPN 网关所在地域。
可用区	选择当前网关所在的可用区。
协议类型	支持 IPSec 和 SSL 两种协议类型。
带宽上限	请根据业务实际情况，合理设置 VPN 网关带宽上限。
关联网络	此处选择云联网。
标签	标签是对 VPN 网关资源的标识，目的是为了方便更快速的查询和管理 VPN 网关资源，非必选配置，您可按需定义。
计费方式	支持按流量计费和包年包月。按流量计费适用于带宽波动较大的场景；包年包月适用于带宽较稳定的场景。

步骤二：关联云联网实例

- 若您已创建云联网实例，请按如下操作关联云联网：

  1.1 返回 “VPN 网关“页面，在 VPN 网关列表中，单击已创建的云联网型 VPN 网关 ID。

  1.2 在“基本信息“页面，单击所属网络右侧的 ，在下拉列表中选择目标云联网实例，并单击**保存**即可。



- 若您未创建云联网实例，请按如下步骤关联云联网：

  1.1 在左侧导航栏单击 **云联网** 。

  1.2 在“云联网”页面上方选择**地域**，单击**新建**。

  1.3 在弹出的“新建云联网实例”窗口中进行如下操作，完成后单击**确定**。

  1.3.1 填写云联网实例名称、描述，选择计费模式、服务质量、限速方式。

  1.3.2 在“关联实例”下方选择 **VPN 网关**，以及已创建的云联网型 VPN 网关的地域和 ID。

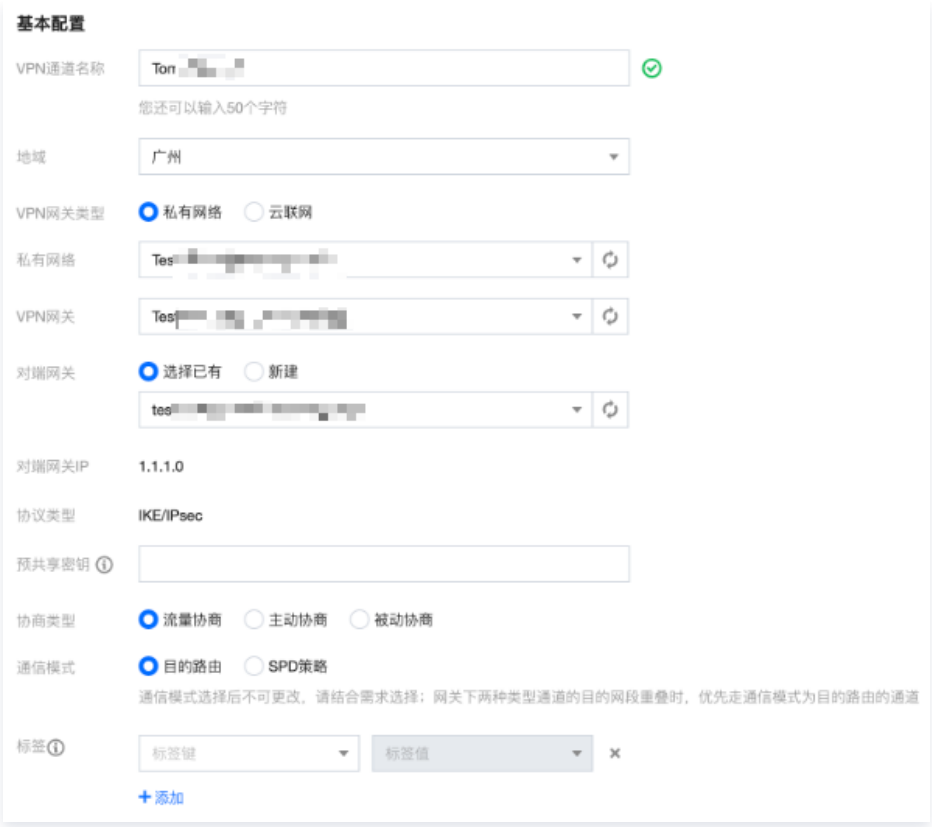
步骤三：创建对端网关

1. 登录 私有网络控制台 。
2. 在左侧导航栏选择 **VPN 连接** > **对端网关**。
3. 在“对端网关”页面上方选择**地域**，并单击**新建**。
4. 在弹出的“新建对端网关”窗口中，填写对端网关名称和 IDC 端 VPN 网关的公网 IP，并单击**创建**。

步骤四：创建 VPN 通道

1. 登录 私有网络控制台 。
2. 在左侧导航栏选择 **VPN 连接** > **VPN 通道**。
3. 在 “VPN 通道”页面上方选择**地域**，并单击**新建**，进入“新建 VPN 通道”页面。
4. 依据界面提示配置 VPN 通道基本信息。

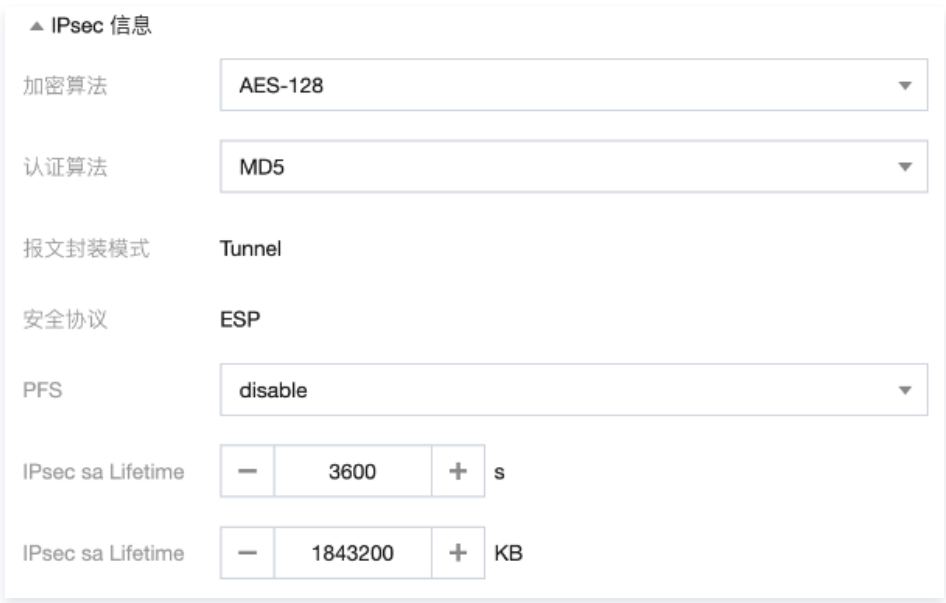
> **注意**
> - 每个规则中的多个对端网段间相互不能重叠。
> - 同一网关下多个通道内的规则不能重叠。
> - SPD 策略中的对端网段可以加入云联网中。



5. DPD 检测配置和健康检查。
   - DPD 检测：保持默认配置，默认开启，如需修改请参见界面参数进行配置。
   - 健康检查：保持默认配置，默认关闭。

6. （可选）配置 IKE 参数，如果不需要高级配置，可直接单击**下一步**。

7. （可选）配置 IPsec 参数，如果不需要配置，可直接单击**完成**。



8. 基本配置和高级配置完成后单击**创建**。

   创建成功后，返回 VPN 通道列表页，在操作栏下单击**更多** > **下载配置文件**并完成下载。

步骤五：配置 VPN 网关路由

VPN 通道配置成功后，需要配置 VPN 网关至对端网关的路由。

1. 在左侧导航栏选择 **VPN 连接** > **VPN 网关**，并在右侧 VPN 网关列表中找到创建好的 VPN 网关，并单击其名称。
2. 在 VPN 网关详情页签，单击**路由表**页签，然后单击**新增路由**。

3. 在**新建路由**页面配置 VPN 网关至对端网关的路由策略。

配置项	说明
目的端	填写待访问的对端网络的网段，即对端网关中配置的 IDC 侧提供对外访问的网段。
下一跳类型	系统自动填充 VPN 通道。
下一跳	选择创建好的 VPN 通道。
权重	0 表示优先级高，100表示优先级低。

4. 单击**确定**。

步骤六：IDC 本地配置

完成前4步后，云上 VPN 网关和 VPN 通道的配置已经完成，需要继续在 IDC 侧的“本地网关”上配置另一侧的 VPN 通道信息，具体请参考 本地网关配置 。

步骤七：启用 IDC 网段

> **说明**
>
> - 本步骤仅针对1.0和2.0版本的VPN网关。3.0版本的 VPN 网关，此处为**路由表**页签，如下图所示。
> - 如果是3.0版本的 CCN 型 VPN 网关，且 VPN 网关已关联至云联网实例时，则下一跳到**云联网**的路由策略，系统将自动学习到并展示在路由条目中，无需手动再次配置。此外，VPN 网关中配置的路由策略也会自动同步到云联网。

3.0版本的 VPN 网关路由表界面展示：

针对1.0和2.0版本的 VPN，请执行如下操作启用 IDC 网段：

1. 登录 私有网络控制台 。
2. 在左侧导航栏中选择 **VPN 连接** > **VPN 网关**。
3. 在 VPN 网关列表中，单击云联网型 VPN 网关 ID。
4. 在 VPN 网关详情页面，选择 **IDC 网段**页签，并启用目标网段。

结果验证

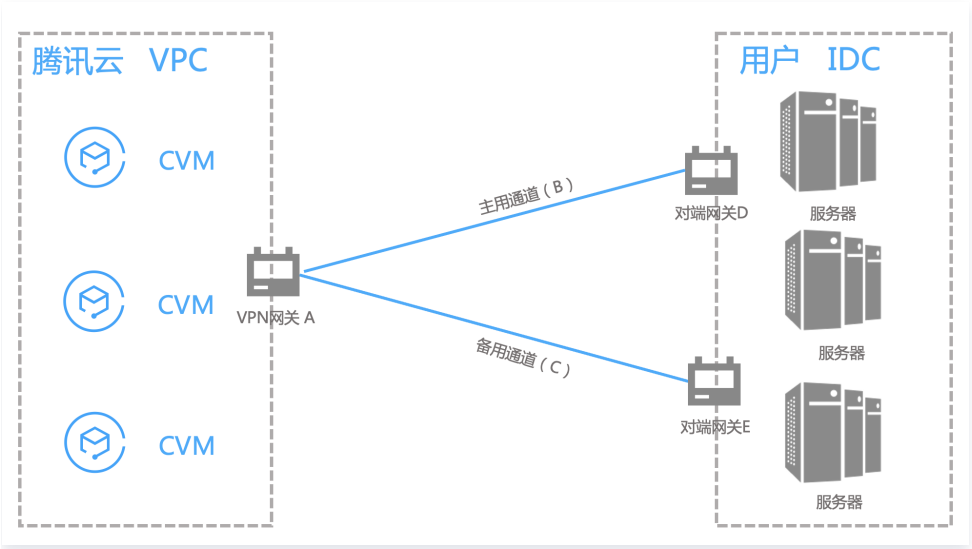
1. 登录 私有网络控制台 。
2. 在左侧导航栏中选择**云联网**。
3. 在云联网列表页中，单击 CCN 型 VPN 网关关联的云联网实例 ID。
4. 在云联网详情页面，选择**路由表**页签，若启用的网段在路由表中，且“状态”为有效，“下一跳”为 CCN 型 VPN 网关，则说明关联成功。

IDC 与单个腾讯云 VPC 实现主备容灾

最近更新时间：2023-07-18 09:58:57

腾讯云 VPN 连接具备高可用性，当用户 IDC 通过主备 VPN 通道上云，且主通道发生故障时，业务将自动切换到备用通道上，保证了业务的持续性、从而提高业务可靠性。本文以 IDC 与单个腾讯云 VPC 实现主备容灾为例。

容灾方案



用户 IDC 仅需要与单个腾讯云 VPC 实现互通，在用户 IDC 侧，用户可以部署两台 IPsec VPN 设备，分别与腾讯云私有网络型 VPN 建立 IPSec VPN 通道。VPN 网关路由表配置两条目的端一致的路由，通过优先级控制，实现主备通道效果，在发生故障时，可以实现路由自动切换。

前提条件

已在腾讯云侧 创建 VPC 网络 。

配置流程

1. 创建 VPN 网关
2. 创建对端网关
3. 创建 VPN 通道（主备）
4. IDC 侧配置
5. 配置 VPN 网关路由
6. 配置通道健康检查
7. 配置 VPC 路由策略
8. 激活 VPN 通道

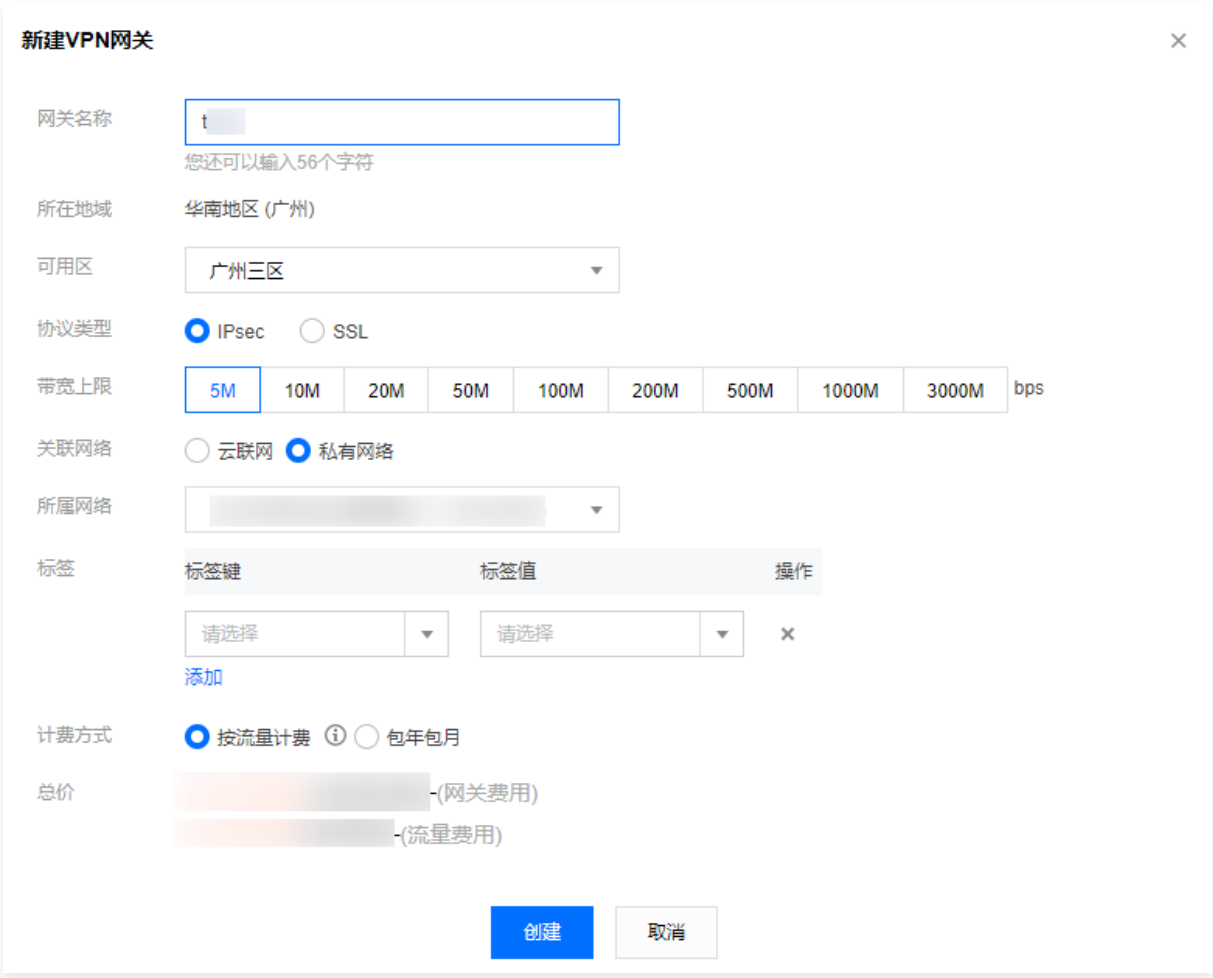
操作步骤

步骤一：创建 VPN 网关

> **说明**
> 本文以3.0版本的 VPN 网关为例。

1. 登录 私有网络控制台 。
2. 在左侧目录中选择 **VPN 连接** > **VPN 网关**，进入管理页。
3. 在 VPN 网关管理页面，单击**新建**。

4. 在弹出的**新建 VPN 网关**对话框中，配置如下网关参数。



参数名称	参数说明
网关名称	填写 VPN 网关名称，不超过60个字符。
所在地域	展示 VPN 网关所在地域。
可用区	选择当前网关所在的可用区。
协议类型	支持 IPSec 和 SSL 两种协议类型。
带宽上限	请根据业务实际情况，合理设置 VPN 网关带宽上限。
关联网络	此处选择私有网络。
所属网络	仅当关联网络为私有网络时，此处需要选择 VPN 网关将要关联的具体私有网络。
标签	标签是对 VPN 网关资源的标识，目的是为了方便更快速的查询和管理 VPN 网关资源，非必选配置，您可按需定义。
计费方式	支持按流量计费和包年包月。按流量计费适用于带宽波动较大的场景；包年包月适用于带宽较稳定的场景。

5. 完成网关参数设置后，单击**创建**启动 VPN 网关的创建。
此时**状态为创建中**，等待约1～2分钟，创建成功的 VPN 网关状态为**运行中**，系统为 VPN 网关分配一个公网 IP。

步骤二：创建对端网关

在腾讯云侧创建对端网关 D。

1. 在左侧导航栏选择 **VPN 连接** > **对端网关**。

2. 在**对端网关**管理页面，选择地域，单击**新建**。
3. 填写对端网关名称，公网 IP 填写对端 IDC 侧的 VPN 网关设备的静态公网 IP ，根据需要设置标签。

- 名称：填写对端网关名称。
- 公网 IP：填写 IDC 侧 VPN 网关所在的 公网 IP 地址。

4. 单击**创建**。

在腾讯云侧创建对端网关 E。

重复对端网关 A 的创建步骤1 ~ 步骤4。

步骤三：创建 VPN 通道（主备）

VPN 网关和对端网关创建完成后，需要创建两条 VPN 网关与 IDC 侧相连的 VPN 通道，一条作为主通道，一条作为备用通道。

创建主用通道 B

1. 在左侧导航栏选择 **VPN 连接** > **VPN 通道**。
2. 在 **VPN 通道**管理页面，选择地域，单击**新建**。
3. 在弹出的页面中填写 VPN 通道信息，具体参数配置请参考 新建 VPN 通道 。通信模式选择“目的路由”。
4. 单击**创建**。

创建备用通道 C

重复主用通道 B 的创建步骤1 ~ 步骤4，通信模式选择“目的路由”。

步骤四：IDC 侧配置

完成前三步骤后，腾讯云上 VPN 网关和 VPN 通道的配置已经完成，需要继续在 IDC 侧的**本地网关**上配置另一侧的 VPN 通道信息，具体请参考 本地网关配置 。IDC 侧的“本地网关”即为 IDC 侧的 IPsec VPN 设备，该设备的公网 IP 记录在 步骤二 的“对端网关”中。

> ⚠ **注意**
> 配置时，主备 VPN 通道对应的 IDC 侧 VPN 网关均需配置。

步骤五：配置 VPN 网关路由

截止至步骤四，已经将主备 VPN 通道配置成功，需要在 VPN 控制台配置 VPN 网关至 VPN 通道的路由。

1. 在左侧导航栏选择 **VPN 连接** > **VPN 网关**，并在右侧 VPN 网关列表中找到步骤一创建的 VPN 网关 A，并单击其名称。
2. 在 VPN 网关 A 详情页签，单击**路由表**页签，并单击**新增路由**。

3. 在**新建路由**页面配置 VPN 网关 A 至 VPN 通道 B 和 VPN 通道 C 的路由策略。

配置项	说明
目的端	填写待访问的对端网络的网段，即 IDC 侧提供对外访问的网段。
下一跳类型	系统自动填充 **VPN 通道**。
下一跳	选择创建好的 VPN 通道。
权重	• VPN 通道 B 填写 0。 • VPN 通道 C 填写100。 0 表示优先级高，100表示优先级低。

4. 单击**确定**。

步骤六：配置通道健康检查

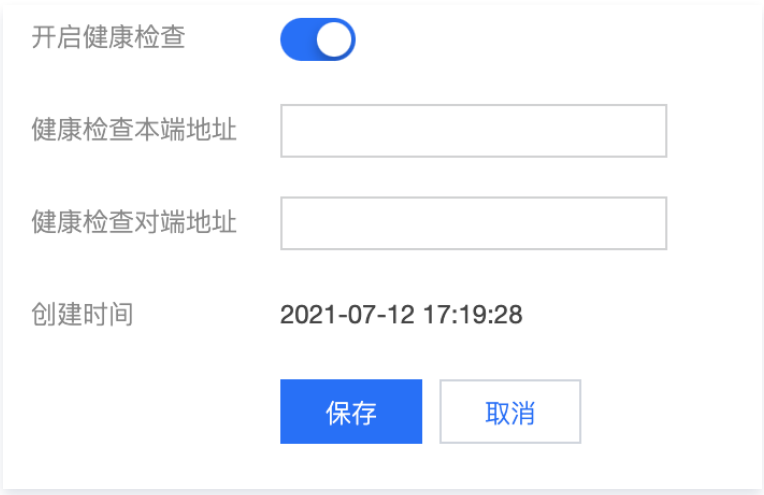
VPN 网关路由配置完成后，为 VPN 通道健康检查（主备通道均需配置）。

> **说明**
> 当健康检查触发主备通道切换，可能会出现短暂的业务中断，请勿担心，1~2秒后主备通道切换成功后业务恢复正常。

主用通道 B 健康检查配置

1. 在左侧导航栏选择 **VPN 连接** > **VPN 通道**，并在右侧 VPN 通道列表中找到创建好的 VPN 通道，然后单击 VPN 通道名称。
2. 在通道**基本信息**页签单击**编辑**。

3. 打开健康检查开关，输入**健康检查本端地址**和**健康检查对端地址**，并单击**保存**。



说明：

- 本端地址：填写腾讯云侧向 IDC 发起健康检查的访问请求 IP 地址。该 IP 地址不能为 VPC 内 IP 地址。
- 对端地址：填写 IDC 侧用于响应腾讯云健康检查请求的 IP 地址。该 IP 地址请勿与腾讯云侧地址相同，以防 IP 冲突。
- 当腾讯云侧发起健康检查请求，访问请求通过通道到达 IDC 后，发现有健康检查响应 IP 地址，表示通道健康正常，如果没有表示异常。

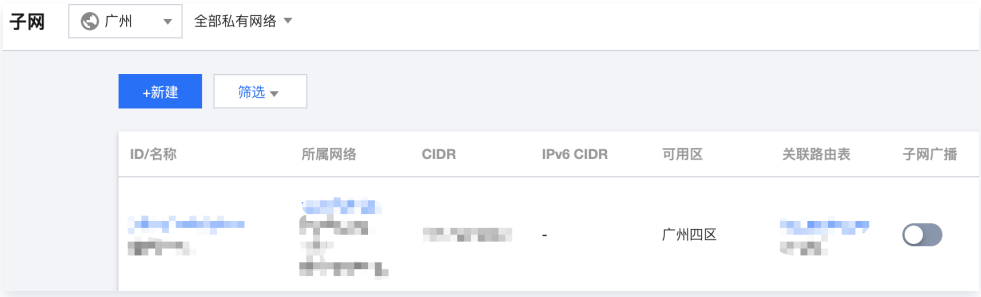
备用通道 C 健康检查配置

重复主用通道健康检查配置步骤1 ~ 步骤3，其中健康检查连接不能与主用通道的健康检查连接相同。

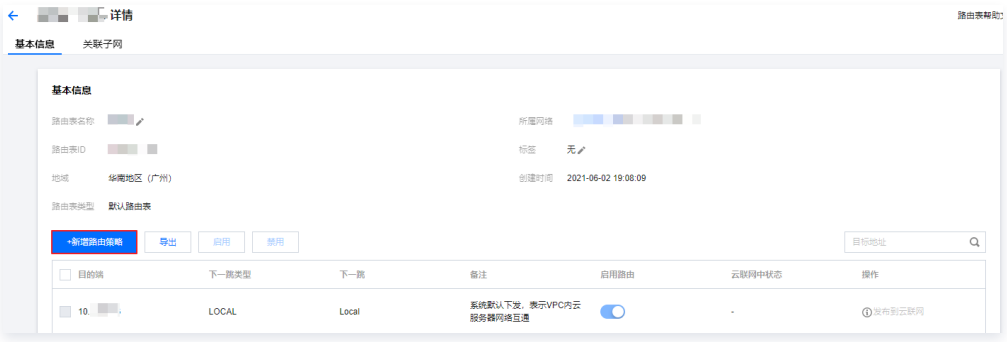
步骤七：配置 VPC 路由策略

截止至步骤五，已经将主备 VPN 通道配置成功，需要配置 VPC 路由策略，将子网中的流量路由至 VPN 网关上，子网中的网段才能与 IDC 中的网段通信。

1. 登录 私有网络控制台 。
2. 在左侧目录中单击**子网**，选择对应的地域和私有网络，单击子网所关联的路由表 ID，进入详情页。



3. 单击**新增路由策略**。



4. 在弹出框中，输入目的端网段，下一跳类型选择**VPN 网关**，下一跳选择刚创建的 VPN 网关，单击**创建**即可。

步骤八：激活 VPN 通道

使用 VPC 内的云服务器 ping 对端网段中的 IP，以激活 VPN 隧道，可以 ping 通表示 VPC 和 IDC 可以正常通信。
当 VPN 路由表中探测 VPN 主用通道 B 路由不可达时，系统自动将流量切换至 VPN 通道 C，确保业务的高可用性。

在腾讯云和 AzureChina 之间建立 VPN 连接

最近更新时间：2022-12-13 10:53:32

在两个公有云之间建议使用 VPN 连接，保证了公有云之间流量使用内网传输，增强了网络安全性，减少了攻击面。

> **说明**
> - 由于 VPN 连接涉及创建腾讯云产品与 AzureChina 云资源，教程中的步骤由于时效性原因可能与产品最新的操作步骤不一致。
> - 本文第三方教程来自 腾讯云产品“用户实践”征集，仅供学习和参考。

本文将为您提供 在腾讯云和 AzureChina 之间建立 VPN 连接 的第三方教程，您可参考教程进行相关实践操作。

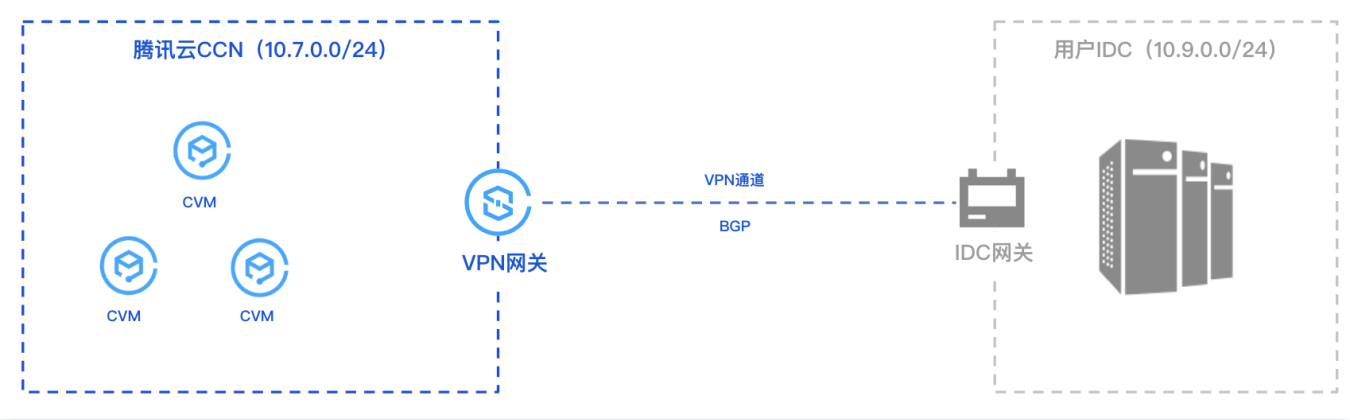
建立 IDC 与云上资源的连接（动态 BGP）

最近更新时间：2024-02-22 18:11:31

本文介绍如何通过 VPN 的动态 BGP 打通 IDC 和云上资源，实现业务通信。

业务场景

用户部分业务部署在云上，使用 VPN 连接打通了 IDC 与云上网络，并通过 BGP 进行通信。



操作流程

1. 创建云联网实例。
2. 创建 CCN 型 VPN 网关，并绑定创建好的云联网实例。
3. 创建对端网关并指定 IDC 侧 ASN。
4. 创建 VPN 通道，配置 BGP 参数。
5. IDC 侧本地配置。

操作步骤

本指引仅介绍操作过程中必要的配置步骤及其参数，其他参数详情请查看各自具体的操作文档。

步骤一：创建云联网实例

您需要在云联网控制台创建所需的云联网实例，具体操作请参见 新建云联网实例 。

步骤二：创建云联网型 VPN 网关

1. 登录 VPN 网关控制台，在VPN网关页面单击**新建**。
2. 在 VPN购买页 配置 CCN 型网关参数。
   - 地域：选择首尔。
   - 网络类型：选择云联网。
   - 带宽：选择200Mbps及以上规格。
   - BGP ASN：腾讯侧 VPN 网关 ASN 号，默认64551，取值范围为 1 – 4294967295，其中 139341、45090、58835 不可用。
3. 在 VPN 网关详情页面，绑定 步骤一 创建好的云联实例。

步骤三：创建对端网关

1. 登录 对端网关控制台，在右边对端网关页面，单击**新建**。
2. 在**新建对端网关**页面，配置 IDC 侧用于公网访问的 IP 地址和所规划的 ASN，详情可参见 创建对端网关 。

步骤四：创建 BGP 路由型 VPN 通道

1. 登录 VPN 通道控制台，在右侧 VPN 通道页面，单击**新建**。
2. 在新建 VPN 通道页面，依据实际情况配置通道基本参数，配置完成继续后续配置。

参数	说明
网络类型	选择云联网。
VPN 网关	选择已配置 ASN 的云联网型 VPN 网关。
对端网关	选择配置有 ASN 对端网关。
通信模式	选择动态 BGP 路由。
BGP 邻居	用于云端和用户端互通的 BGP 隧道网段，该网段必须在 `169.254.128.0/17` 范围内。

云端 BGP 地址	云上与用户互联的 BGP IP 地址。
用户端 BGP 地址	不可修改，自动分配的用户端 BGP 互联地址。 云端 BGP 地址手动修改后，该参数随之自动更新。

步骤五：IDC 本地网关配置

完成前4步后，云上 VPN 网关和 VPN 通道的配置已经完成，需要继续在 IDC 侧的“本地网关”上配置另一侧的 VPN 通道信息，具体请参考 本地网关配置 。

> **说明：**
> IDC 侧的“本地网关”即为 IDC 侧的 IPsec VPN 设备，该设备的公网 IP 记录在创建好的“对端网关”中。

本地网关配置
山石网科防火墙配置

最近更新时间：2022-12-08 16:24:01

使用 IPsec VPN 建立腾讯云 VPC 到用户 IDC 的连接时，在配置完腾讯云 VPN 网关后，您还需要在用户 IDC 本地站点的网关设备中进行 VPN 配置。本文以山石防火墙为例介绍如何在本地站点中进行 VPN 配置。

注意

- 本文以 SG-6000-VM01 型号、SG6000-CloudEdge-5.5R7P9 版本防火墙配置演示，其他版本可能界面略有差异，整体配置逻辑一致。
- 本文所有 IP、接口等参数取值均仅用于举例，请具体配置时，使用实际值进行替换。

前提条件

请确保您已经在腾讯云 VPC 内 创建 VPN，并完成 VPN 通道配置。

数据准备

本文 IPsec VPN 配置数据举例如下：

配置项			示例值
网络配置	VPC 信息	子网 CIDR	10.1.1.0/24
		VPN 网关公网 IP	159.xx.xx.242
	IDC 信息	内网 CIDR	172.16.0.0/16
		网关公网 IP	120.xx.xx.76
IPsec 连接配置	IKE 配置	版本	IKEV1
		身份认证方法	预共享密钥，例如123456
		加密算法	DES
		认证算法	MD5
		协商模式	main
		本端标识	IP Address：120.xx.xx.76
		远端标识	IP Address：159.xx.xx.242
		DH group	DH2
		IKE SA Lifetime	86400
	IPsec 配置	加密算法	AES-128
		认证算法	MD5
		报文封装模式	Tunnel
		安全协议	ESP
		PFS	disable

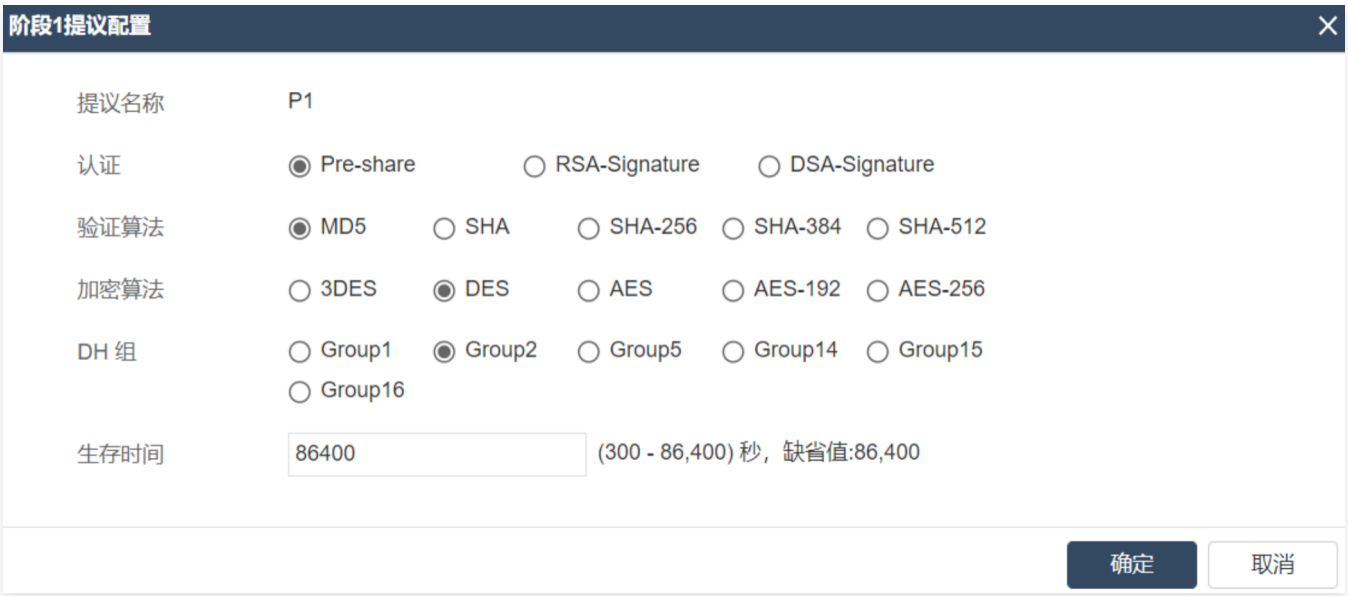
		IPsec SA 生存周期（s）	3600s
		IPsec SA 生存周期（KB）	1843200KB

操作步骤

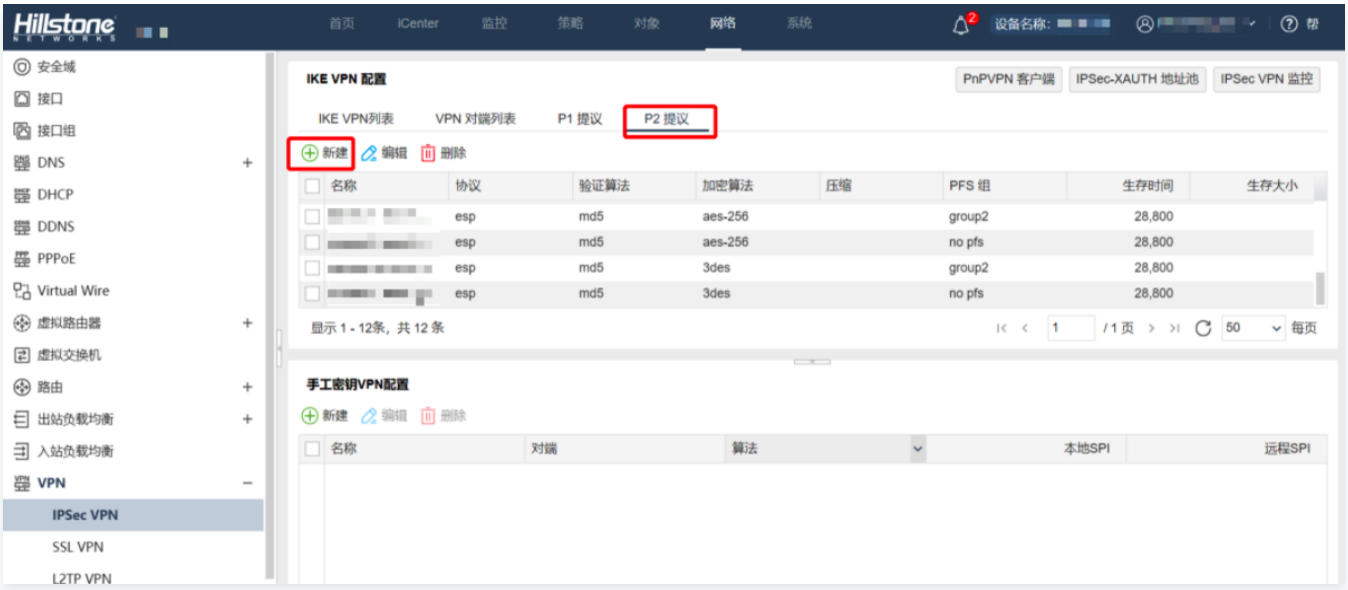
适用于基于 SPD 策略转发的 VPN

1. 登录 Hillstone 防火墙 Web 界面，选择**网络 > VPN > IPsec VPN > P1 提议**，在 **P1 提议**界面，单击**新建**。

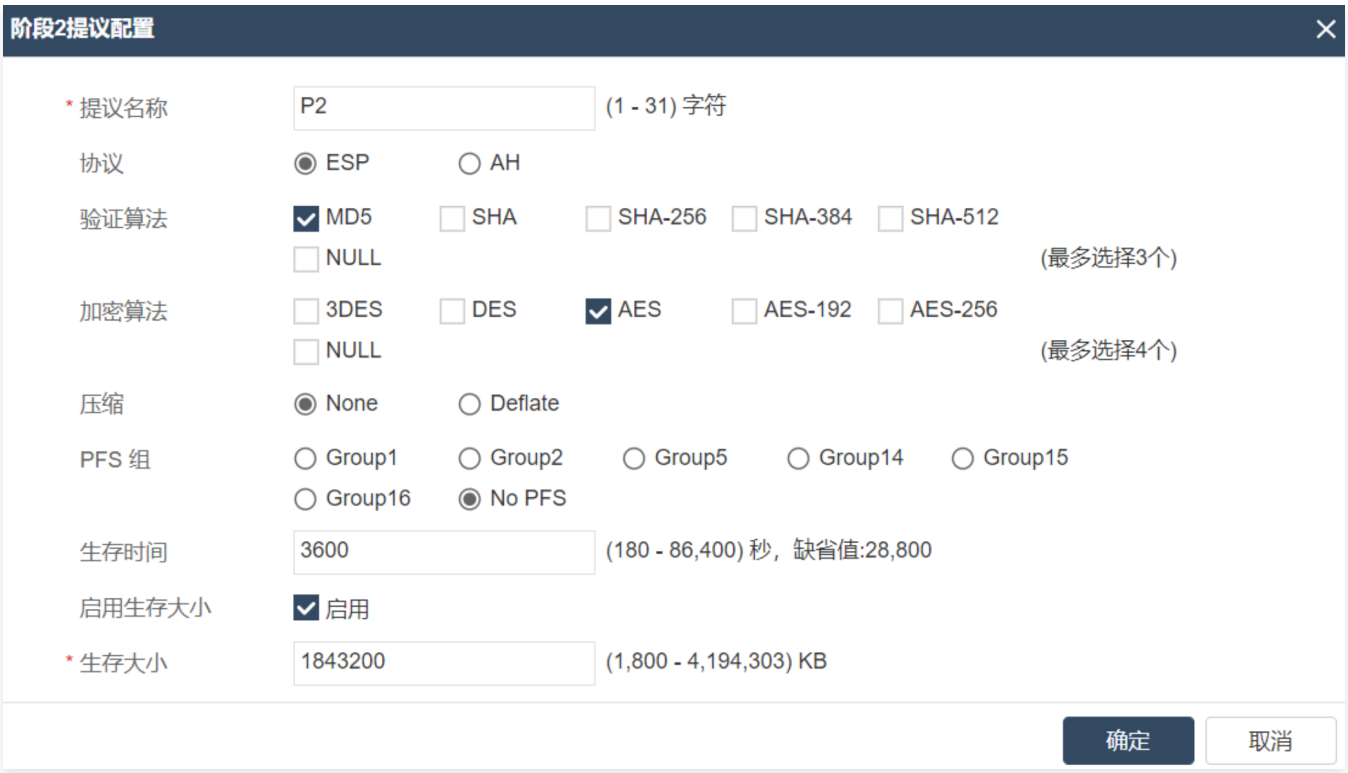
2. 在弹出的**阶段1提议配置**界面，根据腾讯云 VPN 连接的 IKE 协议信息配置 IDC 的 IKE 协议，并单击**确定**。



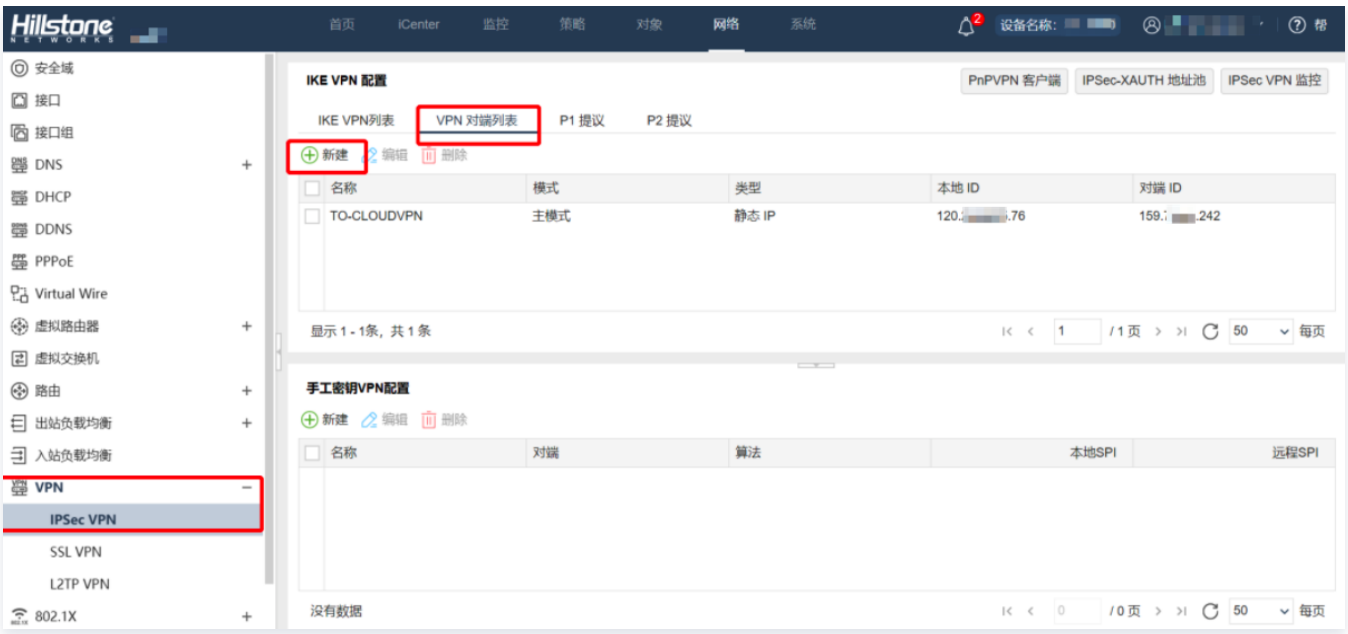
3. 选择 **P2 提议**页签，单击**新建**。



4. 在弹出的**阶段2提议配置**界面，根据腾讯云 VPN 连接的 IPsec 协议信息配置 IDC 的 IPsec 协议，并单击**确定**。



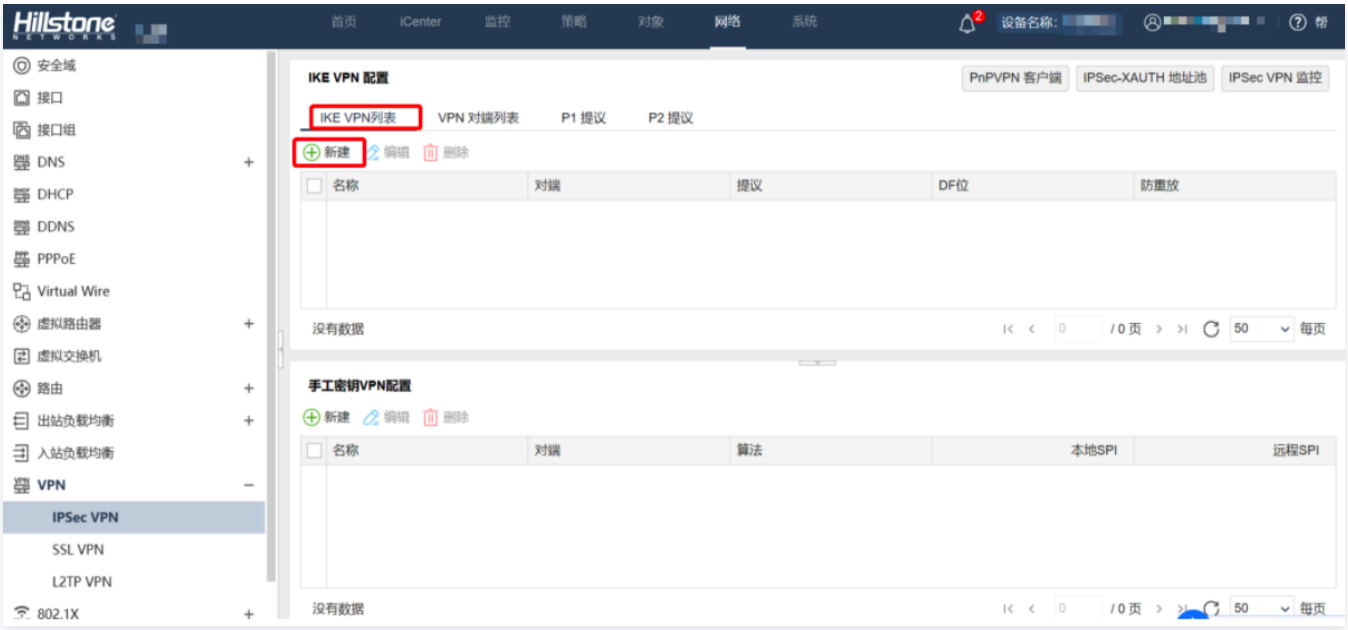
5. 选择 **VPN 对端列表**页签，单击**新建**。



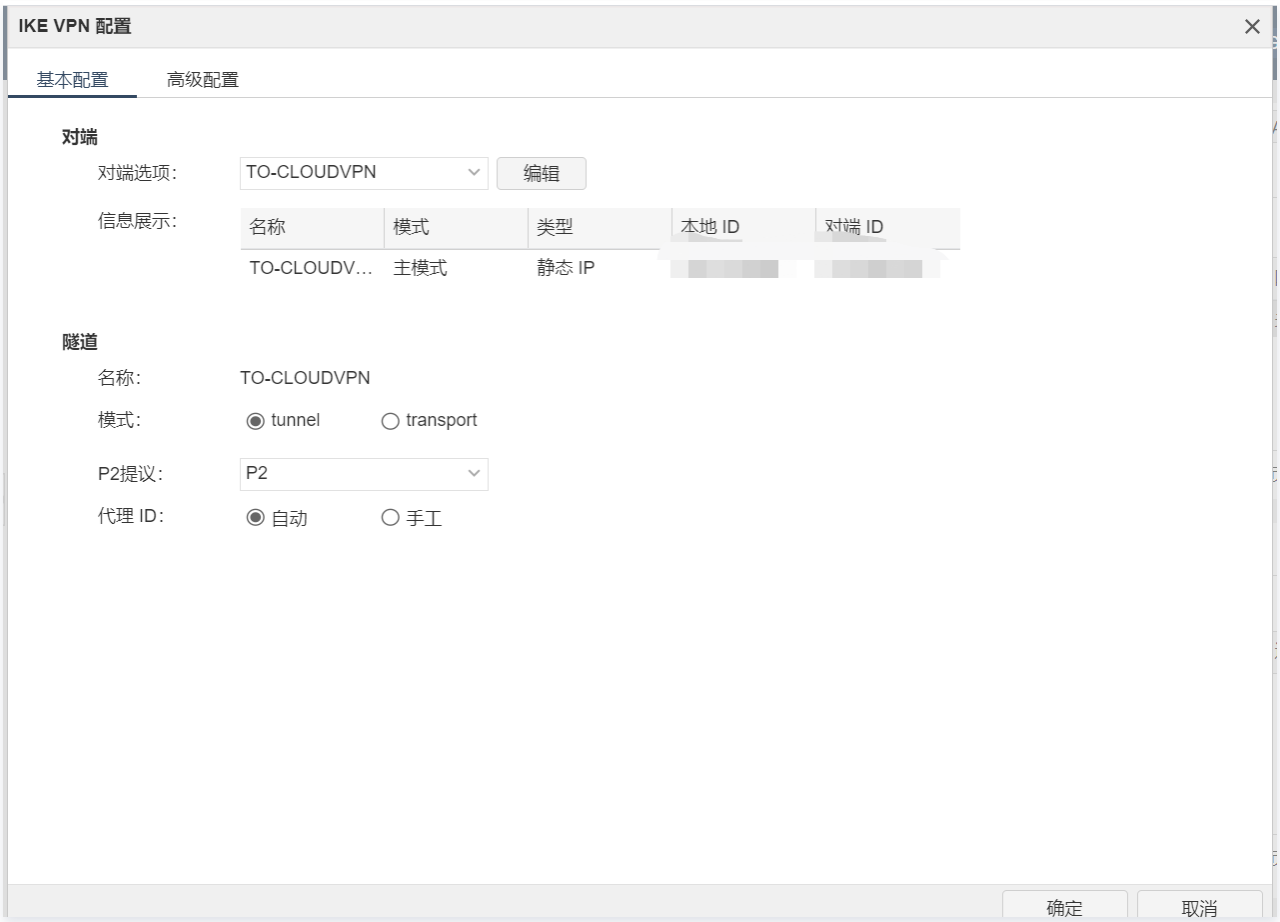
6. 在弹出的 **VPN 对端配置**界面，配置 VPN 对端的相关参数，并单击**确定**。

- 名称：自定义填写 VPN 对端名称，例如 TO-CLOUDVPN
- 对端 IP 地址：填写腾讯云 VPN 网关的公网 IP 地址
- 本端 IP：填写 IDC 本端的公网 IP 地址
- 对端 IP：填写 IDC 对端 VPN 网关的公网 IP 地址
- 提议1：选择 步骤2 创建的 P1 提议
- 预共享密钥：填写与腾讯云 VPN 通道基本配置中一致的预共享密钥，例如本例的123456

7. 选择 **IKE VPN 列表**页签，单击**新建**。



8. **在弹出的 IKE VPN 配置界面，进行 IKE VPN 的基本配置和高级配置，完成后单击确定。**
   - **基本配置**



     - **对端选项：选择 步骤6 创建的 VPN 对端**
     - **P2 提议：选择 步骤4 创建的 P2 提议**
     - **代理 ID：选择自动**
   - **高级配置：将自动连接勾选设置为启用**

9. 选择**网络** > **安全域**，单击**新建**配置安全域。

10. 在弹出的**安全域配置**界面，配置如下参数，完成后，单击**确定**。
    - 安全域名称：自定义名称，例如 VPNhub
    - 虚拟路由器：默认选择 trust-vr

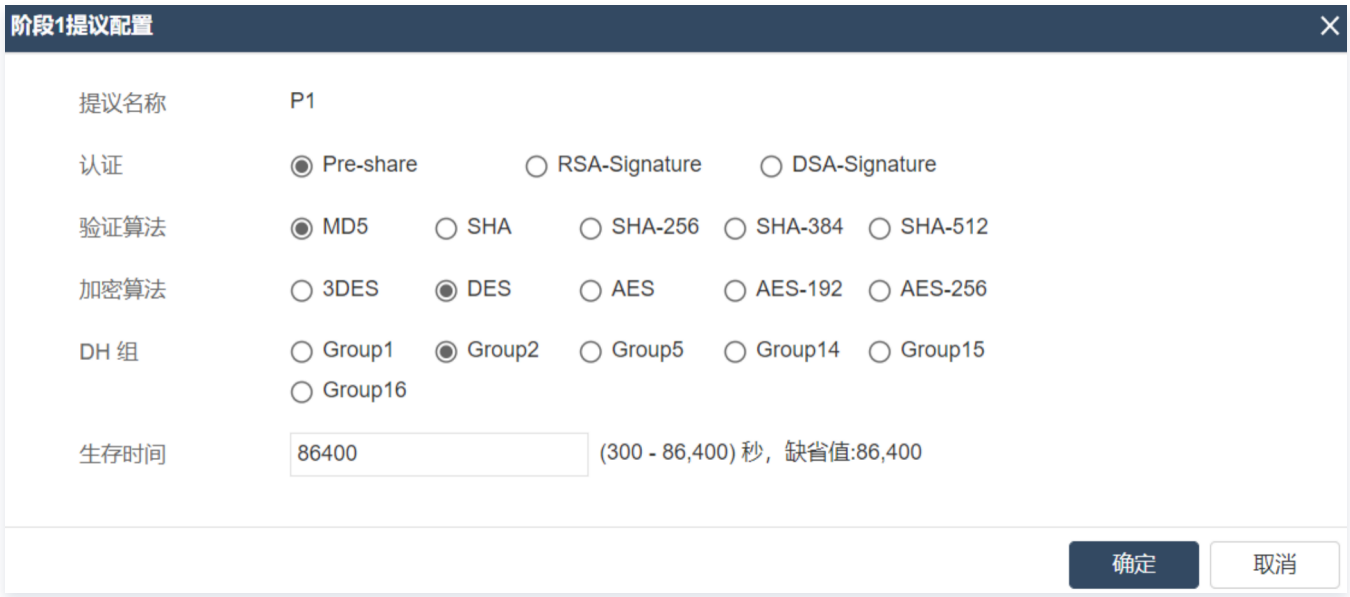
11. 选择**策略 > 策略**，单击**新建**，按照如下参数指导配置策略，完成后单击**确定**。

- **源信息：**
  - **安全域：选择 trust**
  - **地址：填写 IDC 本端网段及掩码**，例如172.16.0.0/16
- **目的信息：**
  - **安全域：选择 VPNHub**
  - **地址：填写腾讯云 VPN 后端子网网段及掩码**，例如10.1.1.0/24
- **服务：选择 any**
- **动作：选择安全连接，隧道选择** 步骤6 创建的 VPN 对端，例如 TO-CLOUDVPN，**勾选双向 VPN 策略**

适用于基于路由转发的 VPN

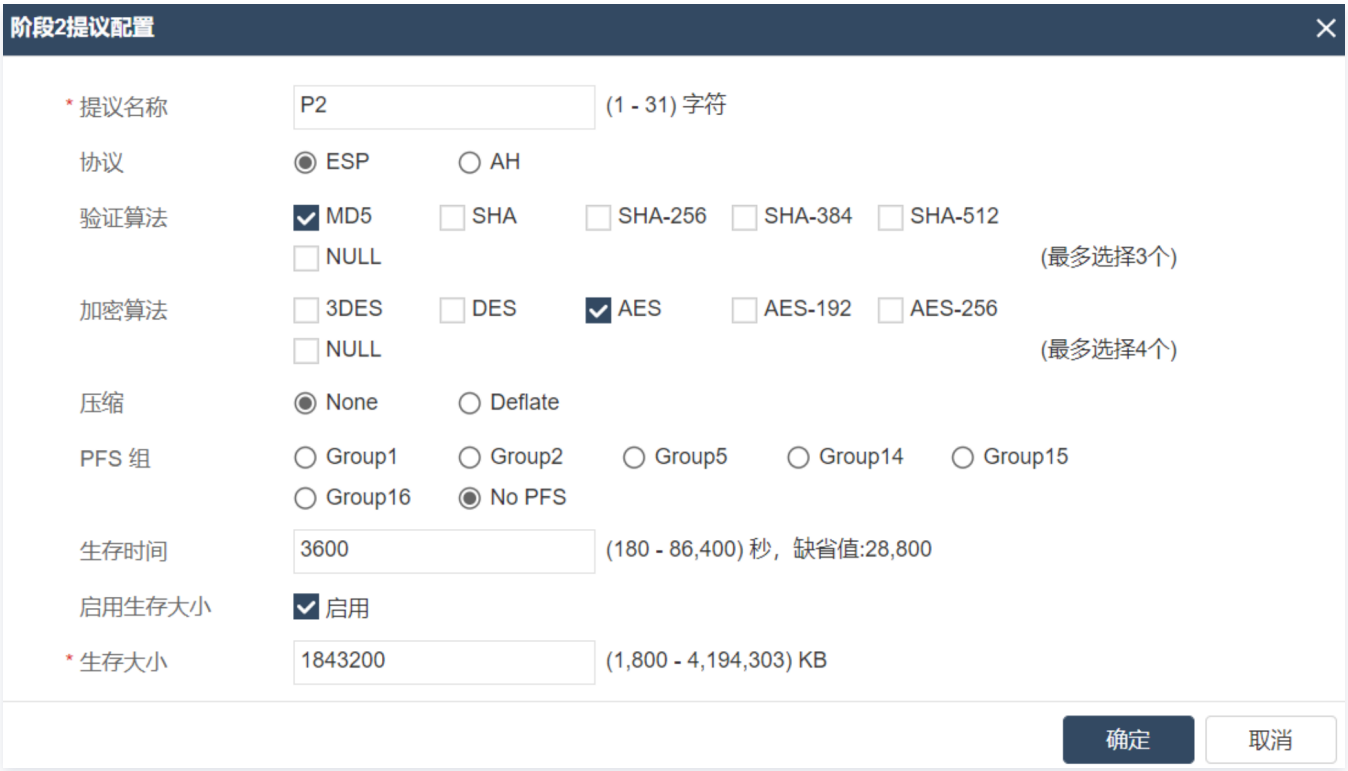
1. 登录 Hillstone 防火墙 Web 界面，选择**网络 > VPN > IPsec VPN > P1提议**，在 **P1 提议**界面，单击**新建**。

2. 在弹出的**阶段1提议配置**界面，根据腾讯云 VPN 连接的 IKE 协议信息配置 IDC 的 IKE 协议，并单击**确定**。



3. 选择 **P2 提议**页签，单击**新建**。

4. 在弹出的**阶段2提议配置**界面，根据腾讯云 VPN 连接的 IPsec 协议信息配置 IDC 的 IPsec 协议，并单击**确定**。

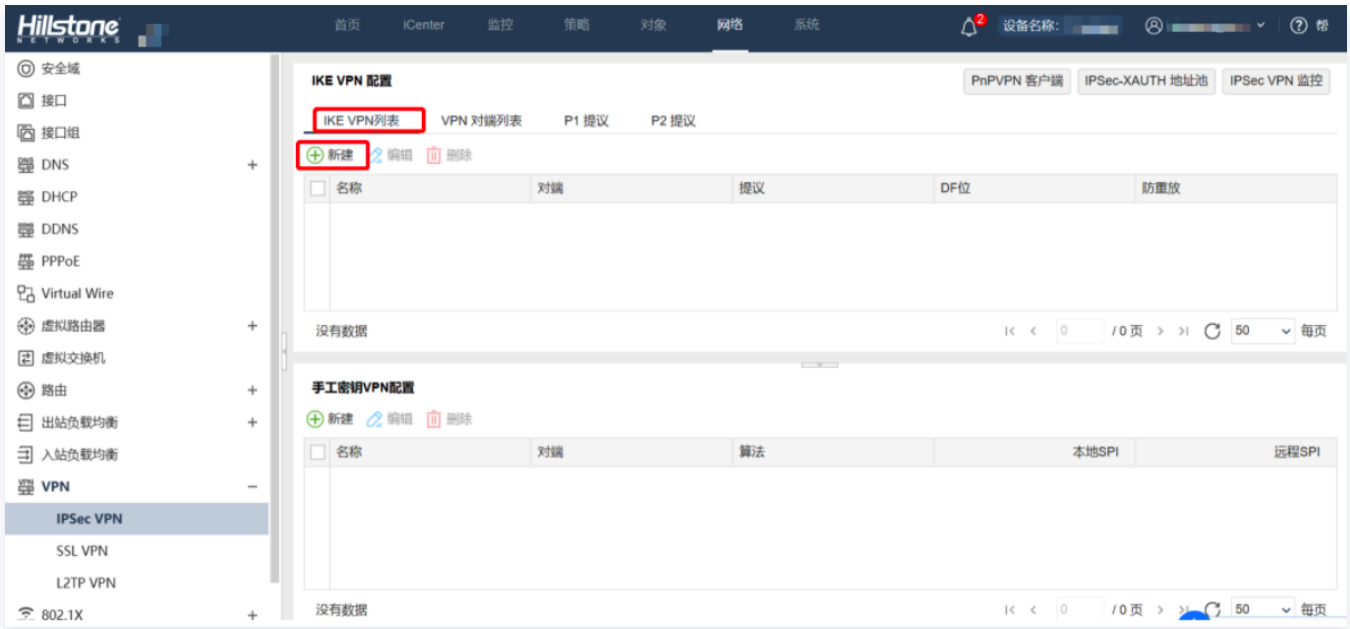


5. 选择 **VPN 对端列表**页签，单击**新建**。

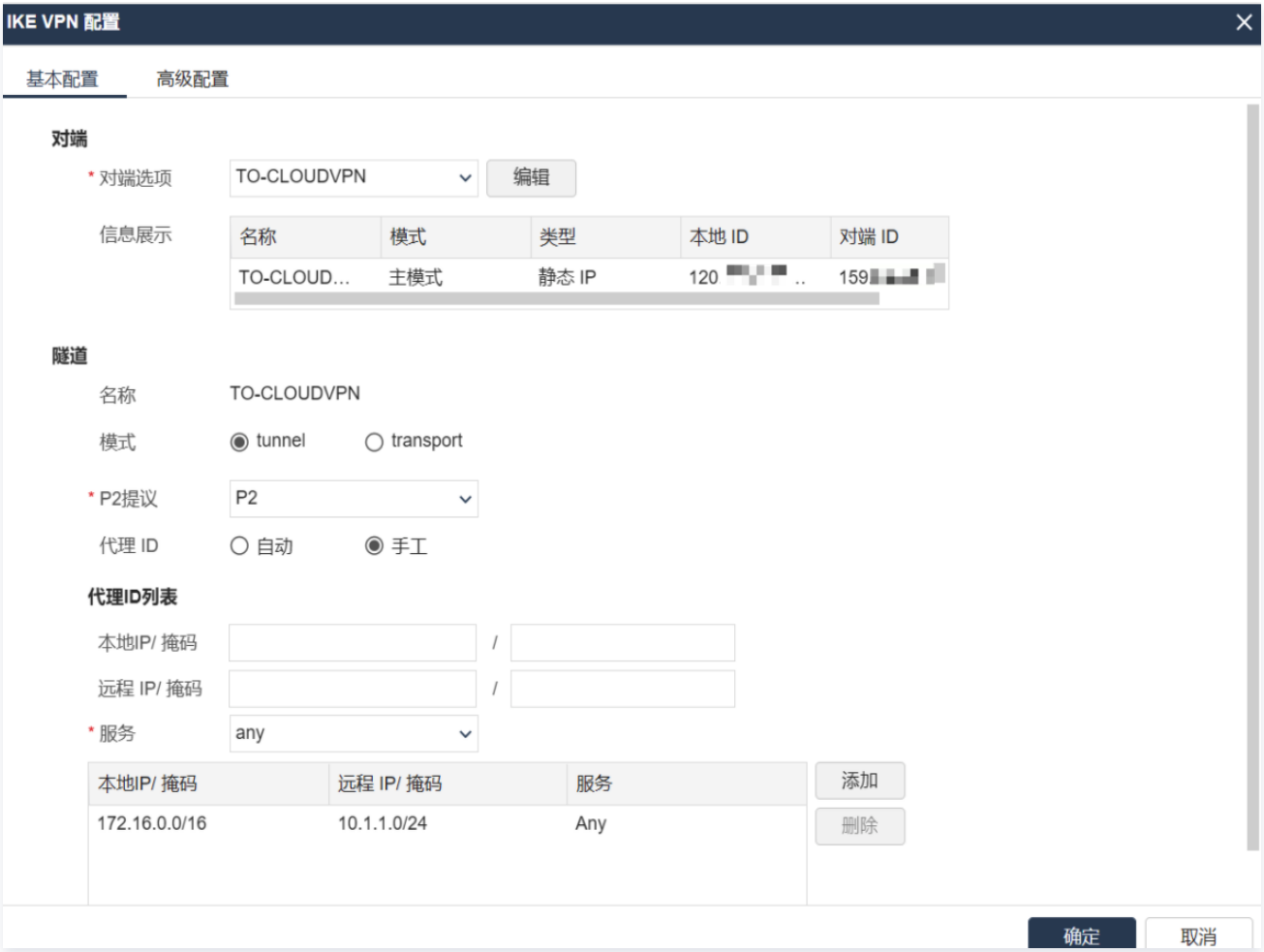
6. 在弹出的 **VPN 对端配置**界面，配置 VPN 对端的相关参数，并单击**确定**。

- 名称：自定义填写 VPN 对端名称，例如 TO-CLOUDVPN
- 对端 IP 地址：填写腾讯云 VPN 网关的公网 IP 地址
- 本端 IP：填写 IDC 本端的公网 IP 地址
- 对端 IP：填写 IDC 对端 VPN 网关的公网 IP 地址
- 提议1：选择 步骤2 创建的 P1 提议
- 预共享密钥：填写与腾讯云 VPN 通道基本配置中一致的预共享密钥，例如本例的123456

7. 选择 **IKE VPN 列表**页签，单击**新建**。



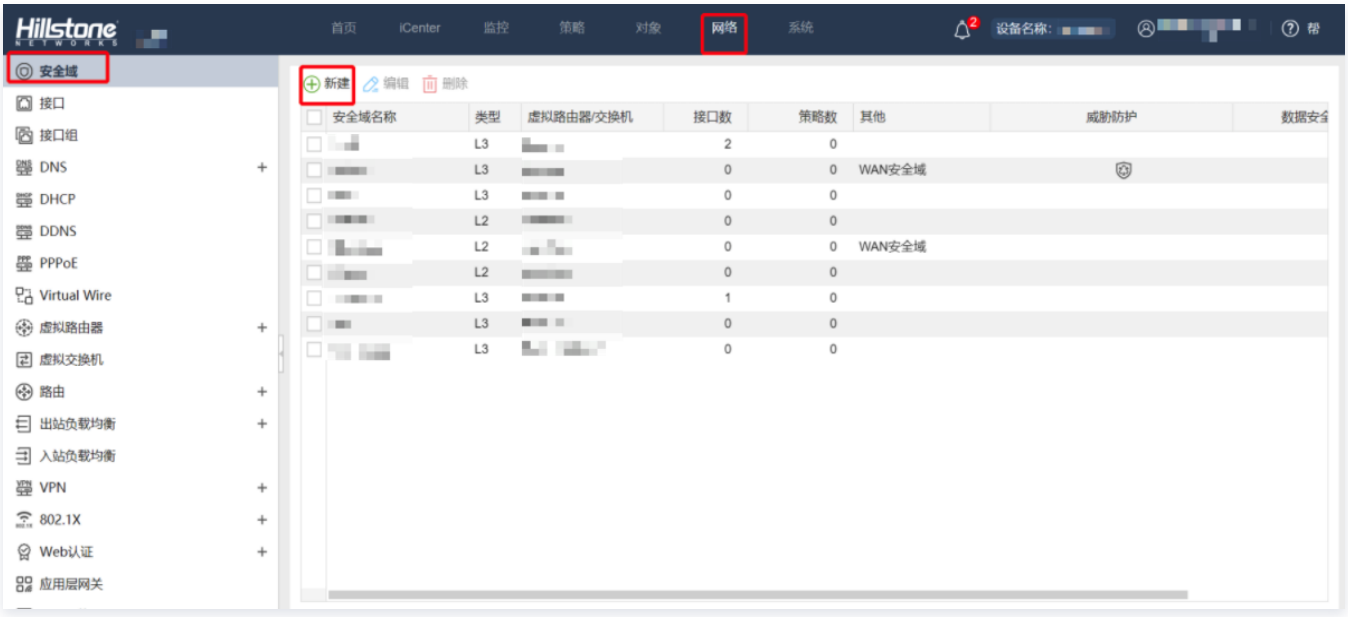
8. 在弹出的 **IKE VPN 配置**界面，进行 IKE VPN 的基本配置和高级配置，完成后单击**确定**。
   - 基本配置



- 对端选项：选择 步骤6 创建的 VPN 对端
- P2 提议：选择 步骤4 创建的 P2 提议
- 代理 ID：选择**手工**，并在**代理 ID 列表**的**本地 IP/掩码**中输入本地 IDC 的内网网段，在**远程 IP/掩码**中输入腾讯云 VPC 的内网网段，然后单击**添加**

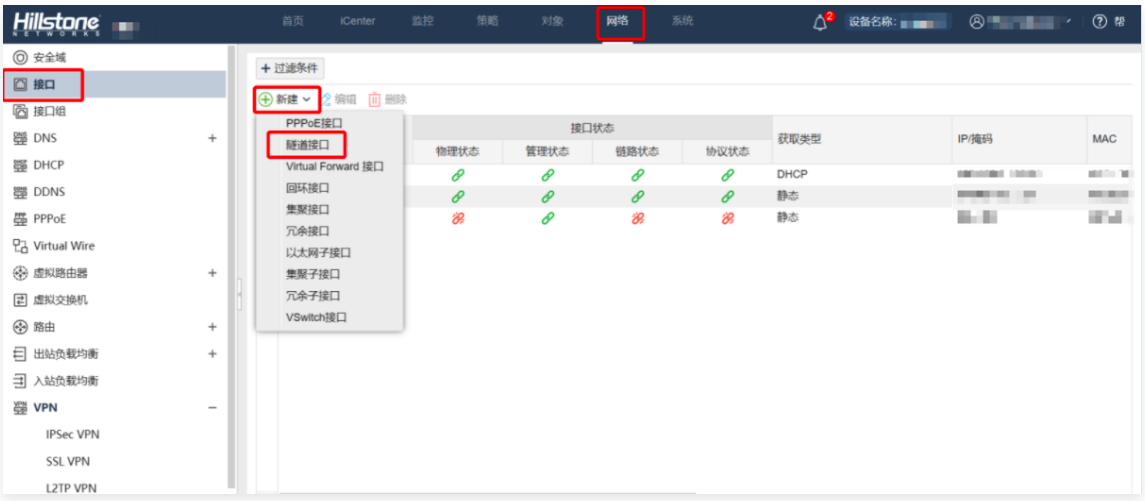
- 高级配置：将**自动连接**勾选设置为**启用**

9. 选择**网络** > **安全域**，单击**新建** 配置安全域。



10. 在弹出的**安全域配置**界面，配置如下参数，完成后，单击**确定**。
    - 安全域名称：自定义名称，例如 **VPNhub**
    - 虚拟路由器：默认选择 **trust-vr**

11. 选择**网络 > 接口**，依次单击**新建 > 隧道接口** 。



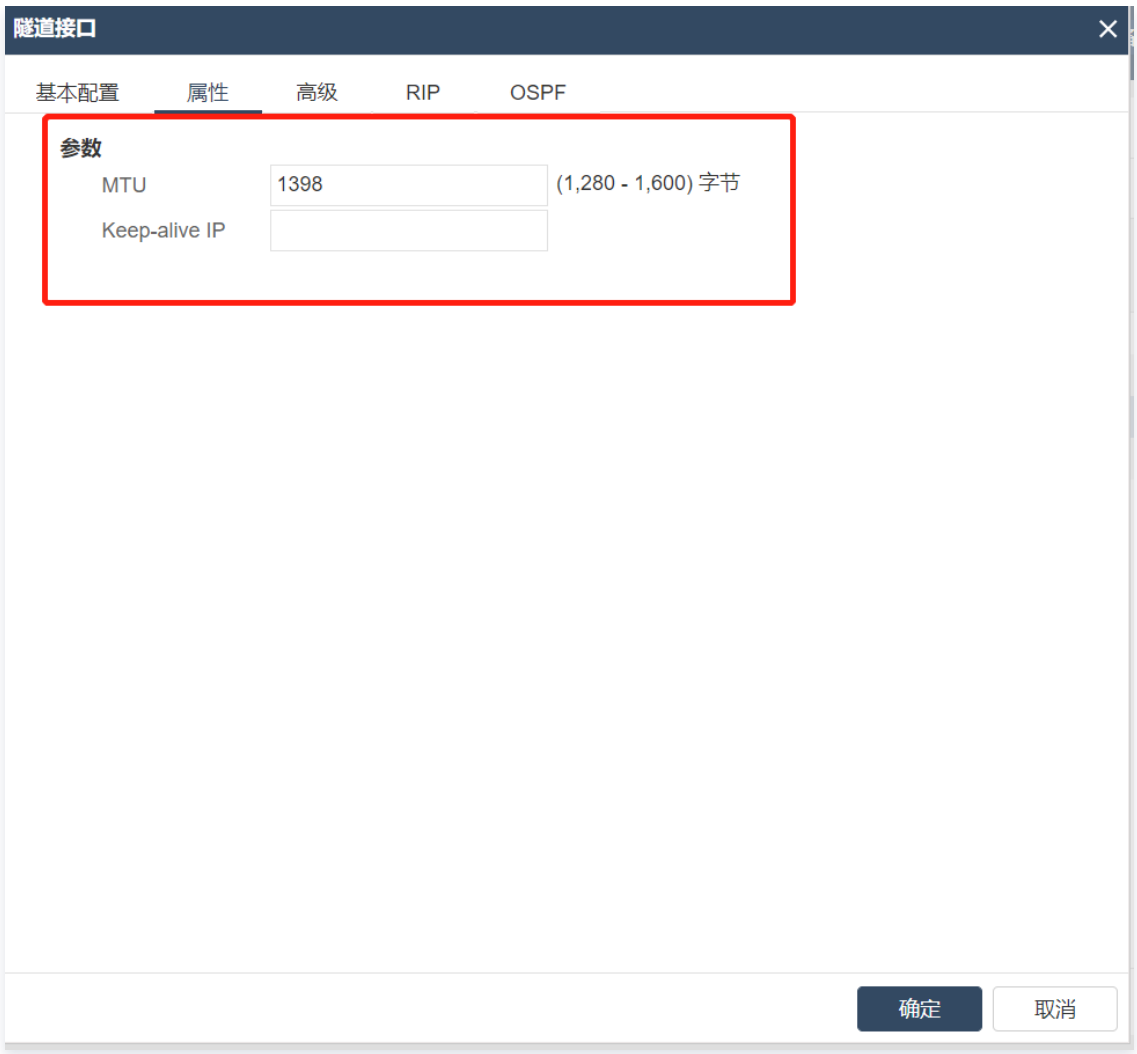
12. 在弹出的**隧道接口**对话框中，配置隧道接口相关参数。

- 接口名称：输入 **tunnelX**，X 的取值范围为1-64，例如 tunnel1
- 安全域：选择 步骤10 创建的安全域
- 隧道类型：选择 **IPsec VPN**
- VPN 名称：选择 步骤6 创建的对端 VPN 名称


隧道接口
基本配置
属性
高级
RIP
OSPF
接口名称
tunnel
1
(1 - 64)
描述
(0 - 63) 字符
绑定安全域
二层安全域
三层安全域
TAP
无绑定
* 安全域
VPNHub
HA同步
启用
NetFlow 配置

IP配置
类型
静态IP
自动获取
PPPoE
IP地址
子网掩码
配置为Local IP
高级选项
DHCP...
管理方式
Telnet
SSH
Ping
HTTP
HTTPS
SNMP
路由
逆向路由
启用
关闭
自动
隧道绑定配置
隧道类型
IPSec VPN
SSL VPN
L2TP VPN
确定
取消


隧道接口
基本配置
属性
高级
RIP
OSPF
子网掩码
配置为Local IP
高级选项
DHCP...
管理方式
Telnet
SSH
Ping
HTTP
HTTPS
SNMP
路由
逆向路由
启用
关闭
自动
隧道绑定配置
隧道类型
IPSec VPN
SSL VPN
L2TP VPN
VPN 名称
TO-CLOUDVPN
网关
VPN 名称
类型
网关
添加
TO-CLOUDVPN
IPSec VPN
删除
带宽
上行带宽
1,000,000,000
(512,000 - 1,000,000,000,000) bps
下行带宽
1,000,000,000
(512,000 - 1,000,000,000,000) bps
确定
取消



13. 选择**策略** > **策略**，单击**新建**配置策略。


策略配置
基本配置
防护状态
数据安全
选项
名称
(0 - 95) 字符
源信息
安全域
trust
地址
any
用户
目的信息
安全域
VPNHub
地址
any
服务
any
应用
动作
允许
拒绝
安全连接
启用Web重定向
确定
取消


策略配置
基本配置
防护状态
数据安全
选项
名称
(0 - 95) 字符
源信息
安全域
VPNHub
地址
any
用户
目的信息
安全域
trust
地址
any
服务
any
应用
动作
允许
拒绝
安全连接
启用Web重定向
确定
取消

14. 选择**网络** > **路由**，单击**新建**分别配置上行和下行路由，完成后单击**确定**。
    - 上行路由：目的地址为腾讯云 VPC 的网段，下一跳为 步骤12 新建的隧道接口，本例为 tunnel1。

    - 下行路由：配置防火墙下行接口路由。

Juniper 防火墙配置

最近更新时间：2023-06-07 09:30:07

使用 IPsec VPN 建立腾讯云 VPC 到用户 IDC 的连接时，在配置完腾讯云 VPN 网关后，您还需在用户 IDC 本地站点的网关设备中进行 VPN 配置。本文以 Juniper 防火墙为例介绍如何在本地站点中进行 VPN 配置。

说明

- 支持 Juniper SRX 系列防火墙以及 vSRX 系列虚拟防火墙，所有版本均支持。
- 本文所有 IP、接口等参数取值均仅用于举例，请具体配置时，使用实际值进行替换。

前提条件

请确保您已经在腾讯云 VPC 内 创建 VPN，并完成 VPN 通道配置。

数据准备

本文 IPsec VPN 配置数据举例如下：

配置项			示例值
网络配置	VPC 信息	子网 CIDR	10.1.1.0/24
		VPN 网关公网 IP	159.xx.xx.242
	IDC 信息	内网 CIDR	172.16.0.0/16
		网关公网IP	120.xx.xx.76
IPsec 连接配置	IKE 配置	版本	IKEV1
		身份认证方法	预共享密钥
		加密算法	AES-128
		认证算法	MD5
		协商模式	main
		本端标识	IP Address：120.xx.xx.76
		远端标识	IP Address：159.xx.xx.242
		DH group	DH2
		IKE SA Lifetime	86400
	IPsec 配置	加密算法	AES-128
		认证算法	MD5
		报文封装模式	Tunnel
		安全协议	ESP
		PFS	disable
		IPsec sa Lifetime	3600s

操作步骤

适用于基于 SPD 策略转发的 VPN

1. 登录防火墙设备的命令行配置界面。

```
ssh -p 22 root@172.16.0.1
# 通过 SSH 命令登录防火墙命令行界面
root@SRX1> configure
Entering configuration mode
# 登录之后为操作模式，键入“configure”进入配置模式
[edit]
root@SRX1#
# “#” 表示已经进入配置模式
root@SRX1# commit
commit complete
# 在配置模式下面修改配置，不会直接生效，通过“commit”命令，修改的配置才会保存并生效
```

2. 配置防火墙网络接口、安全域、地址簿信息。

```
set interfaces ge-0/0/x unit 0 family inet address 172.16.0.1/16
# 为内部接口ge-0/0/x定义IP地址，请更换为实际接口和IP
set interfaces ge-0/0/y unit 0 family inet address 120.xx.xx.76/30
# 为外部接口ge-0/0/y定义IP地址，请更换为实际接口和IP
set security zones security-zone trust interfaces ge-0/0/x.0
# 绑定ge-0/0/x为内部安全区(trust)，对接内部业务区，请更换为实际接口
set security zones security-zone untrust interfaces ge-0/0/y.0  host-inbound-traffic system-services ike
# 绑定ge-0/0/y为外部安全区(untrust)，对接外部广域网，并启用ike服务，表示该区域可以建立VPN
set security zones security-zone untrust address-book address vpn-peer_subnet 10.1.1.0/24
# 定义要访问的VPN对端的业务地址簿，用于后续的访问策略调用，命名可以自定义
set security zones security-zone trust address-book address vpn-local_subnet 172.16.0.0/16
# 定义本地的业务地址簿，用于后续的访问策略调用，命名可以自定义
```

3. 配置 IKE 策略。

```
set security ike proposal ike-proposal-cfgr authentication-method pre-shared-keys
# 定义IPSEC VPN 认证方式（本实例使用共享密钥模式：pre-shared-keys），注意“ike-proposal-cfgr”为定义的命名，
后续设置需要调用该命名
set security ike proposal ike-proposal-cfgr dh-group group2
# 定义IKE的dh-group
set security ike proposal ike-proposal-cfgr authentication-algorithm md5
# 定义IKE认证算法
set security ike proposal ike-proposal-cfgr encryption-algorithm aes-128-cbc
# 定义IKE加密算法
set security ike proposal ike-proposal-cfgr lifetime-seconds 86400
# 定义IKE生存时间， 范围：(180～86400 seconds)
set security ike policy ike-policy-cfgr mode main
# 指定IKE模式
set security ike policy ike-policy-cfgr proposals ike-proposal-cfgr
# 定义IKE策略，需要调用上面步骤中的算法定义命名定义
set security ike policy ike-policy-cfgr pre-shared-key ascii-text "TestPassword"
# 定义密钥，注意密钥不能包含：“@”，”+“，”-“，”=“ 字符
```

4. 配置 IKE 网关、出接口和协议版本。

```
set security ike gateway ike-gate-cfgr ike-policy ike-policy-cfgr
# 调用之前定义的IKE策略命名
set security ike gateway ike-gate-cfgr address 159.xx.xx.242
# 定义IKE的网关地址信息（对端VPN的公网地址）
set security ike gateway ike-gate-cfgr local-identity inet 120.xx.xx.76
set security ike gateway ike-gate-cfgr remote-identity inet 159.xx.xx.242
# 定义VPN标记，可以使用FQDN或者IP地址等，本实例使用本端及远端IP地址
set security ike gateway ike-gate-cfgr external-interface ge-0/0/y
# 绑定VPN的接口，即本地的公网出口
set security ike gateway ike-gate-cfgr version v1-only
# 定义IKE的版本，v1
```

5. 配置 IPsec 策略。

```
set security ipsec proposal ipsec-proposal-cfgr protocol esp
# 定义IPSEC阶段的加密协议
set security ipsec proposal ipsec-proposal-cfgr authentication-algorithm hmac-md5-96
# 定义IPSEC阶段的认证算法
set security ipsec proposal ipsec-proposal-cfgr encryption-algorithm aes-128-cbc
# 定义IPSEC阶段的加密算法
set security ipsec proposal ipsec-proposal-cfgr lifetime-seconds 3600
# 定义IPSEC阶段生存时间（范围：180～86400）
set security ipsec policy ipsec-policy-cfgr proposals ipsec-proposal-cfgr
# 调用之前定义的IPSEC算法定义
```

6. 应用 IPsec 策略。

```
set security ipsec vpn ipsec-vpn-cfgr ike gateway ike-gate-cfgr
# 调用之前定义的IKE网关配置
set security ipsec vpn ipsec-vpn-cfgr ike ipsec-policy ipsec-policy-cfgr
# 调用之前定义的 IPsec 策略配置
set security ipsec vpn ipsec-vpn-cfgr establish-tunnels immediately
# 配置VPN直接建立通道，而不是等待流量触发
set routing-options static route 10.1.1.0/24 next-hop x.x.x.x
# 基于策略的VPN需要将远端的网段配置路由从公网接口发出，x.x.x.x为设备的公网接口下一跳地址
```

7. 配置出站策略。

```
set security policies from-zone trust to-zone vpn policy trust-to-untrust_any_permit match source-address
vpn-local_subnet
set security policies from-zone trust to-zone vpn policy trust-to-untrust_any_permit match destination-
address vpn-peer_subnet
set security policies from-zone trust to-zone vpn policy trust-to-untrust_any_permit match application any
set security policies from-zone untrust to-zone trust policy trust-to-untrust_any_permit then permit tunnel
ipsec-vpn ipsec-vpn-cfgr
set security policies from-zone untrust to-zone trust policy trust-to-untrust_any_permit then permit tunnel
pair-policy untrust-to-trust_any_permit
# 定义访问策略，本策略为本地网段访问VPN对端业务网段方向的策略（trust to untrust），指定调用IPSEC VPN 通
道。具体的访问权限根据实际业务访问情况来设置
```

8. 配置入站策略。

```
set security policies from-zone vpn to-zone trust policy untrust-to-trust_any_permit match source-address
vpn-peer_subnet
set security policies from-zone vpn to-zone trust policy untrust-to-trust_any_permit match destination-
address vpn-local_subnet
set security policies from-zone vpn to-zone trust policy untrust-to-trust_any_permit match application any
set security policies from-zone vpn to-zone trust policy untrust-to-trust_any_permit then permit tunnel
ipsec-vpn ipsec-vpn-cfgr
set security policies from-zone vpn to-zone trust policy untrust-to-trust_any_permit then permit tunnel pair-
policy trust-to-untrust_any_permit
# 定义访问策略，本策略为对端VPN网段访问本地业务网段方向的策略（untrust to trust），指定调用IPSEC VPN 通
道。具体的访问权限根据实际业务访问情况来设置
```

9. 保存配置。

```
root@SRX1# commit
commit complete
# 在配置模式下面修改配置，不会直接生效，通过“commit”命令，修改的配置才会保存并生效
```

适用于基于路由转发的 VPN

1. 登录防火墙设备的命令行配置界面。

```
ssh -p 22 root@172.16.0.1
# 通过 SSH 命令登录防火墙命令行界面
root@SRX1> configure
Entering configuration mode
# 登录之后为操作模式，键入“configure”进入配置模式
[edit]
root@SRX1#
# “#” 表示已经进入配置模式
root@SRX1# commit
commit complete
# 在配置模式下面修改配置，不会直接生效，通过“commit”命令，修改的配置才会保存并生效
```

2. 配置防火墙网络接口、安全域、地址簿信息。

```
set interfaces ge-0/0/x unit 0 family inet address 172.16.0.1/16
# 为内部接口 ge-0/0/x定义 IP 地址，请更换为实际接口和IP
set interfaces ge-0/0/y unit 0 family inet address 120.xx.xx.76/30
# 为外部接口 ge-0/0/y定义 IP 地址，请更换为实际接口和IP
set interfaces st0 unit 0 family inet mtu 1398
# 定义通道接口，默认不设置 IP 地址，通道接口的 unit 后的参数需要指定，一个 unit 号可以绑定一个 VPN 通道，序号
范围：0-16385，同时设置通道接口MTU为1398
set security zones security-zone trust interfaces ge-0/0/x.0
# 绑定 ge-0/0/x 为内部安全区(trust)，对接内部业务区
set security zones security-zone untrust interfaces ge-0/0/y.0  host-inbound-traffic system-services ike
# 绑定ge-0/0/y为外部安全区(untrust)，对接外部广域网，并启用 ike 服务，表示该区域可以建立 VPN
set security zones security-zone vpn interfaces st0.0
```

```
# 绑定通道接口到 vpn 区域(vpn)，作为连接 IPSEC VPN 的逻辑通道,用于后续的路由策略以及访问策略
set security zones security-zone vpn address-book address vpn-peer_subnet 10.1.1.0/24
# 定义要访问的 VPN 对端的业务地址簿，用于后续的访问策略调用，命名可以自定义
set security zones security-zone trust address-book address vpn-local_subnet 172.16.0.0/16
# 定义本地的业务地址簿，用于后续的访问策略调用，命名可以自定义
```

3. 配置 IKE 策略。

```
set security ike proposal ike-proposal-cfgr authentication-method pre-shared-keys
# 定义 IPSEC VPN 认证方式（本实例使用共享密钥模式：pre-shared-keys），注意“ike-proposal-cfgr”为定义的命名，后续设置需要调用该命名
set security ike proposal ike-proposal-cfgr dh-group group2
# 定义 IKE 的 dh-group
set security ike proposal ike-proposal-cfgr authentication-algorithm md5
# 定义 IKE 认证算法
set security ike proposal ike-proposal-cfgr encryption-algorithm aes-128-cbc
# 定义 IKE 加密算法
set security ike proposal ike-proposal-cfgr lifetime-seconds 86400
# 定义 IKE 生存时间， 范围：(180-86400 seconds)
set security ike policy ike-policy-cfgr mode main
set security ike policy ike-policy-cfgr proposals ike-proposal-cfgr
set security ike policy ike-policy-cfgr pre-shared-key ascii-text "TestPassword"
# 定义 IKE 策略，指定模式以及密钥，需要调用上面步骤中的算法定义命名，注意密钥不能包含：“@”，”+“，”-“，”=“字符
```

4. 配置 IKE 网关、出接口和协议版本。

```
set security ike gateway ike-gate-cfgr ike-policy ike-policy-cfgr
# 调用之前定义的 IKE 策略命名
set security ike gateway ike-gate-cfgr address 159.xx.xx.242
# 定义 IKE 的网关地址信息（对端 VPN 的公网地址）
set security ike gateway ike-gate-cfgr local-identity inet 120.xx.xx.76
set security ike gateway ike-gate-cfgr remote-identity inet 159.xx.xx.242
#定义 VPN 标记，可以使用 FQDN 或者 IP 地址等（本实例使用远端及本端 IP 地址）
set security ike gateway ike-gate-cfgr external-interface ge-0/0/y
# 绑定 VPN 的接口，即本地的公网出口
set security ike gateway ike-gate-cfgr version v1-only
# 定义 IKE 的版本，v1
```

5. 配置 IPsec 策略。

```
set security ipsec proposal ipsec-proposal-cfgr protocol esp
# 定义 IPSEC 阶段的加密协议
set security ipsec proposal ipsec-proposal-cfgr authentication-algorithm hmac-md5-96
# 定义 IPSEC 阶段的认证算法
set security ipsec proposal ipsec-proposal-cfgr encryption-algorithm aes-128-cbc
# 定义 IPSEC 阶段的加密算法
set security ipsec proposal ipsec-proposal-cfgr lifetime-seconds 3600
# 定义 IPSEC 阶段的生存时间
set security ipsec policy ipsec-policy-cfgr proposals ipsec-proposal-cfgr
# 调用之前定义的 IPSEC 算法定义
set security ipsec vpn ipsec-vpn-cfgr ike proxy-identity local 172.16.0.0/16
set security ipsec vpn ipsec-vpn-cfgr ike proxy-identity remote 10.1.1.0/24
```

```
#设置 TS（Traffic Selector）或者 SPD 配置，默认为0.0.0.0/0，如果对端也指定了网段，则需要和对端匹配
set security ipsec vpn ipsec-vpn-cfgr bind-interface st0.0
# 绑定 VPN 通道接口
```

6. 应用 IPsec 策略。

```
set security ipsec vpn ipsec-vpn-cfgr ike gateway ike-gate-cfgr
# 调用之前定义的IKE网关配置
set security ipsec vpn ipsec-vpn-cfgr ike ipsec-policy ipsec-policy-cfgr
# 调用之前定义的 IPsec 策略配置
set security ipsec vpn ipsec-vpn-cfgr establish-tunnels immediately
# 配置 VPN 直接建立通道，而不是等待流量触发
set routing-options static route 10.1.1.0/24 next-hop st0.0
# 配置远端的业务 IP 网段，通过虚拟通道接口进行转发
```

7. 配置出站策略。

```
set security policies from-zone trust to-zone vpn policy trust-to-vpn_any_permit match source-address vpn-local_subnet
set security policies from-zone trust to-zone vpn policy trust-to-vpn_any_permit match destination-address vpn-peer_subnet
set security policies from-zone trust to-zone vpn policy trust-to-vpn_any_permit match application any
set security policies from-zone trust to-zone vpn policy trust-to-vpn_any_permit then permit
# 定义访问策略，本策略为本地网段访问 VPN 对端业务网段方向的策略（trust to vpn）。具体的访问权限根据实际业务访问情况来设置
```

8. 配置入站策略。

```
set security policies from-zone vpn to-zone trust policy vpn-to-trust_any_permit match source-address vpn-peer_subnet
set security policies from-zone vpn to-zone trust policy vpn-to-trust_any_permit match destination-address vpn-local_subnet
set security policies from-zone vpn to-zone trust policy vpn-to-trust_any_permit match application any
set security policies from-zone vpn to-zone trust policy vpn-to-trust_any_permit then permit
# 定义访问策略，本策略为对端 VPN 网段访问本地业务网段方向的策略（vpn to trust）。具体的访问权限根据实际业务访问情况来设置
```

9. 保存配置。

```
root@SRX1# commit
commit complete
#在配置模式下面修改配置，不会直接生效，通过“commit”命令，修改的配置才会保存并生效
```

绿盟防火墙配置

最近更新时间：2022-12-08 15:20:18

使用 IPsec VPN 建立腾讯云 VPC 到用户 IDC 的连接时，在配置完腾讯云 VPN 网关后，您还需要在用户 IDC 本地站点的网关设备中进行 VPN 配置。本文以绿盟防火墙为例，介绍如何在本地站点中进行 VPN 配置。

注意

- 本文以 NFNX3-V2000TX 型号、603.168版本防火墙配置演示，其他版本可能界面略有差异，整体配置逻辑一致。
- 本文仅支持 IKEv1 协议的配置。
- 本文所有 IP、接口等参数取值均仅用于举例，请具体配置时，使用实际值进行替换。

前提条件

请确保您已经在腾讯云 VPC 内 创建 VPN，并完成 VPN 通道配置。

数据准备

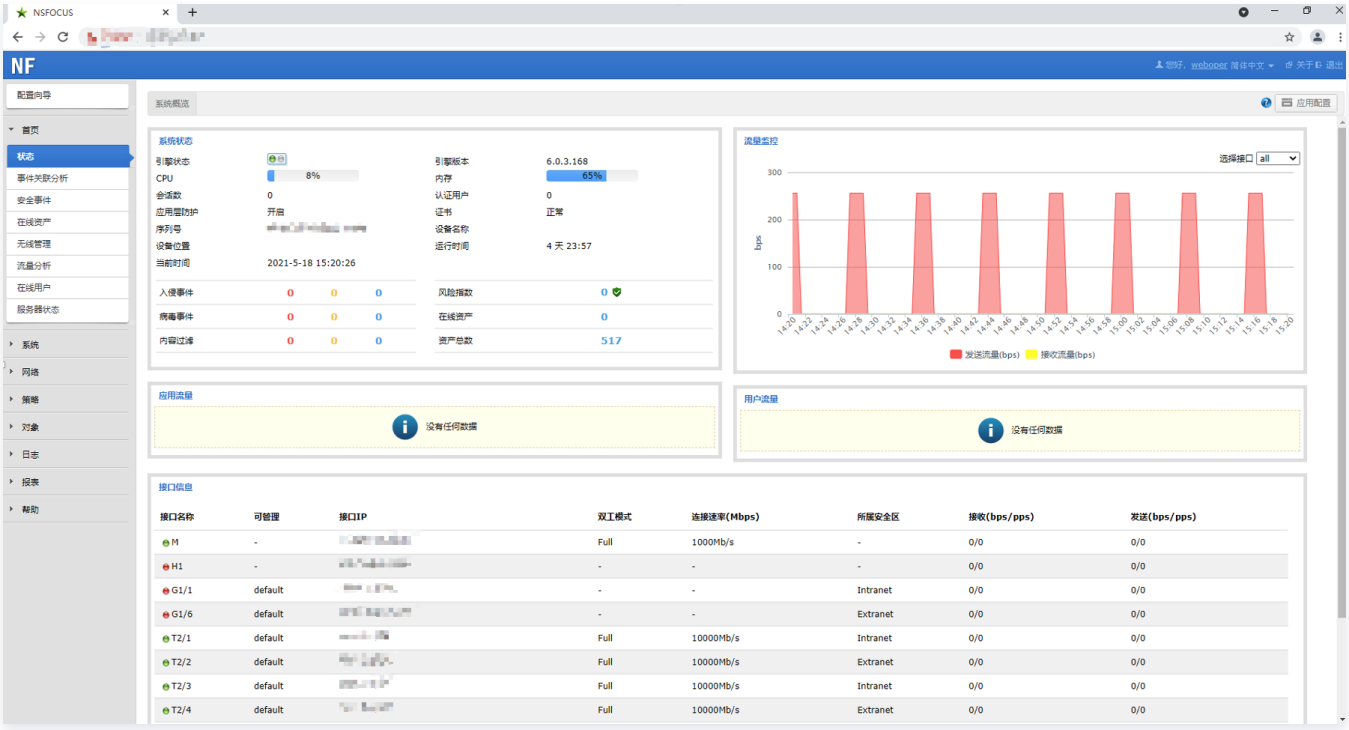
本文 IPsec VPN 配置数据举例如下：

配置项			示例值
网络配置	VPC 信息	子网 CIDR	10.1.1.0/24
		VPN 网关公网 IP	159.xx.xx.242
	IDC 信息	内网 CIDR	172.16.0.0/16
		网关公网 IP	120.xx.xx.76
IPsec 连接配置	IKE 配置	版本	IKEV1
		身份认证方法	预共享密钥
		PSK	tencent@123
		加密算法	AES-128
		认证算法	MD5
		协商模式	main
		本端标识	IP Address：120.xx.xx.76
		远端标识	IP Address：159.xx.xx.242
		DH group	DH2
		IKE SA Lifetime	86400
	IPsec 配置	加密算法	AES-128
		认证算法	MD5
		报文封装模式	Tunnel
		安全协议	ESP
		PFS	disable

		IPsec SA 生存周期（s）	3600s

操作步骤

1. 使用 weboper 登录 NSFOCUS 管理界面。



2. 在左侧菜单栏选择**网络 > 接口**，然后在 IPsec 接口页面单击**新建**。
3. 在**新建**页面配置 IPsec 相关信息，然后单击**确定**。

- 接口类型：选择 VPN。
- 子类型选择：选择 ipsec。
- 接口名称：不可修改，系统默认填充。
- 安全区：选择 **DMZ**。
  为了确保 IPsec 接口到内网的数据不被安全策略拦截阻断，请保持默认选项**DMZ**。
- IPv4：选择本地 VPC 网段，即**数据准备**阶段中 VPC 的子网 CIDR 的示例值10.1.1.1/24。

4. 在左侧菜单栏选择**网络** > **IPSEC** > **IPSEC 隧道**。
5. 在**第一阶段**页签，根据腾讯云 VPN 连接的 IKE 协议信息配置 IDC 侧的 IKE 协议。

*为必配项。

- 隧道名称：填写隧道名称。
- 本地接口：选择规划好的本地接口。
- HA 线路：选 HA 线路。
- IP 地址：选择 IPsec 所在服务器的IP地址。
- 客户端类型：选择**网关客户端**。
- 认证方式：选择**预共享密钥**。
- 预共享密钥：设置预共享密钥。

6. （可选）高级选项配置。
   如果您对 IPsec 策略有更高的要求，如认证算法、加密算法、ISAKMP-SA 存活时间等，需要进行高级配置。

本处仅介绍主要参数的配置说明。

- 本地/对端 ID 类型：
  - IPV4：输入标准的 IPv4 格式的地址。
  - 域名：字符数小于等于30个字符，且只能包含字母、数字、下划线、.（英文点号）和@。
  - 用户名：当前仅支持输入用户邮箱，例如：xxxx@nsfocus.com。
- DH 组：IPsec VPN 隧道使用的 DH 组。
- 认证算法：指定安全认证算法，例如 MD5。
- 加密算法：指定加密算法。

> **说明**
> 如果 步骤5 中认证方式选择了**预共享密钥**，该处可选有 DES、3DES、AES-128、AES-192、AES-256 以及 BLOWFISH，请依据实际需求选择。

7. **第一阶段**配置完成后单击**下一步**。
8. 在**第二阶段**页签，依据腾讯云 VPN 连接的 IPsec 协议信息配置 IDC 侧的 IPsec 协议。

> **注意**
> 子网间请勿存在包含关系。

8.1 在**第二阶段**页签单击**添加**。

8.2 **本地子网**填写 IDC 本端网段及掩码，例如172.16.0.0/16。

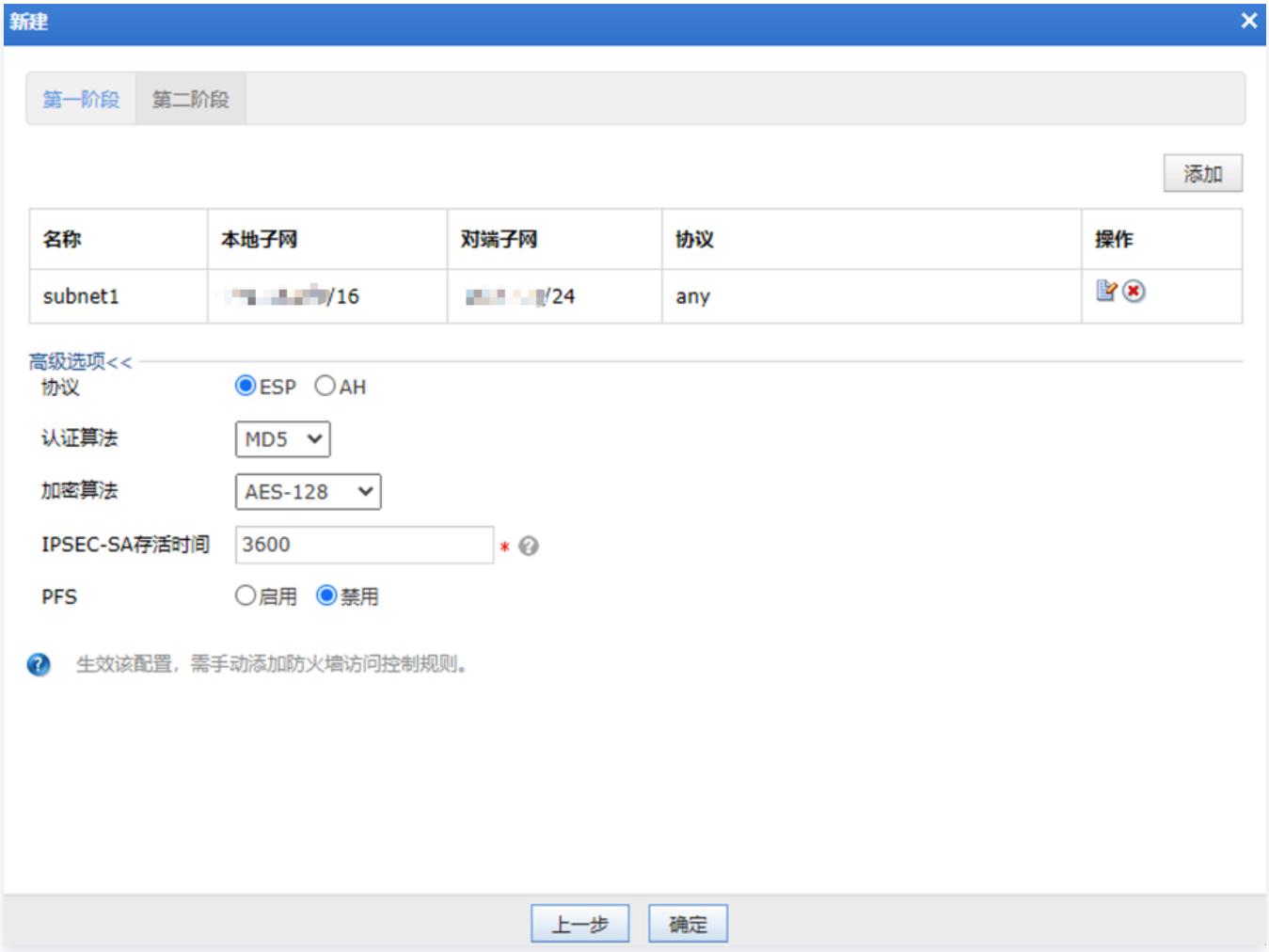
8.3 **对端子网**填写腾讯云 VPN 后端子网网段及掩，例如10.1.1.0/24。

8.4 **协议**选择 **any**。

8.5 高级配置。

- **协议**选择 **ESP**
- **认证算法**选择 **MD5**
- **加密算法**选 **AES-128**
- **IPSEC-SA 存活时间**配置为3600
- **PFS**设置为**禁用**

8.6 单击**确定**。



9. 测试 NSFOCUS 与腾讯云的连通性。

- NSFOCUS 与腾讯云 VPN 建立隧道后，NSFOCUS 侧自动生成相应的隧道信息条目。

隧道名	本地IP	对端地址	本地子网	对端子网	当前隧道状态	建立时间
tencent					ipsec隧道已建立	2021-05-06 10:45:05
tencent					ipsec隧道已建立	2021-05-06 10:45:05

- 在腾讯云 VPN 侧可查看连接状态。

ID/名称	监控	状态	对端网关	所属网络	预共享密钥	操作
ceshi		已联通	cgw	vpc 测试		重置 更多

- 在 NSFOCU 侧使用 Ping 命令 ping 腾讯云 VPC 内的云服务器，可正常通行。

思科防火墙配置

最近更新时间：2024-04-19 14:46:22

使用 IPsec VPN 建立腾讯云 VPC 到用户 IDC 的连接时，在配置完腾讯云 VPN 网关后，您还需要在用户 IDC 本地站点的网关设备中进行 VPN 配置。本文以思科防火墙为例，介绍如何在本地站点中进行 VPN 配置。

注意

- 本文为 Cisco ASA 系列防火墙通用配置，所有版本均支持。
- 本文所有 IP、接口等参数取值均仅用于举例，请具体配置时，使用实际值进行替换。

前提条件

请确保您已经在腾讯云 VPC 内 创建 VPN，并完成 VPN 通道配置。

数据准备

本文 IPsec VPN 配置数据举例如下：

配置项			示例值
网络配置	VPC 信息	子网 CIDR	10.1.1.0/24
		VPN 网关公网 IP	159.xx.xx.242
	IDC 信息	内网 CIDR	172.16.0.0/16
		网关公网 IP	120.xx.xx.76
IPsec 连接配置	IKE 配置	版本	IKEV1
		身份认证方法	预共享密钥
		PSK	tencent@123
		加密算法	AES-128
		认证算法	MD5
		协商模式	main
		本端标识	IP Address：120.xx.xx.76
		远端标识	IP Address：159.xx.xx.242
		DH group	DH2
		IKE SA Lifetime	86400
	IPsec 配置	加密算法	AES-128
		认证算法	MD5
		报文封装模式	Tunnel
		安全协议	ESP
		PFS	disable
		IPsec SA 生存周期（s）	3600s

		IPsec SA 生存周期（KB）	1843200KB
防火墙配置	接口信息	Nameif	outside

操作步骤

适用于基于 SPD 策略转发的 VPN（IKEv1）

1. 登录防火墙设备命令配置界面。

```
  ssh -p admin@10.XX.XX.56

# 通过 SSH 命令登录防火墙配置界面。

User Access Verification
Username: admin
Password: *******
Type help or '?' for a list of available commands.

# 输入账号密码，进入用户模式。

ASA>
ASA> en
Password:

# 输入 enable 和设置的 enable 密码进入特权模式，该模式下只支持查看。

ASA# conf t
ASA(config)#

# 键入“config ter”进入全局模式，在该模式下进行防火墙配置。
```

2. 配置防火墙接口。
在全局模式下配置对接腾讯云端的防火墙接口。

```
interface GigabitEthernet0/0
nameif outside  # 定义端口的安全域名。
security-level 0  # 定义端口的安全域等级。
ip address 120.XX.XX.76 255.255.255.252  # 配置 VPN 通道本端公网 IP 地址。
```

3. 配置 isakmp 策略。

```
crypto ikev1 enable outside  # 在外部接口上启用 IKE。
crypto ikev1 policy 10  # 定义 ikev1 第一阶段协商使用参数，序号为10，序号越小越优先，范围为1-65535。
authentication pre-share  # 配置认证方法为预共享密钥。
encryption AES-128  #配置第一阶段协商数据包封装加密算法，默认为AES-128。
hash MD5  # 为 IKE 策略指定哈希算法为 MD5，默认为 SHA。
group 2  # 为 IKE 策略指定 Diffie-Hellman 组为组2，默认为 group 2
lifetime 86400  # 指定 SA 生命周期，默认为86400秒。
```

4. 配置预共享密码。

```
tunnel-group 159.XX.XX.242 type ipsec-l2l  # 创建一个ipsec隧道组，type 为点到点。
tunnel-group 159.XX.XX.242 ipsec-attributes  # 配置隧道组属性，并指定预共享密钥。
ikev1 pre-shared-key tencent@123  # 密钥可为1～128个字符的字母、数字或者字符串。
```

5. 配置 IPsec 安全协议。

```
crypto ipsec ikev1 transform-set TS esp-aes esp-md5-hmac  # 指定 IPsec 第二阶段协商的加密算法以及哈希算法。
```

6. 配置 ACL。

```
access-list INTERESTING extended permit ip 172.XX.XX.0 255.255.0.0 10.1.1.0 255.255.255.0  # 配置 ACL 抓取 VPN 通道上的数据流。
```

7. 配置 IPsec 策略。

```
crypto map CMAP 1 match address INTERESTING  # 调用 ACL，使满足 ACL 的源网段或者目的网段的数据包在 VPN 通道上流通。
crypto map CMAP 1 set peer 159.XX.XX.242  # 将被 IPsec 保护的流量转发到的对端 VPN 公网地址，本文此处为腾讯云 VPN 公网地址。
crypto map CMAP 1 set ikev1 transform-set TS  # 为加密映射条目配置 IKEv1 协议。
crypto map CMAP 1 set security-association lifetime seconds 3600  # 配置加密密钥的生存时间。
```

8. 启用 IPsec 策略。

```
rypto map CMAP interface outside  # 将上一步配置的加密映射应用于外部接口。
```

9. 配置静态路由。

```
route outside 10.1.1.0 255.255.255.0 159.XX.XX.242 1  # 将待加密保护的数据网段引向 IPsec 隧道，且配置下一跳为 VPN 隧道对端公网 IP。
```

10. 测试 VPN 连通性。

执行 Ping 命令测试 VPN 的连通性。

适用于基于路由转发的 VPN（IKEv1）

1. 登录防火墙设备命令配置界面。

```
  ssh -p admin@10.XX.XX.56

# 通过 SSH 命令登录防火墙配置界面。

User Access Verification
Username: admin
Password: *******
Type help or '?' for a list of available commands.

# 输入账号密码，进入用户模式。

ASA>
ASA> en
Password:

# 输入enable和设置的enable密码进入特权模式，该模式下只支持查看。

ASA# conf t
ASA(config)#

# 键入“config ter”进入全局模式，在该模式下进行防火墙配置。
```

2. 配置防火墙接口。
   在全局模式下配置对接腾讯云端的防火墙接口

```
interface GigabitEthernet0/0
nameif outside  # 定义端口的安全域名。
security-level 0  # 定义端口的安全域等级。
ip address 120.XX.XX.76 255.255.255.252  # 配置 VPN 通道本端的公网 IP 地址。
```

3. 配置 isakmp 策略。

```
crypto ikev1 policy 10  # 定义 ikev1 第一阶段协商使用参数，序号为10，序号越小越优先，范围为1-65535。
authentication pre-share  # 配置认证方法为预共享密钥。
encryption AES-128  # 配置第一阶段协商数据包封装加密算法，默认为AES-128。
hash MD5  # 为 IKE 策略指定哈希算法为 MD5，默认为 SHA。
group 2  # 为 IKE 策略指定 Diffie-Hellman 组为组2，默认为 group 2
lifetime 86400  # 指定 SA 生命周期，默认为86400秒。
```

4. 配置预共享密码。

```
tunnel-group 159.XX.XX.242 type ipsec-l2l  # 创建一个ipsec隧道组，type 为点到点。
tunnel-group 159.XX.XX.242 ipsec-attributes  # 配置隧道组属性，并指定预共享密钥。
 ikev1 pre-shared-key tencent@123  # 密钥可为1～128个字符的字母、数字或者字符串。
```

5. 配置 IPsec 安全协议。

```
crypto ipsec ikev1 transform-set TS esp-aes esp-md5-hmac  # 指定 IPsec 第二阶段协商的加密算法以及哈希算法。
```

6. 配置 IPsec 策略。

```
crypto ipsec profile PROFILE1
set ikev1 transform-set TS  # 为加密映射条目指定IKEv1 ipsec安全提议
set security-association lifetime kilobytes 1843200  # 设置 SA 生命周期内，VPN之间可以传递的流量字节数。
set security-association lifetime seconds 3600  # 设置加密密钥的生命周期，默认千字节数为4,608,000；默认生命周期秒数28,800。
```

7. 启用 IPsec 策略。

```
interface Tunnel100
tunnel source interface outside  # 配置 VPN 的更新源为outside口。
tunnel destination 159.XX.XX.242  # 配置对端 VPN 的公网 IP 地址，本处为腾讯云 VPN 公网 IP 地址。
tunnel mode ipsec ipv4  # 配置 tunnel口 使用的协议。
tunnel protection ipsec profile PROFILE1  # 调用 IPsec 策略对经过 tunnel 口的数据进行保护。
```

8. 配置静态路由。

```
route vti 10.1.1.0 255.255.255.0 159.XX.XX.242  # 将待加密保护的数据包引到 tunnel 口。
```

9. 测试 VPN 连通性。
执行 Ping 命令测试 VPN 的连通性。

适用于基于 SPD 策略转发的 VPN（IKEv2）

1. 登录防火墙设备命令配置界面。

```
ssh -p admin@10.XX.XX.56

# 通过 SSH 命令登录防火墙配置界面。

User Access Verification
Username: admin
```

```
Password: *******
Type help or '?' for a list of available commands.

# 输入账号密码，进入用户模式。

ASA>
ASA> en
Password:

# 输入enable和设置的enable密码进入特权模式，该模式下只支持查看。

ASA# conf t
ASA(config)#

# 键入“config ter”进入全局模式，在该模式下进行防火墙配置。
```

2. 配置防火墙接口。
   在全局模式下配置对接腾讯云端的防火墙接口。

```
interface GigabitEthernet0/0
nameif outside  # 定义端口的安全域名。
security-level 0  # 定义端口的安全域等级。
ip address 120.XX.XX.76 255.255.255.252  # 配置 VPN 通道本端公网 IP 地址。
```

3. 配置 isakmp 策略。

```
crypto ikev2 enable outside  # 在外部接口上启用 IKEv2。
crypto ikev2 policy 10  # 定义 ikev2 第一阶段协商使用参数，序号为10，序号越小越优先，范围为1-65535。
authentication pre-share  # 配置认证方法为预共享密钥。
encryption AES-128  # 配置第一阶段协商数据包封装加密算法，默认为AES-128。
integrity MD5  # 为 IKE 策略指定哈希算法为 MD5，默认为 SHA。
group 2  # 为 IKE 策略指定 Diffie-Hellman 组为组2，默认为 group 2。
prf sha # 设置加密算法。
lifetime seconds 86400  # 设置 SA 生命周期，默认为86400秒。
```

4. 配置组策略

```
group-policy group_policy internal  # 为设备设置组策略。
group-policy group_policy attributes  # 设置组策略属性。
vpn-tunnel-protocol ikev2 # 配置 vpn-tunnel 使用协议为 ikev2。
```

5. 配置预共享密码。

```
tunnel-group 159.XX.XX.242 type ipsec-l2l  # 创建一个ipsec隧道组，type 为点到点。
tunnel-group 159.XX.XX.242 general-attributes default-group-policy group_policy  # 调用上一步定义的组策略。
tunnel-group 159.XX.XX.242 ipsec-attributes  # 配置隧道组的属性，并指定预共享密钥。
ikev2 remote-authentication pre-shared-key tencent@123
ikev2 local-authentication pre-shared-key tencent@123  # 密钥可为1～128个字符的字母、数字或者字符串。
```

6. 配置 IPsec 安全协议。

```
crypto ipsec ikev2 ipsec-proposal ikev2_proposal  # 配置 IPsec 第二阶段协商的加密算法以及哈希算法。
protocol esp encryption aes-128  # 配置加密算法。
protocol esp integrity sha-1 # 配置完整性检查算法。
```

7. 配置 ACL。

```
access-list INTERESTING extended permit ip 172.XX.XX.0 255.255.0.0 10.1.1.0 255.255.255.0  # 配置 ACL 抓取 VPN 通道上的数据流。
```

8. 配置 IPsec 策略。

```
crypto map CMAP 1 match address INTERESTING  # 调用 ACL，使满足 ACL 的源网段或者目的网段的数据包在 VPN 通道上流通。
crypto map CMAP 1 set peer 159.XX.XX.242  # 将被 IPsec 保护的流量转发到的对端 VPN 公网地址，本文此处为腾讯云 VPN 公网地址。
crypto map CMAP 1 set ikev2 ipsec-proposal ikev2_proposal # 为加密映射条目配置 IKEv2 安全协议。
crypto map CMAP 1 set security-association lifetime seconds 3600 # 配置加密密钥的生存时间。
crypto map CMAP 1 set security-association lifetime kilobytes 1843200  # 设置协商在 SA 生命周期内，VPN 间可传递的流量，默认千字节数为4,608,000；默认生命秒数是28,800。
```

9. 启用 IPsec 策略。

```
rypto map CMAP interface outside  # 将上一步配置的加密映射应用于外部接口。
```

10. 配置静态路由。

```
route outside 10.1.1.0 255.255.255.0 159.XX.XX.242 1  # 将待加密保护的数据网段引向 IPsec 隧道，且配置下一跳为 VPN 隧道对端公网 IP。
```

11. 测试 VPN 连通性。

执行 Ping 命令测试 VPN 的连通性。

适用于基于路由转发的 VPN（IKEv2）

1. 登录防火墙设备命令配置界面。

```
ssh -p admin@10.XX.XX.56

# 通过 SSH 命令登录防火墙配置界面。

User Access Verification
Username: admin
Password: *******
Type help or '?' for a list of available commands.

# 输入账号密码，进入用户模式。

ASA>
ASA> en
Password:

# 输入enable和设置的enable密码进入特权模式，该模式下只支持查看。

ASA# conf t
ASA(config)#

# 键入“config ter”进入全局模式，在该模式下进行防火墙配置。
```

2. 配置防火墙接口。
   在全局模式下配置对接腾讯云端的防火墙接口以及Tunnel口。

```
interface GigabitEthernet0/0
nameif outside  # 定义端口的安全域名。
security-level 0 # 定义端口的安全域等级。
ip address 120.XX.XX.76 255.255.255.252  # 配置对接腾讯云 VPN 公网 IP 地址。
interface Tunnel100
nameif vti
ip address 172.XX.XX.2 255.255.255.0 # 该 IP 地址用于激活 Tunnel 口。
```

3. 配置 isakmp 策略。

```
crypto ikev2 policy 1   # 定义 ikev2 第一阶段协商使用参数，序号为1，序号越小越优先，范围为1-65535。
encryption AES-128   # 配置第一阶段协商数据包封装加密使用AES-128算法，默认为AES-128。
integrity MD5  /# 为IKE策略配置哈希算法为MD5，默认为sha。
group 2  # 为IKE策略配置 Diffie-Hellman 组为组2，默认为group 2。
prf sha # 配置加密算法。
lifetime seconds 86400  # 配置 SA 生存时间（即生命周期），默认为86400秒。
```

4. 配置组策略

```
group-policy group_policy internal  # 为设备设置组策略。
group-policy group_policy attributes  # 设置组策略属性。
vpn-tunnel-protocol ikev2 # 配置 vpn-tunnel 使用协议为 ikev2。
```

5. 配置预共享密码。

```
tunnel-group 159.XX.XX.242 type ipsec-l2l  # 创建一个ipsec隧道组，type 为点到点。
tunnel-group 159.XX.XX.242 general-attributes default-group-policy group_policy  # 调用上一步定义的组策略。
tunnel-group 159.XX.XX.242 ipsec-attributes  # 配置隧道组的属性，并指定预共享密钥。
ikev2 remote-authentication pre-shared-key tencent@123
ikev2 local-authentication pre-shared-key tencent@123  # 密钥可为1~128个字符的字母、数字或者字符串。
```

6. 配置 IPsec 安全协议。

```
crypto ipsec ikev2 ipsec-proposal ikev2_proposal  # 设置 IPsec 第二阶段协商的加密算法以及哈希算法。
protocol esp encryption aes-128  # 设置加密算法。
protocol esp integrity sha-1 # 设置完整性检查算法。
```

7. 配置 IPsec 策略。

```
crypto ipsec profile PROFILE1
set ikev2 ipsec-proposal ikev2_proposal  /# 为加密映射条目设置 IKEv2 安全协议。
set security-association lifetime kilobytes 1843200  # 设置 SA 生命周期内，VPN之间可以传递的流量字节数。
set security-association lifetime seconds 3600  # 设置加密密钥的生命周期，默认千字节数为4,608,000；默认生命秒数是28,800。
```

8. 启用 IPsec 策略。

```
interface Tunnel100
tunnel source interface outside  # 配置 VPN 的更新源为outside口。
tunnel destination 159.XX.XX.242  # 配置对端 VPN 的公网 IP 地址，本处为腾讯云 VPN 公网 IP 地址。
tunnel mode ipsec ipv4  #  配置 tunnel口 使用的协议。
tunnel protection ipsec profile PROFILE1  # 调用 IPsec 策略对经过 tunnel 口的数据进行保护。
```

9. 配置静态路由。

```
route vti 10.1.1.0 255.255.255.0 159.XX.XX.242  # 将待加密保护的数据包引到 tunnel 口。
```

10. 测试 VPN 连通性。

执行 Ping 命令测试 VPN 的连通性。

SSL VPN
SSL VPN 访问控制实践指引（okta）

最近更新时间：2024-04-23 16:02:51

本文介绍如何使用第三方 IDP（okta）和 SSL VPN 实现访问控制，提升您业务的安全性。

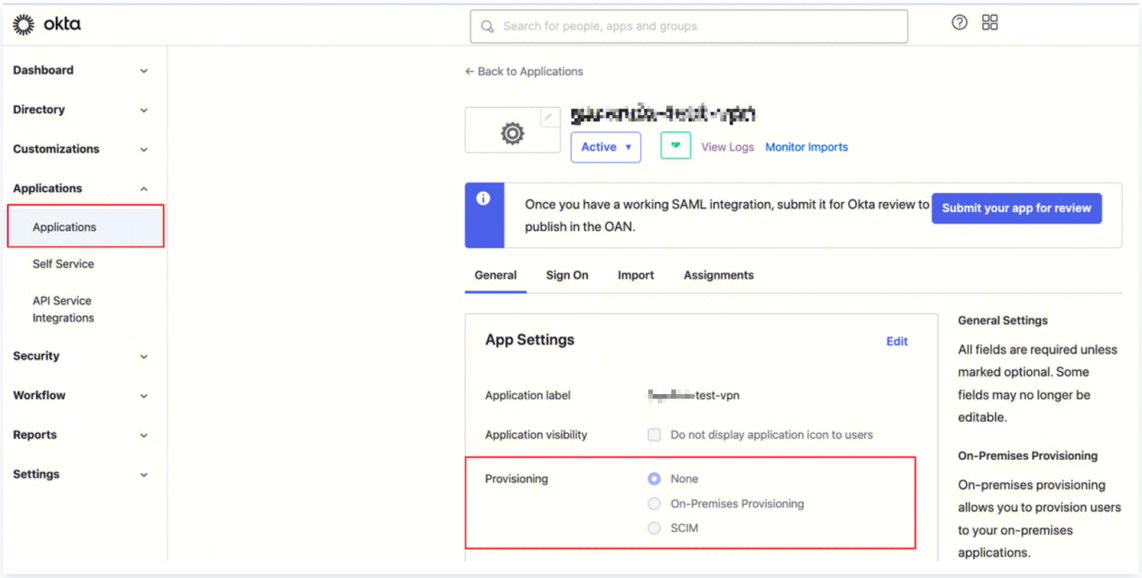
说明：
- 目前 SSO 身份认证功能灰度中，如需使用，请提交 工单申请 。
- 支持基于 SAML2.0 的主流第三方 IDP，如 Okta。
- 支持版本 VPN4.0。

操作流程

步骤1：（租户管理员）IDP 配置（okta）

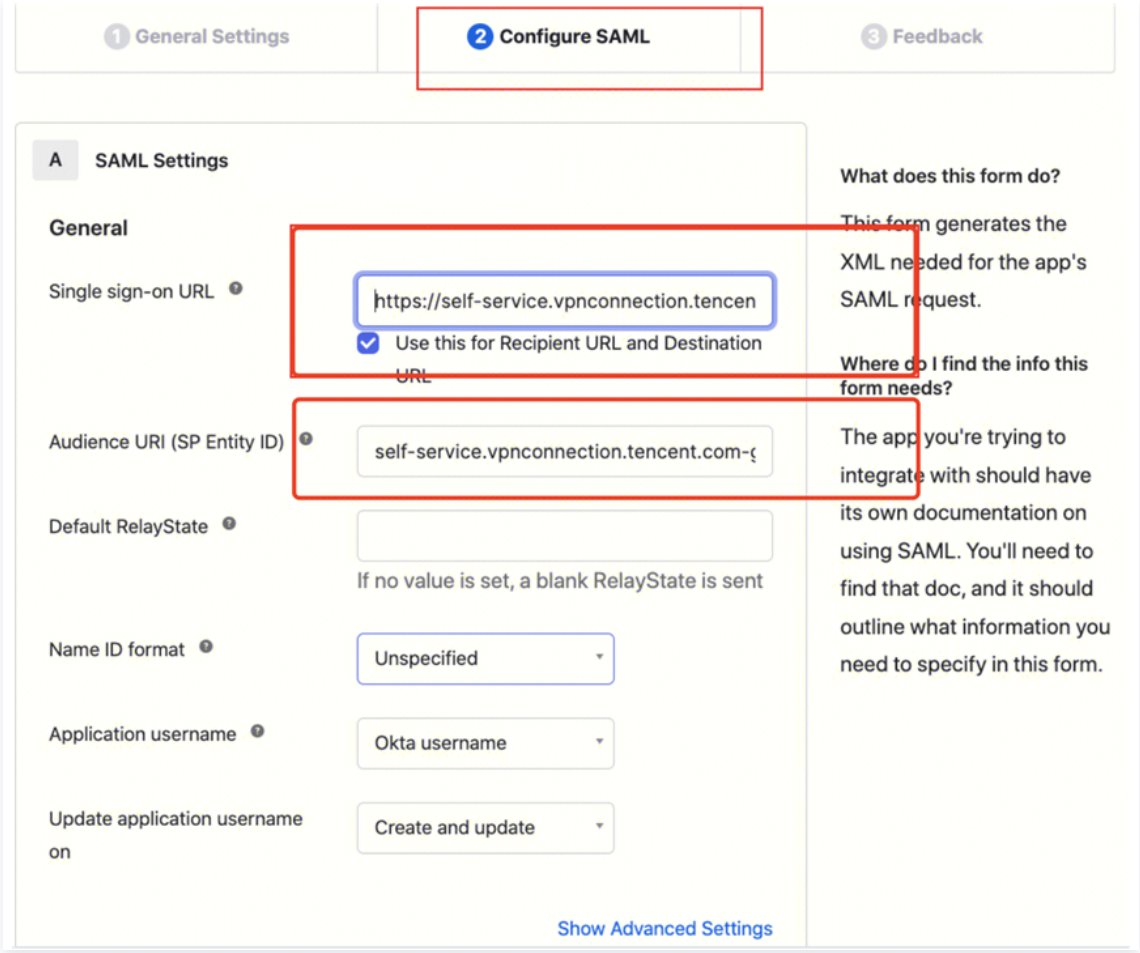
Okta 为第三方 IDP 系统，本节点仅介绍重点参数配置，Okta 具体操作步骤请查看 Okta 官网或者 okta 单点登录腾讯云指南 。
通过本步骤配置 Okta 和腾讯云之间的信任关系使之相互信任。

1. 登录 Okta 官网，并创建 Okta 应用程序。
2. 进入 Applications 页面，并单击应用名称，然后在 General 页签单击 **Edit**。

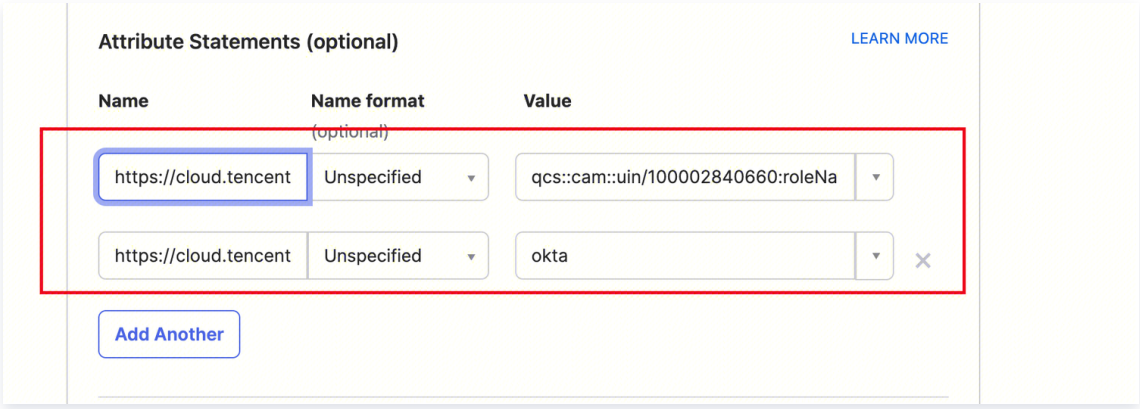


3. 在 Configure SAML 页面配置 Single sign-on URL 和 Audience URL(SP Entity ID)。

说明：
- Single sign-on URL：`https://self-service.vpnconnection.tencent.com/api/auth/sso-v2/saml`，此项为固定值。
- Audience URI (SP Entity ID)：腾讯云 Client VPN 自助服务门户 。

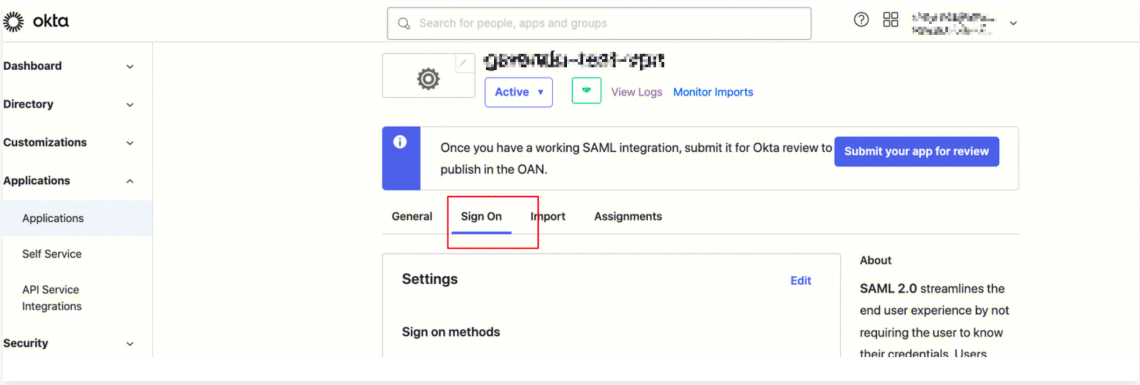


4. 在配置 SAML/Configure SAML 页面将 GENERAL 下 ATTRIBUTE STATEMENTS 补充为以下信息。

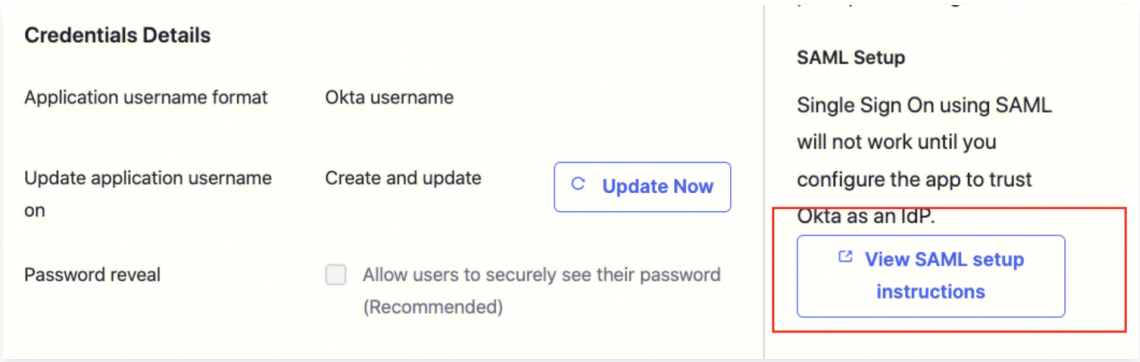


Name	Value
https://cloud.tencent.com/SAML/Attributes/Role:	qcs::cam::uin/{AccountID}:roleName/{RoleName},qcs::cam::uin/{AccountID}:saml-provider/{ProviderName}
https://cloud.tencent.com/SAML/Attributes/RoleSessionName	okta

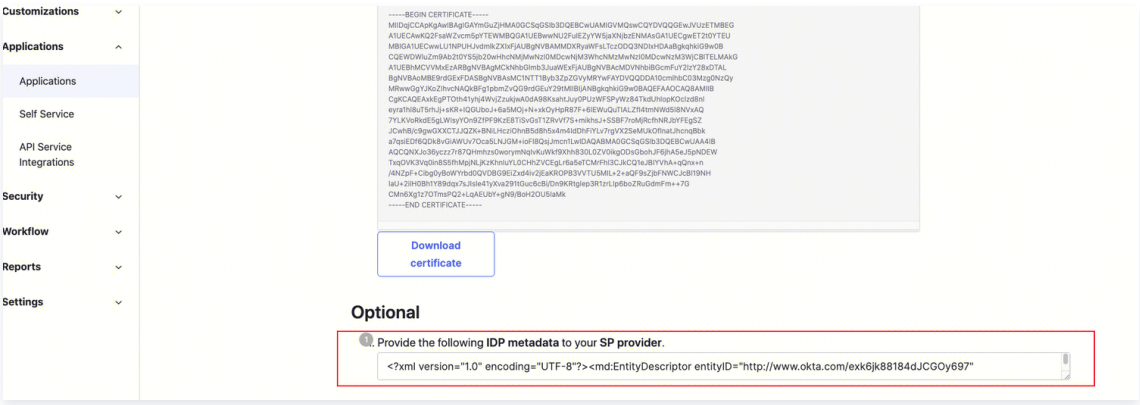
5. 在 Sign on 页签获取生成并下载 IDP 的 SAML-Metadata 文件。



单击 View SAML setup instructions.



单击 Download certificate，下载好的文件需要在腾讯云 CAM 身份配置时上传，



步骤2：（租户管理员）CAM 身份配置

1. 登录访问管理（CAM）控制台，进入 身份提供商 > 角色SSO 页面，单击**新建提供商**。

2. 在新建身份提供商页面，选择提供商类型为 SAML 并配置提供商信息，单击**下一步**。

- 身份提供商名称：输入身份提供商名称。
- 备注信息：输入您对当前身份提供商的备忘信息。
- 元数据文档：即 步骤1：（租户管理员）IDP 配置（okta） 中下载的文件。您需要在元数据文档上传 IDP 配置中下载的 SAML-Metadata 数据文档，元数据文档内容检验合法即可上传成功。

步骤3：（租户管理员）VPN 资源配置

创建 SSL VPN 网关

1. 登录 私有网络控制台，在左侧导航栏中选择 **VPN 连接** > **VPN 网关**，进入管理页。
2. 在 VPN 网关管理页面，单击**新建**，并在弹出的**新建 VPN 网关**页面，依据界面参数配置 SSL VPN 网关。

创建 SSL 服务端

1. 在左侧导航栏中选择 **VPN 连接** > **SSL 服务端**，进入管理页。
2. 在 SSL 服务端管理页面，单击**新建**，在弹出的**新建 SSL 服务端**对话框中，依据界面参数配置 SSL 服务端。
   - 认证方式：该认证方式默认 SSL 服务端可被 SSL 客户端全量访问。
   - 身份提供商：当前身份提供商为腾讯云 CAM，详情可查看 身份提供商 使用说明。

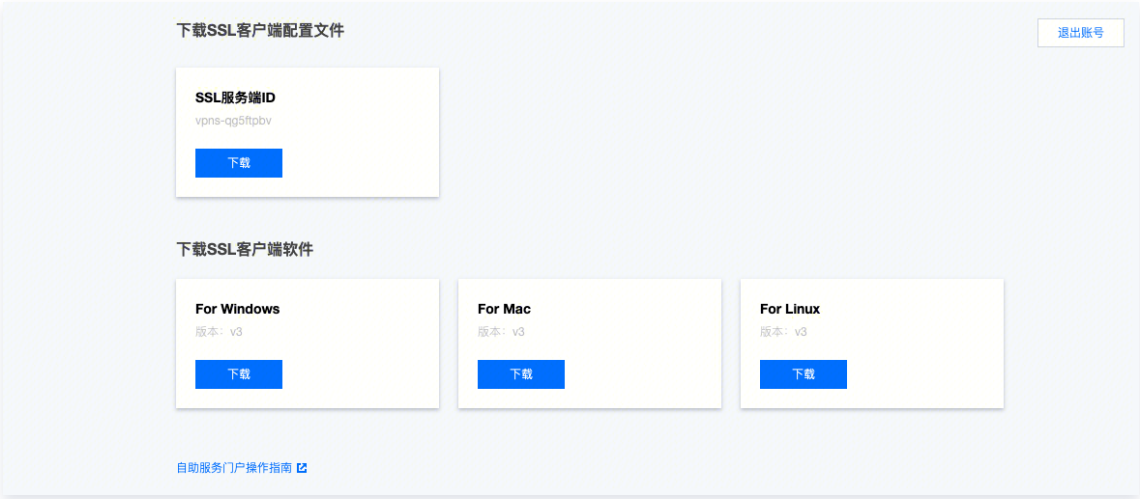
步骤4：（租户）在 Client VPN 门户下载 SSL 客户端配置文件和 SSL 客户端

1. 通过您本地浏览器访问 腾讯云Clinet VPN 自主服务门户 。
2. 在 SSL 服务端 ID 所在行的输入框中输入创建好的 SSL 服务端 ID，然后单击**下一步**，开始 SSO 认证。
   如果您没有或者不确定 SSL 服务端 ID ，可联系租户管理员获取。

3. 单击**跳转进行认证（SAML）**后，您需要完成您的管理员指定的认证程序。

如果您没有账号或在认证登录过程中遇到其他问题，请联系您的租户管理员。在您完成认证并成功登录后，将自动登录您的业务系统。

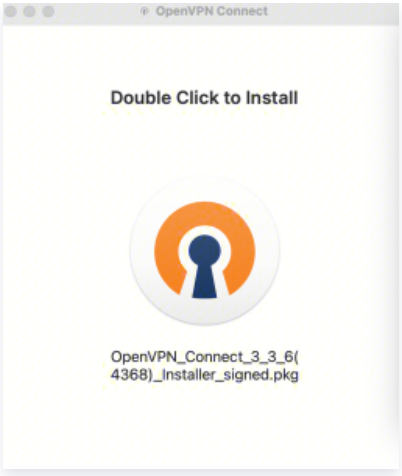
4. 在**下载SSL客户端配置文件**区域找到您需要下载的客户端配置文件，单击**下载**。



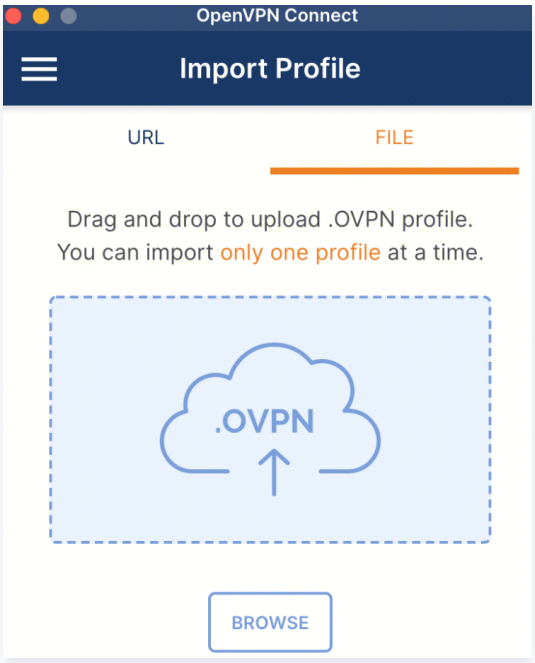
步骤5：（租户）SSL 客户端安装与连接

> **说明：**
> 客户端 OpenVPN 请使用3.4.0及以上版本。

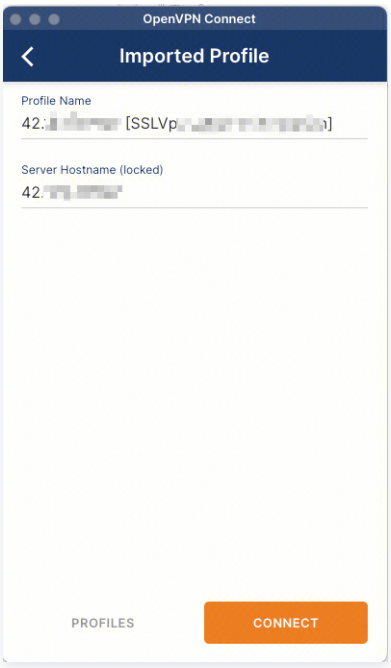
1. 在本地解压安装包，双击安装程序依据界面提示进行安装。



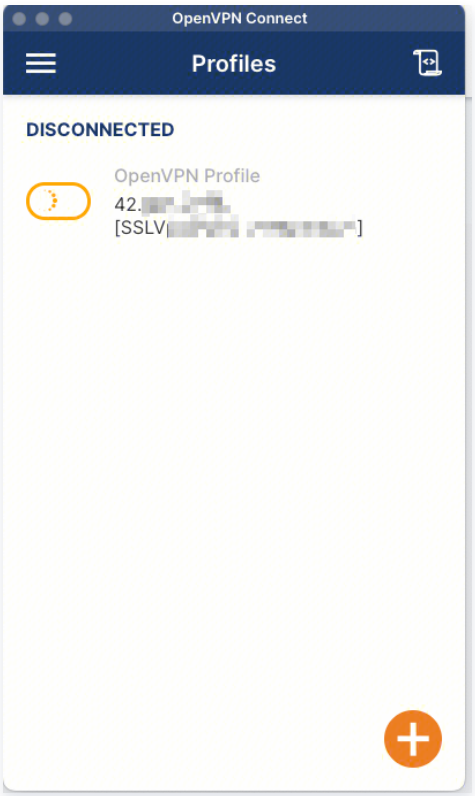
2. SSL 客户端安装完成后，选择“Import Profile”菜单中的“FILE”页面，上传已下载的 SSL 客户端配置文件（.ovpn 格式）。



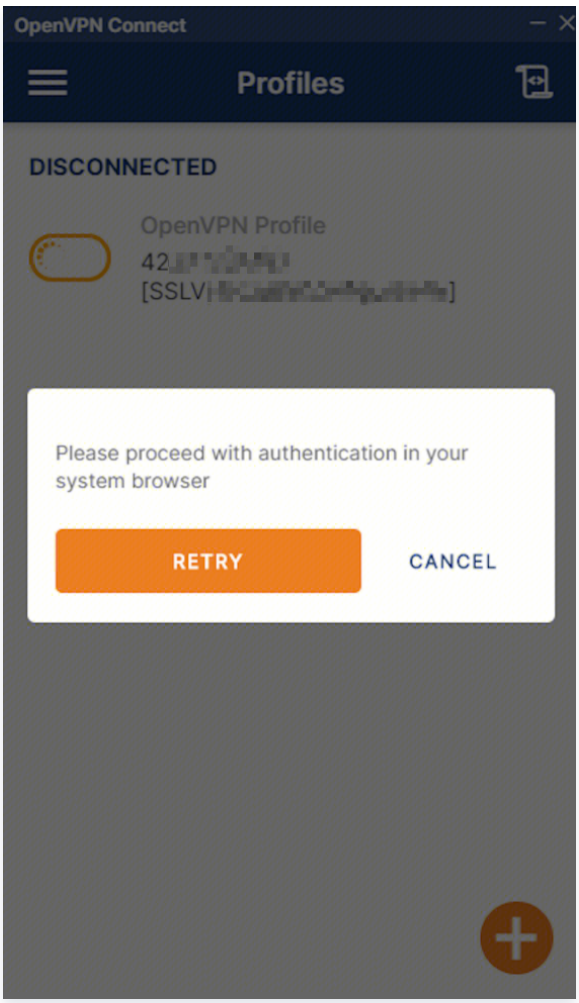
3. 上传成功后，选择 connect 进行连接。



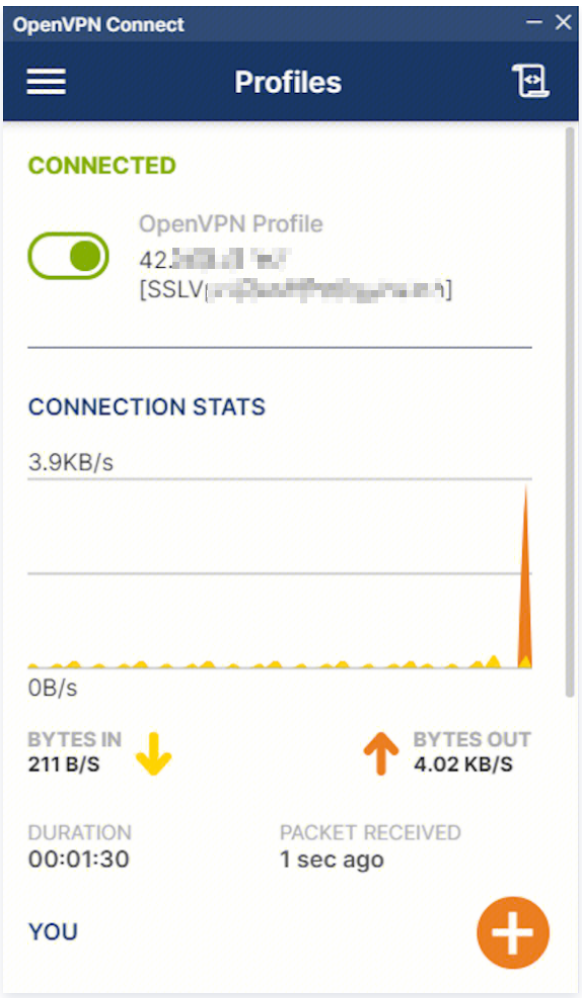
4. Profiles 连接中，请稍候。



5. 进行认证登录。


OpenVPN Connect
Profiles
DISCONNECTED
OpenVPN Profile
42
[SSLV
Please proceed with authentication in your system browser
RETRY
CANCEL

6. 连接成功。


OpenVPN Connect
Profiles
CONNECTED
OpenVPN Profile
42.
[SSLV
CONNECTION STATS
3.9KB/s
0B/s
BYTES IN
211 B/S
BYTES OUT
4.02 KB/S
DURATION
00:01:30
PACKET RECEIVED
1 sec ago
YOU

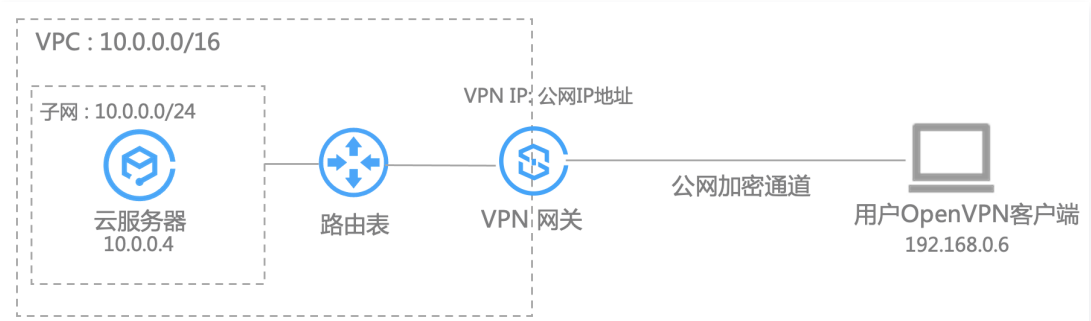
建立客户端与 VPC 连接

最近更新时间：2023-02-03 14:32:57

本文为您介绍 Windows、MAC 和 Linux 客户端如何通过 SSL VPN 连接 VPC。

背景信息

本文以下图场景为例，为您介绍 Windows、MAC 和 Linux 客户端如何使用 SSL VPN 连接VPC。



VPC路由表			SSL 服务端配置	
目的端	下一跳类型	下一跳	本端网段	10.0.0.0/16
10.0.0.0/16	Local	Local	客户端网段	192.168.0.0/16
192.168.0.0/16	VPN网关	vpngw-12345678		

配置流程

客户端通过 SSL VPN 连接 VPC 流程图如下所示：

步骤1：创建 SSL VPN 网关

1. 登录 私有网络控制台 。
2. 在左侧目录中单击 **VPN 连接** > **VPN 网关**，进入管理页。
3. 在 VPN 网关管理页面，单击**新建**。
4. 在弹出的新建 VPN 网关对话框中，配置如下网关参数。

参数名称	参数说明
网关名称	填写 VPN 网关名称，不超过60个字符。
所在地域	展示 VPN 网关所在地域。
可用区	选择当前网关所在的可用区。
协议类型	选择 SSL。
带宽上限	请根据业务实际情况，合理设置 VPN 网关带宽上限。
关联网络	表示您创建私有网络类型的 VPN。
所属网络	选择 VPN 网关将要关联的具体私有网络。
SSL 连接数	连接客户端的数量，一个 SSL 客户端仅允许一个用户连接，不支持一个 SSL 客户端连接多个客户。
计费方式	SSL VPN 默认为按流量计费。

5. 完成网关参数设置后，单击**创建**。

步骤2：创建 SSL 服务端

1. 登录 私有网络控制台 。
2. 在左侧目录中单击 **VPN 连接** > **SSL 服务端**，进入管理页面。

> **说明**
> 一个VPN网关仅支持关联一个SSL 服务端，详情请参见 使用限制 。

3. 在 SSL 服务端管理页面，单击**新建**。
4. 在弹出的新建 SSL 服务端对话框中，配置如下参数。

参数名称	参数说明
名称	填写 SSL 服务端名称，不超过60个字符。
地域	展示 SSL 服务端所在地域。
VPN 网关	选择创建好的 SSL VPN 网关。
云端网段	客户移动端访问的云上网段。
客户端网段	分配给用户移动端进行通信的网段，该网段请勿与腾讯侧 VPC CIDR 冲突，同时也不能与您本地的网段冲突。
协议	服务端传输协议。
端口	填写 SSL 服务端用于数据转发的端口。
认证算法	目前支持 SHA1 和 MD5 两种认证算法。
加密算法	目前支持 AES-128-CBC、AES-192-CBC 和 AES-256-CBC 加密算法。
是否压缩	否。

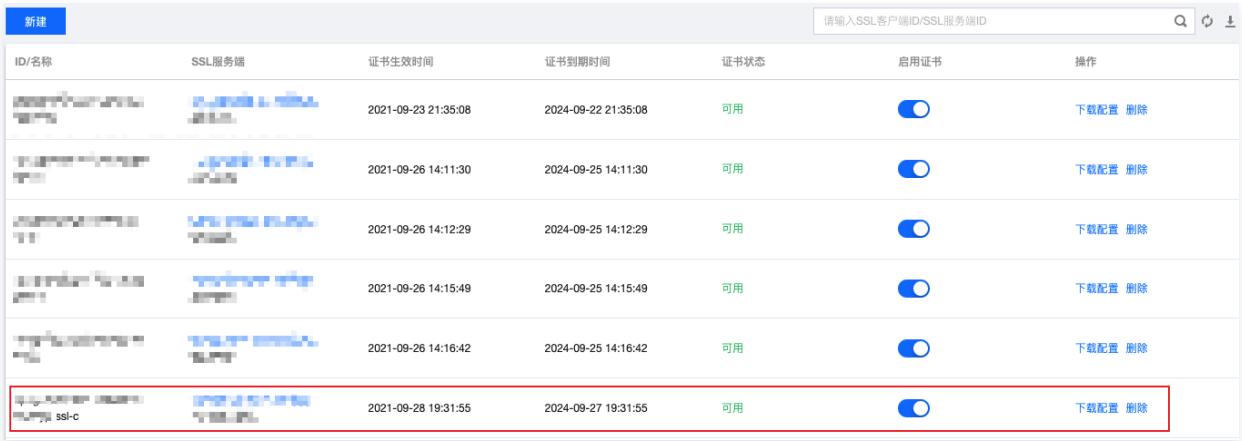
5. 完成网关参数设置后，单击**创建**。

步骤3：创建 SSL 客户端

1. 登录 私有网络控制台 。
2. 在左侧目录中单击 **VPN 连接** > **SSL 客户端**，进入管理页面。
3. 在 SSL 客户端管理页面，单击**新建**。
4. 在弹出的 SSL 客户端对话框中，配置如下参数。

5. 完成 SSL 客户端参数设置后，单击**确定**，当证书状态为可用表示创建完成。
6. 在 SSL 客户端页面，找到已创建的客户端证书，然后在操作列单击**下载配置**。

> **说明**
> 一个 SSL 客户端仅允许一个用户连接，不支持一个 SSL 客户端连接多个客户。



步骤4：配置 VPC 内路由

1. 登录 私有网络控制台 。
2. 在左侧目录中单击路由表，进入管理页面。

3. 在列表中，单击需要修改的路由表 ID，进入详情页，若需新建路由表，可参考 创建自定义路由表 。
4. 单击**新增路由策略**，在弹出框中，配置路由策略。

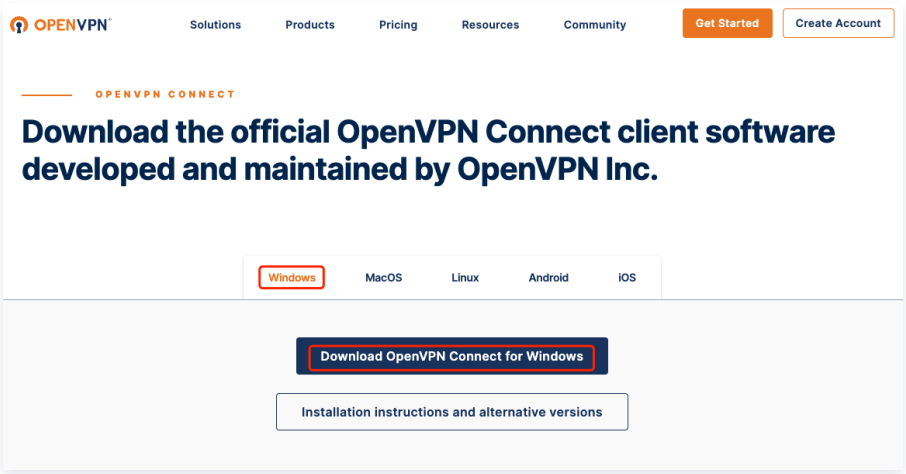
参数名称	参数说明
目的端	请填写 步骤2：创建 SSL 服务端 中创建时配置的客户端网段。
下一跳类型	选择 VPN 网关。
下一跳	下一跳选择创建好的具体 SSL VPN 网关实例。

步骤5：配置客户端

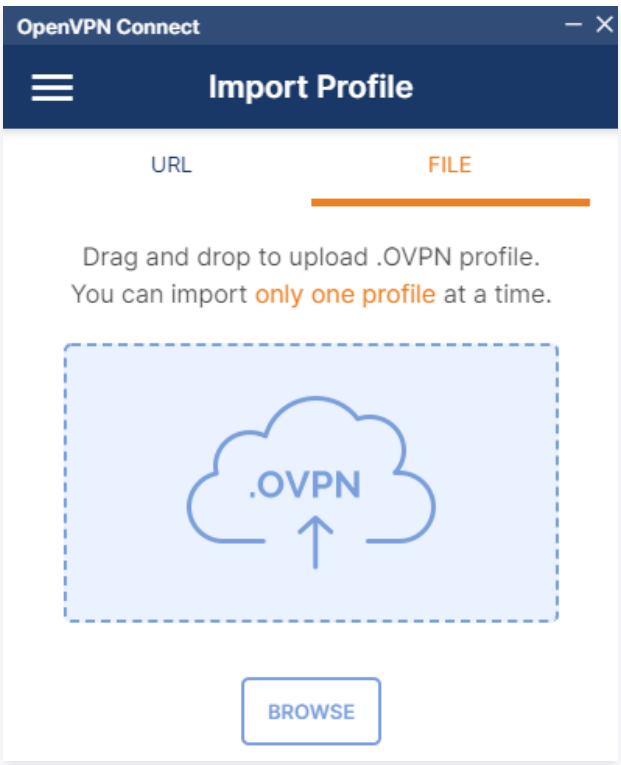
以下内容为您介绍如何配置 Windows、MAC 及 Linux 客户端。

Windows 客户端

1. 首先在 OpenVPN 官方下载页面下载并安装 OpenVPN Connect。

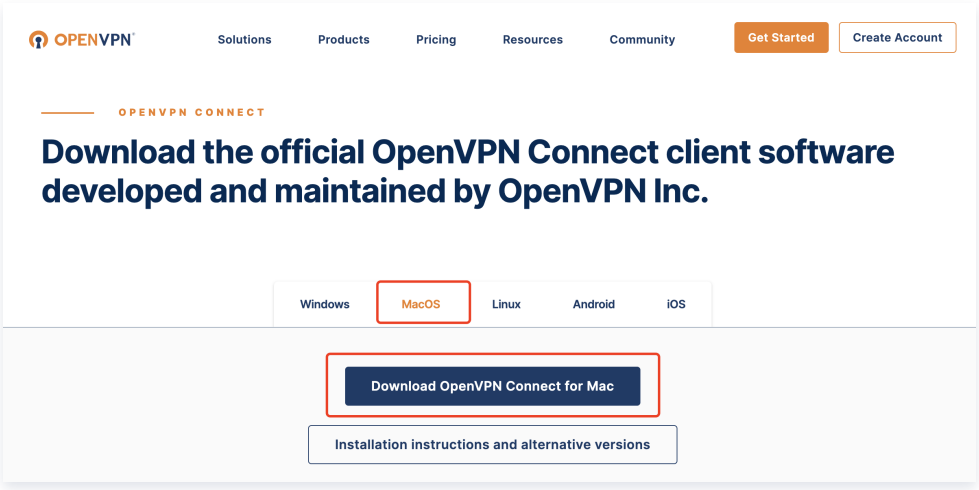


2. SSL 客户端安装完成后，选择 “Import Profile” 菜单中的 “FILE” 页面，上传 步骤3 已下载的 SSL 客户端配置文件（.ovpn 格式）。

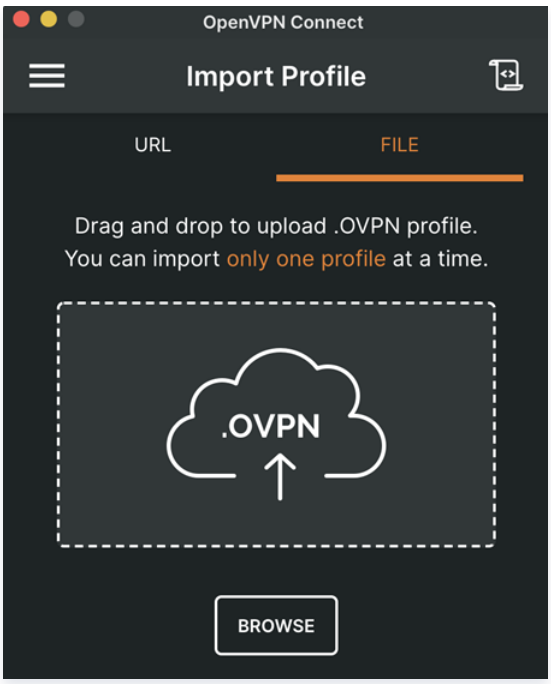


MAC 客户端

1. 首先在 OpenVPN 官方下载页面下载并安装 OpenVPN Connect。



2. SSL 客户端安装完成后，选择 “Import Profile” 菜单中的 “FILE” 页面，上传 步骤3 已下载的 SSL 客户端配置文件（.ovpn 格式）。



Linux 客户端

1. 打开命令行窗口。
2. 执行以下命令安装 OpenVPN 客户端。
   centos 发行版

```
yum install -y openvpn
```

   ubuntu 发行版

```
sudo apt-get install openvpn
```

3. 将 步骤3 已下载的 SSL 客户端证书解压拷贝至/etc/openvpn/conf/目录。
4. 进入/etc/openvpn/conf/目录，执行以下命令建立 VPN 连接。

```
openvpn --config /etc/openvpn/conf/config.ovpn --daemon
```

步骤6：测试连通性

腾讯云侧与用户移动端建立 SSL VPN 连接后，使用 ping 命令检测连通性。
例如：使用 VPC 内的云服务器 ping 客户端网段中的 IP，可以 ping 通表示 VPC 和客户端可以正常通信。